2019

An Invitation to Linear Algebra

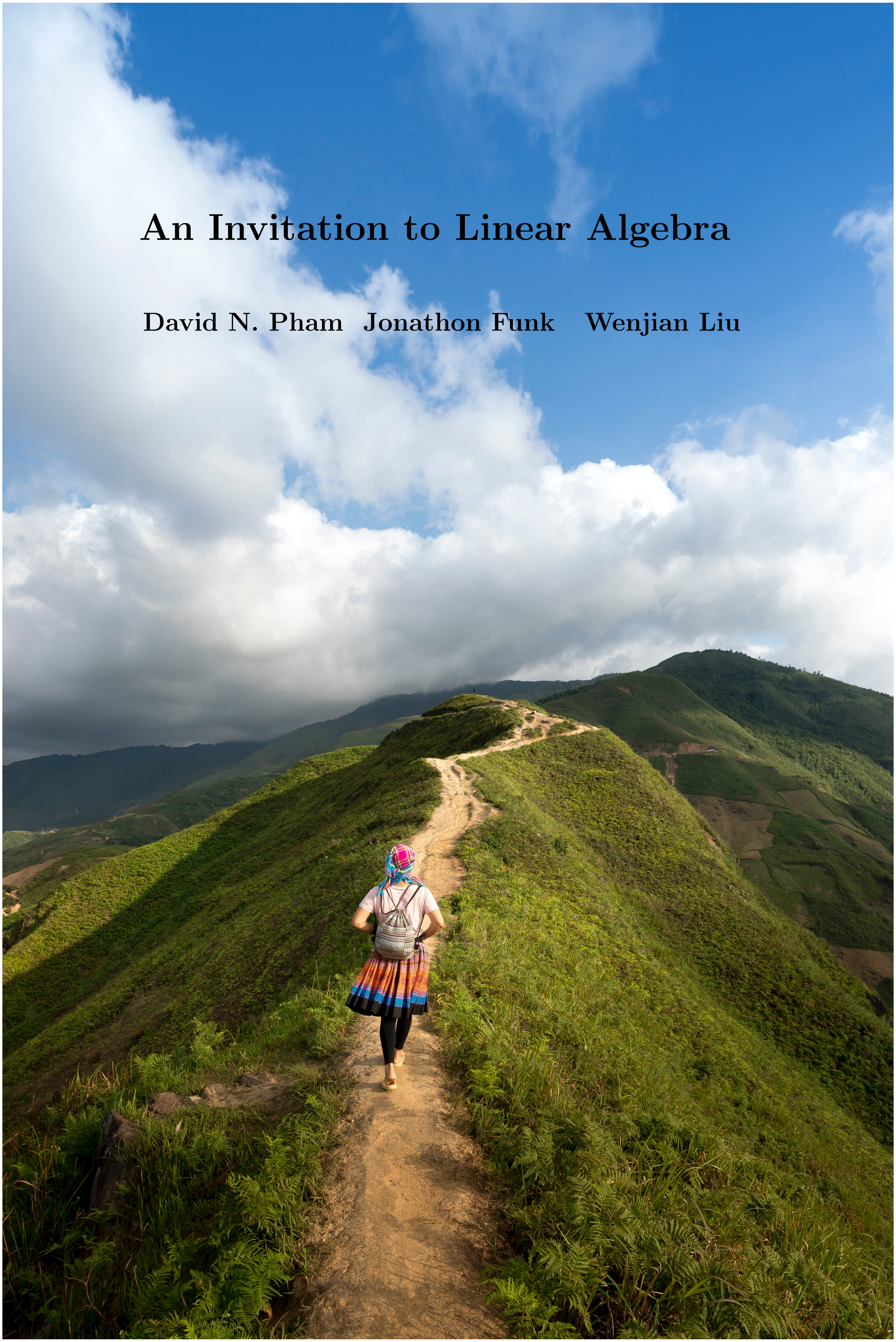
David N. Pham
CUNY Queensborough Community College

Jonathon Funk
CUNY Queensborough Community College

Wenjian Liu
CUNY Queensborough Community College

An Invitation to Linear Algebra

David N. Pham   Jonathon Funk   Wenjian Liu



Dr. David N. Pham
Department of Mathematics and Computer Science
Queensborough Community College of CUNY
222-05 56th Street, Bayside, NY, 11364
email: dnpham@qcc.cuny.edu

Dr. Jonathon Funk
Department of Mathematics and Computer Science
Queensborough Community College of CUNY
222-05 56th Street, Bayside, NY, 11364
email: jfunk@qcc.cuny.edu

Dr. Wenjian Liu
Department of Mathematics and Computer Science
Queensborough Community College of CUNY
222-05 56th Street, Bayside, NY, 11364
email: wliu@qcc.cuny.edu

An Invitation to Linear Algebra

cover photo: *https://www.pexels.com/photo/adventure-beautiful-clouds-2132126/*

Contents

Notation

Here is some common mathematical notation, some of which will be used at various points in the book.

- $\mathbb{Z}$ (the set of integers)
- $\mathbb{Q}$ (the set of rational numbers)
- $\mathbb{R}$ (the set of real numbers)
- $\mathbb{C}$ (the set of complex numbers)
- $:=$ or $\equiv$ (defined as)
- $\exists$ (there exists)
- $\therefore$ (therefore)
- $\forall$ (for all)
- $\in$ (an element of) for example, $x \in M$ means x is an element or member of the set M
- $f : X \to Y$ (f is a function from the set X to the set Y; f is also called a map or mapping)
- $id_X : X \to X$ (the identity map from X to X)
- $A \Rightarrow B$ (A implies B)
- $A \Leftarrow B$ (B implies A)
- $A \iff B$ (A and B are equivalent)
- iff (if and only if)

Preface

This book was created as a zero cost textbook for the course *MA 461 Linear Algebra* at Queensborough Community College. The authors' work was supported by an OER grant from the City University of New York for Fall 2018-Spring 2019.

Part 1

Basics

Chapter 1

Linear Systems & the Gauss Jordan Method

1.1. Linear Equations

Our entry point into Linear Algebra will be **linear equations**. Linear equations appear frequently in such fields as physics, engineering, computer science, and economics. Hence, knowing how to solve systems of linear equations and being able to determine when a system has a unique solution, infinitely many solutions, or no solution turns out to be quite important. With that said, we begin with the definition of a linear equation:

Definition 1.1. *A* ***linear equation*** *in n variables $x_1, \ldots, x_n$ is any equation of the form*

$$a_1x_1 + a_2x_2 + \cdots + a_nx_n = b,$$

where $a_1, \ldots, a_n, b \in \mathbb{R}$ are constants.

Example 1.2. $x_1 + 4x_2 = 12$ *is a linear equation in 2-variables. Note that if we are only dealing with 2 variables, we usually use x and y as variables in place of x_1 and x_2. The names of the variables are not mportant here. What is important is the number of variables. Hence, we can also write $x_1 + 4x_2 = 12$ as $x + 4y = 12$.*

Example 1.3. $x + 4y + 0z = 12$ *is a linear equation in 3-variables. Since the coefficient of* z *(i.e., the number multiplying* z*) is* 0*, we can abbreviate this equation as* $x - 4y = 12$ ***provided*** *that we remember that a solution to this equation is a* ***triple*** (a, b, c) *which satisfies* $x + 4y + 0z = 12$*. For example,* $(4, 2, 0)$ *and* $(4, 2, 10)$ *are both solutions since*

$$4 + 4(2) + 0(0) = 12$$
$$4 + 4(2) + 0(10) = 12.$$

Example 1.4. $3xy + y^2 = 1$ *is not a linear equation. In a linear equation, the variables are never multiplied together. In other words, a linear equation is a polynomial of degree* 1*. An equation which is not linear is called* ***nonlinear****.*

At this point, you might be wondering why linear equations are called "linear"? It turns out that if you plot all solutions to a linear equation in n variables

$$a_1x_1 + a_2x_2 + \cdots + a_nx_n = b,$$

the result will be an $(n-1)$-dimensional plane and a plane is just a higher dimensional version of a line. At this point, do not worry about the exact meaning of dimension. Roughly speaking, the dimension refers to the number of degrees of freedom of the equation. So if you have one equation with n-variables, then $n-1$ of the variables can take on any value. However, this fixes the remaining variable since it has to satisfy the equation. Hence, $n-1$ degrees of freedom. To make more sense of this, let's look at planes in dimension 0, 1, and 2.

Example 1.5. *An equation in 1-variable is* $2x = 6$*. There is only one solution to this equation:* $x = 3$*. Hence, the solution is just a single point located at* $x = 3$ *on the real number line.*

Example 1.6. *An equation in 2-variables is* $x - y = 0$*. Rearranging the equation, we see that the solution is the diagonal line* $y = x$ *in the* xy*-plane which passes through the origin* $(0, 0)$ *and through the point* $(1, 1)$*. A line is a 1-dimensional object. (The dimension is one since one only needs one parameter or "degree of freedom" to describe it.)*

Example 1.7. *An equation in 3-variables is* $0x + 0y + z = 0$*. The solution to this equation is the set* $\{(a, b, 0) \mid a, b \in \mathbb{R}\}$*. In other words, the solution is the entire* xy*-plane (i.e., a flat, infinitely thin table at* $z = 0$ *of infinite length and width).*

From the above examples, the solution to a linear equation in 1-variable is just a single point; a solution to a linear equation in 2-variables is a straight line; and a solution to a linear equation in 3-variables is a 2-dimensional plane. In these examples, the solutions were either a line or some generalization of a line. This provides some motivation for why linear equations are called "linear".

1.2. The Gauss Jordan Method

A natural problem in linear algebra is finding the solution to a *system of linear equations*. A system of linear equations is just a collection of linear equations where all the equations use the same set variables. In general, the number of equations are not equal to the number of variables. For now, we will deal with the case when the number of equations in the system is equal to the number of variables. As an example, here is a linear system of two equation in two variables:

$$\begin{aligned} 5x - 3y &= -2 \\ 3x + 2y &= 14 \end{aligned}$$

This particular system is very easy to solve using basic algebra. In this case, the system has exactly one solution: $x = 2$, $y = 4$. Now suppose that you have to solve a system with n equations and n variables where $n > 2$. Naturally, things are more complicated now. For this reason, we would like to have a systematic way of solving a system of linear equations. In this section, we will introduce the famous *Gauss Jordan method* which provides a very nice way of solving **all** systems of linear equations (and not just the ones where the number of equations equals the number of variables).

The basic idea of the Gauss Jordan method is to use a combination of *three basic transformations* to transform a system of linear equations into an **equivalent** system, one where the solution can be literally read off from the transformed system. Before we describe what the three transformations are, we need to define what it means for two linear systems to be equivalent.

Definition 1.8. *Let $\mathcal{A}$ and $\mathcal{B}$ be two linear systems which use the same set of variables. $\mathcal{A}$ and $\mathcal{B}$ are* **equvialent** *if every solution of $\mathcal{A}$ is a solution of $\mathcal{B}$ and every solution of $\mathcal{B}$ is a solution of $\mathcal{A}$.*

The three transformations used by the Gauss Jordan method does *not* alter the solution set of a linear system. In other words, it preserves the content or information about a linear system. Here are the three basic transformations of the Gauss Jordan method:

1. swapping the order of two equations
2. multiplying (or *scaling*) any equation by a **nonzero** number
3. adding a multiple of one equation to a different equation

Exercise 1.9. *Prove that applying any combination of the three basic transformations to a linear system will not alter the solution set of the original system.*

When we apply the Gauss Jordan method, we express the linear equations as an **augmented matrix**. For example, for the linear system

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

the augmented matrix is

$$\begin{pmatrix} 2 & 4 & 10 \\ -1 & 1 & -2 \end{pmatrix}.$$

Note that the first row is simply the first equation and the second row is the second equation. The first column are the coefficients of the x-variable; the second column are the coefficients of the y-variable; and the last column are the numbers appearing to the right of the equal sign.

Exercise 1.10. *A linear system in 3-variables x, y, and z has the following augmented matrix:*

$$\begin{pmatrix} 1 & 4 & -3 & -8 \\ 2 & 0 & -7 & 2 \\ -3 & 5 & -8 & 6 \end{pmatrix}.$$

Write down the equations for this linear system.

Since we work with augmented matrices when applying the Gauss Jordan method, the three basic transformations for a linear system are expressed as **three row operations**:

1. swapping any two rows (swapping rows i and j will be denoted as $R_i \leftrightarrow R_j$)
2. scaling a multiple of a row by a nonzero number (scaling row i by $c \neq 0$ will be denoted as $cR_i \to R_i$)
3. adding a multiple of one row to a different row (adding c times row i to row j will be denoted as $cR_i + R_j \to R_j$)

We now illustrate the Gauss Jordan method with two examples. The first example is a linear system in 2-variables and 2-equations and the second is a linear system in 3-variables and 3-equations.

Example 1.11.

$$\begin{aligned} 4x + 5y &= 6 \\ x + 4y &= -4 \end{aligned}$$

The first thing we do is express the above system as an augmented matrix:

$$\begin{pmatrix} 4 & 5 & 6 \\ 1 & 4 & -4 \end{pmatrix}.$$

The goal is to use a series of basic transformations to transform the above augmented matrix into one that looks like this:

$$\begin{pmatrix} 1 & 0 & a \\ 0 & 1 & b \end{pmatrix}.$$

The above matrix is said to be in reduced row echelon formHere is one way to do this:

1. $R_1 \leftrightarrow R_2$

$$\begin{pmatrix} 1 & 4 & -4 \\ 4 & 5 & 6 \end{pmatrix}.$$

2. We now use the left-most "1" in the first equation to zero out everything below it. This "1" is called a pivot. In other words, we apply $-4R_1 + R_2 \to R_2$ *which gives*

$$\begin{pmatrix} 1 & 4 & -4 \\ 0 & -11 & 22 \end{pmatrix}.$$

3. $-\frac{1}{11}R_2 \to R_2$

$$\begin{pmatrix} 1 & 4 & -4 \\ 0 & 1 & -2 \end{pmatrix}.$$

4. Use the middle "1" in the second equation to zero out everything above it. This "1" is also a pivot. In other words, we apply $-4R_2+R_1 \to R_1$:
$$\begin{pmatrix} 1 & 0 & 4 \\ 0 & 1 & -2 \end{pmatrix}.$$

An augmented matrix of the above form is in **reduced row echelon form**. The last augmented matrix represents the following linear system:

$$\begin{aligned} x + 0y &= 4 \\ 0x + y &= -2, \end{aligned}$$

Hence, the solution is $x = 4,\ y = -2$.

Example 1.12.

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

As before, we express the system as an augmented matrix

$$\begin{pmatrix} 2 & 1 & 1 & 4 \\ 1 & 1 & 4 & 0 \\ 3 & 2 & 3 & 6 \end{pmatrix}.$$

Here is one way to put the augmented matrix in reduced row echelon form:

1. $R_1 \leftrightarrow R_2$
$$\begin{pmatrix} 1 & 1 & 4 & 0 \\ 2 & 1 & 1 & 4 \\ 3 & 2 & 3 & 6 \end{pmatrix}.$$

2. Use the left most "1" in the first row as a pivot: $-2R_1 + R_2 \to R_2$ *and* $-3R_1 + R_3 \to R_3$
$$\begin{pmatrix} 1 & 1 & 4 & 0 \\ 0 & -1 & -7 & 4 \\ 0 & -1 & -9 & 6 \end{pmatrix}.$$

2. $-R_2 \to R_2$
$$\begin{pmatrix} 1 & 1 & 4 & 0 \\ 0 & 1 & 7 & -4 \\ 0 & -1 & -9 & 6 \end{pmatrix}.$$

3. Next we use the leftmost "1" in the second row as a pivot to zero out everything above it and below it. $-R_2 + R_1 \to R_1$ and $R_2 + R_3 \to R_3$

$$\begin{pmatrix} 1 & 0 & -3 & 4 \\ 0 & 1 & 7 & -4 \\ 0 & 0 & -2 & 2 \end{pmatrix}.$$

4. $-\frac{1}{2}R_3 \to R_3$

$$\begin{pmatrix} 1 & 0 & -3 & 4 \\ 0 & 1 & 7 & -4 \\ 0 & 0 & 1 & -1 \end{pmatrix}.$$

5. Use the leftmost "1" in the third row as a pivot. $3R_3 + R_1 \to R_1$ and $-7R_3 + R_2 \to R_2$

$$\begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 3 \\ 0 & 0 & 1 & -1 \end{pmatrix}.$$

   We now have the augmented matrix in reduced row echelon form. The solution is $x = -1$, $y = 3$, and $z = -1$. Note that once we have the solution we can substitute it back into the original linear system and check that it actually works.

In Examples 1.11 and 1.12, the augmented matrix in reduced echelon form took the following forms respectively

$$\begin{pmatrix} 1 & 0 & a \\ 0 & 1 & b \end{pmatrix} \text{ and } \begin{pmatrix} 1 & 0 & 0 & a \\ 0 & 1 & 0 & b \\ 0 & 0 & 1 & c \end{pmatrix}.$$

These observations motivate the following definition:

Definition 1.13. *The $n \times n$ matrix*

$$I_n = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix}$$

*is called the **identity matrix** of size n. (In components, I_n is the $n \times n$ matrix whose (i, j)-entry is $I_{ij} = 0$ for $i \neq j$ and whose (i, i)-entry is $I_{ii} = 1$.)*

The reason for calling I_n the identity matrix will become clear when we discuss matrix multiplication later on. At this point, we have used the word "matrix" in reference to the *augmented matrix* of a linear system and the *identity matrix*. Let's take a moment to formally define it before continuing:

Definition 1.14. *An $n \times m$ **matrix** is an array of numbers consisting of n rows and m columns. If $n = m$, that is, the matrix has the same number of rows and columns, the matrix is called a **square matrix**. If $m = 1$ and $n > 1$, then the matrix is called a **column vector** of size n. If $n = 1$ and $m > 1$, then the matrix is called a **row vector** of size m.*

At this point, do not worry about the meaning of the word "vector" appearing in Definition 1.14. We will get to vectors soon enough.

Example 1.15.

1. *A 2×3 matrix:*
$$\begin{pmatrix} 3 & 1 & -1 \\ 5 & -2 & 4 \end{pmatrix}$$
2. *A 2×1 matrix (or column vector of size 2):*
$$\begin{pmatrix} -2 \\ 3 \end{pmatrix}$$

Remark 1.16. *It is not always true that a linear system will have a unique solution. A linear system with n-equations and n-variables will have a unique solution if and only its augmented matrix can be transformed into a matrix of the following form:*
$$\begin{pmatrix} I_n & b \end{pmatrix}$$
where b is a column vector of size n.

We conclude this section with a simple example of a linear system whose augmented matrix cannot be expressed in the form given by Remark 1.16:

Example 1.17.
$$-3x + 2y = 2$$
$$6x - 4y = 4$$
The augmented matrix is
$$\begin{pmatrix} -3 & 2 & 2 \\ 6 & -4 & -4 \end{pmatrix}.$$
Let's try to put it in reduced row echelon form and see what happens.

We apply the following row operation: $2R_1 + R_2 \to R_2$

$$\begin{pmatrix} -3 & 2 & 2 \\ 0 & 0 & 0 \end{pmatrix}.$$

The new augmented matrix shows that the original system is actually defined by one equation: the line $-3x + 2y = 2$. Hence, every point on the aforementioned line is a solution to the original system. The solution set is the infinite set

$$\{(a, \frac{3}{2}a + 1) \mid a \in \mathbb{R}\}.$$

1.3. More Gauss-Jordan

In this section, we consider a few examples of linear systems which have infinitely many solutions or no solution.

Example 1.18.

$$\begin{aligned} x + 2y - 7z &= -7 \\ -2x + y + 4z &= -6 \\ -x + y + z &= -5 \end{aligned}$$

The augmented matrix is

$$\begin{pmatrix} 1 & 2 & -7 & -7 \\ -2 & 1 & 4 & -6 \\ -1 & 1 & 1 & -5 \end{pmatrix}.$$

Let's put it in reduced echelon form (REF):

1. $2R_1 + R_2 \to R_2$ *and* $R_1 + R_3 \to R_3$

$$\begin{pmatrix} 1 & 2 & -7 & -7 \\ 0 & 5 & -10 & -20 \\ 0 & 3 & -6 & -12 \end{pmatrix}.$$

2. $\frac{1}{5}R_2 \to R_2$

$$\begin{pmatrix} 1 & 2 & -7 & -7 \\ 0 & 1 & -2 & -4 \\ 0 & 3 & -6 & -12 \end{pmatrix}.$$

3. $-2R_2 + R_1 \to R_1$ *and* $-3R_2 + R_3 \to R_3$

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

The new system (which is equivalent to the original) has two equations: $x - 3z = 1$ and $y - 2z = -4$. Note that given an arbitrary value for z, the values of x and y are uniquely given by $x = 3z + 1$ and $y = 2z - 4$. Hence, the solution set for the original system is $x = 3a + 1$, $y = 2a - 4$, $z = a$ where a is any real number. In set notation, the solution set is $\{(3a + 1, 2a - 4, a) \mid a \in \mathbb{R}\}$.

Exercise 1.19. *Put the following augmented matrix in reduced echelon form (REF):*

$$\begin{pmatrix} 0 & 0 & 2 & -2 & 2 \\ 3 & 3 & -3 & 9 & 12 \\ 4 & 4 & -2 & 11 & 12 \end{pmatrix}.$$

Example 1.20. *Consider the linear system*

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

The augmented matrix for this system is then

$$\begin{pmatrix} 1 & 2 & 1 & 1 \\ 1 & -1 & 2 & -1 \\ 2 & 1 & 3 & 2 \end{pmatrix}.$$

Let's try to put the augmented matrix in REF:

1. $-R_1 + R_2 \to R_3$ *and* $-2R_1 + R_3 \to R_3$

$$\begin{pmatrix} 1 & 2 & 1 & 1 \\ 0 & -3 & 1 & -2 \\ 0 & -3 & 1 & 0 \end{pmatrix}.$$

2. $-R_2 + R_3 \to R_3$

$$\begin{pmatrix} 1 & 2 & 1 & 1 \\ 0 & -3 & 1 & -2 \\ 0 & 0 & 0 & 2 \end{pmatrix}.$$

The last row of the transformed augmented matrix represents the equation $0x + 0y + 0z = 2$ *which has no solution. Hence, the original system has no solution.*

Definition 1.21. *A linear system in n-variables $x_1, \ldots, x_n$ is* ***homogeneous*** *if every equation is set equal to zero, that is, every equation has the form*

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

where $a_1, \ldots, a_n \in \mathbb{R}$.

Note that every homogenous linear system in n-variables has at least one solution, namely, $x_1 = x_2 = \cdots = x_n = 0$.

Example 1.22. *Let's find the general solution for the homogenous system whose augmented matrix is*

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

Here is one way to put it in REF:

1. $-2R_1 + R_3 \to R_3$
$$\begin{pmatrix} 1 & 1 & 1 & 3 & 0 \\ 0 & 1 & -1 & 4 & 0 \\ 0 & -1 & -2 & -7 & 0 \end{pmatrix}.$$
2. $-R_2 + R_1 \to R_1$ *and* $R_2 + R_3 \to R_3$
$$\begin{pmatrix} 1 & 0 & 2 & -1 & 0 \\ 0 & 1 & -1 & 4 & 0 \\ 0 & 0 & -3 & -3 & 0 \end{pmatrix}.$$
3. $-\frac{1}{3}R_3 \to R_3$
$$\begin{pmatrix} 1 & 0 & 2 & -1 & 0 \\ 0 & 1 & -1 & 4 & 0 \\ 0 & 0 & 1 & 1 & 0 \end{pmatrix}.$$
4. $-2R_3 + R_1 \to R_1$ *and* $R_3 + R_2 \to R_2$
$$\begin{pmatrix} 1 & 0 & 0 & -3 & 0 \\ 0 & 1 & 0 & 5 & 0 \\ 0 & 0 & 1 & 1 & 0 \end{pmatrix}.$$

The augmented matrix is now in REF. The linear system representing the transformed augmented matrix is

$$x_1 - 3x_4 = 0, \quad x_2 + 5x_4 = 0, \quad x_3 + x_4 = 0.$$

Every equation contains x_4. Once a value of x_4 is chosen, all the other variables are uniquely determined. So a general solution for this system is

$$x_1 = 3r, \quad x_2 = -5r, \quad x_3 = -r, \quad x_4 = r, \qquad \forall\, r \in \mathbb{R}$$

Chapter 1 Exercises

Solve the following linear systems by the Gauss-Jordan Method. If a system has infinitely many solutions, give the general form of the solution. If a system has no solution, then write no zolution and give a brief explanation why.

1.

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

2.

$$
\begin{aligned}
2x_1 + 4x_2 + 8x_3 - 2x_4 &= -6 \\
3x_1 - x_2 + 2x_3 - x_4 &= 2 \\
x_1 + x_2 + x_3 + x_4 &= 2 \\
4x_1 + 3x_2 + 2x_3 + x_4 &= 3
\end{aligned}
$$

3.

$$
\begin{aligned}
x + 2y + 3z &= 14 \\
2x - y + z &= 3 \\
x - 3y - 2z &= 1
\end{aligned}
$$

4.

$$
\begin{aligned}
x_1 + 4x_2 - 3x_3 - 7x_4 &= -8 \\
3x_1 - x_2 - x_3 + 2x_4 &= 5 \\
2x_1 + 2x_2 - 5x_3 + 2x_4 &= -8
\end{aligned}
$$

5.

$$
\begin{aligned}
x_1 + 2x_2 + 3x_3 - x_4 &= 1 \\
x_1 + x_2 + x_3 - x_4 &= 2 \\
2x_1 - 3x_2 + 2x_3 + x_4 &= 3 \\
2x_1 - 2x_2 + 2x_3 - x_4 &= 4
\end{aligned}
$$

6.

$$
\begin{aligned}
x + 2y + 3z &= 0 \\
x + 4y + 9z &= -4 \\
x + 16y + 81z &= -64
\end{aligned}
$$

7.

$$\begin{aligned} v + w + x - 5y + 4z &= 7 \\ 2v + 2w + x - 8y + 5z &= 9 \\ v + 2w - x - 2y - z &= -4 \end{aligned}$$

8.

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

9.

$$\begin{aligned} x + 2y + 2z &= 5 \\ 3x - 4y + z &= -10 \\ x + y + z &= 2 \end{aligned}$$

10.

$$\begin{aligned} x_1 + x_2 + x_3 - 6x_4 - 2x_5 &= 5 \\ x_1 + 2x_2 + x_3 - 7x_4 - 3x_5 &= 9 \\ x_1 + 2x_2 + 2x_3 - 9x_4 - 2x_5 &= 9 \end{aligned}$$

11.

$$\begin{aligned} w + x + y + z &= 5 \\ 2w + x + 3y - 4z &= -5 \\ w + 2x + 2y + z &= 6 \\ w - x + y + z &= 7 \end{aligned}$$

12.

$$\begin{aligned} x_1 + x_3 + x_4 &= 2 \\ 2x_1 + x_2 + x_3 + x_4 + x_5 &= 2 \\ 3x_2 + x_4 + 2x_5 &= 1 \\ 4x_3 + x_4 + x_5 &= -4 \\ x_1 + 2x_4 + x_5 &= 3 \end{aligned}$$

Express each augmented matrix as a system of linear equations.

13.

$$\begin{pmatrix} 2 & 4 & 1 & 0 & -1 \\ 1 & -1 & 1 & 1 & 5 \\ 0 & 1 & 1 & -3 & 6 \end{pmatrix}$$

14.

$$\begin{pmatrix} 1 & -2 & 3 & -4 & 5 \\ -6 & 1 & 2 & 9 & 7 \\ 0 & 2 & 1 & 4 & 10 \\ 3 & 0 & 5 & 0 & 1 \end{pmatrix}$$

15.

$$\begin{pmatrix} 1 & -1 & 1 & 2 \\ 2 & -1 & 1 & 5 \\ 1 & 2 & 1 & 3 \end{pmatrix}$$

Put each augmented matrix in reduced row echelon form:

16.

$$\begin{pmatrix} 1 & 1 & 4 & -1 \\ 2 & 2 & 8 & -2 \\ 3 & 1 & 6 & -5 \end{pmatrix}$$

17.

$$\begin{pmatrix} 1 & 2 & 3 & 2 \\ 1 & 4 & 9 & 6 \\ 1 & 16 & 81 & 66 \end{pmatrix}$$

18.

$$\begin{pmatrix} 1 & 2 & 3 & -1 & 1 \\ 3 & 2 & 1 & -1 & 1 \\ 2 & 3 & 1 & 1 & 1 \\ 2 & 2 & 2 & -1 & 1 \end{pmatrix}$$

Chapter 2

$\mathbb{R}^n$ as a Vector Space

2.1. Some Motivation

Some quantities in everyday life require only one real number for a complete description. For example, one number is needed to describe the height or weight of a person. Some quantities, on the other hand, require more than one real number for a complete description. One example is the wind. What information is required to describe the wind? Well, for one thing, you need to know its *speed* and *direction*. For a complete description, you also need to know its *location*. For the moment, we will put that third piece of information aside and focus only on the first two pieces of information which define the *wind velocity*. In other words,

$$\text{wind velocity} = \text{wind speed} + \text{wind direction}.$$

Wind velocity is an example of a *vector*. If we knew the wind velocity at every point or location of a space, then we would have a *vector field* which would provide a complete description of the wind. Vector fields are objects which you encounter in a calculus III course or a physics course on electricity (think *electromagnetic field*). Since this is a book on linear algebra, we are going to steer clear of vector fields and just focus on vectors. From our point of view then, we are interested in what is happening at only one point in space as opposed to worrying about what is happening at every location of space.

Let's return to our wind velocity example. To make things even simpler, let's suppose that the wind direction is parallel to the ground (this is how the wind is described in the wind forecast). How might we depict the wind velocity at some fixed point O in, say, Central Park? One way is to represent the wind velocity as an arrow in the xy-plane. The length of the arrow will equal the wind speed and the direction of the arrow will (naturally) represent the wind direction. If we take the coordinates $(0, 0)$ as representing the point O, then we can indicate that the wind velocity is at point O by drawing the arrow with its tail at $(0, 0)$. An example of this representation is given in Figure 1. There the arrow has been labeled as $\vec{u}$. It begins at O and terminates at the point $P(4, 3)$. Using the Pythagorean theorem, the length of the arrow is 5. If we work in units of miles per hour (mph), then the arrow (or vector) u in the xy-plane represents a 5 mph wind at a point O in Central Park which is blowing in a north easterly direction (if we take the positive y-axis as north).

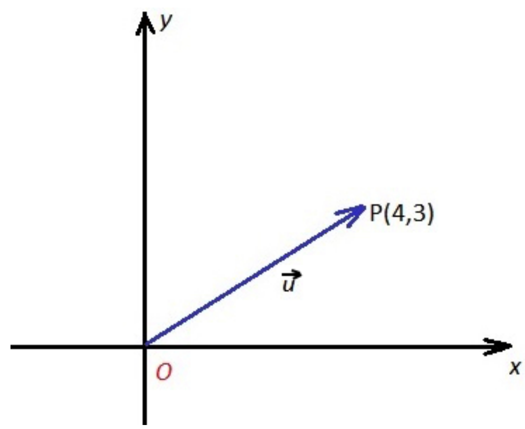


Figure 1. wind velocity at a point O in Central Park represented as an arrow in the xy-plane

So the take away from this example is that an arrow in the xy-plane whose tail is located at the origin $(0, 0)$ is an example of an object called a *vector*. In this chapter, all vectors are going to be arrows whose tails are located at the origin. Since the tail of a vector is $(0, 0)$, a vector is completely determined by the location of the head of the arrow. The xy-plane, the set of all arrows with two components, is an example of a vector space. **However, its not just a set**. It has a structure to it which allows two vectors to be added to produce a new vector. Moreover, vectors can also be *scaled*, which has the effect of altering their length. All of this will be made precise in the next section.

When we talk about the xy-plane as a vector space, its more common to call it $\mathbb{R}^2$. (More formally, $\mathbb{R}^2$ is the Cartesisan product of two copies of $\mathbb{R}$.) As a set, $\mathbb{R}^2$ is simply

$$\mathbb{R}^2 := \mathbb{R} \times \mathbb{R} = \{(a, b) \mid a, b \in \mathbb{R}\}.$$

Once again, this is just the xy-plane. $\mathbb{R}^2$ is an example of a 2-*dimensional* vector space. The set of real numbers $\mathbb{R}^1 := \mathbb{R}$ is an example of a 1-*dimensional* vector space and

$$\mathbb{R}^3 := \mathbb{R} \times \mathbb{R} \times \mathbb{R} = \{(a, b, c) \mid a, b, c \in \mathbb{R}\}$$

is an example of a 3-*dimensional* vector space (see Figure 2.1). Intuitively, the dimension of a vector space refers to the number of independent directions of the space. In $\mathbb{R}^1$, one can only move left-right; in $\mathbb{R}^2$, one can move left-right and up-down; and in $\mathbb{R}^3$, one can move left-right, up-down, and front-back. Of course, having only an intuitive definition (while helpful) is not sufficient from the point of view of mathematics. We will come to the precise meaning of dimension later in this chapter.

Since we live in a world of 3-dimensions, it's very hard, if not impossible, to visualize more than 3-dimensions. However, from the point of view of algebra, there is nothing to stop us from adding more components to a vector and considering n-dimensional vector spaces like $\mathbb{R}^n$ for any positive integer n. While we may no longer

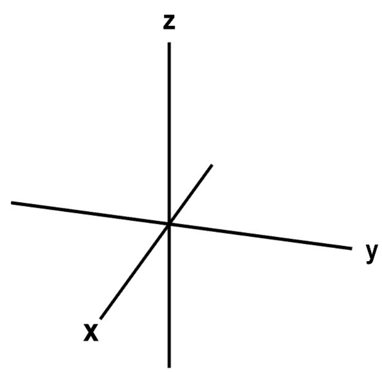


Figure 2. xyz-coordinate axis system

be able to visualize these higher dimensional spaces, we can still understand and work with them using algebra, which is precisely what we will do in this chapter.

2.2. The Vector Space Structure of $\mathbb{R}^n$

$\mathbb{R}^n$, for an integer $n \geq 1$, is the Cartesian product of n copies of $\mathbb{R}$. As a set, $\mathbb{R}^n$ is given by

$$\mathbb{R}^n := \{(a_1, a_2, \ldots, a_n) \mid a_1, \ldots, a_n \in \mathbb{R}\}.$$

If u is a point of $\mathbb{R}^n$ and we wish to regard it as an "arrow" which runs from the origin of $\mathbb{R}^n$ to the point u, we will emphasize this view by denoting the u as $\vec{u}$. This arrow is an example of what we call a *vector* and $\mathbb{R}^n$ (which contains all vectors with n components) is an example of a **real n-dimensional vector space**. (We will give the precise definition of dimension later.) The vector space structure on $\mathbb{R}^n$ is defined as follows:

Definition 2.1. *Let*

$$\vec{u} = (a_1, a_2, \ldots, a_n), \qquad \vec{v} = (b_1, b_2, \ldots, b_n)$$

be vectors in $\mathbb{R}^n$. $\mathbb{R}^n$ has two natural operations:

1. *vector addition*

$$\vec{u} + \vec{v} := (a_1 + b_1, a_2 + b_2, \ldots, a_n + b_n)$$

2. *scalar multiplication*

$$r\vec{u} := (ra_1, ra_2, \ldots, ra_n) \quad \text{for } r \in \mathbb{R}.$$

To develop some geometric intuition, we sketch vector addition and scalar multiplication for $\mathbb{R}^2$ in Figures 3 and 4. From Figure 3, we see that $\vec{u} + \vec{v}$ is obtained

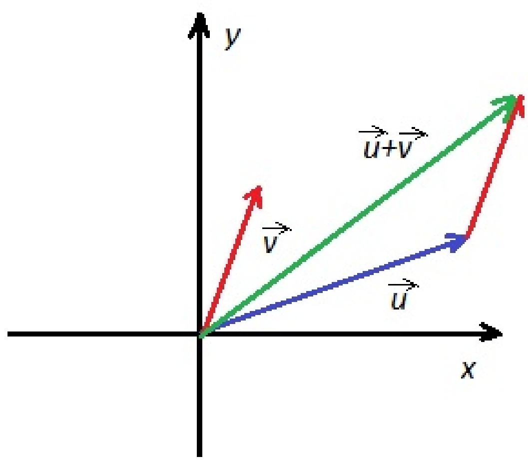


Figure 3. Vector addition in $\mathbb{R}^2$

by moving the tail of $\vec{v}$ (in a parallel manner) to the head of $\vec{u}$. Of course, one can also obtain $\vec{u} + \vec{v}$ by moving the tail of $\vec{u}$ (in a parallel manner) to the head of $\vec{v}$.

In Figure 4, we see that scaling a vector $\vec{u}$ by a number $r > 0$ results in a vector $r\vec{u}$ which points in the same direction as $\vec{u}$, but has a length of rL. On the other hand, if $r < 0$, then $r\vec{u}$ points in the direction opposite of $\vec{u}$ and has a length of $|r|L$.

Definition 2.2. *The zero vector of $\mathbb{R}^n$ is the element $\vec{0} \in \mathbb{R}^n$ defined by $\vec{0} := (0, 0, \ldots, 0)$.*

The next result follows easily from the defintion of vector addition and scalar multiplication in $\mathbb{R}^n$:

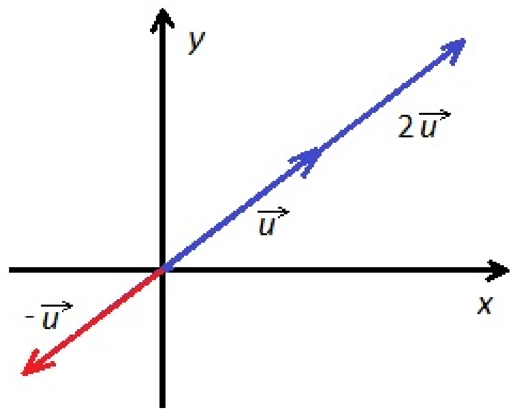


Figure 4. Scalar multiplication in $\mathbb{R}^2$

Proposition 2.3. *Let $\vec{u}$, $\vec{v}$, $\vec{w} \in \mathbb{R}^n$ and let $r, s \in \mathbb{R}$. Then*

(1) $\vec{u} + \vec{v} = \vec{v} + \vec{u}$ *(commutativity)*
(2) $(\vec{u} + \vec{v}) + \vec{w} = \vec{u} + (\vec{v} + \vec{w})$ *(associativity)*
(3) $\vec{u} + \vec{0} = \vec{0} + \vec{u} = \vec{u}$ *(zero property)*
(4) $\vec{u} + (-\vec{u}) = (-\vec{u}) + \vec{u} = \vec{0}$ *(additive inverse)*
(5) $r(\vec{u} + \vec{v}) = r\vec{u} + r\vec{v}$ *(distributive property 1)*
(6) $(r + s)\vec{u} = r\vec{u} + s\vec{u}$ *(distributive property 2)*
(7) $r(s\vec{u}) = (rs)\vec{u}$ *(associativity of scalar multiplication)*
(8) $0\vec{u} = \vec{0}$ *(scalar multiplicatin by 0)*
(9) $1\vec{u} = \vec{u}$ *(scalar multiplication by 1)*

Remark 2.4. *Proposition 2.3 is literally the blueprint for the definition of an abstract vector space. More formally, a real vector space is a set V with a zero element 0_V and a vector addition operation*

$$V \times V \to V, \qquad (u, v) \mapsto u + v$$

and a sclar multiplication operation:

$$\mathbb{R} \times V \to V, \qquad (r, u) \mapsto ru$$

which satisfies conditions (1)-(9) in Proposition 2.3. We will return to abstract vector spaces later on.

Definition 2.5. *Let $\vec{v} \in \mathbb{R}^n$. $\vec{v}$ is a **linear combination** of vectors $\vec{u}_1, \vec{u}_2, \ldots, \vec{u}_m \in \mathbb{R}^n$ if there exists $c_1, c_2, \ldots, c_m \in \mathbb{R}$ such that*

$$\vec{v} = c_1\vec{u}_1 + c_2\vec{u}_2 + \cdots + c_m\vec{u}_m.$$

Example 2.6. *Let $\vec{u} = (2, -1, 3)$, $\vec{v} = (-3, 2, 2)$, and $\vec{w} = (-4, 3, 7)$. Then $\vec{w}$ is a linear combination of $\vec{u}$ and $\vec{v}$ since $\vec{w} = \vec{u} + 2\vec{v}$.*

Exercise 2.7. *Let $\vec{u} = (1, 0, 0)$, $\vec{v} = (0, 1, 0)$, and $\vec{w} = (1, 3, 7)$. Show that $\vec{w}$ is* ***not*** *a linear combination of $\vec{u}$ and $\vec{v}$.*

Given a vector $\vec{v} \in \mathbb{R}^n$ and a set of vectors $\vec{u}_1, \ldots, \vec{u}_m \in \mathbb{R}^n$, a natural question to ask is whether $\vec{v}$ is a linear combination of $\vec{u}_1, \ldots, \vec{u}_m$. Answering this question amounts to solving a system of linear equations in m variables and n equations. Hence, we can use the Gauss Jordan method to solve these types of problems.

Example 2.8. *Determine if $\vec{v} = (2, -6, 9)$ is a linear combination of $\vec{u}_1 = (1, -1, 2)$ and $\vec{u}_2 = (2, 2, -1)$. If so, find $c_1, c_2 \in \mathbb{R}$ such that $\vec{v} = c_1\vec{u}_1 + c_2\vec{u}_2$.*

SOLUTION: *If $\vec{v}$ is a linear combination of $\vec{u}_1$ and $\vec{u}_2$, then*

$$(2, -6, 9) = c_1(1, -1, 2) + c_2(2, 2, -1)$$

for some $c_1, c_2 \in \mathbb{R}$. Comparing the components of the vectors on the left and right sides of the equations gives the linear system

$$\begin{aligned} c_1 + 2c_2 &= 2 \\ -c_1 + 2c_2 &= -6 \\ 2c_1 - c_2 &= 9. \end{aligned}$$

The augmented matrix for this system is

$$\begin{pmatrix} 1 & 2 & 2 \\ -1 & 2 & -6 \\ 2 & -1 & 9 \end{pmatrix}.$$

We now put it in reduced row echelon form:

1. $R_1 + R_2 \to R_2$, $-2R_1 + R_3 \to R_3$

$$\begin{pmatrix} 1 & 2 & 2 \\ 0 & 4 & -4 \\ 0 & -5 & 5 \end{pmatrix}$$

2. $\frac{1}{4}R_2 \to R_2$

$$\begin{pmatrix} 1 & 2 & 2 \\ 0 & 1 & -1 \\ 0 & -5 & 5 \end{pmatrix}$$

3. $-2R_2 + R_1 \to R_1$, $5R_2 + R_3 \to R_3$

$$\begin{pmatrix} 1 & 0 & 4 \\ 0 & 1 & -1 \\ 0 & 0 & 0 \end{pmatrix}$$

Hence, the system has a (unique) solution $c_1 = 4$ and $c_2 = -1$ which shows that $\vec{v}$ is a linear combination of $\vec{u}_1$ and $\vec{u}_2$. Specifically, $\vec{v} = 4\vec{u}_1 - \vec{u}_2$.

2.3. Subspaces of $\mathbb{R}^n$

Definition 2.9. *A subspace of $\mathbb{R}^n$ is a subset V of $\mathbb{R}^n$ which is* ***closed*** *under vector addition and scalar multiplication, that is,*

(1) $\vec{v} + \vec{w} \in V$ for all $\vec{v}, \vec{w} \in V$
(2) $r\vec{v} \in V$ for all $r \in \mathbb{R}$ and $\vec{v} \in V$.

Example 2.10. *Let $V := \{(a, b, a + 2b) \mid a, b \in \mathbb{R}\}$. To show that V is a subspace of $\mathbb{R}^3$, we need to check that V is closed under vector addition and scalar multiplication. So let $\vec{v}_1 = (a_1, b_1, a_1 + 2b_1)$ and $\vec{v}_2 = (a_2, b_2, a_2 + 2b_2)$ be arbitrary elements of V. Then*

$$\vec{v}_1 + \vec{v}_2 = (a_1 + a_2, b_1 + b_2, (a_1 + a_2) + 2(b_1 + b_2)).$$

Setting $a = a_1 + a_2$ and $b = b_1 + b_2$ in the defintion of V, we see that $\vec{v}_1 + \vec{v}_2$ is an element of V. Also, for $r \in \mathbb{R}$, we have

$$r\vec{v}_1 = (ra_1, rb_1, ra_1 + 2rb_1).$$

Setting $a = ra_1$ and $b = rb_1$ in the definition of V, we see that $r\vec{v}_1 \in V$. Hence, V is a subspace of $\mathbb{R}^3$.

Example 2.11. *Let $\mathbb{Z}$ be the set of integers. For any integers m, n, we have $m + n \in \mathbb{Z}$. This shows that $\mathbb{Z}$ is closed under the vector addition of $\mathbb{R}$. However, $\mathbb{Z}$ is not closed under scalar multiplication. For example, $\frac{1}{3}2 = \frac{2}{3} \notin \mathbb{Z}$. From this, we conclude that $\mathbb{Z}$ is not a subspace of $\mathbb{R}$.*

Example 2.12. *Let* $V := \{(a, a^2) \mid a \in \mathbb{R}\}$*. We now verify that* V *is not closed under scalar multiplication. To see this, let* $\vec{u} = (1, 1) \in V$*. It's easy to see that* $2\vec{u} = (2, 2)$ *cannot lie in* V*. Indeed, if it did, there must exist exist a number* $a \in \mathbb{R}$ *such that*

$$(2, 2) = (a, a^2).$$

The above equation implies $a = 2$ *and* $a^2 = 2$ *which is ridiculous. Hence,* $2\vec{u} \notin V$*, which shows that* V *is not a subspace of* $\mathbb{R}^2$*.*

Recall that a homogeneous linear system in n-variables $x_1, x_2, \ldots, x_n$ is a linear system where the linear equations are all set to zero. In other words, every linear equation is of the form

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

where $a_1, \ldots, a_n \in \mathbb{R}$. An equation of this form is called a *homogeneous linear equation*. The following result shows that the space of solutions of a homogenoeous linear system is subspace.

Theorem 2.13. *The solution space of a homogeneous linear system in* n*-variables is a subspace of* $\mathbb{R}^n$*.*

Proof. Let L be the set of linear equations of a homogeneous linear system in n-variables $x_1, \ldots, x_n$. Let $S \subset \mathbb{R}^n$ be the set of solutions for the homogeneous linear system L. Note that S is not empty since it contains the zero vector $\vec{0} = (0, \ldots, 0) \in \mathbb{R}^n$. Suppose $\vec{u} = (u_1, u_2, \ldots, u_n)$ and $\vec{v} = (v_1, v_2, \ldots, v_n)$ are solutions of this system. For S to be a subspace, we need to show that

$$\vec{u} + \vec{v} \in S, \qquad r\vec{u} \in S \quad \forall\, r \in \mathbb{R}.$$

Let $a_1x_1 + \cdots a_nx_n = 0$ be any linear equation of the system, that is, it is an arbitrary element of L. Since $\vec{u}$ and $\vec{v}$ are solutiions to this system, we have

$$\begin{aligned} a_1u_1 + a_2u_2 + \cdots + a_nu_n &= 0 \\ a_1v_1 + a_2v_2 + \cdots + a_nv_n &= 0. \end{aligned}$$

Substituting

$$\vec{u} + \vec{v} = (u_1 + v_1, u_2 + v_2, \ldots, u_n + v_n)$$

into the equation $a_1x_1 + \cdots a_nx_n = 0$ gives

$$\begin{aligned} a_1(u_1 + v_1) + \cdots + a_n(u_n + v_n) &= (a_1u_1 + \cdots + a_nu_n) + (a_1v_1 + \cdots + a_nv_n) \\ &= 0 + 0 \\ &= 0. \end{aligned}$$

Hence, $\vec{u}+\vec{v}$ is a solution to $a_1x_1+\cdots a_nx_n=0$. Since this equation was chosen arbitrarily from L, it follows that $\vec{u}+\vec{v}$ is a solution to every equation in L. Hence $\vec{u}+\vec{v}\in S$.

In addition, for $r\in\mathbb{R}$, we also have

$$\begin{aligned} a_1(ru_1)+\cdots+a_n(ru_n) &= r[a_1u_1+\cdots+a_nu_n] \\ &= r0 \\ &= 0. \end{aligned}$$

Hence, $r\vec{u}$ is also a solution to $a_1x_1+\cdots a_nx_n=0$ and therefore a solution to every equation in L. In other words, $r\vec{u}\in S$. This completes the proof. □

For convenience and later use, let us also define the "subspace of a subspace":

Definition 2.14. *Let V be a subspace of $\mathbb{R}^n$. A* ***subspace*** *of V is a subset W of V such that*

(i) $\vec{w}+\vec{w}'\in W$ for all $\vec{w},\vec{w}'\in W$

(ii) $r\vec{w}\in W$ for all $r\in\mathbb{R}$, $w\in W$.

Exercise 2.15. *Show that if W is a subspace of V and V is a subspace of $\mathbb{R}^n$, then W is also a subspace of $\mathbb{R}^n$.*

When we introduce the general definition of a vector space, we will see that there is really only one definition of a vector subspace.

2.4. Linear Independence, Bases, & Dimension

For the remainder of this chapter, we will use the term "vector space" to mean any subspace of $\mathbb{R}^n$. Since $\mathbb{R}^n$ is also a subspace of itself, the term "vector space" also includes $\mathbb{R}^n$. Later on in Chapter 5, when we finally give the general definition of a vector space, we will see that $\mathbb{R}^n$ and all its subspaces are simply examples of vector spaces (albeit important ones). Not every vector space is $\mathbb{R}^n$ or one of its subspaces. This is why linear algebra has a wide range of applicability in so many areas of mathematics, physics, statistics, and engineering. We can think of $\mathbb{R}^n$ and its subspaces as a concrete "warm-up" for the general theory of vector spaces. Indeed, all of the key ideas and results about vector spaces are on full display by working with $\mathbb{R}^n$ and its subspaces. For this reason, Chapter 5 will feel very much like *déjà vu* as we revisit all the essential definitions and results of the previous chapters and put them in a more general setting.

Ok, that was a rather long digression! Its time to get back to business. We begin this section with the idea of *linear independence* which is fundamental to general theory of vector spaces.

Let V be a vector space (i.e. V is a subspace of $\mathbb{R}^m$ for some $m \geq 1$) and let $\vec{v}_1, \ldots, \vec{v}_n \in V$. Then $\vec{v}_1, \ldots, \vec{v}_n$ are called **linearly independent** if

$$a_1\vec{v}_1 + a_2\vec{v}_2 + \cdots + a_n\vec{v}_n = 0$$

only when $a_1 = a_2 = \cdots = a_n = 0$. Otherwise, $\vec{v}_1, \ldots, \vec{v}_n$ are called **linearly dependent**.

Example 2.16. *Let $\vec{e}_1 = (1,0)$ and $\vec{e}_2 = (0,1)$. It is easy to see that $\vec{e}_1$ and $\vec{e}_2$ are linearly independent. Indeed, since*

$$a\vec{e}_1 + b\vec{e}_2 = (a,b),$$

it follows that $a\vec{e}_1 + b\vec{e}_2 = \vec{0}$ if and only if $a = b = 0$. Hence, $\vec{e}_1$ and $\vec{e}_2$ are linearly independent.

Example 2.17. *Let $\vec{v}_1 = (1,1,0)$, $\vec{v}_2 = (-1,1,0)$, and $\vec{v}_3 = (0,2,0)$. Since*

$$\vec{v}_1 + \vec{v}_2 - \vec{v}_3 = \vec{0},$$

it follows that $\vec{v}_1$, $\vec{v}_2$, and $\vec{v}_3$ are linearly dependent.

Definition 2.18. *Let V be a vector space. $\vec{v}_1, \ldots, \vec{v}_n$ is said to **span** V if for any $\vec{v} \in V$ there exists $a_1, \ldots, a_n \in \mathbb{R}$ such that*

$$a_1\vec{v}_1 + a_2\vec{v}_2 + \cdots + a_n\vec{v}_n = \vec{v}.$$

In other words, every element of V is a linear combination of $\vec{v}_1, \ldots, \vec{v}_n$. When a set of vectors $\{\vec{v}_1, \ldots, \vec{v}_n\}$ span a vector space V, we write

$$V = span\{\vec{v}_1, \ldots, \vec{v}_n\}.$$

Example 2.19. *The vectors $\vec{e}_1$ and $\vec{e}_2$ in Example 2.16 span $\mathbb{R}^2$.*

Example 2.20. *The vectors $\vec{v}_1 = (1,1,0)$, $\vec{v}_2 = (-1,1,0)$, $\vec{v}_3 = (0,2,0)$, and $\vec{v}_4 = (0,0,2)$ span $\mathbb{R}^3$. Indeed let $\vec{u} = (a,b,c)$ be an arbitrary vector of $\mathbb{R}^3$. Then*

$$\frac{1}{2}(a+b)\vec{v}_1 + \frac{1}{2}(b-a)\vec{v}_2 + 0\vec{v}_3 + \frac{c}{2}\vec{v}_4 = \vec{u}$$

Since we do not actually use $\vec{v}_3$, the following is also true:

$$V = \text{span}\{\vec{v}_1, \vec{v}_2, \vec{v}_3, \vec{v}_4\} = \text{span}\{\vec{v}_1, \vec{v}_2, \vec{v}_4\}.$$

For completeness, we also point out the following fact:

Proposition 2.21. *Let $\vec{v}_1, \vec{v}_2, \ldots, \vec{v}_k$ be vectors in $\mathbb{R}^n$. Define*

$$S := \{a_1\vec{v}_1 + \cdots + a_k\vec{v}_k \mid a_1, \ldots, a_k \in \mathbb{R}\}.$$

Then S is a subspace of $\mathbb{R}^n$. In particular, $S = span\{\vec{v}_1, \ldots, \vec{v}_k\}$.

Proof. Let $\vec{u}, \vec{v} \in S$. By definition of S, we have

$$\vec{u} = a_1\vec{v}_1 + \cdots + a_k\vec{v}_k$$
$$\vec{v} = b_1\vec{v}_1 + \cdots + b_k\vec{v}_k$$

for some $a_1, \ldots, a_k, b_1, \ldots, b_k \in \mathbb{R}$. Then

$$\vec{u} + \vec{v} = (a_1 + b_1)\vec{v}_1 + \cdots + (a_k + b_k)\vec{v}_k \in S.$$

Also, for $r \in \mathbb{R}$, we have

$$r\vec{u} = (ra_1)\vec{v}_1 + \cdots + (ra_k)\vec{v}_k \in S.$$

Hence, S is a subspace of $\mathbb{R}^n$. □

Next, we introduce the notion of a vector space *basis* which is another fundamental idea in the theory of vector spaces:

Definition 2.22. *Let V be a vector space. A* ***basis*** *of V is an ordered set $\{\vec{v}_1, \ldots, \vec{v}_n\}$ such that*

(i) $\{\vec{v}_1, \ldots, \vec{v}_n\}$ is linearly independent
(ii) $V = span\{\vec{v}_1, \ldots, \vec{v}_n\}$

Proposition 2.23. *Let V be a vector space and let $\{\vec{v}_1, \ldots, \vec{v}_n\}$ be a basis on V. Then every element of V is a unique linear combinaton of the basis elements $\{\vec{v}_1, \ldots, \vec{v}_n\}$.*

Proof. Let $\vec{v} \in V$. Since a basis spans V, we can express $\vec{v}$ as a linear combination of the basis elements:

$$\vec{v} = a_1\vec{v}_1 + a_2\vec{v}_2 + \cdots + a_n\vec{v}_n$$

for some $a_1, a_2, \ldots, a_n \in \mathbb{R}$. We must show that the a_i's are in fact unique. So let's suppose that $\vec{v}$ can also be expressed as

$$\vec{v} = b_1\vec{v}_1 + b_2\vec{v}_2 + \cdots + b_n\vec{v}_n$$

for some $b_1, b_2, \ldots, b_n \in \mathbb{R}$. We now show that $a_i = b_i$ for $i = 1, \ldots, n$. Indeed, from the equation

$$a_1\vec{v}_1 + a_2\vec{v}_2 + \cdots + a_n\vec{v}_n = \vec{v} = b_1\vec{v}_1 + b_2\vec{v}_2 + \cdots + b_n\vec{v}_n,$$

we see that

$$(a_1 - b_1)\vec{v}_1 + \cdots + (a_n - b_n)\vec{v}_n = \vec{0}.$$

Since a basis in also linearly independent, the only way the left side of the above equation can sum to zero is if $a_i - b_i = 0$ for $i = 1, \ldots, n$. Hence, $a_i = b_i$ for $i = 1, \ldots, n$. This completes the proof. □

Example 2.24. *The vector space $\mathbb{R}^n$ has a natural basis $\{\vec{e}_1, \vec{e}_2, \ldots, \vec{e}_n\}$ where $\vec{e}_i$ is the vector in $\mathbb{R}^n$ whose components are all zero except for trhe i-th component which is 1. This basis is typically called the* ***standard basis*** *on $\mathbb{R}^n$.*

Exercise 2.25. *Verify that the standard basis on $\mathbb{R}^n$ is indeed a basis on $\mathbb{R}^n$, that is, show that it is linearly independent and spans $\mathbb{R}^n$.*

Note that a vector space has many different bases (actually infintely many). The following example provides a simple demonstration of this:

Example 2.26. *Consider the vector space $\mathbb{R}^2$ and let $\{\vec{e}_1, \vec{e}_2\}$ denote the standard basis on $\mathbb{R}^2$. Then for any $a \in \mathbb{R}$,*

$$\{\vec{e}_1, \vec{e}_2 + a\vec{e}_1\}$$

is also a basis on $\mathbb{R}^2$. Note that since a basis is an ***ordered*** *set, the basis $\{\vec{e}_2, \vec{e}_1\}$ is actually different than the basis $\{\vec{e}_1, \vec{e}_2\}$ (even though both contain the same basis elements).*

While a vector space has many different bases, it turns out that the number of elements in each basis is **always the same**. We state this important fact formally with the following theorem:

Theorem 2.27. *Let V be a vector space. Every basis on V has the same number of basis elements.*

We will prove this theorem shortly. In Chapter 1, we gave a vague definition of vector space dimension as somehow being the number of "independent directions" (or degrees of freedom) of a vector space. Here, at last, is the precise definition of vector space dimension:

Definition 2.28. *Let V be a vector space. The* ***dimension*** *of V (denoted as $\dim V$) is the number of elements in a basis of V (i.e., the cardinarlity of the basis).*

Note that for the definition to make sense (or be *well defined*), the definition requires any two bases of V to have the same number of basis elements. This is why Theorem 2.27 is critical to the definition of vector space dimension. To prove

Theorem 2.27, we need to introduce a technique of proof called *proof by inductiion*. This technique works as follows: let P_n be a property which depends on an integer n. We wish to prove that this property holds for all integers $n \geq K$ where K is some integer (which in practice is typically 0 or 1). The strategy has two steps. The first step is to prove that P_K is true. The second step is to prove that if P_n is true (for some arbitrary n), then P_{n+1} must also be true. The last step is called the *inductive step*. In this way, one has proven that P_n holds for all integers $n \geq K$. Indeed, if one completes these two steps, then one has shown that P_{K+1} is true which in turn implies that P_{K+2} is true which in turn implies that P_{K+3} is true and so on and so on. The following definitions will prove useful in establishing Theorem 2.27.

Definition 2.29. *Let $X := \{1, 2, \ldots, n\}$. The set S_n of permutations of X is the set of all one-to-one and onto maps $\sigma : X \to X$.*

Remark 2.30. *Recall that $\sigma : X \to X$ is one-to-one means that if $\sigma(i) = \sigma(j)$ for some $i, j \in X$, then $i = j$. The statement that σ is onto means that for any $k \in X$, there exists an $i \in X$ such that $\sigma(i) = k$.*

Definition 2.31. *Let V be a vector space and let $\mathcal{B} := \{\vec{v}_1, \ldots, \vec{v}_n\}$ be a basis of V. A reordering of the basis $\mathcal{B}$ is a new basis $\mathcal{B}_\sigma := \{\vec{v}_{\sigma(1)}, \vec{v}_{\sigma(2)}, \ldots, \vec{v}_{\sigma(n)}\}$ where σ is some element of S_n.*

Remark 2.32. *Note that if $\mathcal{B}_\sigma$ is a reordering of a basis $\mathcal{B}$ of a vector space V, then $\mathcal{B}_\sigma$ and $\mathcal{B}$ contains the same set of basis elements, but the order of those elements are different. Recall that a basis is defined to be an ordered set. Hence, changing the order of a basis results in a different basis.*

Example 2.33. *Consider the standard basis $\{\vec{e}_1, \vec{e}_2, \vec{e}_3\}$ of $\mathbb{R}^3$. Then $\{\vec{e}_2, \vec{e}_3, \vec{e}_1\}$ is a reordering of the standard basis. Note that the permutation $\sigma \in S_3$ associated with this reodering is given by $\sigma(1) = 2$, $\sigma(2) = 3$, $\sigma(3) = 1$.*

Theorem 2.27 is a direct consequence of the following well known theorem:

Theorem 2.34 (Replacement Theorem)**.** *Let V be a vector space. Let $\mathcal{B} := \{\vec{v}_1, \vec{v}_2, \ldots, \vec{v}_n\}$ be a basis on V and let $\mathcal{U} := \{\vec{u}_1, \ldots, \vec{u}_m\}$ be a linearly independent subset of V. Then $m \leq n$ and there is a reordering $\mathcal{B}_\sigma$ of $\mathcal{B}$ such that a new basis $\mathcal{B}_{\sigma,m}$ can be obtained by replacing the first m basis vectors of $\mathcal{B}_\sigma$ by those of $\mathcal{U}$. In other words,*

$$\mathcal{B}_{\sigma,m} := \{\vec{u}_1, \vec{u}_2, \ldots, \vec{u}_m, \vec{v}_{\sigma(m+1)}, \ldots, \vec{v}_{\sigma(n)}\}$$

is a basis of V.

Proof. We prove this by induction on the cardinality of $\mathcal{U}$. First, consider the case where $\mathcal{U} = \{\vec{u}_1\}$. Since $\mathcal{B}$ is a basis, we have

$$\vec{u}_1 = a_1\vec{v}_1 + a_2\vec{v}_2 + \cdots + a_n\vec{v}_n$$

for some (unique) $a_i \in \mathbb{R}$, $i = 1, \ldots, n$. Since $\vec{u}_1 \neq 0$, there must be some $a_i \neq 0$. Let $\sigma \in S_n$ be any permutation such that $\sigma(1) = i$. Then $a_{\sigma(1)} = a_i$ and we can reorder the above sum as

$$\vec{u}_1 = a_{\sigma(1)}\vec{v}_{\sigma(1)} + a_{\sigma(2)}\vec{v}_{\sigma(2)} + \cdots + a_{\sigma(n)}\vec{v}_{\sigma(n)}. \tag{1}$$

Since $a_{\sigma(1)} = a_i \neq 0$, we can solve for $\vec{v}_{\sigma(1)}$:

$$\vec{v}_{\sigma(1)} = \frac{1}{a_{\sigma(1)}}\vec{u}_1 - \frac{a_{\sigma(2)}}{a_{\sigma(1)}}\vec{v}_{\sigma(2)} - \cdots - \frac{a_{\sigma(n)}}{a_{\sigma(1)}}\vec{v}_{\sigma(n)}$$

Since

$$\mathcal{B}_\sigma := \{\vec{v}_{\sigma(1)}, \vec{v}_{\sigma(2)}, \ldots, \vec{v}_{\sigma(n)}\}$$

is a basis of V and $\vec{v}_{\sigma(1)}$ is a linear combination of $\vec{u}_1, \vec{v}_{\sigma(2)}, \ldots, \vec{v}_{\sigma(n)}$, it follows that

$$V = \operatorname{span}\{\vec{u}_1, \vec{v}_{\sigma(2)}, \ldots, \vec{v}_{\sigma(n)}\}.$$

Let $\mathcal{B}_{\sigma,1} := \{\vec{u}_1, \vec{v}_{\sigma(2)}, \ldots, \vec{v}_{\sigma(n)}\}$. We now show that $\mathcal{B}_{\sigma,1}$ is linearly independent. So suppose that

$$c_1\vec{u}_1 + c_2\vec{v}_{\sigma(2)} + \cdots + c_n\vec{v}_{\sigma(n)} = \vec{0}. \tag{2}$$

Consider first the case where $c_1 = 0$. Then

$$c_2\vec{v}_{\sigma(2)} + \cdots + c_n\vec{v}_{\sigma(n)} = \vec{0}.$$

Since $\vec{v}_{\sigma(2)}, \ldots, \vec{v}_{\sigma(n)}$ is linearly independent, it follows that $c_2 = c_3 = \cdots = c_n = 0$. Now suppose that $c_1 \neq 0$. Then we can divide both sides of (2) by c_1 to obtain

$$\vec{u}_1 + c'_2\vec{v}_{\sigma(2)} + \cdots + c'_n\vec{v}_{\sigma(n)} = \vec{0}, \tag{3}$$

where $c'_k = c_k/c_1$ for $k = 2, \ldots, n$. Now let us substitute (1) into (3):

$$a_{\sigma(1)}\vec{v}_{\sigma(1)} + (c'_2 + a_{\sigma(2)})\vec{v}_{\sigma(2)} + \cdots + (c'_n + a_{\sigma(n)})\vec{v}_{\sigma(n)} = \vec{0}.$$

Since the vectors in the above sum are linearly indpendent, we have $a_{\sigma(1)} = 0$. However, this is a contradiction since $a_{\sigma(1)} = a_i \neq 0$. From this, we conclude that $c_1 = 0$, which in turn implies that $c_2 = c_3 = \cdots = c_n = 0$ by the first case. This proves that $\mathcal{B}_{\sigma,1}$ is linearly indpendent and hence is a basis.

We have now verified that the Replacement Theorem holds when $\mathcal{U}$ has cardinarlity 1. Suppose now that the Replacement Theorem holds for all linearly independent sets of cardinality m where $m \leq n$. If $m = n$, then there are no more basis vectors to replace and hence nothing to prove. So let us suppose that $m < n$. Now let $\mathcal{U}$ be a linearly independent set of cardinality $m+1$:

$$\mathcal{U} = \{\vec{u}_1, \vec{u}_2, \ldots, \vec{u}_{m+1}\}.$$

By the induction hypothesis, there exists a permutation $\sigma \in S_n$ such that

$$\mathcal{B}_{\sigma,m} := \{\vec{u}_1, \ldots, \vec{u}_m, \vec{v}_{\sigma(m+1)}, \ldots, \vec{v}_{\sigma(n)}\}$$

is a basis on V. Since $\mathcal{B}_{\sigma,m}$ is a basis, we have

$$\vec{u}_{m+1} = c_1\vec{u}_1 + \cdots + c_m\vec{u}_m + c_{m+1}\vec{v}_{\sigma(m+1)} + \cdots + c_n\vec{v}_{\sigma(n)} \tag{4}$$

for some (unique) $c_i \in \mathbb{R}$, $i = 1, \ldots, n$. Since $\mathcal{U}$ is a linearly independent set, it follows that there must be some $j \geq m+1$ such that $c_j \neq 0$. (If not, $\mathcal{U}$ would not be linearly independent!) Choose any permutation $\tau \in S_n$ such that $\tau(i) = i$ for $i \leq m$ and $\tau(m+1) = j$. Let $\rho \in S_n$ be defined by $\rho = \sigma \circ \tau$. Consider the reordering

$$\mathcal{B}_\rho := \{\vec{v}_{\rho(1)}, \vec{v}_{\rho(2)}, \ldots, \vec{v}_{\rho(m)}, \vec{v}_{\rho(m+1)}, \ldots, \vec{v}_{\rho(n)}\}.$$

Observe that

$$\vec{v}_{\rho(i)} = \vec{v}_{\sigma\circ\tau(i)} = \vec{v}_{\sigma(i)} \quad \text{for } i \leq m \tag{5}$$

and

$$\vec{v}_{\rho(i)} \in \{\vec{v}_{\sigma(m+1)}, \ldots, \vec{v}_{\sigma(n)}\} \quad \text{for } i \geq m+1 \tag{6}$$

where $\vec{v}_{\rho(m+1)} = \vec{v}_{\sigma\circ\tau(m+1)} = \vec{v}_{\sigma(j)}$. In other words, the first m vectors of $\mathcal{B}_\sigma$ and $\mathcal{B}_\rho$ are exactly the same and the last $n-m$ vectors of $\mathcal{B}_\rho$ is simply a reshuffling of the last $n-m$ vectors of $\mathcal{B}_\sigma$. Using these observations, we can rewrite (4) as

$$\vec{u}_{m+1} = c_1\vec{u}_1 + \cdots + c_m\vec{u}_m + c_{\tau(m+1)}\vec{v}_{\rho(m+1)} + \cdots + c_{\tau(n)}\vec{v}_{\rho(n)}. \tag{7}$$

Since $c_{\tau(m+1)} = c_j \neq 0$, we can express $\vec{v}_{\rho(m+1)}$ as a linear combination of the vectors

$$\mathcal{B}_{\rho,m+1} := \{\vec{u}_1, \ldots, \vec{u}_m, \vec{u}_{m+1}, \vec{v}_{\rho(m+2)}, \ldots, \vec{v}_{\rho(n)}\}.$$

Also, note that (5) and (6) imply that the set

$$\{\vec{u}_1, \ldots, \vec{u}_m, \vec{v}_{\rho(m+1)}, \ldots, \vec{v}_{\rho(n)}\} \tag{8}$$

is a basis on V. (This is just $\mathcal{B}_{\sigma,m}$ with the last $n-m$ vectors reshuffled.) This in turn implies that

$$V = \text{span } \mathcal{B}_{\rho,m+1}.$$

We now show that $\mathcal{B}_{\rho,m+1}$ is linearly independent. So suppose

$$\alpha_1\vec{u}_1 + \cdots + \alpha_{m+1}\vec{u}_{m+1} + \alpha_{m+2}\vec{v}_{\rho(m+2)} + \cdots + \alpha_n\vec{v}_{\rho(n)} = \vec{0} \tag{9}$$

for some $\alpha_1, \ldots, \alpha_n \in \mathbb{R}$. If $\alpha_{m+1} = 0$, then the linear independence of (8) implies that $\alpha_i = 0$ for all i. So suppose that $\alpha_{m+1} \neq 0$. By dividing (9) by α_{m+1}, we may assume that $\alpha_{m+1} = 1$. Let us now substitute (7) into (9):

$$(\alpha_1 + c_1)\vec{u}_1 + \cdots + (\alpha_m + c_m)\vec{u}_m \\ + c_{\tau(m+1)}\vec{v}_{\rho(m+1)} + (\alpha_{m+2} + c_{\tau(m+2)})\vec{v}_{\rho(m+2)} + \cdots + (\alpha_n + c_{\tau(n)})\vec{v}_{\rho(n)} = \vec{0}.$$

By the linear independence of (8), it follows that all of the coefficients in the above sum are zero. In particular, $c_{\tau(m+1)} = 0$. However, this is a contradiction since $c_{\tau(m+1)} = c_j \neq 0$. Hence, we must have $\alpha_{m+1} = 0$. As we saw earlier, this implies that $\alpha_i = 0$ for all i in (9) which in turn proves the linear independence of $\mathcal{B}_{\rho,m+1}$. Hence, $\mathcal{B}_{\rho,m+1}$ is the desired basis. This proves the induction step.

Lastly, we show that if $\mathcal{U} = \{\vec{u}_1, \ldots, \vec{u}_m\}$ is a linearly independent set of m vectors, then $m \leq n$. Suppose, on the contrary, that $m > n$. Let $\mathcal{U}' := \{\vec{u}_1, \ldots, \vec{u}_n\}$. The above work implies that we can obtain a new basis by replacing the original basis $\{\vec{v}_1, \ldots, \vec{v}_n\}$ with all the elements of $\mathcal{U}'$. In other words, $\mathcal{U}'$ is a basis. Since $\mathcal{U}'$ is a basis, this implies that $\vec{u}_{n+1}$ is a linear combination of the elements of $\mathcal{U}'$, which contradicts the fact that $\mathcal{U}$ is a linearly independent set. Hence, we must have $m \leq n$. This completes the proof. □

The proof of Theorem 2.27 is given below and follows readily from the Replacement Theorem.

Proof. Let $\mathcal{B}_1$ and $\mathcal{B}_2$ be two bases on V of cardinalities n_1 and n_2 respectively. Since $\mathcal{B}_1$ is a basis, Theorem 2.34 implies that $n_2 \leq n_1$. On the other hand, since $\mathcal{B}_2$ is a basis, we also have $n_2 \geq n_1$. This proves that $n_1 = n_2$ which completes the proof. □

Example 2.35. *The standard basis on $\mathbb{R}^n$ consists of the vectors $\vec{e}_1, \ldots, \vec{e}_n$ where $\vec{e}_i$ is the vector whose components are all zero except for the ith component which is* 1*. Hence, the dimension of $\mathbb{R}^n$ is n. In particular, any basis on $\mathbb{R}^n$ must consist of exactly n vectors.*

Corollary 2.36. *Let V be a vector space of dimension n and suppose $V = span\{\vec{v}_1, \ldots, \vec{v}_n\}$ for some vectors $\vec{v}_i \in V$, $i = 1, \ldots, n$. Then $\{\vec{v}_1, \ldots, \vec{v}_n\}$ must be a basis on V.*

Proof. Let $S := \{\vec{v}_1, \ldots, \vec{v}_n\}$. To prove Corollary 2.36, it only remains to show that S is linearly independent. We will prove this by contradiction. So let us suppose that S is linearly dependent. Then there exists a reordering

$$S_\sigma := \{\vec{v}_{\sigma(1)}, \ldots, \vec{v}_{\sigma(n)}\}$$

such that for some $k < n$, $T := \{v_{\sigma(1)}, \ldots, v_{\sigma(k)}\}$ is linearly independent and the vectors $\vec{v}_{\sigma(k+1)}, \ldots, \vec{v}_{\sigma(n)}$ are all linear combinatiions of the elements of T. However, this means that $V = \operatorname{span} T$. Since T is also linearly independent, this implies that T is a basis of V of cardinality $k < n$. By Theorem 2.27, all bases of a vector space have the same cardinality and the dimension of a vector space is defined to be the number of elements in a basis. This implies that $\dim V = k \neq n$, which is a contradiction. Hence, S must be linearly independent. □

Corollary 2.37. *Let V be a vector space of dimension n and suppose $\{\vec{v}_1, \ldots, \vec{v}_n\}$ is a linearly independent subset of V. Then $\{\vec{v}_1, \ldots, \vec{v}_n\}$ must be a basis on V.*

Proof. This is a direct consequence of the Replacement Theorem (Theorem 2.34). Since $\dim V = n$, any basis of V must contain precisely n elements. Let $\mathcal{B} := \{\vec{x}_1, \ldots, \vec{x}_n\}$ be a basis on V. Since $\{\vec{v}_1, \ldots, \vec{v}_n\}$ is linearly independent, the Replacement Theorem implies that a new basis can be formed by replacing every vector of $\mathcal{B}$ with all the elements of $\{\vec{v}_1, \ldots, \vec{v}_n\}$. However, the resulting set after the replacement is simply $\{\vec{v}_1, \ldots, \vec{v}_n\}$. Hence, we conlcude that $\{\vec{v}_1, \ldots, \vec{v}_n\}$ is a basis. □

Let V be a vector space of dimension n and suppose we would like to verify if a set of n vectors is a basis on V. Corollary 2.37 shows that we only need to check that the vectors are linearly independent to determine if they form a basis.

Exercise 2.38. *Consider the vectors $\vec{v}_1 = (2, 1, -1)$, $\vec{v}_2 = (0, 1, 1)$, $\vec{v}_3 = (1, 0, -1)$ in $\mathbb{R}^3$. Determine if $\vec{v}_1, \vec{v}_2, \vec{v}_3$ is a basis on $\mathbb{R}^3$.*

Exercise 2.39. *Consider the vectors $\vec{v}_1 = (2, 1, 1)$, $\vec{v}_2 = (1, 4, -1)$, $\vec{v}_3 = (-3, 2, -3)$ in $\mathbb{R}^3$. Determine if $\vec{v}_1, \vec{v}_2, \vec{v}_3$ is a basis on $\mathbb{R}^3$.*

We conclude this section with an important example.

Example 2.40. *Consider the subset V of $\mathbb{R}^n$ consisting only of the zero vector $\vec{0}$. Since $\vec{0} + \vec{0} = \vec{0}$ and $r\vec{0} = \vec{0}$ for all $r \in \mathbb{R}$, we see that V is a subspace of $\mathbb{R}^n$. What is the dimension of V? Clearly, it must be zero. Indeed, V (which consists only of $\vec{0}$) has no linearly independent subsets since $r\vec{0} = \vec{0}$ for all $r \in \mathbb{R}$. The only nonempty subset of $V = \{0\}$ is V itself and $1\vec{0} = \vec{0}$. Hence, V has no linearly independent subsets. V is called the **trivial vector space**.*

2.5. The Dot Product

The dot product will provide us with a way of computing the angle between two vectors in $\mathbb{R}^n$. The dot product is formally defined as follows:

Definition 2.41. *Let $\vec{u} = (u_1, \ldots, u_n)$ and $\vec{v} = (v_1, \ldots, v_n)$ be two vectors in $\mathbb{R}^n$. The **dot product** of $\vec{u}$ and $\vec{v}$ is given by*

$$\vec{u} \cdot \vec{v} := \sum_{i=1}^{n} u_i v_i = u_1 v_1 + u_2 v_2 + \cdots + u_n v_n.$$

Proposition 2.42 (Properties of the dot product)**.** *Let $\vec{u}, \vec{v}, \vec{w} \in \mathbb{R}^n$ and $c \in \mathbb{R}^n$. Then*

(1) $\vec{u} \cdot \vec{v} = \vec{v} \cdot \vec{u}$
(2) $(\vec{u} + \vec{v}) \cdot \vec{w} = \vec{u} \cdot \vec{w} + \vec{v} \cdot \vec{w}$
(3) $\vec{w} \cdot (\vec{u} + \vec{v}) = \vec{w} \cdot \vec{u} + \vec{w} \cdot \vec{v}$
(4) $(c\vec{u}) \cdot \vec{v} = c(\vec{u} \cdot \vec{v}) = \vec{u} \cdot (c\vec{v})$
(5) $\vec{u} \cdot \vec{u} \geq 0$ *and is* 0 *if and only if* $\vec{u} = \vec{0}$

Proof. (1): This follows from the commutativity of the multiplication on $\mathbb{R}$:

$$\vec{u} \cdot \vec{v} = \sum_{i=1}^{n} u_i v_i = \sum_{i=1}^{n} v_i u_i = \vec{v} \cdot \vec{u}$$

(2): This follows from the distributive property on $\mathbb{R}$:

$$\begin{aligned}(\vec{u} + \vec{v}) \cdot \vec{w} &= \sum_{i=1}^{n} (u_i + v_i) w_i \\ &= \sum_{i=1}^{n} (u_i w_i + v_i w_i) \\ &= \sum_{i=1}^{n} u_i w_i + \sum_{i=1}^{n} v_i w_i \\ &= \vec{u} \cdot \vec{w} + \vec{v} \cdot \vec{w}.\end{aligned}$$

(3): This follows from (1) and (2) (although we can use an argument to (2) as well):

$$\begin{aligned}\vec{w} \cdot (\vec{u} + \vec{v}) &= (\vec{u} + \vec{v}) \cdot \vec{w} \\ &= \vec{u} \cdot \vec{w} + \vec{v} \cdot \vec{w} \\ &= \vec{w} \cdot \vec{u} + \vec{w} \cdot \vec{v},\end{aligned}$$

where the first and third qualities follow from (1) and the second equality follows from (2).

(4): The first part follows from the associativity of the multiplication on $\mathbb{R}$:

$$(c\vec{u}) \cdot \vec{v} = \sum_{i=1}^{n} (cu_i)v_i = \sum_{i=1}^{n} c(u_i v_i) = c \sum_{i=1}^{n} u_i v_i = c(\vec{u} \cdot \vec{v})$$

The proof of the second part is similar:

$$(c\vec{u}) \cdot \vec{v} = \sum_{i=1}^{n} (cu_i)v_i = \sum_{i=1}^{n} u_i(cv_i) = \vec{u} \cdot (c\vec{v}).$$

(5): The dot product $\vec{u} \cdot \vec{u}$ is necessarily non-negative since it is a sum of squares

$$\vec{u} \cdot \vec{u} = \sum_{i=1}^{n} u_i^2.$$

Also, $\vec{u} \cdot \vec{u} = 0$ if and only if every term in the above sum is zero. This implies that $u_i = 0$ for $i = 1, \ldots, n$. Hence, $\vec{u} = 0$. □

Definition 2.43. *Let V be a vector space. The* ***norm*** *(or length) of a vector $\vec{v} = (v_1, \ldots, v_n) \in V$ is defined by*

$$\|\vec{v}\| := \sqrt{\vec{v} \cdot \vec{v}} = \sqrt{v_1^2 + \cdots + v_n^2}.$$

The motivation for this definition comes from the fact that if V is a subspace of $\mathbb{R}^2$ or $\mathbb{R}^3$, then the norm $\|\vec{v}\|$ of a vector $\vec{v} \in V$ is just the usual Euclidean length of the arrow $\vec{v}$. From Figure 5, the length of a vector $(a, b) \in \mathbb{R}^2$ is easily obtained by one application of the Pythagorean theorem:

$$\|(a, b)\| = \sqrt{a^2 + b^2}.$$

Similarly, from Figure 6, the norm (or length) of a vector $(a, b, c) \in \mathbb{R}^3$ can be computed by using two applications of the Pythagorean theorem:

$$\|(a, b, c)\| = \sqrt{u^2 + v^2} = \sqrt{a^2 + b^2 + c^2}.$$

The above formulas are just special cases of Definition 2.43.

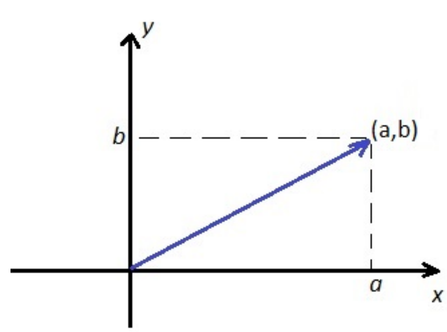


Figure 5. a vector (a, b) in $\mathbb{R}^2$ has norm $\|(a, b)\| = \sqrt{a^2 + b^2}$

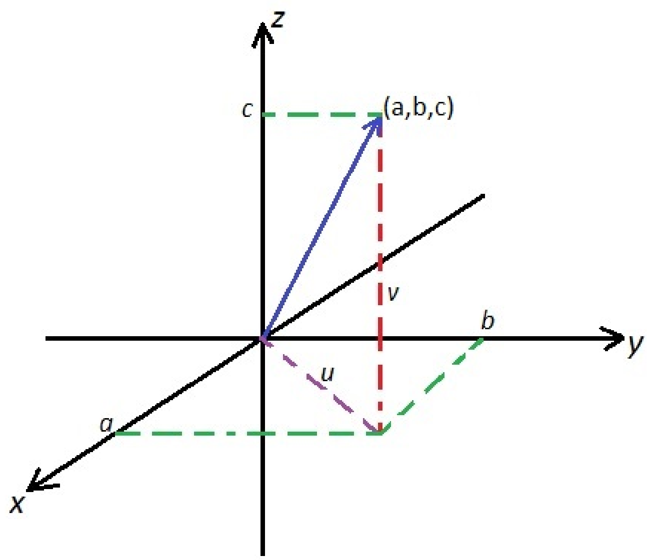


Figure 6. a vector (a, b, c) in $\mathbb{R}^3$ has norm $\|(a, b, c)\| = \sqrt{a^2 + b^2 + c^2}$

Definition 2.44. *A vector $\vec{u} \in \mathbb{R}^n$ is callled a **unit vector** if it has norm 1, that is, $\|\vec{u}\| = 1$.*

Let $\vec{v}$ be any nonzero vector. We now show that the vector $\vec{u} := \vec{v}/\|\vec{v}\|$ is a unit vector:

$$\begin{aligned} \|\vec{u}\|^2 &= \vec{u} \cdot \vec{u} \\ &= \frac{\vec{v}}{\|\vec{v}\|} \cdot \frac{\vec{v}}{\|\vec{v}\|} \\ &= \frac{1}{\|\vec{v}\|^2} \vec{v} \cdot \vec{v} \\ &= \frac{1}{\|\vec{v}\|^2} \|\vec{v}\|^2 \\ &= 1. \end{aligned}$$

Definition 2.45. *Let $\vec{v}$ be a nonzero vector. Then $\vec{v}/\|\vec{v}\|$ is called the **normalized vector associated to** $\vec{v}$. ($\vec{v}/\|\vec{v}\|$is also called the **direction** of $\vec{v}$ since it points in the same direction as $\vec{v}$.)*

Example 2.46. *The direction of the vector $\vec{v} = (1, -1, 2)$ is*

$$\frac{\vec{v}}{\|\vec{v}\|} = \frac{1}{\sqrt{1+1+4}}(1, -1, 2) = (\frac{1}{\sqrt{6}}, \frac{-1}{\sqrt{6}}, \frac{2}{\sqrt{6}})$$

Let u and v be two points in $\mathbb{R}^n$. How shall we define the **distance** from the point u to the point v? For starters, let's think of u and v as vectors (or arrows) in $\mathbb{R}^n$. Then we can define the distance from u to v, which we will denote as $d(u, v)$, as the norm of the vector $\vec{w} = \vec{u} - \vec{v}$:

$$d(u,v) := \|\vec{u} - \vec{v}\| = \sqrt{(u_1 - v_1)^2 + (u_2 - v_2)^2 + \cdots + (u_n - v_n)^2} \qquad (10)$$

The above definition agrees with our usual notion of distance when we consider the distance between points in $\mathbb{R}^2$ (or $\mathbb{R}^3$) (see Figure 7).

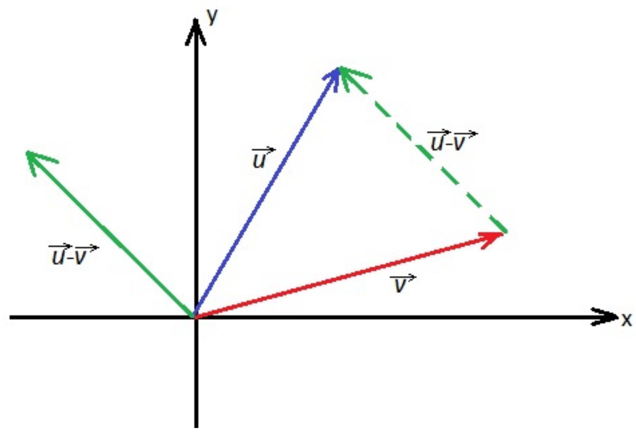


Figure 7. distance between two points u and v in $\mathbb{R}^2$

Example 2.47. *The distance from the point* $x = (-1, 1, 2, 0)$ *to the point* $y = (0, 1, 0, 1)$ *in* $\mathbb{R}^4$ *is*

$$d(x, y) = \|\vec{x} - \vec{y}\| = \sqrt{(-1-0)^2 + (1-1)^2 + (2-0)^2 + (0-1)^2} = \sqrt{6}.$$

Next, we will use the dot product to define the angle between two vectors in $\mathbb{R}^n$. In order to motivate the definition, we first consider how to express the angle between two vectors in $\mathbb{R}^2$ in terms of the dot product. Let $0 \leq \theta \leq \pi$ denote the angle between the vectors $\vec{u}$ and $\vec{v}$ in Figure 7. Consider the triangle formed by the vectors $\vec{u}$, $\vec{v}$, and $\vec{u} - \vec{v}$ in Figure 7. Using the *Law of Cosines*, we can relate θ to the norms (or lengths) of the vectors making up the sides of the aforementioned triangle:

$$\|\vec{u} - \vec{v}\|^2 = \|\vec{u}\|^2 + \|\vec{v}\|^2 - 2\,\|\vec{u}\|\,\|\vec{v}\| \cos\theta. \qquad (11)$$

Since the square of the norm of a vector is just the dot product of the vector with itself, we can rewrite the above expression as

$$(\vec{u} - \vec{v}) \cdot (\vec{u} - \vec{v}) = \vec{u} \cdot \vec{u} + \vec{v} \cdot \vec{v} - 2\,\|\vec{u}\|\,\|\vec{v}\| \cos\theta. \qquad (12)$$

The left side of the above equation expands as

$$\vec{u}\cdot\vec{u} - 2\vec{u}\cdot\vec{v} + \vec{v}\cdot\vec{v}. \tag{13}$$

Substituting (13) in to (12) and simplifying gives

$$\vec{u}\cdot\vec{v} = \|\vec{u}\|\,\|\vec{v}\|\cos\theta. \tag{14}$$

From (14), we obtain

$$\cos\theta = \frac{\vec{u}\cdot\vec{v}}{\|\vec{u}\|\,\|\vec{v}\|}. \tag{15}$$

The same argument applied to two vectors in $\mathbb{R}^3$ yields the same angle formula as (15). This motivates the following definition:

Definition 2.48. *Let $\vec{u}$ and $\vec{v}$ be two non-zero vectors in $\mathbb{R}^n$. The angle $0 \le \theta \le \pi$ between $\vec{u}$ and $\vec{v}$ is defined by the following relation:*

$$\cos\theta = \frac{\vec{u}\cdot\vec{v}}{\|\vec{u}\|\,\|\vec{v}\|}.$$

Since $|\cos\theta| \le 1$, Definition 2.48 is sensible only if

$$-1 \le \frac{\vec{u}\cdot\vec{v}}{\|\vec{u}\|\,\|\vec{v}\|} \le 1 \tag{16}$$

for any vectors $\vec{u}, \vec{v} \in \mathbb{R}^n$. The inequality (16) is an immediate consequence of the following result:

Theorem 2.49 (Cauchy-Schwartz Inequality)**.** $|\vec{u}\cdot\vec{v}| \le \|\vec{u}\|\,\|\vec{v}\|$ *for any vectors $\vec{u}, \vec{v} \in \mathbb{R}^n$. Moreover, if $\vec{u}$ and $\vec{v}$ are nonzero, then $\vec{u}\cdot\vec{v} = \|\vec{u}\|\,\|\vec{v}\|$ if and only if $\vec{u} = \lambda\vec{v}$ for some positive $\lambda \in \mathbb{R}$.*

Proof. Let $\vec{w}$ and $\vec{z}$ be unit vectors. Then

$$\begin{aligned} 0 &\le (\vec{w}-\vec{z})\cdot(\vec{w}-\vec{z}) \\ &\le \vec{w}\cdot\vec{w} - 2\vec{w}\cdot\vec{z} + \vec{z}\cdot\vec{z} \\ &\le 2 - 2\vec{w}\cdot\vec{z}. \end{aligned}$$

The last inequality implies

$$\vec{w}\cdot\vec{z} \le 1.$$

Similarly, we have

$$\begin{aligned} 0 &\le (\vec{w}+\vec{z})\cdot(\vec{w}+\vec{z}) \\ &\le \vec{w}\cdot\vec{w} + 2\vec{w}\cdot\vec{z} + \vec{z}\cdot\vec{z} \\ &\le 2 + 2\vec{w}\cdot\vec{z}. \end{aligned}$$

The last inequality implies

$$-1 \le \vec{w}\cdot\vec{z}.$$

Combining these two inequalities gives

$$|\vec{w}\cdot\vec{z}| \le 1. \tag{17}$$

We now use (17) to prove the Cauchy-Schwartz inequality. First, note that if $\vec{u}=\vec{0}$ or $\vec{v}=\vec{0}$, we see that the Cauchy-Schwartz inequality automatically holds. So let us assume that $\vec{u}$ and $\vec{v}$ are non-zero vectors. Let $\vec{w}=\vec{u}/\left\|\vec{u}\right\|$ and $\vec{z}=\vec{v}/\left\|\vec{v}\right\|$. Then (17) implies

$$|\vec{w}\cdot\vec{z}| = \Big|\frac{\vec{u}}{\|\vec{u}\|}\cdot\frac{\vec{v}}{\|\vec{v}\|}\Big| \le 1.$$

The above inequality can be rewritten as $|\vec{u}\cdot\vec{v}| \le \|\vec{u}\|\,\|\vec{v}\|$, which is the Cauchy-Schwartz inequality.

For the last statement, let $\vec{u}$ and $\vec{v}$ be nonzero vectors. Suppose that $\vec{u}=\lambda\vec{v}$ for some $\lambda>0$. Then

$$\|\vec{u}\|\,\|\vec{v}\| = \|\lambda\vec{v}\|\,\|\vec{v}\| = |\lambda|\,\|\vec{v}\|^2 = \lambda(\vec{v}\cdot\vec{v}) = (\lambda\vec{v})\cdot\vec{v} = \vec{u}\cdot\vec{v}.$$

On the other hand, suppose that $\vec{u}\cdot\vec{v}=\|\vec{u}\|\,\|\vec{v}\|$. Let $\vec{w}=\vec{u}/\left\|\vec{u}\right\|$ and $\vec{z}=\vec{v}/\left\|\vec{v}\right\|$. Then $\vec{w}$ and $\vec{z}$ are unit vectors such that $\vec{w}\cdot\vec{z}=1$. Snice $\vec{w}\cdot\vec{w}=\vec{z}\cdot\vec{z}=1$, it follows that

$$\vec{w}\cdot(\vec{w}-\vec{z}) = \vec{z}\cdot(\vec{w}-\vec{z}) = 0.$$

This in turn implies that $(\vec{w}-\vec{z})\cdot(\vec{w}-\vec{z})=0$. From this, we conclude that $\vec{w}=\vec{z}$. The definition of $\vec{w}$ and $\vec{z}$ implies that

$$\vec{u} = \frac{\|\vec{u}\|}{\|\vec{v}\|}\vec{v}.$$

Since $\frac{\|\vec{u}\|}{\|\vec{v}\|}>0$, this completes the proof. □

Definition 2.50. *Two (nonzero) vectors $\vec{u},\vec{v}\in\mathbb{R}^n$ are **orthogonal** if the angle between them is 90°. We will denote this condition with the notation: $\vec{u}\perp\vec{v}$.*

Corollary 2.51. *Two non-zero vectors $\vec{u},\vec{v}\in\mathbb{R}^n$ are orthogonal if and only if $\vec{u}\cdot\vec{v}=0$.*

Proof. Let $0\le\theta\le\pi$ be the angle formed by $\vec{u}$ and $\vec{v}$. By Definition 2.48, $\theta\in[0,\pi]$ is uniquely determined by the following equation:

$$\cos\theta = \frac{\vec{u}\cdot\vec{v}}{\|\vec{u}\|\,\|\vec{v}\|}.$$

From the above equation, we see that $\cos\theta=0$ if and only if $\vec{u}\cdot\vec{v}=0$. Since θ is restricted to the interval $[0,\pi]$, the statement that $\cos\theta=0$ is equivalent to the statement that $\theta=\pi/2$. This completes the proof. □

Example 2.52. *Let's calculate the angle between* $\vec{u} = (1, 0, 1)$ *and* $\vec{v} = (1, 0, -1)$*. Using Definition 2.48, we have*

$$\cos\theta = \frac{\vec{u} \cdot \vec{v}}{\|\vec{u}\| \, \|\vec{v}\|} = \frac{1}{\sqrt{2}\sqrt{2}} = \frac{1}{2},$$

which implies that $\theta = \pi/3$*.*

We conclude this section with a well known result called the *triangle inequality*:

Theorem 2.53 (Triangle Inequality)**.** *Let* $\vec{u}, \vec{v} \in \mathbb{R}^n$*. Then*

$$\|\vec{u} + \vec{v}\| \leq \|\vec{u}\| + \|\vec{v}\|$$

Proof. Using the properties of the dot product and the Cauchy-Schwartz inequality (see Theorem 2.49), we have

$$\begin{aligned} \|\vec{u} + \vec{v}\|^2 &= (\vec{u} + \vec{v}) \cdot (\vec{u} + \vec{v}) \\ &= \vec{u} \cdot \vec{u} + 2\vec{u} \cdot \vec{v} + \vec{v} \cdot \vec{v} \\ &= \|\vec{u}\|^2 + 2\vec{u} \cdot \vec{v} + \|\vec{v}\|^2 \\ &\leq \|\vec{u}\|^2 + 2\,\|\vec{u}\|\,\|\vec{v}\| + \|\vec{v}\|^2 \\ &\leq (\|\vec{u}\| + \|\vec{v}\|)^2, \end{aligned} \tag{18}$$

where the second to last line follows from the Cauchy-Schwartz inequality. Taking the square root of both sides of (18) gives

$$\|\vec{u} + \vec{v}\| \leq \|\vec{u}\| + \|\vec{v}\|.$$

□

Intuitively, the triangle inequality is obvious for vectors in $\mathbb{R}^2$ (and $\mathbb{R}^3$). However, since we deal with vectors in $\mathbb{R}^n$ for $n \geq 1$, it is worthwhile to prove it for the general case.

The proof of the triangle inequality leads to the *generalized pythagorean theorem*:

Corollary 2.54 (Generalized Pythagorean Theorem)**.** *Let* $\vec{u}$ *and* $\vec{v}$ *be orthogonal vectors in* $\mathbb{R}^n$*. Then* $\|\vec{u} + \vec{v}\|^2 = \|\vec{u}\|^2 + \|\vec{v}\|^2$*.*

Proof. By direct calculation, we have

$$\begin{aligned} \|\vec{u} + \vec{v}\|^2 &= (\vec{u} + \vec{v}) \cdot (\vec{u} + \vec{v}) \\ &= \vec{u} \cdot \vec{u} + 2\vec{u} \cdot \vec{v} + \vec{v} \cdot \vec{v} \\ &= \|\vec{u}\|^2 + \|\vec{v}\|^2 \end{aligned}$$

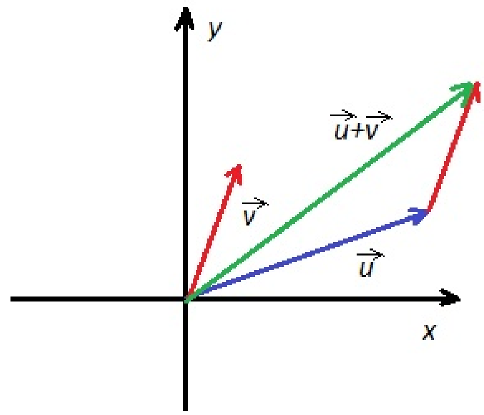


Figure 8. For vectors $\vec{u}, \vec{v} \in \mathbb{R}^2$, it is intuitively clear that $\|\vec{u}+\vec{v}\| \leq \|\vec{u}\| + \|\vec{v}\|$. The proof of the triangle inequality shows that this relation holds in general for vectors in $\mathbb{R}^n$ for $n \geq 1$.

where the last equality follows from the fact that $\vec{u}$ and $\vec{v}$ are orthogonal which is equivalent to the statement that $\vec{u} \cdot \vec{v} = 0$. □

2.6. Orthogonal Projection & the Gram-Schmidt Process

In this section, we continue to explore some of the consequences of the dot product and the notion of orthogonality. To do this, we need to first introduce several definitions that are essential to this goal.

Definition 2.55. *Let $\{\vec{v}_1, \ldots, \vec{v}_k\}$ be a set of vectors in $\mathbb{R}^n$. $\{\vec{v}_1, \ldots, \vec{v}_k\}$ is called an* ***orthogonal set*** *if $\vec{v}_i \neq \vec{0}$ for $i = 1, \ldots, k$ and $\vec{v}_i \cdot \vec{v}_j = 0$ for all $1 \leq i < j \leq k$.*

In other words, a set of vectors in $\mathbb{R}^n$ form an orthogonal set if they are all nonzero and mutually orthogonal to one another.

Example 2.56. *The vectors $\vec{v} = (1, -1, 1)$ and $\vec{u} = (2, 2, 0)$ in $\mathbb{R}^3$ form an an orthogonal set.*

Proposition 2.57. *Let $\{\vec{v}_1, \ldots, \vec{v}_k\}$ be an orthogonal set in $\mathbb{R}^n$. Then $\{\vec{v}_1, \ldots, \vec{v}_k\}$ is a linearly independent set.*

Proof. Suppose that

$$r_1\vec{v}_1 + \cdots + r_k\vec{v}_k = \vec{0}.$$

Let $i \in \{1, \ldots, k\}$ be arbitrary and take the dot product of both sides of the equation with $\vec{v}_i$:

$$\begin{aligned} r_1\vec{v}_1 \cdot \vec{v}_i + \cdots + r_k\vec{v}_k \cdot \vec{v}_i &= \vec{0} \cdot \vec{v}_i \\ r_i\vec{v}_i \cdot \vec{v}_i &= 0 \\ r_i \left\|\vec{v}_i\right\|^2 &= 0 \end{aligned}$$

where the second equality follows from the fact that $\vec{v}_j \cdot \vec{v}_i = 0$ for all $j \neq i$. Since $\vec{v}_i \neq 0$ (by definition of an orthogonal set), we have $r_i = 0/\left\|\vec{v}_i\right\|^2 = 0$. This completes the proof. □

Corollary 2.58. *Let $\{\vec{v}_1, \ldots, \vec{v}_k\}$ be an orthogonal set in $\mathbb{R}^n$. Then $k \leq n$.*

Proof. By Proposition 2.57, $\{\vec{v}_1, \ldots, \vec{v}_k\}$ is a linearly independent set. Since $\dim \mathbb{R}^n = n$, any linearly independent set contains at most n elements. Hence, $k \leq n$. □

For the remainder of this section, let V be vector space and let $n = \dim V$. (Recall that in this chapter, vector space means a fixed subspace of $\mathbb{R}^m$ for some $m \geq 1$.) As we saw previously, given an arbitrary basis $\{\vec{v}_1, \ldots, \vec{v}_n\}$ on V and an arbitrary vector $\vec{v} \in V$, one must use the Gauss Jordan method to calculate the coefficients $r_1, \ldots, r_n$ so that

$$r_1\vec{v}_1 + r_2\vec{v}_2 + \cdots + r_n\vec{v}_n = \vec{v}.$$

If n is large, a good bit of work is needed to compute these coefficients. On the other hand, if one works with an **orthogonal basis** (or even better an **orthonormal basis**), computing the coefficients $r_1, \ldots, r_n$ is a simple matter. This is one of the advantages of the notion of orthogonality. Naturally, one defines an orthogonal basis and an orthonormal basis as follows:

Definition 2.59. *Let $\{\vec{v}_1, \ldots, \vec{v}_k\}$ be a set of vectors in $\mathbb{R}^n$. $\{\vec{v}_1, \ldots, \vec{v}_k\}$ is called an **orthonormal set** if $\{\vec{v}_1, \ldots, \vec{v}_k\}$ is an orthogonal set and $\|\vec{v}_i\| = 1$ for $i = 1, \ldots, k$.*

Definition 2.60. *Let $\mathcal{B} := \{\vec{v}_1, \ldots, \vec{v}_n\}$ be a basis of V. If $\mathcal{B}$ is an orthogonal set, then $\mathcal{B}$ is called an **orthogonal basis**. If $\mathcal{B}$ is an orthonormal set, then $\mathcal{B}$ is called an **orthonormal basis**.*

Example 2.61. *The standard basis $\vec{e}_1, \ldots, \vec{e}_n$ on $\mathbb{R}^n$ is an orthonormal basis.*

Theorem 2.62. *Let* $\{\vec{u}_1, \ldots, \vec{u}_n\}$ *be an orthonormal basis on* V*. Let* $\vec{v} \in V$*. Then*

$$\vec{v} = r_1\vec{u}_1 + r_2\vec{u}_2 + \cdots + r_n\vec{u}_n.$$

where $r_i = \vec{v} \cdot \vec{u}_i$ *for* $i = 1, \ldots, n$*.*

Proof. Since $\{\vec{u}_1, \ldots, \vec{u}_n\}$ is a basis, we can express $\vec{v} \in V$ as

$$\vec{v} = r_1\vec{u}_1 + r_2\vec{u}_2 + \cdots + r_n\vec{u}_n$$

for some (unique) $r_i \in \mathbb{R}$, $i = 1, \ldots, n$. Let $i \in \{1, \ldots, n\}$ be arbitrary and take the dot product of both sides of the above equation with $\vec{u}_i$:

$$\begin{aligned} \vec{v} \cdot \vec{u}_i &= r_1\vec{u}_1 \cdot \vec{u}_i + r_2\vec{u}_2 \cdot \vec{u}_i + \cdots + r_n\vec{u}_n \cdot \vec{u}_i \\ &= r_i\vec{u}_i \cdot \vec{u}_i \\ &= r_i \end{aligned}$$

where the second equality follows from the fact that $\vec{u}_j \cdot \vec{u}_i = 0$ for $j \neq i$ and $\vec{u}_i \cdot \vec{u}_i = 1$. This completes the proof. □

Example 2.63. *Consider the basis*

$$\vec{u}_1 = (0, 1, 0), \quad \vec{u}_2 = \frac{1}{13}(5, 0, 12), \quad \vec{u}_3 = \frac{1}{13}(-12, 0, 5).$$

of $\mathbb{R}^3$*. By inspection, we see that this basis is actually orthonormal. Let* $\vec{v} = (1, 2, 3)$*. Using Theorem 2.62, we have*

$$\vec{v} = r_1\vec{u}_1 + r_2\vec{u}_2 + r_3\vec{u}_3$$

where

$$r_1 = \vec{v} \cdot \vec{u}_1 = 2, \qquad r_2 = \vec{v} \cdot \vec{u}_2 = \frac{41}{13}, \qquad r_3 = \vec{v} \cdot \vec{u}_3 = \frac{3}{13}.$$

After introducing the idea of an orthonormal basis, the natural question is *how does one actually find an orthonormal basis for* V? The answer is the **Gram-Schmidt process**. Central to the Gram-Schmidt process is the idea of **orthogonal projection** which we now describe.

Consider two vectors $\vec{v}$ and $\vec{u}$ in $\mathbb{R}^n$. Orthogonal projection addresses the following question: *how "much" of the vector* $\vec{v}$ *lies in the direction of* $\vec{u}$? More precisely, we wish to find a decomposition of $\vec{v}$ of the form

$$\vec{v} = \vec{a} + \vec{b}$$

where $\vec{a}$ points in the same direction as $\vec{u}$ and $\vec{b}$ is orthogonal to $\vec{u}$. The vector $\vec{a}$ is the component of $\vec{v}$ which lies in the direction of $\vec{u}$ and is called the *orthogonal projection of* $\vec{v}$ *onto* $\vec{u}$ (see Figure 9).
Note that if $\vec{a}$ is known, then $\vec{b} = \vec{v} - \vec{a}$ is uniquely determined. There are two natural questions here: (1) *is* $\vec{a}$ *unique?* (2) *if so, how does one actually compute*

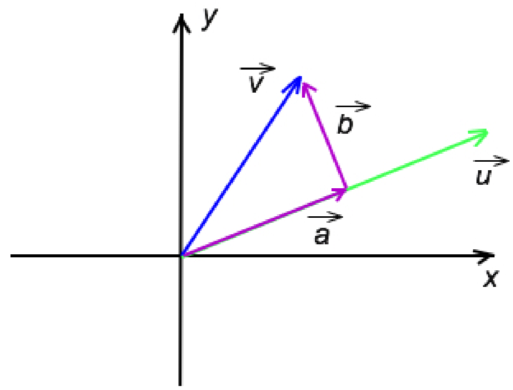


Figure 9. The orthogonal projection of $\vec{v}$ onto $\vec{u}$ is the vector $\vec{a}$

$\vec{a}$? These questions are answered by the following result:

Theorem 2.64. *Let $\vec{v}$ and $\vec{u}$ be vectors in $\mathbb{R}^n$ with $\vec{u} \neq \vec{0}$.*

(1) There are unique vectors $\vec{a}, \vec{b} \in \mathbb{R}^n$ such that $\vec{v} = \vec{a} + \vec{b}$ where $\vec{a}$ points in the direction of $\vec{u}$ (or $-\vec{u}$) and $\vec{a}$ and $\vec{b}$ are orthogonal.

(2) $\vec{a}$ is given by the following formula:

$$\vec{a} = \frac{\vec{v} \cdot \vec{u}}{\|\vec{u}\|^2}\vec{u}. \tag{19}$$

Proof. Suppose there exists vectors $\vec{a}$ and $\vec{b}$ such that

$$\vec{v} = \vec{a} + \vec{b} \tag{20}$$

where $\vec{a}$ points in the same direction as $\vec{u}$ and $\vec{b}$ is orthogonal to $\vec{a}$. Since $\vec{a}$ points in the same direction as $\vec{u}$, $\vec{a}$ must be of the form

$$\vec{a} = k\vec{u}$$

for some $k \in \mathbb{R}$. This implies that $\vec{b}$ is orthogonal to $\vec{u}$. Taking the dot product of both sides of (20) with $\vec{u}$ gives

$$\vec{v} \cdot \vec{u} = k \|\vec{u}\|^2 .$$

Solving for k gives

$$k = \frac{\vec{v} \cdot \vec{u}}{\|\vec{u}\|^2}.$$

This shows that $\vec{a}$ (if it exists!) is uniquely given by the formula in statement (2) of Theorem 2.64:

$$\vec{a} = \frac{\vec{v} \cdot \vec{u}}{\|\vec{u}\|^2}\vec{u}. \tag{21}$$

The uniqueness of $\vec{a}$ then implies that $\vec{b}$ is uniquely given by $\vec{b} = \vec{v} - \vec{a}$. This proves the uniqueness claim of Theorem 2.64.

To prove the rest of Theorem 2.64, we let $\vec{a}$ be defined by (21) and $\vec{b} = \vec{v} - \vec{a}$. Clearly, we have $\vec{v} = \vec{a} + \vec{b}$. Moreover, since $\vec{a}$ is a multiple of $\vec{u}$, $\vec{a}$ also points in the direction of $\vec{u}$ (or -$\vec{u}$ if $k < 0$). To complete the proof, it remains to show that $\vec{a}$ and $\vec{b}$ are orthogonal. The following calculation verifies this:

$$\begin{aligned}\vec{a} \cdot \vec{b} &= \vec{a} \cdot (\vec{v} - \vec{a}) \\ &= \vec{a} \cdot \vec{v} - \vec{a} \cdot \vec{a} \\ &= \frac{\vec{v} \cdot \vec{u}}{\|\vec{u}\|^2}\vec{u} \cdot \vec{v} - \left(\frac{\vec{v} \cdot \vec{u}}{\|\vec{u}\|^2}\right)^2 \vec{u} \cdot \vec{u} \\ &= \frac{(\vec{v} \cdot \vec{u})^2}{\|\vec{u}\|^2} - \frac{(\vec{v} \cdot \vec{u})^2}{\|\vec{u}\|^4}\|\vec{u}\|^2 \\ &= \frac{(\vec{v} \cdot \vec{u})^2}{\|\vec{u}\|^2} - \frac{(\vec{v} \cdot \vec{u})^2}{\|\vec{u}\|^2} \\ &= 0.\end{aligned}$$

This completes the proof. □

The orthogonal projection of $\vec{v}$ onto $\vec{u}$ will be denoted as follows:

$$\text{proj}_{\vec{u}}\vec{v} = \frac{\vec{u} \cdot \vec{v}}{\|\vec{u}\|^2}\vec{u}.$$

Example 2.65. *Let $\vec{v} = (v_1, v_2, \ldots, v_n)$ and let $\vec{e}_1, \vec{e}_2, \ldots, \vec{e}_n$ denote the standard basis on $\mathbb{R}^n$. For $i \leq n$, the orthogonal projection of $\vec{v}$ onto $\vec{e}_i$ is simply*

$$proj_{\vec{e}_i}\vec{v} = \frac{\vec{v} \cdot \vec{e}_i}{\|\vec{e}_i\|^2}\vec{e}_i = v_i\vec{e}_i,$$

which agrees nicely with our intuition.

Example 2.66. *Let $\vec{v} = (1, 2)$ and let $\vec{u} = (1, -1)$. The orthogonal projection of $\vec{v}$ onto $\vec{u}$ is*

$$proj_{\vec{u}}\vec{v} = \frac{\vec{v} \cdot \vec{u}}{\|\vec{u}\|^2}\vec{u} = \frac{-1}{2}(1, -1) = (-1/2, 1/2).$$

Setting

$$\vec{b} = \vec{v} - proj_{\vec{u}}\vec{v} = (3/2, 3/2),$$

we obtain the unique decomposition $\vec{v} = proj_{\vec{u}}\vec{v} + \vec{b}$ where $proj_{\vec{u}}\vec{v}$ points in the direction of $-\vec{u}$ and $proj_{\vec{u}}\vec{v}$ and $\vec{b}$ are orthogonal:

$$proj_{\vec{u}}\vec{v} \cdot \vec{b} = (-1/2, 1/2) \cdot (3/2, 3/2) = -3/4 + 3/4 = 0.$$

Example 2.67. *Let $\vec{v}$ be a non-zero vector. The orthogonal projection of $\vec{v}$ onto $\vec{v}$ is then*

$$proj_{\vec{v}}\vec{v} = \frac{\vec{v}\cdot\vec{v}}{\|\vec{v}\|^2}\vec{v} = \vec{v}$$

as we would expect. On the other hand, if $\vec{u}$ is any non-zero vector which is orthogonal to $\vec{v}$, then the orthogonal projection of $\vec{v}$ onto $\vec{u}$ is

$$proj_{\vec{u}}\vec{v} = \frac{\vec{u}\cdot\vec{v}}{\|\vec{u}\|^2}\vec{u} = 0\vec{u} = \vec{0},$$

which again agrees with our intuition. If $\vec{v}$ and $\vec{u}$ are orthogonal, then we expect nothing of $\vec{v}$ to lie in the direction of $\vec{u}$.

We are now in a position to describe the Gram-Schmidt process:

The Gram-Schmidt process

Let V be a subspace of $\mathbb{R}^m$ for some $m \geq 1$. The Gram-Schmidt process generates an orthogonal basis from an existing basis on V. Once one obtains the orthogonal basis, one can normalize it to obtain an orthonormal basis. Let $\mathcal{B} = \{\vec{v}_1, \vec{v}_2, \ldots, \vec{v}_n\}$ be **any** basis on V. We obtain an orthogonal basis

$$\mathcal{B}' := \{\vec{b}_1, \vec{b}_2, \ldots, \vec{b}_n\}$$

as follows:

1. Define $\vec{b}_1 := \vec{v}_1$
2. For $k = 2, \ldots, n$, define

$$\vec{b}_k := \vec{v}_k - \sum_{i=1}^{k-1} \mathrm{proj}_{\vec{b}_i}\vec{v}_k$$

The corresponding orthonormal basis is then $\{\vec{u}_1, \vec{u}_2, \ldots, \vec{u}_n\}$ where

$$\vec{u}_i := \frac{\vec{b}_i}{\left\|\vec{b}_i\right\|}, \quad i = 1, \ldots, n$$

Theorem 2.68. *Let V be a subspace of $\mathbb{R}^m$ for some $m \geq 1$ and let*

$$\mathcal{B} = \{\vec{v}_1, \vec{v}_2, \ldots, \vec{v}_n\}$$

*be **any** basis on V. Then the set $\mathcal{B}' := \{\vec{b}_1, \vec{b}_2, \ldots, \vec{b}_n\}$ given by the Gram-Schmidt process is an orthogonal basis for V.*

Proof. We will prove Theorem 2.68 by induction on the dimension of V. Suppose first that $\dim V = 1$, that is, $\mathcal{B} = \{\vec{v}_1\}$. It follows from Definition 2.55 that $\mathcal{B}$ is an orthogonal set in a trivial way. Indeed, if $\mathcal{B}$ contains only one non-zero element $\vec{v}_1$, then there are no other vectors in the set for $\vec{v}_1$ to be orthogonal to. Consequently, the condition of orthogonality is satisfied by default. (This is analogous to a basketball game where only one team shows up for the game and wins by default.) With $\dim V = 1$, the set generated by the Gram-Schmidt process is $\mathcal{B}' = \mathcal{B} = \{\vec{v}_1\}$ which is an orthogonal set (albeit in a boring way). Hence, the result holds for the $\dim V = 1$ case.

Now suppose that the Gram-Schmidt process works for all n-dimensional subspaces and let V be a subspace of dimension $n+1$ with basis

$$\mathcal{B} = \{\vec{v}_1, \vec{v}_2, \ldots, \vec{v}_n, \vec{v}_{n+1}\}.$$

Let U be the subspace spanned by the first n-elements of $\mathcal{B}$. In other words, U has basis

$$\mathcal{B}_1 = \{\vec{v}_1, \vec{v}_2, \ldots, \vec{v}_n\}.$$

Since $\dim U = n$, our induction hypothesis implies that we can apply the Gram-Schmidt process to the basis $\mathcal{B}_1'$ to obtain an orthogonal basis

$$\mathcal{B}_1' = \{\vec{b}_1, \vec{b}_2, \ldots, \vec{b}_n\},$$

for U where $\vec{b}_1 := \vec{v}_1$ and

$$\vec{b}_k := \vec{v}_k - \sum_{i=1}^{k-1} \operatorname{proj}_{\vec{b}_i} \vec{v}_k, \qquad k = 2, \ldots, n.$$

Let us define

$$\vec{b}_{n+1} := \vec{v}_{n+1} - \sum_{i=1}^{n} \operatorname{proj}_{\vec{b}_i} \vec{v}_{n+1}.$$

Consider the set

$$\mathcal{B}' := \{\vec{b}_1, \vec{b}_2, \ldots, \vec{b}_n, \vec{b}_{n+1}\}.$$

Since $\mathcal{B}_1'$ is an orthogonal basis, $\mathcal{B}_1'$ is also an orthogonal set. Hence, $\vec{b}_i \neq 0$ for $i = 1, \ldots, n$ and $\vec{b}_i \cdot \vec{b}_j = 0$ for $1 \leq i < j \leq n$. We will now show that $\mathcal{B}'$ is also an orthogonal set. First, since

$$U = \operatorname{span} \mathcal{B}_1 = \operatorname{span} \mathcal{B}_1',$$

it follows that $\vec{v}_{n+1} \notin U$. Also, since

$$\operatorname{proj}_{\vec{b}_i} \vec{v}_{n+1} := \left(\frac{\vec{b}_i \cdot \vec{v}_{n+1}}{\left\| \vec{b}_i \right\|^2} \right) \vec{b}_i \in U$$

for $i = 1, \ldots, n$, the definition of $\vec{b}_{n+1}$ implies that $\vec{b}_{n+1} \neq \vec{0}$. (Indeed, $\vec{b}_{n+1} = \vec{0}$ would imply $\vec{v}_{n+1} \in U$, which is a contradiction.) Next, we show that $\vec{b}_{n+1}$ is orthogonal to $\vec{b}_k$ for $k = 1, \ldots, n$. This follows by a direct calculation:

$$\begin{aligned}
\vec{b}_{n+1} \cdot \vec{b}_k &= (\vec{v}_{n+1} - \sum_{i=1}^{n} \operatorname{proj}_{\vec{b}_i} \vec{v}_{n+1}) \cdot \vec{b}_k \\
&= \vec{v}_{n+1} \cdot \vec{b}_k - \sum_{i=1}^{n} \left[\operatorname{proj}_{\vec{b}_i} \vec{v}_{n+1}\right] \cdot \vec{b}_k \\
&= \vec{v}_{n+1} \cdot \vec{b}_k - \sum_{i=1}^{n} \left(\frac{\vec{b}_i \cdot \vec{v}_{n+1}}{\left\|\vec{b}_i\right\|^2} \right) \vec{b}_i \cdot \vec{b}_k \\
&= \vec{v}_{n+1} \cdot \vec{b}_k - \left(\frac{\vec{b}_k \cdot \vec{v}_{n+1}}{\left\|\vec{b}_k\right\|^2} \right) \vec{b}_k \cdot \vec{b}_k \\
&= \vec{v}_{n+1} \cdot \vec{b}_k - \left(\frac{\vec{b}_k \cdot \vec{v}_{n+1}}{\left\|\vec{b}_k\right\|^2} \right) \left\|\vec{b}_k\right\|^2 \\
&= \vec{v}_{n+1} \cdot \vec{b}_k - \vec{b}_k \cdot \vec{v}_{n+1} \\
&= 0,
\end{aligned}$$

where the fourth equality follows from the fact that $\mathcal{B}_1'$ is an orthogonal set. Hence, $\vec{b}_i \cdot \vec{b}_k = 0$ for $i \leq n$ and $i \neq k$. This proves that $\mathcal{B}'$ is an orthogonal set. By Proposition 2.57, any orthogonal set is also linearly independent. Since $\mathcal{B}'$ has cardinality $n+1$ and $\dim V = n+1$, it follows that $\mathcal{B}'$ is also a basis for V. This completes the proof. □

Example 2.69. *Let V be the subspace of $\mathbb{R}^4$ defined by*

$$V = \{(a, a-2b, b+c, c) \mid a, b, c \in \mathbb{R}\}.$$

Let us find an orthonormal basis for V using the Gram-Schmidt process. To apply the Gram-Schmidt process, we first need to find a basis on V. This is easy to do. An arbitrary element of V decomposes as

$$(a, a-2b, b+c, c) = a(1,1,0,0) + b(0,-2,1,0) + c(0,0,1,1).$$

From this, we see that the vectors

$$\vec{v}_1 = (1,1,0,0), \quad \vec{v}_2 = (0,-2,1,0), \quad \vec{v}_3 = (0,0,1,1)$$

span V. In addition, a simple calculation shows that the vectors $\vec{v}_1$, $\vec{v}_2$, and $\vec{v}_3$ are also linearly independent. Hence, $\{\vec{v}_1, \vec{v}_2, \vec{v}_3\}$ is a basis on V. Let us now apply the Gram-Schmidt process to this basis to obtain the orthogonal basis $\{\vec{b}_1, \vec{b}_2, \vec{b}_3\}$, where

$$\vec{b}_1 = \vec{v}_1 = (1,1,0,0)$$
$$\vec{b}_2 = \vec{v}_2 - \text{proj}_{\vec{b}_1}\vec{v}_2 = \vec{v}_2 - \frac{\vec{b}_1 \cdot \vec{v}_2}{\left\|\vec{b}_1\right\|^2}\vec{b}_1 = (1,-1,1,0)$$
$$\vec{b}_3 = \vec{v}_3 - \text{proj}_{\vec{b}_1}\vec{v}_3 - \text{proj}_{\vec{b}_2}\vec{v}_3 = \vec{v}_3 - \frac{\vec{b}_1 \cdot \vec{v}_3}{\left\|\vec{b}_1\right\|^3}\vec{b}_1 - \frac{\vec{b}_2 \cdot \vec{v}_3}{\left\|\vec{b}_2\right\|^3}\vec{b}_2 = \frac{1}{3}(-1,1,2,3)$$

Normalizing the above basis gives the orthonormal basis:

$$\vec{u}_1 = \frac{1}{\left\|\vec{b}_1\right\|}\vec{b}_1 = \frac{1}{\sqrt{2}}(1,1,0,0)$$
$$\vec{u}_2 = \frac{1}{\left\|\vec{b}_2\right\|}\vec{b}_2 = \frac{1}{\sqrt{3}}(1,-1,1,0)$$
$$\vec{u}_3 = \frac{1}{\left\|\vec{b}_3\right\|}\vec{b}_3 = \frac{1}{\sqrt{15}}(-1,1,2,3)$$

Exercise 2.70. *Let W be the subspace of $\mathbb{R}^4$ defined by*

$$W = \{(a+2b, a-b, a+c, 2c) \mid a,b,c \in \mathbb{R}\}.$$

Find an orthonormal basis for W.

2.7. Orthogonal Complements & the Direct Sum

Intuitively speaking, when one thinks of the angle between two vectors $\vec{u}$ and $\vec{v}$ in $\mathbb{R}^n$, one expects $\vec{u}$ and $\vec{v}$ to have nonzero lengths. In other words, our intutition tells us that $\vec{u}$ and $\vec{v}$ should be nonzero vectors. In fact, the formula defining the angle between two vectors $\vec{u}$ and $\vec{v}$ (Definition 2.48) only makes sense if $\|\vec{u}\| \neq 0$ and $\|\vec{v}\| \neq 0$. Even so, it is convenient to define the angle between any vector $\vec{u} \in \mathbb{R}^n$ and the zero vector $\vec{0} \in \mathbb{R}^n$ to be $90°$ especially in light of Corollary 2.51. Taking this view, we introduce the following definition:

Definition 2.71. *Let W be a subspace of $\mathbb{R}^n$. The **orthogonal complement** of W is defined as*

$$W^{\perp} := \{\vec{v} \in \mathbb{R}^n \mid \vec{v} \cdot \vec{w} = 0, \quad \forall\, \vec{w} \in W\}$$

The meaning of the word "complement" will be justified later on in this chapter. For now, we have the following simple observation:

Proposition 2.72. *Let W be a subspace of $\mathbb{R}^n$. Then $W^\perp$ is a subspace of $\mathbb{R}^n$.*

Proof. Let $\vec{u}, \vec{v} \in W^\perp$ and let $r \in \mathbb{R}$. Then for all $\vec{w} \in W$, we have

$$\begin{aligned}(\vec{u}+\vec{v})\cdot\vec{w} &= \vec{u}\cdot\vec{w} + \vec{v}\cdot\vec{w}\\ &= 0+0\\ &= 0\end{aligned}$$

and

$$\begin{aligned}(r\vec{u})\cdot\vec{w} &= r(\vec{u}\cdot\vec{w})\\ &= r0\\ &= 0.\end{aligned}$$

This shows that $\vec{u}+\vec{v} \in W^\perp$ and $r\vec{u} \in W^\perp$. Hence, $W^\perp$ is a subspace of $\mathbb{R}^n$. □

Example 2.73. *Let W be a subspace of $\mathbb{R}^3$ which is spanned by the vector $\vec{w} = (1,3,1)$. In other words,*

$$W = \{r\vec{w} \mid r \in \mathbb{R}\}.$$

Let us determine what $W^\perp$ is. By definition of $W^\perp$, a vector $\vec{u} = (a,b,c)$ is in $W^\perp$ if and only if

$$\vec{u}\cdot(r\vec{w}) = r(\vec{u}\cdot\vec{w}) = 0 \quad \forall\ r \in \mathbb{R}.$$

The above condition is of course equivalent to the requirement that

$$\vec{u}\cdot\vec{w} = a + 3b + c = 0.$$

Hence, to compute $W^\perp$, we only have to find the general solution to the above linear system. Since the system consists of a single equation, there really is no need to apply the Gauss Jordan method to solve this system. We have one equation in the three variables a, b, and c. Hence, two of the variables are "free" (i.e. they can take on any value) provided that the third remaining variable is chosen to satisfy the above equation. Let b and c be free variables and let us solve for a in terms of b and c:

$$a = -3b - c.$$

Hence, $W^\perp$ is given by

$$W^\perp = \{(-3b - c, b, c) \mid b, c \in \mathbb{R}\}.$$

An arbitrary element of $W^\perp$ decomposes as

$$(-3b - c, b, c) = (-3b, b, 0) + (-c, 0, c) = b(-3, 1, 0) + c(-1, 0, 1).$$

Since b and c are arbitrary real numbers, we see that $W^\perp$ is spanned by the vectors $(-3, 1, 0)$ and $(-1, 0, 1)$. In addition, its clear that these two vectors are also linearly independent. Hence, $(-3, 1, 0)$ and $(-1, 0, 1)$ form a basis for $W^\perp$. From this, we conclude that $\dim W^\perp = 2$.

Observe that in Example 2.73

$$\dim W + \dim W^\perp = \dim \mathbb{R}^3 = 1 + 2 = 3.$$

Also, note that $\vec{w}$ together with the basis vectors $(-3, 1, 0)$ and $(-1, 0, 1)$ of $W^\perp$ form a basis of $\mathbb{R}^3$. As you might have guessed, this is far from a coincidence. The following definitions will prove useful in helping us understand why.

Let V be a vector space. (Recall that in this chapter, this means that V is a subspace of $\mathbb{R}^m$ for some $m \geq 1$.)

Definition 2.74. *Let W_1 and W_2 be two subspaces of V (recall Definition 2.14). Define the* ***sum*** *of W_1 and W_2 by*

$$W_1 + W_2 := \{\vec{w}_1 + \vec{w}_2 \mid \vec{w}_1 \in W_1,\ \vec{w}_2 \in W_2\}.$$

Proposition 2.75. *Let W_1 and W_2 be two subspaces of V. Then $W_1 + W_2$ is a subspace of V.*

Proof. Let $\vec{u}, \vec{u}' \in W_1 + W_2$. Then

$$\vec{u} = \vec{w}_1 + \vec{w}_2$$
$$\vec{u}' = \vec{w}_1' + \vec{w}_2'$$

for some $\vec{w}_1, \vec{w}_1' \in W_1$ and $\vec{w}_2, \vec{w}_2' \in W_2$. Hence,

$$\vec{u} + \vec{u}' = (\vec{w}_1 + \vec{w}_1') + (\vec{w}_2 + \vec{w}_2').$$

Since W_1 and W_2 are subspaces of V, we have $\vec{w}_1 + \vec{w}_1' \in W_1$ and $\vec{w}_2 + \vec{w}_2' \in W_2$. From the definition of $W_1 + W_2$, it follows that $\vec{u} + \vec{u}' \in W_1 + W_2$. Lastly, let $r \in \mathbb{R}$. Then

$$r\vec{u} = r\vec{w}_1 + r\vec{w}_2.$$

Again, since W_1 and W_2 are subspaces of V, we have $r\vec{w}_1 \in W_1$ and $r\vec{w}_2 \in W_2$ which implies that $r\vec{u} \in W_1 + W_2$. □

The following result will prove useful in a moment:

Lemma 2.76 (Basis Extension Lemma). *Let V be a vector space of dimension n and let W be a subspace of V. Let $\{\vec{w}_1, \ldots, \vec{w}_k\}$ be a basis of W. Then there exists $\vec{w}_{k+1}, \ldots, \vec{w}_n \in V$ such that*

$$\{\vec{w}_1, \ldots, \vec{w}_k, \vec{w}_{k+1}, \ldots, \vec{w}_n\}$$

is a basis of V.

Proof. Let $\mathcal{B} := \{\vec{v}_1, \ldots, \vec{v}_n\}$ be any basis on V. By the Replacement Theorem (Theorem 2.34), there exists a reordering of $\mathcal{B}$,

$$\mathcal{B}_\sigma = \{\vec{v}_{\sigma(1)}, \ldots, \vec{v}_{\sigma(n)}\},$$

such that $\{\vec{w}_1, \ldots, \vec{w}_k, \vec{v}_{\sigma(k+1)}, \ldots, \vec{v}_{\sigma(n)}\}$ is a basis of V. Setting $\vec{w}_j := \vec{v}_{\sigma(j)}$ for $j = k+1, \ldots, n$ proves the lemma. □

The following result is often useful in computing the dimension of a subspace.

Proposition 2.77. *Let W_1 and W_2 be subspaces of V. Then*

(i) $W_1 \cap W_2$ *is also a subspace of* V

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

Proof. (i): Let $\vec{x}, \vec{y} \in W_1 \cap W_2$. Since W_1 and W_2 are both subspaces, it follows that $\vec{x} + \vec{y}$ lies in both W_1 and W_2. In other words, $\vec{x} + \vec{y} \in W_1 \cap W_2$. Likewise, if $r \in \mathbb{R}$, it follows that $r\vec{x} \in W_1 \cap W_2$. This proves that $W_1 \cap W_2$ is a subspace of V.

(ii): Suppose first that $W_1 \cap W_2 = \{\vec{0}\}$. Let

$$\mathcal{B}_1 = \{\vec{u}_1, \ldots, \vec{u}_a\}, \quad \mathcal{B}_2 = \{\vec{v}_1, \ldots, \vec{v}_b\}$$

be bases on W_1 and W_2 respectively. Clearly, $W_1 + W_2 = \operatorname{span} \mathcal{B}_1 \cup \mathcal{B}_2$. To see that $\mathcal{B}_1 \cup \mathcal{B}_2$ is linearly independent, suppose that

$$\alpha_1\vec{u}_1 + \cdots + \alpha_a\vec{u}_a + \beta_1\vec{v}_1 + \cdots + \beta_b\vec{v}_b = \vec{0}.$$

We can rewrite this as

$$\alpha_1\vec{u}_1 + \cdots + \alpha_a\vec{u}_a = -\beta_1\vec{v}_1 - \cdots - \beta_b\vec{v}_b. \tag{22}$$

Let $\vec{x} := \alpha_1\vec{u}_1 + \cdots + \alpha_a\vec{u}_a$. Note that the left side of (22) is an element of W_1 while the right side is an element of W_2. Hence, $\vec{x} \in W_1 \cap W_2 = \{0\}$. Since $\mathcal{B}_1$ is linearly indpendent, this impllies that $\alpha_1 = \cdots = \alpha_a = 0$. Likewise, since $\mathcal{B}_2$ is linearly independent, this implies that $\beta_1 = \cdots = \beta_b = 0$. This shows that $\mathcal{B}_1 \cup \mathcal{B}_2$ is linearly independent. From this, we conclude that $\mathcal{B}_1 \cup \mathcal{B}_2$ is a basis for $W_1 + W_2$.

Hence,

$$\begin{aligned}\dim(W_1 + W_2) &= a + b \\ &= \dim W_1 + \dim W_2 \\ &= \dim W_1 + \dim W_2 - \dim W_1 \cap W_2,\end{aligned}$$

where in the last equality we use the fact that $\dim W_1 \cap W_2 = \dim\{\vec{0}\} = 0$ (see Example 2.40).

Now suppose that $W_1 \cap W_2 \neq \{0\}$. Let $a := \dim W_1$ and $b := \dim W_2$. Also, let $\{\vec{w}_1, \ldots, \vec{w}_k\}$ be a basis on $W_1 \cap W_2$. Since $W_1 \cap W_2$ is a subspace of both W_1 and W_2, the Basis Extension Lemma (Lemma 2.76) implies that there exists elements $\vec{x}_1, \ldots, \vec{x}_{a-k}$ of W_1 and elements $\vec{y}_1, \ldots, \vec{y}_{b-k}$ such that

$$\{\vec{w}_1, \ldots, \vec{w}_k, \vec{x}_1, \ldots, \vec{x}_{a-k}\}$$

is a basis on W_1 and

$$\{\vec{w}_1, \ldots, \vec{w}_k, \vec{y}_1, \ldots, \vec{y}_{b-k}\}$$

is a basis on W_2. Let

$$\mathcal{B} := \{\vec{w}_1, \ldots, \vec{w}_k, \vec{x}_1, \ldots, \vec{x}_{a-k}, \vec{y}_1, \ldots, \vec{y}_{b-k}\}.$$

Note that $W_1 + W_2 = \text{span } \mathcal{B}$. We now show that $\mathcal{B}$ is also linearly independent. So let us suppose that

$$\alpha_1\vec{w}_1 + \cdots + \alpha_k\vec{w}_k + \beta_1\vec{x}_1 + \cdots + \beta_{a-k}\vec{x}_{a-k} + \gamma_1\vec{y}_1 + \cdots + \gamma_{b-k}\vec{y}_{b-k} = \vec{0} \quad (23)$$

for some α_i's, β_i's, and γ_i's in $\mathbb{R}$. Let

$$\begin{aligned}\vec{w} &:= \alpha_1\vec{w}_1 + \cdots + \alpha_k\vec{w}_k \in W_1 \cap W_2 \\ \vec{x} &:= \beta_1\vec{x}_1 + \cdots + \beta_{a-k}\vec{x}_{a-k} \in W_1 \\ \vec{y} &:= +\gamma_1\vec{y}_1 + \cdots + \gamma_{b-k}\vec{y}_{b-k} \in W_2.\end{aligned}$$

Then (23) can be rewritten as

$$\vec{w} + \vec{y} = -\vec{x}. \quad (24)$$

Note that the left side of (24) belongs to W_1 while the right side belongs to W_2. This implies that $-\vec{x}$ (and hence $\vec{x}$) belongs to $W_1 \cap W_2$. Then there exists $r_1, \ldots, r_k \in \mathbb{R}$ such that

$$r_1\vec{w}_1 + \cdots + r_k\vec{w}_k = \vec{x} \quad (25)$$

Expanding $\vec{x}$ in terms of the basis elements $\vec{x}_1, \ldots, \vec{x}_{a-k}$, (24) can be rewritten as

$$r_1\vec{w}_1 + \cdots + r_k\vec{w}_k - \beta_1\vec{x}_1 - \cdots - \beta_{a-k}\vec{x}_{a-k} = \vec{0}. \quad (26)$$

Since $\vec{w}_1, \ldots, \vec{w}_k, \vec{x}_1, \ldots, \vec{x}_{a-k}$ is a basis on W_1, it follows that all the r_i's and β_i's are zero. Using this fact, (23) can be rewritten as

$$\alpha_1\vec{w}_1 + \cdots + \alpha_k\vec{w}_k + \gamma_1\vec{y}_1 + \cdots + \gamma_{b-k}\vec{y}_{b-k} = \vec{0}.$$

Since $\vec{w}_1, \ldots, \vec{w}_k, \vec{y}_1, \ldots, \vec{y}_{b-k}$ is a basis on W_2, it follows that all the α_i's and γ_i's are also zero. This proves that $\mathcal{B}$ is linearly independent and hence a basis on $W_1 + W_2$. Hence,

$$\begin{aligned}\dim(W_1 + W_2) &= |\mathcal{B}| \\ &= k + (a-k) + (b-k) \\ &= a + b - k \\ &= \dim W_1 + \dim W_2 - \dim(W_1 \cap W_2).\end{aligned}$$

This completes the proof. □

Definition 2.78. *Let V be a vector space and let W_1 and W_2 be subspaces of V. V is said to be a* ***direct sum*** *of W_1 and W_2 if the following conditions are satisfied:*

(i) $V = W_1 + W_2$

(ii) $W_1 \cap W_2 = \{\vec{0}\}$.

When V is a direct sum of W_1 and W_2, one replaces the "+" symbol with the direct sum symbol "⊕" and writes $V = W_1 \oplus W_2$.

Here are some equivalent characterizations of the direct sum:

Proposition 2.79. *Let V be a vector space and let W_1 and W_2 be subspaces of V. The following statements are equivalent:*

(1) $V = W_1 \oplus W_2$

(2) Every $\vec{v} \in V$ can be expressed ***uniquely*** *as $\vec{v} = \vec{w}_1 + \vec{w}_2$ for some $\vec{w}_1 \in W_1$ and $\vec{w}_2 \in W_2$*

(3) $\dim V = \dim W_1 + \dim W_2$ *and* $W_1 \cap W_2 = \{\vec{0}\}$

Proof. (1) ⇒ (2): Suppose that $V = W_1 \oplus W_2$ and let $\vec{v} \in V$. By definition of the direct sum, there exists $\vec{w}_1 \in W_1$ and $\vec{w}_2 \in W_2$ such that $\vec{v} = \vec{w}_1 + \vec{w}_2$. To prove this direction, we must show that $\vec{w}_1$ and $\vec{w}_2$ are the **only** elements in W_1 and W_2 respectively which sum to $\vec{v}$. Suppose that we are given another $\vec{x}_1 \in W_1$ and $\vec{x}_2 \in W_2$ such that $\vec{v} = \vec{x}_1 + \vec{x}_2$. This implies that

$$\vec{w}_1 + \vec{w}_2 = \vec{x}_1 + \vec{x}_2,$$

which in turn implies that

$$\vec{w}_1 - \vec{x}_1 = \vec{x}_2 - \vec{w}_2.$$

Since the left side of the above equation is an element of W_1 while the right side is an element of W_2, we conclude that $\vec{w}_1 - \vec{x}_1$ and $\vec{x}_2 - \vec{w}_2$ belong to $W_1 \cap W_2$. However, $W_1 \cap W_2 = \{\vec{0}\}$. This implies that $\vec{x}_1 = \vec{w}_2$ and $\vec{x}_2 = \vec{w}_2$ which proves the uniqueness claim.

(1) $\Leftarrow$ (2): Suppose that statement (2) holds. Then we immediately have $V = W_1 + W_2$. For V to be a direct sum of W_1 and W_2, it only remains to show that $W_1 \cap W_2 = \{\vec{0}\}$. Let $\vec{w} \in W_1 \cap W_2$. Since $\vec{w}$ is also an element of V, statement 2 says there exists unique $\vec{w}_1 \in W_1$ and unique $\vec{w}_2 \in W_2$ such that $\vec{w} = \vec{w}_1 + \vec{w}_2$. Since $\vec{w}$ belongs to both W_1 and W_2, one can take $\vec{w}_1 = \vec{w}$ and $\vec{w}_2 = \vec{0}$ and obtain $\vec{w} = \vec{w}_1 + \vec{w}_2$. On the other hand, one can take $\vec{w}_1 = \vec{0}$ and $\vec{w}_2 = \vec{w}$ and again obtain $\vec{w} = \vec{w}_1 + \vec{w}_2$. However, statement (2) says there is only one way to express $\vec{w}$ in the form $\vec{w} = \vec{w}_1 + \vec{w}_2$ for some $\vec{w}_1 \in W_1$ and $\vec{w}_2 \in W$. From this, we conclude that $\vec{w}_1 = \vec{0}$ and $\vec{w}_2 = \vec{0}$, which implies that $\vec{w} = \vec{0}$. Since $\vec{w}$ was arbitraily chosen from $W_1 \cap W_2$, it follows that $W_1 \cap W_2 = \{\vec{0}\}$.

(1) $\Rightarrow$ (3): Suppose that $V = W_1 \oplus W_2$. From the definition of the direct sum, we automatically have $W_1 \cap W_2 = \{0\}$. Using Proposition 2.77, we have

$$\begin{aligned} \dim V &= \dim(W_1 + W_2) \\ &= \dim W_1 + \dim W_2 - \dim W_1 \cap W_2 \\ &= \dim W_1 + \dim W_2 \end{aligned}$$

where the last equality follows from the fact that $W_1 \cap W_2$ is the zero vector space, and thus, has dimension zero. This proves (3).

(1) $\Leftarrow$ (3): Suppose that $\dim V = \dim W_1 + \dim W_2$ and $W_1 \cap W_2 = \{\vec{0}\}$. Let $\vec{x}_1, \ldots, \vec{x}_a$ be a basis on W_1 and let $\vec{y}_1, \ldots, \vec{y}_b$ be a basis on W_2. We now show that

$$\mathcal{B} := \{\vec{x}_1, \ldots, \vec{x}_a, \vec{y}_1, \ldots, \vec{y}_b\} \tag{27}$$

is a linearly independent set. So suppose that

$$\alpha_1\vec{x}_1 + \cdots + \alpha_a\vec{x}_a + \beta_1\vec{y}_1 + \cdots + \beta_b\vec{y}_b = \vec{0}.$$

Let $\vec{x} := \alpha_1\vec{x}_1 + \cdots + \alpha_a\vec{x}_a$ and $\vec{y} = \beta_1\vec{y}_1 + \cdots + \beta_b\vec{y}_b$. Then the above equation can be rearranged as

$$\vec{x} = -\vec{y}. \tag{28}$$

Since the left side of (28) belongs to W_1 while the right side belongs to W_2, it follows that $\vec{x}$ and $-\vec{y}$ belong to $W_1 \cap W_2$. Moreover, since $W_1 \cap W_2$ is also a subspace by Proposition 2.77, we also have $\vec{y} \in W_1 \cap W_2$. However, $W_1 \cap W_2 = \{\vec{0}\}$ by hypothesis which implies that $\vec{x} = \vec{y} = \vec{0}$. Since $\vec{x}_1, \ldots, \vec{x}_a$ is a basis on W_1 (and hence linearly independent), it follows that $\alpha_1 = \cdots = \alpha_a = 0$. Similarly, $\beta_1 = \cdots = \beta_b = 0$. This proves that $\mathcal{B}$ is linearly independent. However, the number of elements in $\mathcal{B}$ is equal to $a + b = \dim W_1 + \dim W_2 = \dim V$. The Replacement Theorem (Theorem 2.34) now implies that $\mathcal{B}$ is in fact a basis on V. Hence, every element $\vec{v} \in V$ is of the form

$$\begin{aligned} \vec{v} &= r_1\vec{x}_1 + \cdots + r_a\vec{x}_a + s_1\vec{y}_1 + \cdots + s_b\vec{y}_b \\ &= \vec{w}_1 + \vec{w}_2 \end{aligned}$$

for some $r_1, \ldots, r_a, s_1, \ldots, s_b \in \mathbb{R}$, where $\vec{w}_1 =_1 \vec{x}_1 + \cdots + r_a\vec{x}_a \in W_1$ and $\vec{w}_2 = s_1\vec{y}_1 + \cdots + s_b\vec{y}_b \in W_2$. This shows that $V = W_1 + W_2$. Since we already have $W_1 \cap W_2 = \{\vec{0}\}$, we see that $V = W_1 \oplus W_2$ as required. □

We conclude this chapter with the following result which will explain the results of Example 2.73:

Theorem 2.80. *Let W be a subspace of $\mathbb{R}^n$ and let $W^\perp$ be its orthogonal complement. Then*

(i) $\mathbb{R}^n = W \oplus W^\perp$

(ii) $\dim W^\perp = n - \dim W$

Proof. (i): Let $\vec{x} \in W \cap W^\perp$ be an arbitrary element. Since $\vec{x}$ belongs to $W^\perp$, we must have (by definition) $\vec{x}$ is orthogonal to every vector in W. In other words, $\vec{x} \cdot \vec{w} = 0$ for all $\vec{w} \in W$. However, $\vec{x}$ also belongs to W, which implies that $\vec{x} \cdot \vec{x} = 0$. This in turn implies that $\vec{x} = \vec{0}$. Since $\vec{x}$ was an arbitrary element of $W \cap W^\perp$, we conclude that $W \cap W^\perp = \{\vec{0}\}$. To prove (i), it only remains to show that $\mathbb{R}^n = W + W^\perp$, that is, every element $\vec{v}$ of $\mathbb{R}^n$ can be expressed as $\vec{v} = \vec{x} + \vec{y}$ for some $\vec{x} \in W$ and $\vec{y} \in W^\perp$. Using the Gram-Schmidt process, we can construct an orthogonal basis on W. Let

$$\{\vec{b}_1, \ldots, \vec{b}_k\}$$

denote an orthonormal basis on W. For $\vec{v} \in \mathbb{R}^n$, define $\vec{x} \in W$ by

$$\vec{x} = \text{proj}_{\vec{b}_1} \vec{v} + \text{proj}_{\vec{b}_2} \vec{v} + \cdots + \text{proj}_{\vec{b}_k} \vec{v}.$$

Note that since $\text{proj}_{\vec{b}_i} \vec{v}$ is a multiple of $\vec{b}_i$ and $\vec{b}_i \in W$ for $i = 1, \ldots, k$, it follows that $\vec{x}$ is indeed an element of W. Now let $\vec{y} = \vec{v} - \vec{x}$. Clearly, we have $\vec{v} = \vec{x} + \vec{y}$ where $\vec{x} \in W$. We have to check that $\vec{y} \in W^\perp$. Since the $\vec{b}_i$'s form a basis on W, every element of W is a linear combination of the $\vec{b}_i$'s. Hence, to show that $\vec{y} \in W^\perp$ is equivalent to showing that $\vec{y}$ is orthogonal to $\vec{b}_i$ for $i = 1, \ldots, k$. The following calculation verifies this:

$$\begin{aligned}
\vec{y} \cdot \vec{b}_i &= (\vec{v} - \vec{x}) \cdot \vec{b}_i \\
&= \vec{v} \cdot \vec{b}_i - \vec{x} \cdot \vec{b}_i \\
&= \vec{v} \cdot \vec{b}_i - \sum_{j=1}^{k} (\text{proj}_{\vec{b}_j} \vec{v}) \cdot \vec{b}_i \\
&= \vec{v} \cdot \vec{b}_i - (\text{proj}_{\vec{b}_i} \vec{v}) \cdot \vec{b}_i \\
&= \vec{v} \cdot \vec{b}_i - \left(\frac{\vec{v} \cdot \vec{b}_i}{\left\| \vec{b}_i \right\|^2} \right) \vec{b}_i \cdot \vec{b}_i \\
&= \vec{v} \cdot \vec{b}_i - \vec{v} \cdot \vec{b}_i \\
&= 0.
\end{aligned}$$

This shows that $\vec{y} \in W^\perp$, which in turn proves that $\mathbb{R}^n = W + W^\perp$. Since we have already shown that $W \cap W^\perp = \{\vec{0}\}$, we have proven that $\mathbb{R}^n = W \bigoplus W^\perp$.

(ii): Using part (3) of Proposition 2.79 and the fact that $\mathbb{R}^n = W \bigoplus W^\perp$, we have

$$\dim \mathbb{R}^n = \dim W + \dim W^\perp.$$

Solving for $\dim W^\perp$ and using the fact that $\dim \mathbb{R}^n = n$ gives $\dim W^\perp = n - \dim W$ as required. $\square$

Part (i) of Theorem 2.80 and part (2) of Proposition 2.79 immediately imply the following:

Corollary 2.81. *Let W be a subspace of $\mathbb{R}^n$. For every $\vec{v} \in \mathbb{R}^n$, there exists a unique element $\vec{x} \in W$ and a unique element $\vec{y} \in W^\perp$ such that $\vec{v} = \vec{x} + \vec{y}$. This element $\vec{x}$ is called the* ***orthogonal projection of $\vec{v}$ onto the subspace*** *W and is denoted by $\text{proj}_W \vec{v}$.*

The proof of Theorem 2.80 does more than simply prove the existence and uniqueness of $\text{proj}_W \vec{v}$. **It also tells us exactly how to compute it!**

Calculating $\text{proj}_W \vec{v}$

Let W be a subspace of $\mathbb{R}^n$ and let $\vec{v} \in V$. Also, let $\vec{b}_1, \ldots, \vec{b}_k$ be **any** orthogonal basis on W. Then

$$\text{proj}_W \vec{v} = \text{proj}_{\vec{b}_1} \vec{v} + \text{proj}_{\vec{b}_2} \vec{v} + \cdots + \text{proj}_{\vec{b}_k} \vec{v}.$$

Example 2.82. *Let V be the subspace of $\mathbb{R}^4$ defined by*

$$V = \{(a, a-2b, b+c, c) \mid a, b, c \in \mathbb{R}\}.$$

Find the orthogonal projection of $\vec{a} = (1,2,2,1)$ onto V. To compute $\text{proj}_V \vec{a}$, we first need an orthogonal basis of V. Fortunately, we already found one in Example 2.69:

$$\vec{b}_1 = (1,1,0,0)$$
$$\vec{b}_2 = (1,-1,1,0)$$
$$\vec{b}_3 = \frac{1}{3}(-1,1,2,3)$$

Note that $3\vec{b}_3 = (-1,1,2,3)$ is also orthogonal to $\vec{b}_1$ and $\vec{b}_2$. Since any orthogonal basis will do, let's use the basis $\vec{b}_1$, $\vec{b}_2$, and $3\vec{b}_3$ instead so we can avoid that pesky factor of $1/3$. From this point forth, we set $\vec{b}_3 = (-1,1,2,3)$. The projection of $\vec{a}$ onto V is then given by

$$
\begin{aligned}
\text{proj}_V\vec{a} &= \text{proj}_{\vec{b}_1}\vec{a} + \text{proj}_{\vec{b}_2}\vec{a} + \text{proj}_{\vec{b}_3}\vec{a} \\
&= \frac{\vec{b_1}\cdot\vec{a}}{\left\|\vec{b}_1\right\|^2}\vec{b}_1 + \frac{\vec{b_2}\cdot\vec{a}}{\left\|\vec{b}_2\right\|^2}\vec{b}_2 + \frac{\vec{b_3}\cdot\vec{a}}{\left\|\vec{b}_3\right\|^2}\vec{b}_3 \\
&= (\frac{3}{2},\frac{3}{2},0,0) + (\frac{1}{3},-\frac{1}{3},\frac{1}{3},0) + (-\frac{8}{15},\frac{8}{15},\frac{16}{15},\frac{24}{15}) \\
&= (\frac{13}{10},\frac{17}{10},\frac{14}{10},\frac{24}{15}) \\
&= \frac{1}{10}(13,17,14,16).
\end{aligned}
$$

At the same time, we compute the element of $\vec{y} \in V^{\perp}$ such that

$$\vec{a} = \text{proj}_V\vec{a} + \vec{y}.$$

This, of course, is simply

$$\vec{y} = \vec{a} - \text{proj}_V\vec{a} = \frac{1}{10}(-3,3,6,-6)$$

If our calculation is correct, $\vec{y}$ should be orthogonal to V. This is equivalent to showing that $\vec{y}$ is orthogonal to any basis of V. Let's verify this by computing the dot product of $\vec{y}$ with the basis vectors $\vec{b}_1$, $\vec{b}_2$, and $\vec{b}_3$:

$$
\begin{aligned}
\vec{y}\cdot\vec{b}_1 &= 0 \\
\vec{y}\cdot\vec{b}_2 &= 0 \\
\vec{y}\cdot\vec{b}_3 &= 0.
\end{aligned}
$$

This shows that $\vec{y} \in V^{\perp}$ as required.

2.8. Orthogonal Projection & Distance to a Subspace

In Section 2.5, we defined the distance between two points u and v in $\mathbb{R}^n$ by

$$d(u,v) = \|\vec{u} - \vec{v}\|$$

(Recall our notation: when we regard an element of $\mathbb{R}^n$ as a point and not a vector, we drop the arrow symbol.) As we saw in Section 2.5, the above formula generalizes the distance between two points in $\mathbb{R}^1$, $\mathbb{R}^2$, and $\mathbb{R}^3$. In this section, we generalize things even further by considering the distance between a point v of $\mathbb{R}^n$ and a subspace W of $\mathbb{R}^n$. Naturally, this distance should be defined to be the smallest distance from v to a point in W. In other words, the distance is

$$d(v,W) := \inf\{\|\vec{v} - \vec{w}\| \mid \vec{w} \in W\}. \tag{29}$$

The "inf" in (29) is short for *infimum*, which is defined as the greatest lower bound of a set of numbers. As an example, consider the set

$$S = \{a_n \mid a_n := 2 + \frac{1}{n},\ n = 1, 2, \dots\}.$$

The infimum of S is the largest number κ for which $a_n \geq \kappa$ for $n = 1, 2, \dots$. A moment's thought shows that the infimum of S is $\inf S = 2$.

Naturally, we are interested in computing this distance. In addition, we would like to know which point in W is closest to v. The answers to these questions is given by the following result which relies crucially on orthogonal projection:

Theorem 2.83. *Let $\vec{v} \in \mathbb{R}^n$ and let W be a subspace of $\mathbb{R}^n$. Then*

$$d(\vec{v}, W) = \sqrt{\|\vec{v}\|^2 - \|proj_W \vec{v}\|^2}.$$

In addition, $d(\vec{v}, \vec{w}) = d(\vec{v}, W)$ if and only if $\vec{w} = proj_W \vec{v}$.

Proof. By Corollary 2.81, we can decompose the **vector** $\vec{v}$ (uniquely) as

$$\vec{v} = \text{proj}_W \vec{v} + \vec{y} \tag{30}$$

where $\vec{y} \in W^{\perp}$. Let $\vec{w}$ be an arbitrary element of W. Using (30), we expand the square of $d(v, w)$ and obtain an upper bound for this quantity:

$$\begin{aligned} d(v, w)^2 &= \|\vec{v} - \vec{w}\|^2 \\ &= (\vec{v} - \vec{w}) \cdot (\vec{v} - \vec{w}) \\ &= \vec{v} \cdot \vec{v} - 2\vec{v} \cdot \vec{w} + \vec{w} \cdot \vec{w} \\ &= \|\vec{v}\|^2 - 2(\text{proj}_W \vec{v} + \vec{y}) \cdot \vec{w} + \|\vec{w}\|^2 \\ &= \|\vec{v}\|^2 - 2(\text{proj}_W \vec{v}) \cdot \vec{w} + \|\vec{w}\|^2 \\ &\geq \|\vec{v}\|^2 - 2\,\|\text{proj}_W \vec{v}\|\,\|\vec{w}\| + \|\vec{w}\|^2, \end{aligned} \tag{31}$$

where the last inequality follows from the Cauchy Schwartz Theorem (Theorem 2.49). Since $\vec{v}$ is a fixed vector, the right side of (30) only depends on the value of $\|\vec{w}\|$. *What value of $\|\vec{w}\|$ will minimize the right side of (30)?* To answer this question, let

$$f(t) = \|\vec{v}\|^2 - 2\,\|\text{proj}_W \vec{v}\|\, t + t^2.$$

The graph of $f(t)$ is a quadratic which attains an absolute minimum value at

$$t = \|\text{proj}_W \vec{v}\|. \tag{32}$$

Hence, the absolute minimum value of f is

$$f(\|\text{proj}_W \vec{v}\|) = \|\vec{v}\|^2 - \|\text{proj}_W \vec{v}\|^2. \tag{33}$$

Using (31) and (33), it follows that for any $w \in W$, we have

$$d(v,w)^2 \geq \|\vec{v}\|^2 - \|\text{proj}_W \vec{v}\|^2 \tag{34}$$

From the calculation for (31) and (32), we see that $w \in W$ satisfies

$$d(v,w)^2 = \|\vec{v}\|^2 - \|\text{proj}_W \vec{v}\|^2$$

if and only if $(\text{proj}_W \vec{v}) \cdot \vec{w} = \|\text{proj}_W \vec{v}\| \, \|\vec{w}\|$ and $\|\vec{w}\| = \|\text{proj}_W \vec{v}\|$. The Cauchy Schwartz Theorem implies that $\vec{w} = \text{proj}_W \vec{v}$ is the only element of W which satisfies both of these conditions. Hence,

$$d(v, \text{proj}_W \vec{v}) = \sqrt{\|\vec{v}\|^2 - \|\text{proj}_W \vec{v}\|^2}.$$

From the inequality (34) and the above discussion, we see that if $\vec{w} \in W$ and $\vec{w} \neq \text{proj}_W \vec{v}$, we have $d(v,w) > d(v, \text{proj}_W \vec{v})$. From this, we conclude that $\text{proj}_W \vec{v}$ is the element of W closest to v and

$$d(v, W) = \sqrt{\|\vec{v}\|^2 - \|\text{proj}_W \vec{v}\|^2}.$$

This completes the proof. □

Example 2.84. *Let V be the subspace of $\mathbb{R}^4$ defined by*

$$V = \{(a, a-2b, b+c, c) \mid a, b, c \in \mathbb{R}\}.$$

Let $\vec{a} = (1, 2, 2, 1)$. From Example 2.82,

$$proj_V \vec{a} = \frac{1}{10}(13, 17, 14, 16).$$

By Theorem 2.83, $proj_V \vec{a}$ is the element of V closest to $\vec{a}$. The distance from $\vec{a}$ to V is

$$d(\vec{a}, V) = \sqrt{\|\vec{a}\|^2 - \left\|\vec{proj_V \vec{a}}\right\|^2} \approx 0.949.$$

Chapter 2 Exercises

1. Determine if $\vec{w} = (-4, 6, 1)$ is a linear combination of $\vec{u} = (1, 0, -1)$ and $\vec{v} = (1, -11, 3)$. If so, then express $\vec{w}$ as a linear combination of $\vec{u}$ and $\vec{v}$.

2. Determine if the vectors $(3, 2, 0)$, $(-3, 0, 1)$, and $(1, 1, -9)$ span all of $\mathbb{R}^3$. Do these vectors form a basis?

3. Let $\vec{u} = (1, 1, -1)$ and $\vec{v} = (2, 1, 3)$. Determine if $\vec{w} = (7, 6, 3)$ is a linear combination of $\vec{u}$ and $\vec{v}$. If so, express $\vec{w}$ as a linear combination of $\vec{u}$ and $\vec{v}$.

4. Let

$$\vec{x}_1 = (2, -1, 3, 1), \qquad \vec{x}_2 = (1, 0, -1, 1), \qquad \vec{x}_3 = (0, 1, 4, 2).$$

   (i) Determine if $\vec{x}_1$, $\vec{x}_2$, and $\vec{x}_3$ are linearly independent. Justify your answer.
   (ii) Determine if $\vec{v} = (2, -1, 3, 1)$ is a linear combination of $\vec{x}_1$, $\vec{x}_2$, and $\vec{x}_3$. If so, express $\vec{v}$ as a linear combination of $\vec{x}_1$, $\vec{x}_2$, and $\vec{x}_3$. If not, justify your answer.
   (iii) Determine if $\vec{u} = (1, 0, 0, 1)$ is a linear combination of $\vec{x}_1$, $\vec{x}_2$, and $\vec{x}_3$. If so, express $\vec{u}$ as a linear combination of $\vec{x}_1$, $\vec{x}_2$, and $\vec{x}_3$. If not, justify your answer.

5. Consider the following subset of $\mathbb{R}^4$:

$$W := \{(a - b, 4a, 2b + 3c, b - c) \mid a, b, c \in \mathbb{R}\}.$$

   Determine if W is a subspace of $\mathbb{R}^4$. If W is a subspace, find a basis for W and state its dimension. If W is not a subspace, explain why.

6. Consider the following subset of $\mathbb{R}^3$:

$$U := \{(a + b, 4b, a + b - 1) \mid a, b \in \mathbb{R}\}.$$

   Determine if U is a subspace of $\mathbb{R}^3$. If U is a subspace, find a basis for U and state its dimension. If U is not a subspace, explain why.

7. Solve the following homogeneous linear system in 3-variables:

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

   Let $W \subset \mathbb{R}^3$ denote the solution space for the above homogenous system. What is the dimension of W as a subspace of $\mathbb{R}^3$? Find a basis for W.

8. Solve the following homogeneous linear system in 5-variables:

$$
\begin{aligned}
x_1 + 2x_2 - 2x_3 - 6x_4 + 3x_5 &= 0 \\
2x_1 + 5x_2 - x_3 - 4x_4 + 2x_5 &= 0 \\
-x_1 - x_2 + 6x_3 + 17x_4 - 4x_5 &= 0.
\end{aligned}
$$

   Let $U \subset \mathbb{R}^5$ denote the solution space for the above homogenous system. What is the dimension of U as a subspace of $\mathbb{R}^5$? Find a basis for U.

9. Let $\vec{u} = (1, -1, 0)$ and $\vec{v} = (1, 2, 1)$.
   (i) Verify that $\vec{u}$ and $\vec{v}$ are linearly independent.
   (ii) Extend the set $\{\vec{u}, \vec{v}\}$ to a basis on $\mathbb{R}^3$ (i.e. find a vector $\vec{w} \in \mathbb{R}^3$ such that $\{\vec{u}, \vec{v}, \vec{w}\}$ is a basis of $\mathbb{R}^3$).

10. Let $\vec{u} = (1, 0, -1, 1) \in \mathbb{R}^4$. Extend $\vec{u}$ to a basis of $\mathbb{R}^4$, that is, find vectors $\vec{x}_1, \vec{x}_2, \vec{x}_3 \in \mathbb{R}^4$ such that

$$\{\vec{u}, \vec{x}_1, \vec{x}_2, \vec{x}_3\}$$

    is a basis of $\mathbb{R}^4$.

11. Determine if the following set of vectors form a basis of $\mathbb{R}^3$.

$$\{(1, 1, -1),\ (0, 2, 1),\ (1, -3, -3)\}.$$

12. Normalize the following vectors:
    (a) $\vec{v} = (1, -1)$
    (b) $\vec{u} = (1, 2, 2)$
    (c) $\vec{w} = (1, -1, 1, -1)$

13. Find the distance between the following vectors:
    (a) $\vec{u}_1 = (1, 0, -1)$ and $\vec{u}_2 = (1, 2, 1)$
    (b) $\vec{v}_1 = (1, 1, -1, -1)$ and $\vec{v}_2 = (0, 1, 0, -1)$

14. Give an equation for a sphere in $\mathbb{R}^3$ centered at the origin and with radius r.

15. To the nearest hundredth in radians, calculate the angle between the following pairs of vectors:
    (a) $(1, 1)$ and $(2, 5)$
    (b) $(1, 2, -1)$ and $(1, 1, 1)$
    (c) $(1, 0, -1, 2)$ and $(-1, 1, 2, 2)$

16. Let $a_i, b_i \in \mathbb{R}$ be positive numbers for $i = 1, 2, \ldots, n$. Is the following equality true?

$$\left(\sum_{i=1}^{n} a_i b_i\right)^2 \leq \left(\sum_{i=1}^{n} a_i^2\right)\left(\sum_{i=1}^{n} b_i^2\right)$$

    If so, explain why. If not, give a counterexample.

17. Are the two vectors orthogonal?

$$\begin{pmatrix} 2 \\ 3 \\ -5 \end{pmatrix}, \qquad \begin{pmatrix} 2 \\ -1 \\ 3 \end{pmatrix}$$

18. Show that $\vec{u} = (2, -4)$ and $\vec{v} = (8, 4)$ is an orthogonal basis of $\mathbb{R}^2$. Express $(-3, 1)$ as a linear combination of $\vec{u}$ and $\vec{v}$.

19. Determine t such that the two vectors

$$\begin{pmatrix} -3 \\ t \\ 4 \\ -1 \end{pmatrix}, \qquad \begin{pmatrix} 1 \\ -3 \\ t \\ 5 \end{pmatrix}$$

are orthogonal.

20. Consider the vector $\vec{v} = (1, 1, 2, -1)$.
    (a) Let W be the subspace of $\mathbb{R}^4$ consisting of all vectors orthogonal to $\vec{v}$.
    (b) Give a basis for W.
    (c) What is the dimension of W?

21. Compute the orthogonal projection $\text{proj}_{\vec{u}}\vec{v}$ for each case:
    (a) $\vec{u} = (1, -1)$, $\vec{v} = (2, 3)$
    (b) $\vec{u} = (1, 2, 1)$, $\vec{v} = (0, 1, 1)$
    (c) $\vec{u} = (2, 1, 1, 1)$, $\vec{v} = (1, -1, -1, 1)$

22. Apply the Gram-Schmidt Process to the following basis of $\mathbb{R}^3$:

$$\{(1, 1, 1),\ (-1, 1, -1),\ (0, 1, 2)\}$$

23. Consider the subspace V of $\mathbb{R}^4$ given by

$$V = \{(a + 2c, a + b - 3c, c - a, a + 4c) \mid a, b, c \in \mathbb{R}\}.$$

    (a) Construct an orthonormal basis of V.
    (b) Express the orthogonal complement $V^{\perp}$ as a set. Also, give a basis for $V^{\perp}$.

24. Use the Gram-Schmidt process to find an orthogonal basis of the subspace of $\mathbb{R}^3$ spanned by the vectors: $(1, 3, -2)$ and $(1, 5, 1)$.

25. Use the Gram-Schmidt process to find an orthogonal basis of the subspace of $\mathbb{R}^4$ spanned by the vectors:

$$\{(1, -2, 1, 1),\ (0, -1, -3, 1)\}.$$

26. Show that $\vec{u} = (-2, 5, 2)$ and $\vec{v} = (2, 2 - 3)$ are orthogonal. Find a third vector $\vec{w}$ that together with $\vec{u}$ and $\vec{v}$ make an orthogonal basis of $\mathbb{R}^3$. Express $(-1, -3, 1)$ as a linear combination of $\vec{u}$, $\vec{v}$ and $\vec{w}$.

27. Consider the subspace W of $\mathbb{R}^4$ given by

$$V = \{(a, a + 2b, b, a) \mid a, b \in \mathbb{R}\}.$$

    (a) Construct an orthonormal basis of W.

(b) Express the orthogonal complement $W^\perp$ as a set. Also, give a basis for $W^\perp$.

28. Suppose that W is the subspace spanned by
$$\{(5,1,4),\ (1,3,-2)\}.$$
Find a basis of $W^\perp$.

29. Let W_1 and W_2 be subspaces of $\mathbb{R}^4$ given by
$$W_1 := \{(a, 2b, a+c, c) \mid a, b, c \in \mathbb{R}\}$$
and
$$W_2 := \{(a, 2a, b, a) \mid a, b \in \mathbb{R}\}$$
(a) Does $W_1 + W_2 = \mathbb{R}^4$. Justify your answer.
(b) Does $W_1 \oplus W_2 = \mathbb{R}^4$. Justify your answer.

30. Let U_1 and U_2 be subspaces of $\mathbb{R}^3$ given by
$$U_1 := \{(a, b, a+2b) \mid a, b \in \mathbb{R}\}$$
and
$$U_2 := \{(a, a, 2a) \mid a \in \mathbb{R}\}.$$
(a) Does $U_1 + U_2 = \mathbb{R}^3$. Justify your answer.
(b) Does $U_1 \oplus U_2 = \mathbb{R}^3$. Justify your answer.

31. Find the orthogonal projection of $(-2,5,1)$ into the subspace of $\mathbb{R}^3$ defined by
$$W := \text{span}\ \{(-1,1,2),\ (-1,2,4)\}.$$

32. Let W be the subspace of $\mathbb{R}^3$ given by
$$W := \{(a, a+b, b) \mid a, b \in \mathbb{R}\}$$
(a) Find the projection of $\vec{v} = (1,0,2)$ onto W.
(b) Calculate the distance from $\vec{v}$ to W.

33. Let W be the subspace of $\mathbb{R}^4$ given by
$$W := \{(a, a, a+b, b) \mid a, b \in \mathbb{R}\}.$$
(a) Find the projection of $\vec{v} = (1,2,0,1)$ onto W.
(b) Calculate the distance from $\vec{v}$ to W.

34. Find the distance of $(-1,2,4)$ to the subspace of $\mathbb{R}^3$ spanned by the vectors $(-2,-4,1)$ and $(-3,2,0)$.

35. Find the distance of $(-2,1,0)$ to the plane $3x - y + z = 0$.

Chapter 3

Matrices

3.1. Basic Definitions

As we saw in Chapter 1, a matrix is simply an array of numbers arranged in rows and columns. Recall that a matrix

$$A = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix}$$

with m rows and n columns is said to be of **size** $m \times n$. The matrix A is then called an $m \times n$ matrix. The individual numbers making up the matrix are called the **entries** or **elements** of A.

Example 3.1. *The matrix shown below is an example of a* 2×3 *matrix:*

$$\begin{pmatrix} 11 & 2 & 5 \\ 1 & 15 & -10 \end{pmatrix}.$$

The individual numbers making up the matrix are called the **entries** or **elements** of the matrix. For an $m \times n$ matrix A, the element in the ith row and jth column is called the (i, j)-th element or (i, j)-the entry and is typically denoted in one of the following ways:

$$a_{ij},\ a_{i,j},\ A_{ij},\ A_{i,j}.$$

In this book, we will typically denote the (i, j)-th element of a matrix A as a_{ij} or A_{ij}.

Example 3.2. *The matrix A shown below has size 3×4:*

$$A = \begin{pmatrix} 9 & 7 & 4 & 0 \\ -4 & 27 & 12 & 8 \\ 2 & 2 & -4 & 1 \end{pmatrix},$$

The number in red is its $(1,3)$-entry, which we can write as

$$a_{13} = 4.$$

To further simplify notation, an $m \times n$ matrix A is sometimes denoted as (a_{ij}) with the understanding that $1 \leq i \leq m$ and $1 \leq j \leq n$.

Naturally, a matrix whose entries are elements of $\mathbb{R}$ is called a **real matrix** while a matrix whose entries are elements of $\mathbb{C}$ is called a **complex matrix**.

Example 3.3. *For instance, the matrix in Example 3.1 is a real matrix while the following is a complex one of size 3×2:*

$$\begin{pmatrix} 7+i & 2i \\ -9-5i & 5 \\ 6+i & -10i \end{pmatrix}.$$

Remark 3.4. *So far, every matrix in this book has been enclosed with parentheses. For the sake of completeness, we also point out that another common notation is to use square brackets in place of parentheses.*

For example, the 2×3 matrix from Example 3.1 would be written as

$$\begin{bmatrix} 11 & 2 & 5 \\ 1 & 15 & -10 \end{bmatrix}.$$

In this book, we primarily use parentheses to enclose matrices.

From Chapter 2, we recall the following definition:

Definition 3.5. *A matrix with exactly one row is called a* ***row vector*** *while a matrix with exactly one column is called a* ***column vector****.*

Example 3.6. *A (real) row vector of size* 1×3*:*

$$\begin{pmatrix} 2 & 9 & 6 \end{pmatrix} \in \mathbb{R}^3$$

A (complex) column vector of size 4×1*:*

$$\begin{pmatrix} 3+2i \\ -3i \\ 2-7i \\ 10 \end{pmatrix} \in \mathbb{C}^4$$

Whether one depicts the elements of $\mathbb{R}^n$ *(or* $\mathbb{C}^n$*) as row vectors or column vectors is a matter of taste. However, once we introduce the idea of linear transformations, it becomes more natural to express vectors as column vectors.*

As we saw in the previous two chapters, we denote row vectors and column vectors typically as lower case letters with a little arrow overheard (e.g., $\vec{u}$*,* $\vec{v}$*). We typically denote matrices which are neither row or column vectors with capital letters.*

Definition 3.7. *A matrix with the same number of rows and columns is called a **square matrix**. A square matrix of size* $n \times n$ *is said to have **order*** n*.*

Example 3.8. *A square matrix of order* 4*:*

$$\begin{pmatrix} 2 & 1 & -12 & \pi \\ 10 & 2 & \sqrt{2} & 8 \\ 6 & -1 & 4 & -15 \\ 2 & 2 & e & -3 \end{pmatrix}$$

3.2. Matrix Addition and Scalar Multiplication

The goal of the next few sections is to generalize the four basic operations of *addition*, *subtraction*, *multiplication*, and *division* to matrices. We begin this section with the definition of matrix addition:

Definition 3.9. *Let A and B be two matrices $m \times n$ matrices. The sum of A and B is the $m \times n$ matrix $A + B$ whose (i, j)-element is given via*

$$(A + B)_{ij} := A_{ij} + B_{ij}.$$

Example 3.10. *Let*

$$A = \begin{pmatrix} -2 & 1 & 0 \\ 4 & -3 & 2 \end{pmatrix}, \qquad B = \begin{pmatrix} 5 & 3 & 1 \\ 2 & 6 & -1 \end{pmatrix}$$

Then

$$A + B = \begin{pmatrix} -2+5 & 1+3 & 0+1 \\ 4+2 & -3+6 & 2-1 \end{pmatrix} = \begin{pmatrix} 3 & 4 & 1 \\ 6 & 3 & 1 \end{pmatrix}.$$

The definition of matrix addition is quite natural. We just add the matrices component wise. However, we stress that matrix addition is only defined for matrices of the same size. We now introduce the natural idea of the **zero matrix**:

Definition 3.11. *The $m \times n$ **zero matrix** is defined to be the $m \times n$ matrix whose entires are all zero. We denote this matrix as $\mathbf{0}_{m\times n}$.*

To simplify notation, we will drop the indices m, n from $\mathbf{0}_{m\times n}$ and denote the zero matrix as $\mathbf{0}$. The size of the matrix will be clear from the context in which it is used. For example, if A is an $m \times n$ matrix, then the statement $A + \mathbf{0}$ only makes sense if $\mathbf{0}$ denotes the $m \times n$ zero matrix. Observe that for a matrix A, we have the following identity: $A + \mathbf{0} = A$.

The next operation we introduce is the notion of scalar multiplication for matrices. The definition is quite obvious, but let's state it formally anyway:

Definition 3.12. *Let A be an $m \times n$ matrix and c a scalar (if A is real, then $c \in \mathbb{R}$; if A is complex, then $c \in \mathbb{C}$). The **scalar multiplication** of c on A is the $m \times n$ matrix cA whose (i, j)-entry is given by*

$$(cA)_{ij} := cA_{ij}.$$

Example 3.13. *Consider the square matrix of order 2:*

$$A = \begin{pmatrix} 4 & -1 \\ 2 & 3 \end{pmatrix}. \tag{35}$$

Then

$$2A = \begin{pmatrix} 8 & -2 \\ 4 & 6 \end{pmatrix}. \tag{36}$$

In light of the zero matrix, we make the following definition:

Definition 3.14. *The **additive inverse** of a matrix A is the matrix*

$$-A := (-1)A.$$

The name additive inverse comes from the simple fact that $A + (-A) = \mathbf{0}$. Armed with the additive inverse, we define the difference between two matrices A and B of the **same size** to be

$$A - B := A + (-B).$$

Of course, this is exactly how we define the difference of two real (or complex) numbers.

Example 3.15.

$$4\begin{pmatrix} 5 & -2 \\ -1 & -2 \\ 1 & 0 \end{pmatrix} - 3\begin{pmatrix} 2 & -2 \\ 5 & 1 \\ 4 & -1 \end{pmatrix} = \begin{pmatrix} 14 & -2 \\ -19 & -11 \\ -8 & 3 \end{pmatrix}$$

We conclude this brief section with a summary of the basic properties of matrix addition and scalar multiplication. All of these properties follow mmediately from the associativity, commutativity, and distributive properties of real and complex numbers.

Basic Properties of Matrix Addition & **Scalar Multiplication**

Let A, B, and C be $m \times n$ matrices and let c be a scalar.

- $(A + B) + C = A + (B + C)$ (Associativity)
- $A + B = B + A$ (Commutativity)
- $A + \mathbf{0} = A$ (Additive Identity)
- $A + (-A) = 0$ (Additive inverse)
- $c(A + B) = cA + cB$ (Distributivity of the scalar)

3.3. The Transpose

By definition, a matrix is a rectangular array of numbers. This fact leads to the idea of the transpose:

Definition 3.16. *The **transpose** of an $m \times n$ matrix A is the $n \times m$ matrix A^T formed by interchanging the rows and columns of A. In other words, A^T is the $m \times n$ matrix defined via*

$$(A^T)_{ij} = A_{ji}.$$

Example 3.17.

$$\begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{pmatrix}^T = \begin{pmatrix} 1 & 4 \\ 2 & 5 \\ 3 & 6 \end{pmatrix}$$

The following result summarizes the basic properties of the transpose as it relates to matrix addition and scalar multiplication. This result is very straightforward, but lets work it out anyway since it provides practice with the definitions of matrix addition, scalar multiplication, and the transpose.

Proposition 3.18. *Let A and B be $m \times n$ matrices and let c be a scalar. Then*

(i) $\big(A + B\big)^T = A^T + B^T$
(ii) $(cA)^T = cA^T$
(iii) $\big(A^T\big)^T = A$

Proof. For (i), we have

$$\begin{aligned} \big[(A+B)^T\big]_{ij} &= (A+B)_{ji} \\ &= A_{ji} + B_{ji} \\ &= (A^T)_{ij} + (B^T)_{ij}. \end{aligned}$$

This in turn implies $(A + B)^T = A^T + B^T$. Likewise for (ii), we have

$$\begin{aligned} \big[(cA)^T\big]_{ij} &= (cA)_{ji} \\ &= cA_{ji} \\ &= c(A^T)_{ij} \\ &= (cA^T)_{ij}. \end{aligned}$$

This gives $(cA)^T = cA^T$. Lastly, for (iii), we have

$$\begin{aligned} \big[(A^T)^T\big]_{ij} &= (A^T)_{ji} \\ &= A_{ij}. \end{aligned}$$

Hence, $(A^T)^T = A$. □

The transpose applies to both real and complex matrices alike. However, in the case of complex matrices, there is a variation of the transpose that has greater use. This variation is called the **conjugate transpose**. First, let us recall that the conjugate of a complex number $z = a + ib$ is defined by

$$\bar{z} := a - ib.$$

The **conjugate transpose** is then defined as follows:

Definition 3.19. *Let A be an $m \times n$ matrix. The conjugate transpose is the $n \times m$ matrix A^* whose (i,j)-element is given by*

$$(A^*)_{ij} := \overline{A}_{ji}.$$

In other words, to obtain the conjugate transpose of a complex matrix A, we first conjugate every element of A, and then take the transpose of the resulting matrix.

Example 3.20. *Consider the 2×3 matrix*

$$A = \begin{pmatrix} 2+3i & 1-i & 4+2i \\ 2i & 3 & 3+4i \end{pmatrix}.$$

Then

$$A^* = \begin{pmatrix} 2-3i & -2i \\ 1+i & 3 \\ 4-2i & 3-4i \end{pmatrix}.$$

Example 3.21. *Of course, if A is a real matrix, then the conjugate transpose and the ordinary transpose coincide:*

$$A^* = A^T$$

In fact, a matrix A is real if and only if the above condition is satisfied.

We will give some motivation for the transpose and the conjugate transpose when we get to matrix multiplication in the next section. For now, here is the complex version of Proposition 3.18:

Proposition 3.22. *Let A and B be $m \times n$ matrices and let c be a scalar. Then*

(i) $(A + B)^* = A^* + B^*$
(ii) $(cA)^* = \overline{c}A^*$
(iii) $(A^*)^* = A$

Proof. The proof is very similar to the proof of Proposition 3.18. In proving Proposition 3.22, one has to remember the following conjugation identities:

$$\overline{z_1 + z_2} = \overline{z}_1 + \overline{z}_2, \qquad \overline{z_1 z_2} = \overline{z}_1 \overline{z}_2, \qquad \forall\, z_1, z_2 \in \mathbb{C}.$$

□

By definition, the transpose takes an $m \times n$ matrix and transforms it into an $n \times m$ matrix. Hence, in general, the transpose alters the size of the matrix. On the other hand, if A is an $n \times n$ matrix, then A^T is still an $n \times n$ matrix. We can take things one step further by considering matrices which are left completely unchanged by the transpose. This idea leads to the following definition:

Definition 3.23. *Let A be an $n \times n$ matrix. The matrix A is a **symmetric matrix** if $A^T = A$.*

Example 3.24. *Let*

$$A = \begin{pmatrix} 4 & -1 & 2 \\ -1 & 3 & 5 \\ 2 & 5 & 0 \end{pmatrix}.$$

Then $A^T = A$. Hence, A is a (real) symmetric matrix.

For complex matrices, one has the following variation of a symmetric matrix which has greater use:

Definition 3.25. *Let A be an $n \times n$ matrix. The matrix A is a **Hermitian matrix** if $A^* = A$.*

Example 3.26. *Let*

$$A = \begin{pmatrix} 1 & 2+3i \\ 2-3i & 5 \end{pmatrix}.$$

Then $A^T = A$. Hence, A is a Hermitian matrix.

At this point, we are going to introduce a very important type of matrix:

Definition 3.27. *Let A be an $n \times n$ matrix. A is called a* ***diagonal matrix*** *if $A_{ij} = 0$ for all $i \neq j$. The elements A_{ii} for $i = 1, \ldots, n$ are called the diagonal elements of A. The set of diagonal elements*

$$A_{11},\ A_{22}, \ldots, A_{nn}$$

is called the ***main diagonal*** *of A.*

Example 3.28. *The 3×3 matrix*

$$A = \begin{pmatrix} 2 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & -3 \end{pmatrix}$$

is a diagonal matrix.

Proposition 3.29. *Let A be a Hermitian matrix. Then its diagonal elements are all real numbers.*

Proof. Consider the diagonal element A_{ii}. Since $A^* = A$, we have

$$(A^*)_{ii} = \overline{A}_{ii} = A_{ii}.$$

The above equality implies that the imaginary part of A_{ii} is zero. In other words, A_{ii} is real. □

For the sake of completeness, we will introduce other types of symmetries associated to the transpose and the conjugate transpose:

Definition 3.30. *Let A be an $n \times n$ matrix.*

1. *A is a* ***skew-symmetric*** *matrix if $A^T = -A$.*
2. *A is a* ***skew-Hermitian*** *matrix if $A^* = -A$.*

Proposition 3.31. *Let A be an $n \times n$ matrix.*

(1) If A is a skew-symmetric matrix, then its diagonal elements are all zero.
(2) If A is a skew-Hermitian matrix, then its diagonal elements are all imaginary.

Proof. (1): Let A be a skew-symmetric matrix. Since $A^T = -A$, we have

$$A_{ji} = -A_{ij}.$$

In particular, $A_{ii} = -A_{ii}$ for all i.

(2): Let A be a skew-Hermitian matrix. Since $A^* = -A$, we have

$$\overline{A}_{ji} = -A_{ij}.$$

In particular, $\overline{A}_{ii} = -A_{ii}$. Write $A_{ii} = a + b\sqrt{-1}$. Then the aforementioned condition implies that

$$a - b\sqrt{-1} = -a - b\sqrt{-1}.$$

From this, we see that $a = 0$. Hence, A_{ii} is imaginary. □

Example 3.32.

- ***Symmetric Matrix:*** $\begin{pmatrix} 1 & 7 & 3 \\ 7 & 4 & -5 \\ 3 & -5 & 6 \end{pmatrix}$
- ***Skew-symmetric Matrix:*** $\begin{pmatrix} 0 & 2 & -1 \\ -2 & 0 & -4 \\ 1 & 4 & 0 \end{pmatrix}$
- ***Hermitian Matrix:*** $\begin{pmatrix} 2 & 2+i & 4 \\ 2-i & 3 & i \\ 4 & -i & 1 \end{pmatrix}$
- ***Skew-Hermitian Matrix:*** $\begin{pmatrix} 3 & 1+2i & 2-3i \\ 1-2i & 2 & 3+4i \\ 2+3i & 3-4i & 1 \end{pmatrix}$

Exercise 3.33. *Identify each of the following as symmetric, skew symmetric, or neither.*

(a) $\begin{pmatrix} 1 & -3 & 3 \\ -3 & 4 & -3 \\ 3 & 3 & 0 \end{pmatrix}$

(b) $\begin{pmatrix} 0 & -3 & -3 \\ 3 & 0 & 1 \\ 3 & -1 & 0 \end{pmatrix}$

(c) $\begin{pmatrix} 1 & 2 & 0 \\ 2 & 1 & 0 \end{pmatrix}$

3.4. Matrix Multiplication

In this section, we define matrix multiplication and study its properties. It will become apparent right away that matrix multiplication does not behave like the usual multiplication of real or complex numbers in one key respect.

Definition 3.34. *Let A be an $m \times n$ matrix and let B be a $n \times p$ matrix. Then the product of A and B is the $m \times p$ matrix AB whose (i, j)-entry is given by*

$$(AB)_{ij} = \sum_{k=1}^{n} A_{ik}B_{kj} = A_{i1}B_{1j} + A_{i2}b_{2j} + \cdots + A_{in}B_{nj}.$$

From the above definition, the product AB is only defined if **the number of columns of A is equal to the number of rows of B**. Hence, if AB is defined, then it is not necessarily true that BA is defined. This is one key difference between matrix multiplication and the usual multiplication of real and complex numbers.

Remark 3.35. *Definition 3.34 may seem a little mysterious at this point. The reader may be wondering why matrix multiplication is not defined componentwise like matrix addition. The reason why matrix multiplication is defined the way it is has to do with a type of map called a* ***linear map*** *which will be defined in Chapter 5. In Chapter 6, we will see that these linear maps can be represented as matrices! Moreover, we will see that matrix multiplication, as defined in Definition 3.34, is exactly what is needed to represent the composition of two linear maps! However, all of this will have to wait for Chapter 6.*

At this point, its time to look at some examples:

Example 3.36. *Let*

$$A = \begin{pmatrix} -2 & 3 & 4 \end{pmatrix}, \qquad B = \begin{pmatrix} 3 \\ -2 \\ 1 \end{pmatrix}.$$

Then

$$AB = \begin{pmatrix} 2 & 5 & 4 \end{pmatrix} \begin{pmatrix} 3 \\ 7 \\ 1 \end{pmatrix} = (2)(3) + (5)(7) + (4)(1) = 45.$$

As expected, since A is a 1×3 matrix and B is a 3×1 matrix, AB is a 1×1 matrix, i.e. a number.

Note also that BA is also defined. The end result is a 3×3 matrix:

$$BA = \begin{pmatrix} 3 \\ 7 \\ 1 \end{pmatrix} \begin{pmatrix} 2 & 5 & 4 \end{pmatrix} = \begin{pmatrix} 6 & 15 & 12 \\ 14 & 35 & 28 \\ 2 & 5 & 4 \end{pmatrix}.$$

Example 3.36 demonstrates that even when one has two matrices A and B for which AB and BA are defined, one in general, has

$$AB \neq BA.$$

This result is a far cry from the usual multiplication of numbers! The technical term for this is to say that matrix multiplication is **noncommutative**. In other words, when it comes to matrix multiplication, order matters. Interestingly, this feature of noncommutativity of matrices enters prominently in *quantum mechanics* and leads to the famous *Heisenberg Uncertainty Principle*, which says that it is impossible to measure both the position and velocity of a particle simultaneously with arbitrary accuracy.

Here's a few more examples:

Example 3.37. *Let*

$$A = \begin{pmatrix} 1 & 2 & 3 \\ -2 & -1 & 5 \end{pmatrix}, \qquad B = \begin{pmatrix} 0 & 4 \\ 5 & -1 \\ 3 & 2 \end{pmatrix}.$$

Let's compute, for example, the $(2,2)$*-entry of* AB*:*

$$(AB)_{22} = (-2)(4) + (-1)(-1) + (5)(2) = 3.$$

Here is the full calculation for AB*:*

$$AB = \begin{pmatrix} 1 & 2 & 3 \\ -2 & -1 & 5 \end{pmatrix} \begin{pmatrix} 0 & 4 \\ 5 & -1 \\ 3 & 2 \end{pmatrix} = \begin{pmatrix} 19 & 2 \\ 10 & 3 \end{pmatrix}.$$

Example 3.38. *Let*

$$A = \begin{pmatrix} 1+i & 2i \\ 3 & 2+3i \end{pmatrix}, \quad B = \begin{pmatrix} 4i & 2 \\ 1-i & -2i \end{pmatrix}.$$

Then

$$AB = \begin{pmatrix} 1+i & 2i \\ 3 & 2+3i \end{pmatrix} \begin{pmatrix} 4i & 2 \\ 1-i & -2i \end{pmatrix} = \begin{pmatrix} -2+6i & 6+2i \\ 5+13i & 12-4i \end{pmatrix}$$

The following example is a very convenient result to keep in mind:

Example 3.39. *Let $\vec{u}, \vec{v} \in \mathbb{R}^n$ be column vectors. Then the dot product of $\vec{u}$ and $\vec{v}$ can be expressed in terms of matrix multiplication and the transpose:*

$$\begin{aligned}\vec{u} \cdot \vec{v} &= u_1 v_1 + u_2 v_2 + \cdots + u_n v_n \\ &= \begin{pmatrix} u_1 & u_2 & \cdots & u_n \end{pmatrix} \begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{pmatrix} \\ &= \vec{u}^T \vec{v}.\end{aligned}$$

We now look at some of the basic properties of matrix multiplication. We begin by proving the associativity of matrix multiplication:

Theorem 3.40. *Let A, B, and C be matrices such that AB and BC are defined. Then*

$$(AB)C = A(BC). \tag{37}$$

Proof. Let A be an $m \times n$ matrix, B an $n \times p$ matrix, and C a $p \times q$ matrix. Lets compute the (i, j)-element of the left side of (37) and see what happens:

$$\begin{aligned}\big[(AB)C\big]_{ij} &= \sum_{k=1}^{p} (AB)_{ik} C_{kj} \\ &= \sum_{k=1}^{p} \left(\sum_{r=1}^{n} A_{ir} B_{rk} \right) C_{kj} \\ &= \sum_{r=1}^{n} \sum_{k=1}^{p} A_{ir} B_{rk} C_{kj} \\ &= \sum_{r=1}^{n} A_{ir} \left(\sum_{k=1}^{p} B_{rk} C_{kj} \right) \\ &= \sum_{r=1}^{n} A_{ir} (BC)_{rj} \\ &= \big[A(BC)\big]_{ij}.\end{aligned}$$

From this, we conclude that $(AB)C = A(BC)$. □

Next we verify that matrix multiplication is distributive with respect to matrix addition and scalar multiplication:

Theorem 3.41. *Let B and C be matrices of the same size and let A and D be matrices such that AB, AC, BD, and CD are all defined. Also, let α be any scalar. Then*

(a) $A(B+C) = AB + AC$

(b) $(B+C)D = BD + CD$

(c) $\alpha(AB) = (\alpha A)B = A(\alpha B)$.

Proof. Let B and C be $m \times n$ matrices and let A and D be $l \times m$ and $n \times p$ matrices respectively. Then

$$\begin{aligned}
[A(B+C)]_{ij} &= \sum_{k=1}^{m} A_{ik}(B+C)_{kj} \\
&= \sum_{k=1}^{m} A_{ik}(B_{kj} + C_{kj}) \\
&= \sum_{k=1}^{m} A_{ik}B_{kj} + A_{ik}C_{kj} \\
&= (AB)_{ij} + (AC)_{ij} \\
&= (AB + AC)_{ij}.
\end{aligned}$$

Hence, $A(B+C) = AB + AC$. This proves (a).

The proof of (b) is entirely similar to (a) so we omit it and leave it as exercise for the reader.

For (c), we have

$$\begin{aligned}
\big[\alpha(AB)\big]_{ij} &= \alpha(AB)_{ij} \\
&= c\left(\sum_{k=1}^{n} A_{ik}B_{kj}\right) \\
&= \left(\sum_{k=1}^{n} (\alpha A_{ik})B_{kj}\right) = \left(\sum_{k=1}^{n} A_{ik}(\alpha B_{kj})\right) \\
&= \left(\sum_{k=1}^{n} (\alpha A)_{ik}B_{kj}\right) = \left(\sum_{k=1}^{n} A_{ik}(\alpha B)_{kj}\right) \\
&= \big[(\alpha A)B\big]_{ij} = \big[A(\alpha B)\big]_{ij}.
\end{aligned}$$

□

At this point, lets check the above results against some examples:

Example 3.42. *Let*

$$A = \begin{pmatrix} 3 & 1 & -2 \\ 1 & 4 & 3 \end{pmatrix}, \quad \begin{pmatrix} 5 & -2 \\ 3 & 4 \\ -1 & -4 \end{pmatrix}, \quad \begin{pmatrix} 0 & 2 \\ -1 & 3 \end{pmatrix}.$$

Then

$$\begin{aligned} (AB)C &= \left[\begin{pmatrix} 3 & 1 & -2 \\ 1 & 4 & 3 \end{pmatrix}\begin{pmatrix} 5 & -2 \\ 3 & 4 \\ -1 & -4 \end{pmatrix}\right]\begin{pmatrix} 0 & 2 \\ -1 & 3 \end{pmatrix} \\ &= \begin{pmatrix} 20 & 6 \\ 14 & 2 \end{pmatrix}\begin{pmatrix} 0 & 2 \\ -1 & 3 \end{pmatrix} \\ &= \begin{pmatrix} -6 & 58 \\ -2 & 34 \end{pmatrix} \end{aligned}$$

and

$$\begin{aligned} A(BC) &= \begin{pmatrix} 3 & 1 & -2 \\ 1 & 4 & 3 \end{pmatrix}\left[\begin{pmatrix} 5 & -2 \\ 3 & 4 \\ -1 & -4 \end{pmatrix}\begin{pmatrix} 0 & 2 \\ -1 & 3 \end{pmatrix}\right] \\ &= \begin{pmatrix} 3 & 1 & -2 \\ 1 & 4 & 3 \end{pmatrix}\begin{pmatrix} 2 & 4 \\ -4 & 18 \\ 4 & -14 \end{pmatrix} \\ &= \begin{pmatrix} -6 & 58 \\ -2 & 34 \end{pmatrix} \end{aligned}$$

Example 3.43. *Let*

$$A = \begin{pmatrix} 6 & 3 \\ -2 & 5 \end{pmatrix}, \quad B = \begin{pmatrix} -1 & 1 & 4 \\ -2 & 3 & -2 \end{pmatrix}, \quad C = \begin{pmatrix} 3 & -2 & 4 \\ 4 & -2 & 3 \end{pmatrix}$$

Then

$$\begin{aligned} A(B+C) &= \begin{pmatrix} 6 & 3 \\ -2 & 5 \end{pmatrix}\left[\begin{pmatrix} -1 & 1 & 4 \\ -2 & 3 & -2 \end{pmatrix} + \begin{pmatrix} 3 & -2 & 4 \\ 4 & -2 & 3 \end{pmatrix}\right] \\ &= \begin{pmatrix} 6 & 3 \\ -2 & 5 \end{pmatrix}\begin{pmatrix} 2 & -1 & 8 \\ 2 & 1 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 18 & -3 & 51 \\ 6 & 7 & -11 \end{pmatrix} \end{aligned}$$

and

$$AB + AC = \begin{pmatrix} 6 & 3 \\ -2 & 5 \end{pmatrix}\begin{pmatrix} -1 & 1 & 4 \\ -2 & 3 & -2 \end{pmatrix} + \begin{pmatrix} 6 & 3 \\ -2 & 5 \end{pmatrix}\begin{pmatrix} 3 & -2 & 4 \\ 4 & -2 & 3 \end{pmatrix}$$

$$= \begin{pmatrix} -12 & 15 & 18 \\ -8 & 13 & -18 \end{pmatrix} + \begin{pmatrix} 30 & -18 & 33 \\ 14 & -6 & 7 \end{pmatrix}$$
$$= \begin{pmatrix} 18 & -3 & 51 \\ 6 & 7 & -11 \end{pmatrix}$$

The next result is used numerous times during the course of the book.

Proposition 3.44. *Let A be an $m \times n$ matrix and let B be an $n \times p$ matrix. Let $\vec{b}_j$ denote the jth column of B. Then*

$$AB = \begin{pmatrix} A\vec{b}_1 & A\vec{b}_2 & \cdots & A\vec{b}_n \end{pmatrix}.$$

Proof. The (i, j)-entry of AB is

$$(AB)_{ij} = \sum_{k=1}^{n} a_{ik} b_{kj} = (A\vec{b}_j)_i,$$

where $(A\vec{b}_j)_i$ denotes the ith element of $A\vec{b}_j$. Hence, the jth column of AB is $A\vec{b}_j$. □

We now look at the relationship between matrix multiplication and the transpose and the conjugate transpose.

Proposition 3.45. *Let A and B be matrices such that AB are defined. Then*

(a) $(AB)^T = B^T A^T$

(b) $(AB)^* = B^* A^*$

Proof. Let A be an $m \times n$ matrix and B be an $n \times p$ matrix. For (a), we have

$$\begin{aligned} \left[(AB)^T\right]_{ij} &= (AB)_{ji} \\ &= \sum_{k=1}^{n} A_{jk} B_{ki} \\ &= \sum_{k=1}^{n} B_{ki} A_{jk} \\ &= \sum_{k=1}^{n} \left[B^T\right]_{ik} \left[A^T\right]_{kj} \\ &= \left[B^T A^T\right]_{ij}, \end{aligned}$$

which implies $(AB)^T = B^T A^T$. The proof of (b) is similar so we leave it to the reader as an exercise. □

Example 3.46. *Let*

$$A = \begin{pmatrix} 2 & 3 \\ -1 & 4 \end{pmatrix}, \qquad B = \begin{pmatrix} 0 & -1 \\ 2 & 5 \end{pmatrix}.$$

Then

$$(AB)^T = \left(\begin{pmatrix} 2 & 3 \\ -1 & 4 \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 2 & 5 \end{pmatrix} \right) = \begin{pmatrix} 6 & 13 \\ 8 & 21 \end{pmatrix}^T = \begin{pmatrix} 6 & 8 \\ 13 & 21 \end{pmatrix}$$

and

$$B^T A^T = \begin{pmatrix} 0 & 2 \\ -1 & 5 \end{pmatrix} \begin{pmatrix} 2 & -1 \\ 3 & 4 \end{pmatrix} = \begin{pmatrix} 6 & 8 \\ 13 & 21 \end{pmatrix}.$$

At this point, we now introduce the matrix-equivalent of the number 1:

Definition 3.47. *The **identity matrix** of order n is the $n \times n$ diagonal matrix whose diagonal elements are all 1, that is,*

$$I_n := \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix}.$$

The name "identity matrix" is justified by the following result:

Proposition 3.48. *Let A be an $m \times n$ matrix. Then $I_m A = A I_n = A$.*

Proof. By direct calculation, we have

$$\begin{aligned} (I_m A)_{ij} &= \sum_{k=1}^{m} (I_m)_{ik} A_{kj} \\ &= \sum_{k \neq i} (I_m)_{ik} A_{kj} + I_{ii} A_{ij} \\ &= \sum_{k \neq i} 0 A_{kj} + 1 A_{ij} \\ &= A_{ij}. \end{aligned}$$

Hence, $I_m A = A$. Likewise, we have

$$\begin{aligned}(AI_n)_{ij} &= \sum_{k=1}^{n} A_{ik}(I_n)_{kj} \\ &= \sum_{k\neq j} A_{ik}(I_m)_{kj} + A_{ij}(I_n)_{jj} \\ &= \sum_{k\neq j} A_{ik}0 + A_{ij}1 \\ &= A_{ij}.\end{aligned}$$

□

Exercise 3.49. *Let A be a square matrix. Show that $A^T A$ and AA^T are both symmetric.*

Some Motivation for the Conjugate Transpose

Consider a complex number $z = a + ib \in \mathbb{C}$. Since a complex number has two components, a real and an imaginary part, we can identify $\mathbb{C}$ with $\mathbb{R}^2$. Explicitly, we regard the complex number $z = a + ib$ with the real vector

$$\vec{z} = (a, b) \in \mathbb{R}^2.$$

The square of the length of this vector is conveniently given by the dot product: $\vec{z} \cdot \vec{z}$. However, this same quantity can also be computed using conjugation:

$$z\overline{z} = \vec{z} \cdot \vec{z} = a^2 + b^2.$$

From Example 3.39, the dot product of two real column vectors $\vec{u}, \vec{v} \in \mathbb{R}^n$ (can be expressed in terms of the transpose via

$$\vec{u} \cdot \vec{v} = \vec{u}^T \vec{v}.$$

Recall that one of the properties of the dot product is that $\vec{u} \cdot \vec{u} \geq 0$ for all real vectors $\vec{u}$ and zero precisely when $\vec{u} = \vec{0}$. Geometrically, $\vec{u} \cdot \vec{u}$ represents the square of the length of the vector $\vec{u}$. Suppose now that we wanted to construct a "complex dot product" and we want our "complex dot product" to have properties similar to the real dot product. In particular, we would like our "complex dot product" to satisfy the condition $\vec{u} \cdot \vec{u} \geq 0$ for all $\vec{u} \in \mathbb{C}^n$ and to be zero only when $\vec{u} = \vec{0}$. Naively, we might define our complex dot product in terms of the ordinary transpose (just like the real case). However, this does not work. In fact, it does not even yield a real number.

At this point, you probably know exactly how to fix this problem. We simply replace the ordinary transpose with the conjugate transpose.

$$\vec{u} \cdot \vec{v} = (\vec{u})^* \vec{v}.$$

Its a simple exercise to see that $(\vec{u})^* \vec{u} \geq 0$ for all $\vec{u} \in \mathbb{C}^n$ and zero precisely when $\vec{u} = \vec{0}$. The above dot product is called the **standard Hermitian inner product** on $\mathbb{C}^n$. This is an idea we will cover later in this book.

3.5. The Inverse of a Matrix

In the last section, we introduced the identity matrix I_n (of order n), which plays the same role as the number 1 for $\mathbb{R}$ and $\mathbb{C}$ with regard to multiplication. If a is a nonzero number, then there exists a number a^{-1} such that

$$aa^{-1} = a^{-1}a = 1.$$

Given a matrix A, we would like to know where there exists a matrix A^{-1} such that

$$AA^{-1} = A^{-1}A = I_n. \tag{38}$$

Equation (38) implies that A and A^{-1} are both square matrices of order n. The matrix A^{-1} (if it exists) is called the **inverse** of A. Before we consider how to compute the matrix inverse, we first prove a basic result about A^{-1}.

Proposition 3.50. *Let A be an $n \times n$ matrix.*

(i) The matrix inverse of A (if it exists) is unique.
(ii) If A^{-1} exists, then $(A^{-1})^{-1} = A$.

Proof. (i): Suppose that A_1^{-1} and A_2^{-1} are both inverses of A. Then

$$\begin{aligned} A_1^{-1} &= A_1^{-1} I_n \\ &= A_1^{-1}(AA_2^{-1}) \\ &= (A_1^{-1}A)A_2^{-1} \\ &= I_n A_2^{-1} \\ &= A_2^{-1}. \end{aligned}$$

(ii): This is immediate. If A^{-1} exists, then $AA^{-1} = A^{-1}A = I_n$. Hence, A is an inverse of A^{-1}. Moreover, by statement (i), this is the only inverse of A^{-1}. This proves (ii). □

For the sake of concreteness, we are going to assume that all matrices in this section are real. However, we point out that all the arguments given in this section work equally well for complex matrices. The question of when the inverse of a square matrix exists is answered by the following result:

Theorem 3.51. *Let A be a square matrix of order n. Let $\vec{a}_i$ denote the ith column of A. Then A^{-1} exists if and only if*

$$\{\vec{a}_1, \ldots, \vec{a}_n\}$$

is a basis of $\mathbb{R}^n$.

Proof. ($\Rightarrow$) Suppose A^{-1} exists. Let $\vec{\alpha}_i$ denote the ith column of A^{-1}. Then

$$AA^{-1} = A\begin{pmatrix} \vec{\alpha}_1 & \vec{\alpha}_2 & \cdots & \vec{\alpha}_n \end{pmatrix} = \begin{pmatrix} A\vec{\alpha}_1 & A\vec{\alpha}_2 & \cdots & A\vec{\alpha}_n \end{pmatrix}$$

Let $\vec{e}_i$ denote the ith standard basis of $\mathbb{R}^n$ (expressed as a column vector). Observe that

$$I_n = \begin{pmatrix} \vec{e}_1 & \vec{e}_2 & \cdots & \vec{e}_n \end{pmatrix}.$$

Since $AA^{-1} = I_n$, it follows that

$$A\vec{\alpha}_i = \vec{e}_i. \tag{39}$$

Since $A\vec{\alpha}_i$ is a linear combination of the columns of A, it follows from (39) that

$$\begin{aligned} \mathbb{R}^n &= \text{span}\,\{A\vec{\alpha}_1, \ldots, A\vec{\alpha}_n\} \\ &= \text{span}\,\{\vec{a}_1, \ldots, \vec{a}_n\}. \end{aligned} \tag{40}$$

Since $\dim \mathbb{R}^n = n$, it follows from (40) that $\{\vec{a}_1, \ldots, \vec{a}_n\}$ is a basis of $\mathbb{R}^n$.

($\Leftarrow$) Suppose that the columns of A form a basis of $\mathbb{R}^n$. Hence, for any vector $\vec{v} \in \mathbb{R}^n$, there exists (unique) $c_1, \ldots, c_n \in \mathbb{R}$ such that

$$c_1\vec{a}_1 + c_2\vec{a}_2 + \cdots + c_n\vec{a}_n = \vec{v}. \tag{41}$$

Let $\vec{c} \in \mathbb{R}^n$ be the column vector whose ith component is c_i, (41) is equivalent to the matrix equation

$$A\vec{c} = \vec{v}. \tag{42}$$

In particular, for each standard basis vector $\vec{e}_i$, there exists a vector $\vec{b}_i$ such that

$$A\vec{b}_i\vec{e}_i. \tag{43}$$

Let B be the $n \times n$ matrix whose ith column is $\vec{b}_i$. Then (43) implies

$$AB = I_n.$$

We now show that we also have $BA = I_n$. To do this, note that

$$A = I_nA = (AB)A = A(BA). \tag{44}$$

(44) implies that

$$A(I_n - BA) = \mathbf{0}. \tag{45}$$

Let $\vec{c}_i$ denote the ith column of $I_n - BA$. Then (45) implies that

$$A\vec{c}_i = \vec{0} \tag{46}$$

for $i = 1, \ldots, n$. Since the columns of A are a basis of $\mathbb{R}^n$ (and hence linearly independent), it follows that $\vec{c}_i = \vec{0}$ for $i = 1, \ldots, n$. This proves that $I_n - BA = \mathbf{0}$. In other words, $BA = I_n$. We have thus constructed a matrix B satisfying $AB = BA = I_n$. By definition, B is the (unique) inverse of A. □

Definition 3.52. *A matrix whose inverse exists is said to be* ***invertible*** *(or* ***nonsingular****).*

The following result will prove useful:

Corollary 3.53. *Let A be an $n \times n$ matrix. If there exists an $n \times n$ matrix B such that $AB = I_n$, then A is invertible and $A^{-1} = B$.*

Proof. Suppose there exists a square matrix B of order n such that $AB = I_n$. Let $\vec{b}_i$ denote the ith column of B. As we saw in the proof of Theorem 3.51, the equation $AB = I_n$ implies that

$$\{A\vec{b}_1, \ldots, A\vec{b}_n\}$$

is a basis of $\mathbb{R}^n$. This in turn implies that the columns of A form a basis of $\mathbb{R}^n$. By Theorem 3.51, A^{-1} exists. Hence,

$$A^{-1} = A^{-1}I_n = A^{-1}AB = I_nB = B.$$

□

Corollary 3.53 (and the proof of Theorem 3.51) give us a strategy for computing the inverse of an $n \times n$ matrix A (assuming it exists). To find the inverse of A, it suffices to find an $n \times n$ matrix B satisfying

$$AB = I_n.$$

Let $\vec{b}_i$ be the ith column of B. The above equation amounts to solving the following n matrix equations:

$$A\vec{b}_i = \vec{e}_i, \qquad \text{for } i = 1, 2, \ldots, n.$$

Each matrix equation is just a linear system of n equations in n variables. Hence, we can use the Gauss-Jordan method to solve for each column $\vec{b}_i$. The good news is that we can solve all n matrix equations simultaneously. To do this, we form the augmented $n \times 2n$ matrix:

$$A' := \begin{pmatrix} A & I_n \end{pmatrix}.$$

The idea now is to put the first n columns of A' in reduced echelon form. If we can transform A' into the following form

$$\begin{pmatrix} I_n & B \end{pmatrix}$$

via row operations, then A has an inverse and the inverse is $A^{-1} = B$. Let's put this strategy to the test with a simple example:

Example 3.54. *Let*

$$A = \begin{pmatrix} 2 & 1 \\ 3 & 2 \end{pmatrix}.$$

Now we form the augmented matrix

$$A' = \begin{pmatrix} 2 & 1 & 1 & 0 \\ 3 & 2 & 0 & 1 \end{pmatrix}.$$

Now apply Gauss Jordan to A'

1. $-R_1 + R_2 \to R_2$:

$$A' = \begin{pmatrix} 2 & 1 & 1 & 0 \\ 1 & 1 & -1 & 1 \end{pmatrix}$$

2. $R_1 \leftrightarrow R_2$

$$A' = \begin{pmatrix} 1 & 1 & -1 & 1 \\ 2 & 1 & 1 & 0 \end{pmatrix}$$

3. $-2R_1 + R_2 \to R_2$

$$A' = \begin{pmatrix} 1 & 1 & -1 & 1 \\ 0 & -1 & 3 & -2 \end{pmatrix}$$

4. $R_2 + R_1 \to R_1$

$$A' = \begin{pmatrix} 1 & 0 & 2 & -1 \\ 0 & -1 & 3 & -2 \end{pmatrix}$$

5. $-R_2 \to R_2$

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

From this, we conclude that

$$A^{-1} = \begin{pmatrix} 2 & -1 \\ -3 & 2 \end{pmatrix}.$$

Let's check that $AA^{-1} = A^{-1}A = I_2$:

$$AA^{-1} = \begin{pmatrix} 2 & 1 \\ 3 & 2 \end{pmatrix} \begin{pmatrix} 2 & -1 \\ -3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

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

The need to calculate the inverse of a 2×2 matrix happens quite often. For this reason, the following result is convenient to keep in mind:

Proposition 3.55. *Let*

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

Then A is invertible if and only if $ad - bc \neq 0$ and

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

Exercise 3.56. *Check Proposition 3.55.*

The quantity $ad - bc$ in Proposition 3.55 is called the **determinant** of the 2×2 matrix A. The determinant is an extremely important idea in linear algebra. We will study determinants in more detail in Chapter 4.

Example 3.57. *Let*

$$A = \begin{pmatrix} 0 & 2 & 0 \\ 4 & 0 & -2 \\ 2 & 0 & 0 \end{pmatrix}.$$

As before, form the augmented matrix A':

$$A' = \begin{pmatrix} 0 & 2 & 0 & 1 & 0 & 0 \\ 4 & 0 & -2 & 0 & 1 & 0 \\ 2 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

Now apply Gauss-Jordan to A':

1. $-2R_1 + R_2 \to R_2$:
$$A' = \begin{pmatrix} 0 & 2 & 0 & 1 & 0 & 0 \\ 0 & 0 & -2 & 0 & 1 & -2 \\ 2 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$
2. $R_1 \to R_2$:
$$A' = \begin{pmatrix} 0 & 0 & -2 & 0 & 1 & -2 \\ 0 & 2 & 0 & 1 & 0 & 0 \\ 2 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$
3. $R_1 \to R_3$:
$$A' = \begin{pmatrix} 2 & 0 & 0 & 0 & 0 & 1 \\ 0 & 2 & 0 & 1 & 0 & 0 \\ 0 & 0 & -2 & 0 & 1 & -2 \end{pmatrix}$$
4. $\frac{1}{2}R_1 \to R_1$, $\frac{1}{2}R_2 \to R_2$, $-\frac{1}{2}R_3 \to R_3$:
$$A' = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1/2 \\ 0 & 1 & 0 & 1/2 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1/2 \end{pmatrix}$$

Hence,

$$A^{-1} \begin{pmatrix} 0 & 0 & 1/2 \\ 1/2 & 0 & 0 \\ 0 & 1 & 1/2 \end{pmatrix}.$$

We leave it to the reader to check that the above matrix is indeed the inverse of A.

Example 3.58. *Let*

$$A = \begin{pmatrix} 1 & -1 & 1 \\ -1 & -1 & 1 \\ 1 & 1 & 1 \end{pmatrix}.$$

The augmented matrix is

$$A' = \begin{pmatrix} 1 & -1 & 1 & 1 & 0 & 0 \\ -1 & -1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 \end{pmatrix}.$$

Now we apply Gauss-Jordan to A':

1. $R_1 + R_2 \to R_2$, $-R_1 + R_3 \to R_3$:
$$\begin{pmatrix} 1 & -1 & 1 & 1 & 0 & 0 \\ 0 & -2 & 2 & 1 & 1 & 0 \\ 0 & 2 & 0 & -1 & 0 & 1 \end{pmatrix}$$
2. $R_3 + R_2 \to R_2$:
$$\begin{pmatrix} 1 & -1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 2 & 0 & 1 & 1 \\ 0 & 2 & 0 & -1 & 0 & 1 \end{pmatrix}$$
3. $R_2 \leftrightarrow R_3$:
$$\begin{pmatrix} 1 & -1 & 1 & 1 & 0 & 0 \\ 0 & 2 & 0 & -1 & 0 & 1 \\ 0 & 0 & 2 & 0 & 1 & 1 \end{pmatrix}$$
4. $1/2R_2 + R_1 \to R_1$, $-1/2R_3 + R_1 \to R_1$:
$$\begin{pmatrix} 1 & 0 & 0 & 1/2 & -1/2 & 0 \\ 0 & 2 & 0 & -1 & 0 & 1 \\ 0 & 0 & 2 & 0 & 1 & 1 \end{pmatrix}$$
5. $1/2R_2 \to R_2$, $1/2R_3 \to R_3$
$$\begin{pmatrix} 1 & 0 & 0 & 1/2 & -1/2 & 0 \\ 0 & 1 & 0 & -1/2 & 0 & 1/2 \\ 0 & 0 & 1 & 0 & 1/2 & 1/2 \end{pmatrix}$$

Hence,

$$A^{-1} = \begin{pmatrix} 1/2 & -1/2 & 0 \\ -1/2 & 0 & 1/2 \\ 0 & 1/2 & 1/2 \end{pmatrix}.$$

We conclude this section by revisiting systems of linear equations. Consider the following system of n equations and n variables:

$$\begin{gathered} a_{11}x_1 + \cdots + a_{1n}x_n = b_1 \\ a_{21}x_1 + \cdots + a_{2n}x_n = b_2 \\ \vdots \\ a_{n1}x_1 + \cdots + a_{nn}x_n = b_n \end{gathered}$$

One of the nice features of matrices is that we can use them to transform a system of linear equations into a single concise matrix equation (as we saw earlier). In this case, let A be the $n \times n$ matrix whose (i,j)-element is a_{ij}, let $\vec{x}$ be the column vector whose ith component is x_i, and let $\vec{b}$ be the column vector whose ith component is b_i. Then the above linear system is completely encapsulated by the following matrix equation:

$$A\vec{x} = \vec{b}. \tag{47}$$

From here, we obtain the following result:

Theorem 3.59. *Let A be an $n \times n$ matrix and let $\vec{b} \in \mathbb{R}^n$ be any column vector. Then the matrix equation $A\vec{x} = \vec{b}$ has a unique solution if and only if A is invertible. Moreover, the solution is $\vec{x} = A^{-1}\vec{b}$.*

Proof. If A is invertible, then multiplying both sides of (47) from the left by A^{-1} gives

$$\vec{x} = A^{-1}\vec{b}.$$

Now suppose that (47) has a unique solution. In particular, $A\vec{x} = \vec{0}$ has a unique solution. This implies that the columns of A are linearly independent. Since A has n columns, the columns of A must form a basis of $\mathbb{R}^n$. By Theorem 3.51, A is invertible. □

Example 3.60. *Consider the linear system*

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

Setting

$$A = \begin{pmatrix} 1 & -1 & 1 \\ -1 & -1 & 1 \\ 1 & 1 & 1 \end{pmatrix}.$$

We already encountered the matrix A in Example 3.58. Its inverse was found to be

$$A^{-1} = \begin{pmatrix} 1/2 & -1/2 & 0 \\ -1/2 & 0 & 1/2 \\ 0 & 1/2 & 1/2 \end{pmatrix}.$$

Hence, the (unique) solution to the above system is

$$\vec{x} = A^{-1}\vec{b} = \begin{pmatrix} 1/2 & -1/2 & 0 \\ -1/2 & 0 & 1/2 \\ 0 & 1/2 & 1/2 \end{pmatrix} \begin{pmatrix} 5 \\ 2 \\ 4 \end{pmatrix} = \begin{pmatrix} 3/2 \\ -1/2 \\ 3 \end{pmatrix}$$

3.6. Elementary Matrices

Back in Chapter 1, we introduced the following three elementary row operations:

1. $R_i \leftrightarrow R_j$
2. $cR_i \to R_i$ $(c \neq 0)$
3. $cR_i + R_j \to R_j$ $(i \neq j)$

It turns out each of these row operations can be achieved by matrix multiplication. The matrices that are associated to these basic row operations are called **elementary matices**:

Definition 3.61. *An **elementary matrix** of order n is a matrix E which differs from the identity matrix I_n by a single elementary row operation.*

Example 3.62. *Here are some examples of elementary matrices:*

1.
$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

2.
$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 5 \\ 0 & 0 & 1 \end{pmatrix}$$

3.
$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -4 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

The following result shows how elementary matrices induce elementary row operations:

Theorem 3.63. *Let A be an $n \times n$ matrix and let E be an elementary matrix obtained by applying row operation X to I_n. Then EA is the matrix obtained by applying row operation X to A.*

Proof. Let $\vec{e}_1, \dots, \vec{e}_n$ be the standard basis on $\mathbb{R}^n$ expressed as columns vectors. Then

$$I_n = \begin{pmatrix} \vec{e}_1^T \\ \vdots \\ \vec{e}_n^T \end{pmatrix}$$

Lets consider each of the three basic row operations one by one.

case 1: X is $R_i \leftrightarrow R_j$. If $i = j$, then the row operation X leaves the matrix unchanged. With $i = j$, we have $E = I_n$ and $EA = I_nA = A$. Now let us suppose $i < j$. Then

$$E = \begin{pmatrix} \vec{e}_1^T \\ \vdots \\ \vec{e}_j^T \\ \vdots \\ \vec{e}_i^T \\ \vdots \\ \vec{e}_n^T \end{pmatrix}$$

and

$$EA = \begin{pmatrix} \vec{e}_1^T A \\ \vdots \\ \vec{e}_j^T A \\ \vdots \\ \vec{e}_i^T A \\ \vdots \\ \vec{e}_n^T A \end{pmatrix}.$$

Since $\vec{e}_k^T A$ is the kth row of A, we see that EA is A with rows i and j swapped.

case 2: X is $cR_i \to R_i$ with $c \neq 0$. In this case,

$$E = \begin{pmatrix} \vec{e}_1^T \\ \vdots \\ c\vec{e}_i^T \\ \vdots \\ \vec{e}_n^T \end{pmatrix}.$$

Then

$$EA = \begin{pmatrix} \vec{e}_1^T A \\ \vdots \\ c\vec{e}_i^T A \\ \vdots \\ \vec{e}_n^T A \end{pmatrix}.$$

This is almost A with the one difference being that the ith row has been scaled by c. This proves case 2.

case 3: $cR_i + R_j \to R_j$. Without loss of generality, take $i < j$. Then

$$E = \begin{pmatrix} \vec{e}_1^T \\ \vdots \\ \vec{e}_i^T \\ \vdots \\ c\vec{e}_i^T + \vec{e}_i^T \\ \vdots \\ \vec{e}_n^T \end{pmatrix}$$

and

$$EA = \begin{pmatrix} \vec{e}_1^T A \\ \vdots \\ \vec{e}_i^T A \\ \vdots \\ c\vec{e}_i^T A + \vec{e}_j^T A \\ \vdots \\ \vec{e}_n^T \end{pmatrix}.$$

Once again, since $\vec{e}_k^T A$ is just the kth row of A, it follows that EA is the matrix obtained by applying the row operation $cR_i + R_j \to R_j$ to A. □

Example 3.64. *Let*

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

and let

$$E = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 10 & \end{pmatrix}.$$

Then

$$EA = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 7 & 8 & 9 \\ 4 & 5 & 6 \end{pmatrix}.$$

In light of Theorem 3.63, it is a very simple matter to calculate the inverse of an elementary matrix. Think about it. Suppose E_1 is an elementary matrix of order n. For concreteness, take E_1 to be the elementary matrix associated to the row operation $cR_i + R_j \to R_j$. *Then what is the inverse of* E_1? The answer, of course, is that it must be the elementary matrix associated to the row operation which *undoes* $cR_i + R_j \to R_j$. In this case, the inverse is the elementary matrix E_2 associated to the row operation $-cR_i + R_j \to R_j$. Undoing the single row operation associated to E_1 yields I_n. So by Theorem Theorem 3.63, we have

$$E_2 E_1 = I_n.$$

Corollary 3.53 implies $E_1 = E_2^{-1}$, or equivalently, $E_1^{-1} = E_2$. In this way, we have proved the following:

Corollary 3.65. *Let E_1 be an elementary matrix of order n associated to a row operation X_1. Let X_2 be the row operation which undoes X_1. Then $E_1^{-1} = E_2$, where E_2 is the elementary matrix of order n associated to X_2.*

Example 3.66. *Consider the elementary matrix*

$$E_1 = \begin{pmatrix} 1 & 0 & 5 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

The row operation associated to E_1 is $5R_3 + R_1 \to R_1$. The row operation which undoes this is $-5R_3 + R_1 \to R_1$. Hence, the inverse of E_1 is

$$E_2 = \begin{pmatrix} 1 & 0 & -5 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

By direct calculation, we find $E_1E_2 = E_2E_1 = I_3$.

Example 3.67. *Consider the elementary matrix*

$$E_1 = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}.$$

The row operation associated to E_1 is $R_1 \leftrightarrow R_3$. The row operation which undoes this is again $R_1 \leftrightarrow R_3$. Hence, the inverse of E_1 is itself: $E_2 = E_1$. By direct calculation, we have

$$E_1^2 = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}^2 = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

We conclude this section with the following definition, which turns out to be relevant to the existence of the matrix inverse (as well as the notion of the **determinant** as we will see in Chapter 4):

Definition 3.68. *Two square matrices A and B of order n are said to be* ***row equivalent*** *if there exists a finite number of elementary matrices $E_1, \ldots, E_k$ of order n such that*

$$A = E_1E_2 \cdots E_kB.$$

Of course, using Theorem 3.63, Definition 3.68 simply means that B can be transformed into A via a series of row operations. So what does this have to do with the matrix inverse? Well, lets recall how we compute the inverse of a square matrix A of order n. The first step is to form the augmented matrix

$$A' = \begin{pmatrix} A & I_n \end{pmatrix}.$$

Then we apply the Gauss-Jordan method to A' to transform A' into the following form:

$$\begin{pmatrix} I_n & B \end{pmatrix}.$$

The inverse of A is then B. In other words, the inverse of A exists if and only if A can be transformed into I_n via row operations. We have thus proven the following:

Corollary 3.69. *An $n \times n$ matrix A is invertible if and only if it is row equivalent to I_n.*

3.7. The Trace of a Matrix

In linear algebra, there are two well-known operations which transform a square matrix into a single number. The first, and most important of the two, is the **determinant** (which we will cover in Chapter 4). The second is the **trace** of a matrix. In fact, one can actually use the determinant to compute the trace of a matrix. We will see how part of the story behind this in Chapter 4.

We will not do much with the trace in this book. However, for the sake of completeness, we are going to define it and prove some of its basic properties. Formally, the trace of a matrix is defined as follows:

Definition 3.70. *Let A be a square matrix of order n. The trace of A is then $Tr(A) := \sum_{i=1}^{n} A_{ii}$.*

Example 3.71. *Let*

$$A = \begin{pmatrix} 1 & -4 & 3 \\ 5 & -2 & 0 \\ 4 & 7 & 6 \end{pmatrix}.$$

Then $Tr(A) = 1 + (-2) + 6 = 5$.

Example 3.72. *In the case of the identity matrix I_n, we have $Tr(I_n) = n$.*

Proposition 3.73. *Let A and B be an $n \times n$ matrix and let c be a scalar. Then*

(i) $Tr(cA) = c\,Tr(A)$

(ii) $Tr(A + B) = Tr(A) + Tr(B)$.

(iii) $Tr(AB) = Tr(BA)$.

Proof. We will prove statement (iii) only. Statements (i) and (ii) are left to the reader as a very simple exercise.

From the definition of the trace, we have

$$\begin{aligned}
\mathrm{Tr}(AB) &= \sum_{i=1}^{n} (AB)_{ii} \\
&= \sum_{i=1}^{n} \sum_{k=1}^{n} A_{ik} B_{ki} \\
&= \sum_{i=1}^{n} \sum_{k=1}^{n} B_{ki} A_{ik} \\
&= \sum_{k=1}^{n} \sum_{i=1}^{n} B_{ki} A_{ik} \\
&= \sum_{k=1}^{n} (BA)_{kk} \\
&= \mathrm{Tr}(BA).
\end{aligned}$$

□

Chapter 3 Exercises

1. Let

$$A = \begin{pmatrix} 3 & 1 & 8 \\ 2 & -1 & -2 \end{pmatrix}, \quad B = \begin{pmatrix} -2 & 0 & 5 \\ 9 & 5 & 9 \end{pmatrix}, \quad C = \begin{pmatrix} 10 & 3 & 2 \\ -5 & 1 & 4 \end{pmatrix}.$$

   Compute the following:
   (a) $2A + 5B - C$
   (b) $-B - 4C$
   (c) $-3A + 5B + C$

2. Calculate the sum/difference of matrices
   (a)

$$\begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{pmatrix} - \begin{pmatrix} 4 & 5 & 6 \\ 1 & 2 & 3 \end{pmatrix}$$

   (b)

$$\begin{pmatrix} 1+i & i & 3 \\ -2 & 3+3i & 2-4i \end{pmatrix} + \begin{pmatrix} 0 & 5-i & 1+i \\ 2 & -3i & -4i \end{pmatrix}$$

3. Let

$$A = \begin{pmatrix} 2 & -1 & 0 \\ 1 & 3 & -1 \end{pmatrix}, \qquad B = \begin{pmatrix} 2 & 3 \\ -2 & 5 \end{pmatrix}$$

$$C = \begin{pmatrix} 2 & -1 & 4 \end{pmatrix}, \qquad D = \begin{pmatrix} 2 \\ -4 \end{pmatrix}.$$

   (a) Which of the following matrix multiplications make sense?

$AB,\quad BA,\quad AC,\quad AC^T,\quad BD,\quad CD,\quad DC,\quad D^TA,\quad D^TB,\quad A^TB$

   (b) Compute all the matrix multiplications in (a) whose multiplication is defined.

4. Calculate the product of matrices

   (a)

$$\begin{pmatrix} -2 & 2 & 4 \\ -1 & 6 & 0 \\ 5 & 1 & 7 \end{pmatrix} \begin{pmatrix} 3 & 8 & 2 \\ 4 & -1 & -3 \\ 5 & -2 & -4 \end{pmatrix}$$

   (b)

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^n$$

   (c)

$$\begin{pmatrix} a & 1 & 0 \\ 0 & a & 1 \\ 0 & 0 & a \end{pmatrix}^n$$

5. Let

$$A = \begin{pmatrix} 2+3i & 1 \\ 2 & 5i \end{pmatrix}, \qquad B = \begin{pmatrix} 1 & 1+2i \\ 1-2i & 2 \end{pmatrix}.$$

   (a) Compute AB.
   (b) Compute B^*B.
   (c) Compute B^*A^*.

6. If A is a 2×2 matrix, find all possible A such that

$$A^2 = A$$

7. Suppose A is an $n \times n$ real symmetric matrix such that $A^2 = 0$. Show that $A = 0$.

8. Let A be an $n \times n$ matrix and suppose that A commutes with every $n \times n$ matrix B, that is, $AB = BA$. Show that $A = kI_n$ where k is a scalar.

9. Recall that two matrices A and B are called commutative if $AB = BA$. Let
$$A = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}.$$
Find all matrices which commute with A.

10. Let $\vec{u}_1,\ \vec{u}_2, \ldots,\ \vec{u}_k$ be any set of k orthonormal column vectors in $\mathbb{R}^n$. Let Q be the $n \times k$ matrix whose ith column is $\vec{u}_i$. What is $Q^T Q$?

11. Let A be a square matrix.
    (a) Show that $A + A^T$ is symmetric and $A - A^T$ is skew symmetric.
    (b) Prove that there is one and only one way to write A as the sum of a symmetric matrix and a skew-symmetric matrix.

12. What is the inverse of the following matrix (if it exists):
$$A = \begin{pmatrix} 2 & -1 \\ 3 & 4 \end{pmatrix}.$$

13. Use the Gauss-Jordan method to compute the inverse of the following matrix (if it exists):
$$A = \begin{pmatrix} 1 & -1 & 1 \\ -1 & -1 & 1 \\ 0 & 2 & 4 \end{pmatrix}.$$

14. Use the Gauss-Jordan method to compute the inverse of the following matrix (if it exists):
$$A = \begin{pmatrix} 2 & 2 & 1 \\ 4 & 1 & 0 \\ -2 & 1 & 1 \end{pmatrix}.$$

15. Use the Gauss-Jordan method to compute the inverse of the following matrix (if it exists):
$$A = \begin{pmatrix} 1 & 0 & 1 & -1 \\ 0 & -1 & 2 & 1 \\ 2 & 2 & 0 & 1 \\ 0 & 1 & -1 & 1 \end{pmatrix}.$$

16. Let A be an invertible matrix.
    (a) Prove that the inverse of A^T is the transpose of A^{-1}. In other words, show that
    $$(A^T)^{-1} = (A^{-1})^T.$$
    (Due to this result, one often denotes the inverse of A^T by A^{-T}.)
    (b) Show that if A is also symmetric, then A^{-1} is also symmetric.
    (c) Let n be a positive integer. Prove that the inverse of A^n is $(A^{-1})^n$.

17. Let A be a $n \times n$ matrix. Show that if $A^k = 0$, then $I_n - A$ is invertible. Then find its inverse.

18. Let A, B, and C be $n \times n$ matrices satisfying $\text{Tr}(A+B) = 4$, $\text{Tr}(A+2C) = 3$, and $\text{Tr}(A - B + C) = 1$. Find $\text{Tr}(A)$, $\text{Tr}(B)$, and $\text{Tr}(C)$.

19. Let
    $$A = \begin{pmatrix} 1 & -1 & 1 \\ 0 & 2 & 3 \\ 3 & 1 & -2 \end{pmatrix}.$$
    Let E be an elementary matrix and suppose that
    $$EA = \begin{pmatrix} 1 & -1 & 1 \\ 5 & -3 & 8 \\ 3 & 1 & -2 \end{pmatrix}.$$
    (a) What is E? What elementary row operation does it correspond to?
    (b) What is E^{-1}? What elementary row operation does it correspond to?

20. Consider the following linear system:
    $$\begin{aligned} x_1 + x_3 - x_4 &= 2 \\ -x_2 + 2x_3 + x_4 &= 5 \\ 2x_1 + 2x_2 + x_4 &= -1 \\ x_2 - x_3 + x_4 &= 1 \end{aligned}$$
    (a) Express the above system as a matrix equation of the form $A\vec{x} = \vec{b}$. Specifically, specify A and $\vec{b}$.
    (b) Use your calculation from Problem 15. to solve the above system.

21. Use the matrix inverse to solve the following linear system

$$\begin{aligned} x_1 - x_2 + 2x_3 &= 1 \\ x_1 - 2x_2 &= 1 \\ -x_1 + x_2 + x_3 &= 2 \end{aligned}$$

22. Let I_n denote the $n \times n$ identity matrix. Does there exist a pair of $n \times n$ matrices X and Y such that

$$XY - YX = I_n?$$

If so, find such a pair. If not, then prove that there are no $n \times n$ matrices X and Y satisfying the above relation.

Chapter 4

The Determinant, Eigenvalues, and Eigenvectors

4.1. The Determinant

In Chapter 3, we alluded to the **determinant** as an operation which takes a square matrix and transforms it into a scalar. In this way, the determinant is similar to the trace of a matrix. Like the trace, there is an explicit formula for the determinant. However, the formula for the determinant is much more complicated than that of the trace. Fortunately, one can define the determinant recursively and this turns out to be a good deal simpler than the explicit formula and much more practical from a computational standpoint. We will give an alternate view of the determinant in Chapter 10 which leads to a proof of the equivalence between the recursive definition and the explicit formula for the determinant. We begin with some notation:

Notation 4.1. *Let A be an $n \times n$ matrix. Let $A[i, j]$ be the $(n-1) \times (n-1)$ matrix obtained by deleting the ith row and jth column of A.*

Example 4.2. *Let*

$$A = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix}.$$

Then

$$A[1,3] = \begin{pmatrix} 4 & 5 \\ 7 & 8 \end{pmatrix}, \qquad A[3,2] = \begin{pmatrix} 1 & 3 \\ 4 & 6 \end{pmatrix}.$$

We are now in a position to define the determinant.

Definition 4.3. *Let A be an $n \times n$ matrix whose (i,j)-element is a_{ij}. The determinant of an 1×1 matrix $A = (a_{11})$ is just itself:*

$$\det(A) = a_{11}.$$

For $n \geq 2$, the determinant of an $n \times n$ matrix is

$$\det(A) = \sum_{j=1}^{n} (-1)^{j+1} a_{1j} \det(A[1,j])$$

Definition 4.3 tells us that we can compute the determinant of an $n \times n$ matrix by knowing how to compute the determinant of an $(n-1) \times (n-1)$ matrix. Since the determinant of a 1×1 matrix has been explicitly defined in Definition 4.3, we know how to compute the determinant of a 2×2 matrix which in turn means that we can compute the determinant of a 3×3 matrix and so on and so on. Before we do any examples, it will prove convenient to introduce the following terminology:

Definition 4.4. *Let A be an $n \times n$ matrix.*

1. *The (i,j)-**minor** of A is defined to be*

$$M_{ij} := \det(A[i,j])$$

2. *The (i,j)-**cofactor** is defined to be*

$$C_{ij} = (-1)^{i+j} M_{ij}.$$

We can now express the definition of the determinant a little more concisely using the above terminology:

$$\det(A) = a_{11}M_{11} - a_{12}M_{12} + a_{13}M_{13} - a_{14}M_{14} + \cdots + (-1)^{n+1}M_{1n}$$

and

$$\det(A) = a_{11}C_{11} + a_{12}C_{12} + a_{13}C_{13} + a_{14}C_{14} + \cdots + C_{1n}.$$

Example 4.5. *Consider the* 2×2 *matrix*

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

The determinant of A *is then*

$$\begin{aligned} \det(A) &= a_{11}M_{11} - bM_{12} \\ &= a\det(d) - b\det(c) \\ &= ad - bc. \end{aligned}$$

In other words, to compute the determinant of a 2×2 *matrix, we just cross multiply and take the difference. This is a simple formula that is used repeatedly and is easily memorized.*

Example 4.6. *Consider the* 2×2 *matrix*

$$A = \begin{pmatrix} 1 & -2 \\ 3 & 4 \end{pmatrix}.$$

Then $\det(A) = (1)(4) - (-2)(3) = 4 - (-6) = 10.$

Example 4.7. *Consider the* 3×3 *matrix*

$$A = \begin{pmatrix} 2 & 3 & -1 \\ -1 & 3 & 1 \\ 3 & 1 & -2 \end{pmatrix}.$$

Then

$$\begin{aligned} \det(A) &= a_{11}M_{11} - a_{12}M_{12} + a_{13}M_{13} \\ &= 2\det\begin{pmatrix} 3 & 1 \\ 1 & -2 \end{pmatrix} - 3\det\begin{pmatrix} -1 & 1 \\ 3 & -2 \end{pmatrix} + (-1)\det\begin{pmatrix} -1 & 3 \\ 3 & 1 \end{pmatrix} \\ &= 2(-7) - 3(-1) + (-1)(-10) \\ &= -1. \end{aligned}$$

From the above examples, we see that its not hard to actually compute the determinant, but it does get progressively more tedious to compute it as the size of the matrix increases. Lets try one more example:

Example 4.8. *Consider the* 3×3 *matrix*

$$A = \begin{pmatrix} -1 & 2 & 1 \\ 2 & 5 & 2 \\ 4 & 1 & 1 \end{pmatrix}.$$

Then

$$\begin{aligned} \det(A) &= a_{11}M_{11} - a_{12}M_{12} + a_{13}M_{13} \\ &= (-1)\det\begin{pmatrix} 5 & 2 \\ 1 & 1 \end{pmatrix} - 2\det\begin{pmatrix} 2 & 2 \\ 4 & 1 \end{pmatrix} + (1)\det\begin{pmatrix} 2 & 5 \\ 4 & 1 \end{pmatrix} \\ &= (-1)(3) - 2(-6) + (1)(-18) \\ &= -9. \end{aligned}$$

We conclude this section with the following observation:

Proposition 4.9. $\det(I_n) = 1$.

Proof. We prove this by induction on n. For the $n = 1$ case, $I_n = 1$ and $\det(I_n) = 1$. Now suppose that the result holds for I_n for some $n \geq 1$. Consider the identity matrix of order $n+1$:

$$I_{n+1} = \begin{pmatrix} 1 & 0 \\ \mathbf{0} & I_n \end{pmatrix},$$

where $\mathbf{0}$ is an $n \times 1$ matrix consisting entirely of zeroes. Since the first row of I_{n+1} is entirely zero except for the first element, Definition 4.3 and the induction hypothesis implies

$$\det(I_{n+1}) = 1\det(I_n) = 1(1) = 1.$$

□

4.2. Properties of the Determinant

In this section, we familiarize ourselves with the properties of the determinant. We postpone the proofs for Chapter 10. For the time being, we settle for "proof" by example. The first result is quite useful from a practical standpoint:

Theorem 4.10 (Cofactor Expansion Theorem)**.** *Let* A *be an* $n \times n$ *matrix. Then for any* $i, j \in \{1, \ldots, n\}$

(1) $\det(A) = a_{i1}C_{i1} + a_{i2}C_{i2} + \cdots + a_{in}C_{in}$

(2) $\det(A) = a_{1j}C_{1j} + a_{2j}C_{2j} + \cdots + a_{nj}C_{nj}$

The expression (1) in Theorem 4.10 is called the **cofactor expansion of** $\det(A)$ **along the** i**th row** while (2) is called **cofactor expansion of** $\det(A)$ **along the** j**th column**.

Example 4.11. *Consider the* 3×3 *matrix*

$$A = \begin{pmatrix} -1 & 2 & 1 \\ 2 & 5 & 2 \\ 4 & 1 & 1 \end{pmatrix}.$$

In Example 4.8, we calculated $\det(A) = -9$. *Let's compute the cofactor expansion along the second row and see what happens:*

$$\begin{aligned} \det(A) &= a_{21}C_{21} + a_{22}C_{22} + a_{23}C_{23} \\ &= -(2)\det\begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix} + 5\det\begin{pmatrix} -1 & 1 \\ 4 & 1 \end{pmatrix} - (2)\det\begin{pmatrix} -1 & 2 \\ 4 & 1 \end{pmatrix} \\ &= -2(1) + 5(-5) - (2)(-9) \\ &= -9. \end{aligned}$$

Let's now try a cofactor expansion along the the third column:

$$\begin{aligned} \det(A) &= a_{13}C_{13} + a_{23}C_{23} + a_{33}C_{33} \\ &= (1)\det\begin{pmatrix} 2 & 5 \\ 4 & 1 \end{pmatrix} - 2\det\begin{pmatrix} -1 & 2 \\ 4 & 1 \end{pmatrix} + (1)\det\begin{pmatrix} -1 & 2 \\ 2 & 5 \end{pmatrix} \\ &= (1)(-18) - 2(-9) + (1)(-9) \\ &= -9. \end{aligned}$$

One immediate application of Theorem 4.10 concerns the determinant of **upper triangular matrices**, whose definition is given as follows:

Definition 4.12. *A matrix* A *is said to be* ***upper triangular*** *if it takes the following form:*

$$A = \begin{pmatrix} a_{11} & a_{12} & a_{13} & \cdots & a_{1n} \\ 0 & a_{22} & a_{23} & \cdots & a_{2n} \\ 0 & 0 & a_{33} & \cdots & a_{3n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & a_{nn} \end{pmatrix}.$$

In other words, $A = (a_{ij})$ *is upper triangular if* $a_{ij} = 0$ *whenever* $i > j$. A *is said to be* ***strictly upper triangular*** *if* A *is upper triangular* ***and*** *all of its diagonal elements are zero. In other words,* $a_{ij} = 0$ *whenever* $i \geq j$.

The next result shows that the determinant of an upper triangular matrix is incredibly easy to calculate.

Corollary 4.13. *Let A be an $n \times n$ upper triangular matrix whose (i,j)-element is a_{ij}. Then the determinant of A is the product of its diagonal elements:*

$$\det(A) = a_{11}a_{22}\cdots a_{nn}.$$

Proof. We prove this by induction on n. For $n = 1$, we have $\det(A) = \det(a_{11}) = a_{11}$ by Definition 4.3. Hence, the result holds for $n = 1$. Let us suppose that the result holds for all $n \times n$ upper triangular matrices A for some $n \geq 1$. Let A be an $(n+1) \times (n+1)$ upper triangular matrix:

$$A = \begin{pmatrix} a_{11} & a_{12} & a_{13} & \cdots & a_{1,n+1} \\ 0 & a_{22} & a_{23} & \cdots & a_{2,n+1} \\ 0 & 0 & a_{33} & \cdots & a_{3,n+1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & a_{n+1,n+1} \end{pmatrix}.$$

If we compute $\det(A)$ via cofactor expansion along the first column, we obtain:

$$\begin{aligned} \det(A) &= a_{11}C_{11} \\ &= a_{11} \det \begin{pmatrix} a_{22} & a_{23} & \cdots & a_{2,n+1} \\ 0 & a_{33} & \cdots & a_{3,n+1} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & a_{n+1,n+1} \end{pmatrix} \\ &= a_{11}a_{22}\cdots a_{n+1,n+1}, \end{aligned}$$

where the last equality follows from the induction hypothesis. □

Example 4.14. *Let*

$$A = \begin{pmatrix} 1 & 3 & 4 & -6 \\ 0 & 4 & 2 & 0 \\ 0 & 0 & 2 & 1 \\ 0 & 0 & 0 & 3 \end{pmatrix}.$$

Then $\det(A) = (1)(4)(2)(3) = 24$.

The next result shows how the determinant behaves under row and column operations:

Theorem 4.15. *Let A be an $n \times n$ matrix and let R_i and C_i denote the ith row and column of A respectively.*

*(1) Let A_1 be the matrix obtained from A under $R_i \leftrightarrow R_j$ **or** $C_i \leftrightarrow C_j$ for $i \neq j$. Then $\det(A_1) = -\det(A)$.*
*(2) Let A_2 be the matrix obtained from A under $cR_i \to R_i$ **or** $cC_i \to C_i$ for any scalar c. Then $\det(A_2) = c\det(A)$.*
*(3) Let A_3 be the matrix obtained from A under $cR_i + R_j \to R_j$ **or** $cC_i + C_j \to C_j$ for $i \neq j$. Then $\det(A_3) = \det(A)$.*

Theorem 4.15 now implies the following:

Corollary 4.16. *Let A be an $n \times n$ matrix and let R_i and C_i denote the ith row and column of A respectively.*

*(a) If $R_j = cR_i$ **or** $C_j = cC_i$ for some $i \neq j$ and scalar c, then $\det(A) = 0$.*
(b) $\det(cA) = c^n \det(A)$.

Proof. (a): Suppose that $R_j = cR_i$ for some $i \neq j$. Let A_1 be the matrix whose kth row for $k \neq j$ is equal to R_k and whose jth row is R_i. Then one obtains A from A_1 by scaling the j row of A_1 by c. Statement (2) of Theorem 4.15 implies that

$$\det(A) = c\det(A_1).$$

Since the ith and jth rows of A_1 are equal, swapping these two rows does not alter A_1. Statement (1) of f Theorem 4.15 now implies

$$\det(A_1) = -\det(A_1) \Leftrightarrow \det(A_1) = 0.$$

From this, we conclude that $\det(A) = 0$. The case when $C_j = cC_i$ is proved similarly.

(b): In the matrix cA, all n rows of A have been scaled by c. Statement (2) of Theorem 4.15 applied to $\det(cA)$ n times gives

$$\det(cA) = c^n \det(A).$$

□

Example 4.17. *Let*

$$A = \begin{pmatrix} -1 & 2 & 1 \\ 2 & 5 & 2 \\ 4 & 1 & 1 \end{pmatrix}.$$

From Example 4.8, $\det(A) = -9$. *Let* A_1 *be the matrix obtained from the row operation* $R_1 \leftrightarrow R_3$.

$$A_1 = \begin{pmatrix} 4 & 1 & 1 \\ 2 & 5 & 2 \\ -1 & 2 & 1 \end{pmatrix}.$$

According to Theorem 4.15, we should have $\det(A_1) = 9$. *Lets check this:*

$$\begin{aligned} \det(A_1) &= a_{11}C_{11} + a_{12}C_{12} + a_{13}C_{13} \\ &= (4)\det\begin{pmatrix} 5 & 2 \\ 2 & 1 \end{pmatrix} - (1)\det\begin{pmatrix} 2 & 2 \\ -1 & 1 \end{pmatrix} + (1)\det\begin{pmatrix} 2 & 5 \\ -1 & 2 \end{pmatrix} \\ &= (4)(1) - (1)(4) + (1)(9) \\ &= 9. \end{aligned}$$

Let A_2 *be the matrix obtained from* A *via the column operation* $2C_2 \to C_2$

$$A_2 = \begin{pmatrix} -1 & 4 & 1 \\ 2 & 10 & 2 \\ 4 & 2 & 1 \end{pmatrix}.$$

From Theorem 4.15, we should have $\det(A_2) = -18$. *Lets verify this:*

$$\begin{aligned} \det(A) &= a_{11}C_{11} + a_{12}C_{12} + a_{13}C_{13} \\ &= (-1)\det\begin{pmatrix} 10 & 2 \\ 2 & 1 \end{pmatrix} - 4\det\begin{pmatrix} 2 & 2 \\ 4 & 1 \end{pmatrix} + (1)\det\begin{pmatrix} 2 & 10 \\ 4 & 2 \end{pmatrix} \\ &= (-1)(6) - 4(-6) + (1)(-36) \\ &= -18. \end{aligned}$$

Lastly, let A_3 *be the matrix obtained from* A *by applying the row operation* $R_2 + R_3 \to R_3$:

$$A_3 = \begin{pmatrix} -1 & 2 & 1 \\ 2 & 5 & 2 \\ 6 & 6 & 3 \end{pmatrix}.$$

By Theorem 4.15, there should be no change, that is, $\det(A_3) = \det(A) = -9$. *By direct calculation, we have*

$$\begin{aligned} \det(A) &= a_{11}C_{11} + a_{12}C_{12} + a_{13}C_{13} \\ &= (-1)\det\begin{pmatrix} 5 & 2 \\ 6 & 3 \end{pmatrix} - 2\det\begin{pmatrix} 2 & 2 \\ 6 & 3 \end{pmatrix} + (1)\det\begin{pmatrix} 2 & 5 \\ 6 & 6 \end{pmatrix} \\ &= (-1)(3) - 2(-6) + (1)(-18) \\ &= -9. \end{aligned}$$

Theorem 4.15 also provides an efficient way of computing determinants of larger matrices. Given an $n \times n$ matrix A, the idea is to apply row operations to A to transform A into an upper triangular matrix in such a way that the determinant of the new matrix at each stage is $\det(A)$. Lets consider an example:

Example 4.18. *Let*

$$A = \begin{pmatrix} 7 & 10 & 4 & 6 \\ 1 & 5 & 4 & 3 \\ 5 & 3 & 2 & 5 \\ 7 & 6 & 5 & 7 \end{pmatrix}.$$

1. $-7R_2 + R_1 \to R_1,\ -5R_2 + R_3 \to R_3,\ -7R_2 + R_4 \to R_4$

$$A = \begin{pmatrix} 0 & -25 & -24 & -15 \\ 1 & 5 & 4 & 3 \\ 0 & -22 & -18 & -10 \\ 0 & -29 & -23 & -14 \end{pmatrix}.$$

2. $R_1 \leftrightarrow R_2,\ -R_1 \to R_1$

$$A = \begin{pmatrix} -1 & -5 & -4 & -3 \\ 0 & -25 & -24 & -15 \\ 0 & -22 & -18 & -10 \\ 0 & -29 & -23 & -14 \end{pmatrix}.$$

3. $-22/25R_2 + R_3 \to R_3,\ -29/25R_2 + R_4 \to R_4$

$$A = \begin{pmatrix} -1 & -5 & -4 & -3 \\ 0 & -25 & -24 & -15 \\ 0 & 0 & 78/25 & 16/5 \\ 0 & 0 & 121/25 & 17/5 \end{pmatrix}.$$

4. $-121/78R_3 + R_4 \to R_4$

$$A = \begin{pmatrix} -1 & -5 & -4 & -3 \\ 0 & -25 & -24 & -15 \\ 0 & 0 & 78/25 & 16/5 \\ 0 & 0 & 0 & -61/39 \end{pmatrix}.$$

Using Corollary 4.13, we obtain

$$\det(A) = (-1)(-25)(78/25)(-61/39) = -122.$$

Perhaps the most remarkable property of the determinant is the fact that the determinant is multiplicative:

Theorem 4.19. *Let A and B be $n \times n$ matrices. Then* $\det(AB) = \det(A)\det(B)$.

Example 4.20. *Let*

$$A = \begin{pmatrix} 3 & -1 \\ 1 & 2 \end{pmatrix}, \qquad B = \begin{pmatrix} 2 & 5 \\ 1 & 2 \end{pmatrix}.$$

Then

$$AB = \begin{pmatrix} 3 & -1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} 2 & 5 \\ 1 & 2 \end{pmatrix} = \begin{pmatrix} 5 & 13 \\ 4 & 9 \end{pmatrix}.$$

Hence, $\det(AB) = 45 - 52 = -7$. *On the other hand,*

$$\det(A)\det(B) = (7)(-1) = -7.$$

Example 4.21. *Let*

$$A = \begin{pmatrix} -1 & 2 & 1 \\ 2 & 5 & 2 \\ 4 & 1 & 1 \end{pmatrix}.$$

From Example 4.8, $\det(A) = -9$. *By direct calculation, we have*

$$A^2 = \begin{pmatrix} -1 & 2 & 1 \\ 2 & 5 & 2 \\ 4 & 1 & 1 \end{pmatrix} \begin{pmatrix} -1 & 2 & 1 \\ 2 & 5 & 2 \\ 4 & 1 & 1 \end{pmatrix} = \begin{pmatrix} 9 & 9 & 4 \\ 16 & 31 & 14 \\ 2 & 14 & 7 \end{pmatrix}.$$

Then

$$\begin{aligned} \det(A^2) &= 9\det\begin{pmatrix} 31 & 14 \\ 14 & 7 \end{pmatrix} - 9\det\begin{pmatrix} 16 & 14 \\ 2 & 7 \end{pmatrix} + 4\det\begin{pmatrix} 16 & 31 \\ 2 & 14 \end{pmatrix} \\ &= 9(21) - 9(84) + 4(162) \\ &= 81 \\ &= \det(A)^2. \end{aligned}$$

We conclude this section with the following results:

Proposition 4.22. *Let A be an invertible $n \times n$ matrix. Then* $\det(A^{-1}) = 1/\det(A)$.

Proof. Using the multiplicative property of the determinant, we have

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

From this, we have $\det(A^{-1}) = 1/\det(A)$. □

Theorem 4.23. *Let A be an $n \times n$ matrix. Then* $\det(A^T) = \det(A)$.

Proof. We prove this by induction on n. For $n = 1$, we have $A^T = A$ which immediately gives $\det(A^T) = \det(A)$. So let us suppose that the result holds for $(n-1) \times (n-1)$ matrices for some $n \geq 2$.

Let A be an $n \times n$ matrix and let $B = A^T$ and let b_{ij} denote the (i, j)-element of B. Observe that

$$B[i, j] = A^T[i, j] = A[j, i]^T. \tag{48}$$

Using (48) and the induction hypothesis, we have

$$\begin{aligned} \det(B) &= b_{11}\det(B[1,1]) - b_{12}\det(B[1,2]) + \cdots + (-1)^n b_{1n}\det(B[1,n]) \\ &= a_{11}\det(A[1,1]^T) - a_{21}\det(A[2,1]^T) + \cdots + (-1)^n a_{n1}\det(A[n,1]^T) \\ &= a_{11}\det(A[1,1]) - a_{21}\det(A[2,1]) + \cdots + (-1)^n a_{n1}\det(A[n,1]) \\ &= \det(A), \end{aligned}$$

where we note that the second to last equality is the cofactor expansion of $\det(A)$ along the first column. □

Example 4.24. *Let*

$$A = \begin{pmatrix} -1 & 2 & 1 \\ 2 & 5 & 2 \\ 4 & 1 & 1 \end{pmatrix}.$$

From Example 4.8, $\det(A) = -9$. *The transpose of A is then*

$$A^T = \begin{pmatrix} -1 & 2 & 4 \\ 2 & 5 & 1 \\ 1 & 2 & 1 \end{pmatrix}.$$

Lets compute the transpose of A^T by applying row operations to A^T to bring it to upper triangular form without changing $\det(A^T)$ *in the process. By Theorem 4.23, we should find* $\det(A^T) = -9$.

1. $2R_1 + R_2 \to R_2$, $R_1 + R_3 \to R_3$

$$A^T = \begin{pmatrix} -1 & 2 & 4 \\ 0 & 9 & 9 \\ 0 & 4 & 5 \end{pmatrix}$$

2. $-4/9R_2 + R_3 \to R_3$

$$A^T = \begin{pmatrix} -1 & 2 & 4 \\ 0 & 9 & 9 \\ 0 & 0 & 1 \end{pmatrix}.$$

Hence, $\det(A^T) = (-1)(9)(1) = -9$.

4.3. The Determinant and the Matrix Inverse

Now that we know how to compute the determinant, its well past time to ask the following question: *what does the determinant do?* This is the question that we will answer in this section. We begin with the following definition:

Definition 4.25. *Let A be an $n \times n$ matrix. Let*

$$C_{ij} := (-1)^{i+j} \det(A[i,j])$$

be the (i,j)-cofactor of A. Let C be the $n \times n$ matrix whose (i,j)-element is C_{ij}. C is called the ***cofactor matrix*** *. Let adj$(A) := C^T$. adj(A) is called the* ***adjugate matrix****.*

The first clue that the determinant is linked to the matrix inverse is the following result:

Proposition 4.26. *Let A be an $n \times n$ matrix. Then*

$$A \ adj(A) = adj(A) \ A = \begin{pmatrix} \det(A) & 0 & \cdots & 0 \\ 0 & \det(A) & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \det(A) \end{pmatrix}.$$

Proof. Let $B = A\text{adj}(A)$. For $i = 1, 2, \ldots, n$, we have

$$\begin{aligned}(A\text{adj}(A))_{ii} &= \sum_{k=1}^{n} a_{ik} \left[\text{adj}(A)\right]_{ki} \\ &= \sum_{k=1}^{n} a_{ik} C_{ik} \\ &= \det(A),\end{aligned}$$

since the second equality is just the cofactor expansion of $\det(A)$ along row i.

Let $i, j \in \{1, 2, \ldots, n\}$ with $i \neq j$. Then

$$\begin{aligned}(A\text{adj}(A))_{ij} &= \sum_{k=1}^{n} a_{ik} \left[\text{adj}(A)\right]_{kj} \\ &= \sum_{k=1}^{n} a_{ik} C_{jk} \\ &= \sum_{k=1}^{n} (-1)^{j+k} a_{ik} \det(A[j,k]). \qquad (49)\end{aligned}$$

We now show that the above sum is actually zero. Let R_k denote the kth row of A for $k = 1, 2, \ldots, n$. Let $\widehat{A}$ be the matrix obtained from A by replacing the jth row of A with R_i. Since $\widehat{A}$ has two identical rows, Corollary 4.16 implies that $\det(\widehat{A}) = 0$. Let $\widehat{a}_{kl}$ denote the (k, l)-entry of $\widehat{A}$. Note that

$$\widehat{a}_{kl} = a_{kl} \quad \text{if } k \neq j$$

and

$$\widehat{a}_{jl} = a_{il}.$$

Also, note that

$$\widehat{A}[j, k] = A[j, k].$$

Let us compute the cofactor expansion of $\det(\widehat{A}) = 0$ along the jth row of $\widehat{A}$:

$$\begin{aligned} 0 &= \det(\widehat{A}) \\ &= \sum_{k=1}^{n} (-1)^{j+k} \widehat{a}_{jk} \det(\widehat{A}[j, k]) \\ &= \sum_{k=1}^{n} (-1)^{j+k} a_{ik} \det(A[j, k]). \end{aligned} \tag{50}$$

Comparing (49) with (50), we conclude that $(A\mathrm{adj}(A))_{ij} = 0$ for $i \neq j$. Hence, $A\mathrm{adj}(A)$ is a diagonal matrix whose diagonal elements are all equal to $\det(A)$.

The proof that $\mathrm{adj}(A)\, A$ is also a diagonal matrix whose diagonal elements are all equal to $\det(A)$ is extremely similar to the above proof. We leave the minor modifications to the above proof to the reader. □

Exercise 4.27. *Modify the proof of Proposition 4.26 to show that* $\mathrm{adj}(A)\, A$ *is a diagonal matrix whose diagonal elements are all equal to* $\det(A)$.

The following result provides an answer to the question posed at the beginning of this section:

Theorem 4.28. *Let A be an $n \times n$ matrix. Then A^{-1} exists if and only if* $\det(A) \neq 0$. *Moreover, if A^{-1} exists, then*

$$A^{-1} = \frac{1}{\det(A)} \mathrm{adj}(A).$$

Proof. Suppose A^{-1} exists, then using Theorem 4.19 and Proposition 4.9, we have

$$1 = \det(I_n) = \det(AA^{-1}) = \det(A)\det(A^{-1}), \tag{51}$$

which implies that $\det(A) \neq 0$.

Now suppose that $\det(A) \neq 0$. Let

$$B = \frac{1}{\det(A)}\text{adj}(A).$$

Proposition 4.26 now implies

$$\begin{aligned} AB &= \frac{1}{\det(A)}A\text{adj}(A) \\ &= \frac{1}{\det(A)}\begin{pmatrix} \det(A) & 0 & \cdots & 0 \\ 0 & \det(A) & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \det(A) \end{pmatrix} \\ &= \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix}. \end{aligned}$$

From this, we conclude that $A^{-1} = B$. □

Example 4.29. *Let*

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

In Proposition 3.55, we introduced the formula for the inverse of a 2×2 *matrix. Lets derive that formula using the more general result of Theorem 4.28.*

First, lets compute the cofactor matrix:

$$C_{11} = d, \quad C_{12} = -c, \quad C_{21} = -b, \quad C_{22} = a$$

Hence, the adjugate matrix is

$$adj(A) = C^T = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

The inverse of A *is then*

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

Example 4.30. *Let*

$$A = \begin{pmatrix} -1 & 2 & 1 \\ 2 & -1 & 2 \\ 0 & 1 & 2 \end{pmatrix}.$$

Lets calculate the adjugate of A *and then the inverse (if it exists).*

To calculate adj(A), we first need to calculate the cofactor matrix:

$$C = \begin{pmatrix} -4 & -4 & 2 \\ -3 & -2 & 1 \\ 5 & 4 & -3 \end{pmatrix}.$$

The adjugate of A is then

$$\operatorname{adj}(A) = C^T = \begin{pmatrix} -4 & -3 & 5 \\ -4 & -2 & 4 \\ 2 & 1 & -3 \end{pmatrix}.$$

Taking a cofactor expansion along column 1, we compute the determinant of A:

$$\det(A) = (-1)\det(A[1,1]) - 2\det(A[2,1]) = (-1)(-4) - 2(3) = -2.$$

Hence, the inverse of A exists. By Theorem 4.28, we have

$$A^{-1} = \begin{pmatrix} 2 & 3/2 & -5/2 \\ 2 & 1 & -2 \\ -1 & -1/2 & 3/2 \end{pmatrix}$$

We conclude this section with **Cramer's rule**.

Corollary 4.31 (Cramer's rule)**.** *Let A be an $n \times n$ invertible matrix and let $\vec{b} \in \mathbb{R}^n$ be any column vector. Let B_i be the matrix obtained from A by replacing the ith column of A with $\vec{b}$. Then the unique solution to $A\vec{x} = \vec{b}$ is given by*

$$x_i = \frac{\det(B_i)}{\det(A)}$$

where x_i is the ith component of $\vec{x}$ for $i = 1, 2, \ldots, n$.

Proof. Since A^{-1} exists, we have

$$\vec{x} = A^{-1}\vec{b}.$$

By Theorem 4.28,

$$A^{-1} = \frac{1}{\det(A)}\operatorname{adj}(A) = \frac{1}{\det(A)}C^T,$$

where C is the cofactor matrix. From this, it follows that the ith component of $\vec{x}$ is

$$x_i = \frac{1}{\det(A)}\sum_{k=1}^{n}(C^T)_{ik}b_k = \frac{1}{\det(A)}\sum_{k=1}^{n} b_k C_{ki} = \frac{1}{\det(A)}\sum_{k=1}^{n}(-1)^{k+i} b_k \det(A[k,i]). \tag{52}$$

Let B_i be the matrix obtained from A by replacing the ith column of A with $\vec{b}_i$. Then

$$B_i[k,i] = A[k,i].$$

Hence, (52) can be rewritten as

$$x_i = \frac{1}{\det(A)} \sum_{k=1}^{n} (-1)^{k+i} b_k \det(B_i[k,i]) \tag{53}$$

However, the summation appearing in (53) is simply the cofactor expansion of the determinant of B_i along column i. Hence,

$$x_i = \frac{\det(B_i)}{\det(A)}. \tag{54}$$

□

Example 4.32. *Consider the matrix equation $A\vec{x} = \vec{b}$, where*

$$A = \begin{pmatrix} 2 & -1 \\ 3 & 5 \end{pmatrix}$$

and

$$\vec{b} = \begin{pmatrix} 3 \\ -5 \end{pmatrix}.$$

To solve this system using Cramer's rule, we form the matrices

$$B_1 = \begin{pmatrix} 3 & -1 \\ -5 & 5 \end{pmatrix}, \qquad B_2 = \begin{pmatrix} 2 & 3 \\ 3 & -5 \end{pmatrix}.$$

From Cramer's rule, we have

$$x_1 = \frac{\det(B_1)}{\det(A)} = \frac{10}{13}, \qquad x_1 = \frac{\det(B_2)}{\det(A)} = \frac{-19}{13}.$$

4.4. Linear Transformations

The idea of a **linear transformation** is essentially the model or prototype for the general notion of a **linear map** (or **linear homomorphism**) which we will introduce in Chapter 5. In what follows, all vectors in $\mathbb{R}^n$ and $\mathbb{C}^n$ are always expressed as column vectors unless stated otherwise.

Definition 4.33. *Let A be an $m \times n$ matrix.*

(i) If A is a real matrix, then associated to A is the map

$$T_A : \mathbb{R}^n \to \mathbb{R}^m$$

given by $T_A(\vec{v}) := A\vec{v}$ for $\vec{v} \in \mathbb{R}^n$.

(ii) If A is a complex matrix, then associated to A is the map

$$T_A : \mathbb{C}^n \to \mathbb{C}^m$$

given by $T_A(\vec{v}) := A\vec{v}$ for $\vec{v} \in \mathbb{C}^n$.

The map T_A is called a ***linear transformation*** *associated to A.*

For the sake of simplicity, we will assume all matrices to be real unless stated otherwise. All of the results we discuss in this section apply equally well to linear transformations associated to complex matrices.

Proposition 4.34. *Let A be an $m \times n$ matrix. Then the linear transformation $T_A : \mathbb{R}^n \to \mathbb{R}^m$ satisfies the following properties:*

(i) $T_A(c\vec{v}) = cT_A(\vec{v})$

(ii) $T_A(\vec{v} + \vec{u}) = T_A(\vec{v}) + T_A(\vec{u})$

for all $c \in \mathbb{R}$, $\vec{v}, \vec{u} \in \mathbb{R}^n$. Moreover, if B is a $p \times m$ matrix, then $T_B \circ T_A = T_{BA}$.

Proof. Properties (i) and (ii) follow immediately from the basic properties of matrix multiplication that were discussed in Chapter 3. For the last property, let $\vec{v} \in \mathbb{R}^n$. Then

$$\begin{aligned} T_B \circ T_A(\vec{v}) &= T_B(A\vec{v}) \\ &= B(A\vec{v}) \\ &= (BA)\vec{v} \\ &= T_{BA}(\vec{v}). \end{aligned}$$

Hence, $T_B \circ T_A = T_{BA}$. ☐

From Definition 4.33, an $m \times n$ matrix A acts naturally as a map from $\mathbb{R}^n$ to $\mathbb{R}^m$. At this point, we are going to consider a few very simple transformations from $\mathbb{R}^2$ to itself.

I. Reflections

Lets find a matrix A whose linear transformation maps a vector $\vec{v} \in \mathbb{R}^2$ to its reflection across the x-axis (see Figure 1). This type of linear transformation is called a **reflection across the x-axis**. More precisely, given a vector

$$\vec{v} = \begin{pmatrix} a \\ b \end{pmatrix},$$

we seek a matrix A such that

$$A\vec{v} = \begin{pmatrix} a \\ -b \end{pmatrix}$$

This is very easy. Its quite clear that the matrix which accomplishes this is

$$A = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Likewise, to reflect a matrix across the y-axis, we use the matrix

$$B = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}.$$

The linear transformation associated to B sends $\vec{v}$ to

$$\vec{v} = \begin{pmatrix} -a \\ b \end{pmatrix}.$$

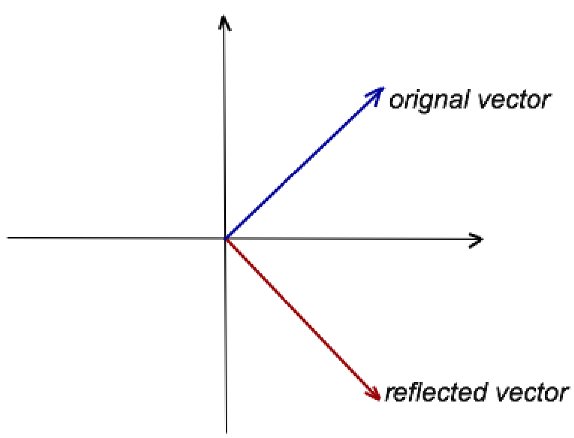


Figure 1. Reflection of a vector across the x-axis

II. Contractions\Dilations

Given a vector $\vec{v} \in \mathbb{R}^n$ and a scalar $r > 0$, we seek a linear transformation which simply sends $\vec{v}$ to $r\vec{v}$. Of course, the matrix which accomplishes this is

$$rI_n.$$

If $0 < r < 1$, then the associated linear transformation is called a **contraction**. If $r > 1$, then the linear transformation is called a **dilation**.

III. Rotations

Given a vector $\vec{v} \in \mathbb{R}^2$, we seek a linear transformation T_A which rotates $\vec{v}$ by an angle θ without changing its length. Lets find the matrix A which accomplishes this. Let

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

Let $\vec{v} = (v_1, v_2)^T$. Then the transformed vector is

$$T_A(\vec{v}) = A\vec{v} = \begin{pmatrix} av_1 + bv_2 \\ cv_1 + dv_2 \end{pmatrix}.$$

This vector should satisfy two conditions. The first is that its length or norm is the same as $\vec{v}$. Hence, we require

$$\|A\vec{v}\|^2 = \|\vec{v}\|^2 .$$

If we expand the above equation, we have

$$(a^2 + c^2)v_1^2 + 2(ab + cd)v_1v_2 + (b^2 + d^2)v_2^2 = v_1^2 + v_2^2.$$

The above equation must hold for all vectors $\vec{v} \in \mathbb{R}^2$. Hence, by replacing $\vec{v}$ with $(1, 0)^T$ and $(0, 1)^T$, we arrive at the following identities:

$$a^2 + c^2 = b^2 + d^2 = 1.$$

This in turn implies that

$$ab + cd = 0.$$

The second requirement is that the angle between $A\vec{v}$ and $\vec{v}$ must be θ. Hence, we require

$$(A\vec{v}) \cdot \vec{v} = \|A\vec{v}\| \|\vec{v}\| \cos\theta = \|\vec{v}\|^2 \cos\theta.$$

Expanding the above equation gives

$$av_1^2 + (b + c)v_1v_2 + dv_2^2 = v_1^2 \cos\theta + v_2^2 \cos\theta.$$

Once again, this must hold for all vectors in $\mathbb{R}^2$. By substituting $\vec{v} = (1, 0)^T$ and $\vec{v} = (0, 1)^T$, we arrive at the following identities:

$$a = d = \cos\theta.$$

Combining this with the above identities implies $b = -c$ and one of the following possibilities:

$$b = -\sin\theta, \quad c = \sin\theta, \qquad \textbf{or} \qquad b = \sin\theta, \quad c = -\sin\theta$$

The matrix which does not alter the length of $\vec{v}$ and gives a **counterclockwise** rotation for $\theta > 0$ is

$$A_\theta := \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}.$$

Using the other choice for b and c would not have altered the length of $\vec{v}$ also, but would have given a **clockwise** rotation for $\theta > 0$.

Example 4.35. *Let us find a matrix A for a linear transformation from $\mathbb{R}^2$ to itself which first reflects a vector across the x-axis, then rotates it by $30°$, and finally scales it by a factor of 2.*

Let us consider the respective matrices which accomplishes each transformation.

For the reflection, we take

$$A_1 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

For the rotation, we take $\theta = \pi/6$ and the rotation matrix is

$$A_\theta = \begin{pmatrix} \cos(\pi/6) & -\sin(\pi/6) \\ \sin(\pi/6) & \cos(\pi/6) \end{pmatrix} = \begin{pmatrix} \sqrt{3}/2 & -1/2 \\ 1/2 & \sqrt{3}/2 \end{pmatrix}.$$

For the dilation by a factor of 2, the corresponding matrix is

$$2I_2 = \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}.$$

Hence, the desired linear transformation is

$$T_A = T_{2I_2} T_{A_\theta} T_{A_1} = T_{2I_2 A_\theta A_1} = T_{2A_\theta A_1},$$

where

$$A = 2A_\theta A_1 = 2\begin{pmatrix} \sqrt{3}/2 & -1/2 \\ 1/2 & \sqrt{3}/2 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} \sqrt{3} & 1 \\ 1 & -\sqrt{3} \end{pmatrix}.$$

Exercise 4.36. *Let A_θ be matrix associated to the linear transformation which rotates a vector by $20°$ without changing its length. Calculate $(A_\theta)^9$. (Hint: think geometrically.)*

Example 4.37. *Let θ_1 and θ_2 be two angles and let A_{θ_1} and A_{θ_2} be the matrices associated to the linear transformations which rotate vectors by an angle of θ_1 and θ_2 respectively without altering their norms. Of course, if one applies these linear transformations one after the other, we obtain a rotation of $\theta_1 + \theta_2$. This implies that*

$$A_{\theta_1+\theta_2} = A_{\theta_1} A_{\theta_2} = A_{\theta_2} A_{\theta_1}.$$

Using the formula for the rotation matrix, we have

$$\begin{aligned} &\begin{pmatrix} \cos(\theta_1+\theta_2) & -\sin(\theta_1+\theta_2) \\ \sin(\theta_1+\theta_2) & \cos(\theta_1+\theta_2) \end{pmatrix} \\ &= \begin{pmatrix} \cos(\theta_1) & -\sin(\theta_1) \\ \sin(\theta_1) & \cos(\theta_1) \end{pmatrix} \begin{pmatrix} \cos(\theta_2) & -\sin(\theta_2) \\ \sin(\theta_2) & \cos(\theta_2) \end{pmatrix}. \end{aligned}$$

Comparing the matrix entries on the left and right gives the following trigonometric identities:

$$\begin{aligned} \cos(\theta_1+\theta_2) &= \cos(\theta_1)\cos(\theta_2) - \sin(\theta_1)\sin(\theta_2) \\ \sin(\theta_1+\theta_2) &= \sin(\theta_1)\cos(\theta_2) + \cos(\theta_1)\sin(\theta_2). \end{aligned}$$

The matrix

$$A_\theta := \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$$

which rotates a vector by an angle θ without changing its length satisfies the following condition:

$$\begin{aligned} A_\theta^T A_\theta &= \begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{pmatrix} \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} \\ &= \begin{pmatrix} \cos^2\theta + \sin^2\theta & -\cos\theta\sin\theta + \cos\theta\sin\theta \\ -\cos\theta\sin\theta + \cos\theta\sin\theta & \cos^2\theta + \sin^2\theta \end{pmatrix} \\ &= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}. \end{aligned}$$

Likewise, $A_\theta A_\theta^T = I_2$. Hence, $A_\theta^{-1} = A_\theta^T$. This observation leads us naturally to the next definition:

Definition 4.38. *Let A be a real $n \times n$ matrix. A is called an **orthogonal matrix** if $A^{-1} = A^T$.*

Theorem 4.39. *Let A be an $n \times n$ matrix. Then A is an orthogonal matrix if and only if the columns of A form an orthonormal basis on $\mathbb{R}^n$.*

Proof. Let $\vec{a}_i$ denote the ith column of A. Then the (i,j)-element of A^TA is

$$(A^TA)_{ij} = \vec{a}_i^T\vec{a}_j = \vec{a}_i \cdot \vec{a}_j. \tag{55}$$

If A is an orthogonal matrix, then (55) implies

$$\vec{a}_i \cdot \vec{a}_j = \begin{cases} 1 & \text{if } i = j \\ 0 & \text{if } i \neq j \end{cases}. \tag{56}$$

This in turn implies that $\{\vec{a}_1, \vec{a}_2, \ldots, \vec{a}_n\}$ is an orthonormal basis on $\mathbb{R}^n$.

On other hand, if $\{\vec{a}_1, \vec{a}_2, \ldots, \vec{a}_n\}$ is an orthonormal basis on $\mathbb{R}^n$, then (55) implies that $A^TA = I_n$. Corollary 3.53 mplies that $(A^T)^{-1} = A$ which in turn implies that $A^{-1} = A^T$. □

Here is the complex version of Definition 4.38:

Definition 4.40. *Let A be a complex $n \times n$ matrix. A is called a **unitary matrix** if $A^{-1} = A^*$.*

Here is the complex version of Theorem 4.39:

Theorem 4.41. *Let A be an $n \times n$ matrix. Let $\{\vec{a}_1, \vec{a}_2, \ldots, \vec{a}_n\}$ be the columns of A. Then A is a unitary matrix if and only if*

$$(\vec{a}_i)^*\vec{a}_j = \begin{cases} 1 & \text{if } i = j \\ 0 & \text{if } i \neq j \end{cases}. \tag{57}$$

for all $i, j = 1, 2, \ldots, n$.

Proof. The proof of Theorem 4.41 is very similar to Theorem 4.39. Essentially one simply swaps out the ordinary transpose in the proof of Theorem 4.39 and the proof still works as before. □

Example 4.42. *The matrix*

$$A = \begin{pmatrix} \sqrt{3}/3 & \sqrt{6}/3 & 0 \\ -\sqrt{3}/3 & \sqrt{6}/6 & \sqrt{2}/2 \\ \sqrt{3}/3 & -\sqrt{6}/6 & \sqrt{2}/2 \end{pmatrix}$$

is orthogonal.

Example 4.43. *The matrix*

$$A = \begin{pmatrix} \frac{1+i}{\sqrt{3}} & -\frac{(1+i)}{\sqrt{6}} \\ \frac{1}{\sqrt{3}} & \sqrt{\frac{2}{3}} \end{pmatrix}$$

is unitary.

4.5. Eigenvalues and Eigenvectors

In this section, we introduce the idea of **eigenvalues** and **eigenvectors** which appear in such areas as ordinary differential equations and quantum mechanics. Here is the formal definition:

Definition 4.44. *Let A be a real (complex) $n \times n$ matrix. An **eigenvector** of A is a nonzero vector $\vec{v} \in \mathbb{R}^n$ ($\vec{v} \in \mathbb{C}^n$) which satisfies an equation of the form*

$$A\vec{v} = \lambda\vec{v} \tag{58}$$

for some scalar $\lambda \in \mathbb{R}$ ($\lambda \in \mathbb{C}$).

*The scalar λ appearing in (58) is called an **eigenvalue** of A. To be more precise, the nonzero vector $\vec{v}$ in (58) is called an **eigenvector of** A **associated to the eigenvalue** λ.*

Given the above definition, the following question is quite natural: *How does one go about finding these eigenvalues and eigenvectors*? The following definition will prove key to this question:

Definition 4.45. *Let A be an $n \times n$ matrix. The **characteristic polynomial** of A is the degree n monic polynomial*

$$p_A(x) := \det(xI_n - A).$$

Here is the relevance of this definition to our question:

Theorem 4.46. *Let A be an $n \times n$ matrix. The eigenvalues of A are precisely the roots or zeroes of its characteristic polynomial.*

Proof. Let λ be an eigenvalue of A. By definition, there exists a nonzero vector $\vec{v}$ such that $A\vec{v} = \lambda v$. This equation can be rewritten as

$$(\lambda I_n - A)\vec{v} = \vec{0}.$$

Since $\vec{v} \neq \vec{0}$, it follows that the columns of $A - \lambda I_n$ are linearly dependent. Theorem 3.51 now implies that the inverse of $\lambda I_n - A$ does not exist. From Theorem 4.28, we conclude that

$$p_A(\lambda) := \det(\lambda I_n - A) = 0. \tag{59}$$

Hence, λ is a root of $p_A(x)$.

On the other hand, suppose λ is a root of $p_A(x)$. Then $p_A(\lambda) = \det(\lambda I_n - A) = 0$. By Theorem 4.28, $\lambda I_n - A$ is not invertible. This implies that the columns of $\lambda I_n - A$ are linearly dependent by Theorem 3.51. Hence, there must be some nonzero $\vec{v}$ for which $(\lambda I_n - A)\vec{v} = \vec{0}$. This implies that $\vec{v}$ is an eigenvector of A. Hence, λ is an eigenvalue of A. □

Before we consider some examples, we introduce the following related definition:

Definition 4.47. *Let A be an $n \times n$ matrix and let λ be an eigenvalue of A. Define E_λ to be the set of* ***all*** *vectors $\vec{v}$ satisfying $A\vec{v} = \lambda\vec{v}$. E_λ is called the* ***eigenspace*** *of A associated to λ.*

Note that $\vec{0}$ (which is not an eigenvector) also belongs to E_λ since $A\vec{0} = \vec{0} = \lambda\vec{0}$.

Exercise 4.48. *Show that E_λ is a subspace.*

Example 4.49. *Let*

$$A = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}.$$

Lets find all the eigenvalues and the corresponding eigenspaces for each eigenvalue.

By definition, the characteristic polynomial is given by

$$\begin{aligned} p_A(x) &= \det(xI_2 - A) \\ &= \det \begin{pmatrix} x-1 & -2 \\ -2 & x-1 \end{pmatrix} \\ &= (x-1)^2 - 4 \\ &= x^2 - 2x - 3 \\ &= (x+1)(x-3). \end{aligned}$$

Hence, the eigenvalues of A are -1 and 3. To find E_{-1}, we have to solve the matrix equation

$$A\vec{v} = -\vec{v}.$$

We can rewrite this equation as

$$(A + I_2)\vec{v} = \begin{pmatrix} 2 & 2 \\ 2 & 2 \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}.$$

The above matrix equation is just a homogeneous linear system of two equations in two variables. The general solution to this system is clearly

$$E_{-1} = \{(a, -a)^T \mid a \in \mathbb{R}\}.$$

For E_3, we solve the matrix equation

$$(A - 3I_2)\vec{v} = \begin{pmatrix} -2 & 2 \\ 2 & -2 \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}.$$

The general solution is clearly

$$E_3 = \{(a, a)^T \mid a \in \mathbb{R}\}.$$

Example 4.50.

$$A = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

Lets find all the eigenvalues and the corresponding eigenspaces for each eigenvalue.

The characteristic polynomial is

$$p_A(x) = \det(xI_2 - A) = \det \begin{pmatrix} x & -1 \\ 1 & x \end{pmatrix} = x^2 + 1.$$

If we regard A strictly as a real matrix, then A has no eigenvalues and we are done.

However, since $\mathbb{R} \subset \mathbb{C}$, we can make things more interesting by viewing A as a complex matrix. The roots of $p_A(x)$ are then i and $-i$.

To find E_i, we solve the matrix equation:

$$(A - iI_2)\vec{v} = \begin{pmatrix} -i & 1 \\ -1 & -i \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix},$$

where $a, b \in \mathbb{C}$ now. From this, we conclude that

$$E_i = \{(iz, -z)^T \mid z \in \mathbb{C}\}.$$

For E_{-i}, we solve

$$(A + iI_2)\vec{v} = \begin{pmatrix} i & 1 \\ -1 & i \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$$

and obtain

$$E_{-i} = \{(iz, z)^T \mid z \in \mathbb{C}\}.$$

Example 4.51. *Let*

$$A = \begin{pmatrix} 7/2 & 1/2 & -1 \\ 1/2 & 7/2 & 1 \\ -3/2 & -1/2 & 3 \end{pmatrix}.$$

The characteristic polynomial of A *is*

$$\begin{aligned} p_A(x) &= \det(xI_3 - A) \\ &= \det \begin{pmatrix} x - 7/2 & -1/2 & 1 \\ -1/2 & x - 7/2 & -1 \\ 3/2 & 1/2 & x - 3 \end{pmatrix} \\ &= (x - 7/2)((x - 7/2)(x - 3) + 1/2) + 1/2(-1/2(x - 3) + 3/2) \\ &+ (-1/4 - 3/2(x - 7/2)) \\ &= x^3 - 10x^2 + 32x - 32 \\ &= (x - 4)^2(x - 2). \end{aligned}$$

Hence, the eigenvalues of A *are* 4 *and* 2*. Lets find a basis for* E_4 *and* E_2*. For* E_4*, we consider the matrix equation*

$$(A - 4I_3)\vec{v} = \begin{pmatrix} -1/2 & 1/2 & -1 \\ 1/2 & -1/2 & 1 \\ -3/2 & -1/2 & -5 \end{pmatrix} \begin{pmatrix} a \\ b \\ c \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}.$$

Using Gauss-Jordan, we find a general solution

$$E_4 = \{(-3r, -r, r)^T \mid r \in \mathbb{R}\}.$$

Hence, a basis for E_4 *is* $\{(-3, -1, 1)^T\}$*. For* E_2*, we consider the matrix equation*

$$(A - 2I_3)\vec{v} = \begin{pmatrix} 3/2 & 1/2 & -1 \\ 1/2 & 3/2 & 1 \\ -3/2 & -1/2 & 1 \end{pmatrix} \begin{pmatrix} a \\ b \\ c \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}.$$

In this case, $E_2 = \{(r, -r, r)^T \mid r \in \mathbb{R}\}$*. Hence, a basis for* E_2 *is* $\{(1, -1, 1)^T\}$.

Example 4.52. *Here is a small application of eigenvectors and eigenvalues. Consider the first order system of ordinary differential equations.*

$$x_1(t) + 2x_2(t) = x_1'(t)$$
$$2x_1(t) + x_2(t) = x_2'(t).$$

The first thing we can do here is rewrite the above system as a (differential) matrix equation:

$$\begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} \begin{pmatrix} x_1(t) \\ x_2(t) \end{pmatrix} = \begin{pmatrix} x_1'(t) \\ x_2'(t) \end{pmatrix}.$$

One way to make progress with differential equations is to ***guess*** *the form of the solution and see where it leads. In this case, we guess*

$$x_1(t) = ae^{\lambda t}, \qquad x_2(t) = be^{\lambda t},$$

Substituting this into the above matrix equation and simplifying gives

$$\begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix} = \lambda \begin{pmatrix} a \\ b \end{pmatrix}.$$

In other words, finding a solution to the above first order system amounts to finding an eigenvalue and eigenvector of the matrix

$$A = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}.$$

We calculated the eigenvalues and eigenspaces of this matrix in Example 4.49. Using the calculation from Example 4.49, we obtain two sets of solutions (one for each eigenvalue):

$$x_1(t) = C_1 e^{-t}, \qquad x_2(t) = -C_1 e^{-t}$$

and

$$x_1(t) = C_2 e^{3t}, \qquad x_2(t) = C_2 e^{3t},$$

for any $C_1, C_2 \in \mathbb{R}$. With a little bit of thought, it becomes clear that we can simply add the two sets of solutions together to produce a more general solution:

$$x_1(t) = C_1 e^{-t} + C_2 e^{3t}, \qquad x_2(t) = -C_1 e^{-t} + C_2 e^{3t}$$

We conclude this section by introducing an important idea which we will make use of in the next section.

Definition 4.53. *Let A and B be $n \times n$ matrices. A and B are* ***similar matrices*** *if there exists an invertible matrix P such that*

$$B = P^{-1}AP.$$

The significance of similar matrices is summarized by the following result:

Theorem 4.54. *Let A and B be similar $n \times n$ matrices. Let P be the matrix relating A and B, that is, $B = P^{-1}AP$. Then*

(i) $\mathit{Tr}(A) = \mathit{Tr}(B)$
(ii) $\det(A) = \det(B)$
(iii) $p_A(x) = p_B(x)$. *In particular, A and B have the same eigenvalues.*
(iv) If λ is an eigenvalue of A (and hence of B) and $\vec{v}$ is an eigenvector of A associated to λ, then $P^{-1}\vec{v}$ is an eigenvector of B associated to λ.

Proof. (i): Using Proposition 3.73, we have

$$\begin{aligned}\mathrm{Tr}(B) &= \mathrm{Tr}(P^{-1}AP)\\ &= \mathrm{Tr}(APP^{-1})\\ &= \mathrm{Tr}(A).\end{aligned}$$

(ii): Using the multiplicative property of the determinant, we have

$$\begin{aligned}\det(B) &= \det(P^{-1}AP)\\ &= \det(P^{-1})\det(A)\det(P)\\ &= \frac{1}{\det(P)}\det(A)\det(P)\\ &= \det(A),\end{aligned}$$

where the third equality follows from Proposition 4.22.

(iii): From the definition of the characteristic polynomial, we have

$$\begin{aligned}p_B(x) &= \det(xI_n - B)\\ &= \det(xI_n - P^{-1}AP)\\ &= \det(P^{-1}(xI_n)P - P^{-1}AP)\\ &= \det(P^{-1}(xI_n - A)P)\\ &= \det(P^{-1})\det(xI_n - A)\det(P)\\ &= \det(xI_n - A)\\ &= p_A(x).\end{aligned}$$

(iv): Suppose $A\vec{v} = \lambda\vec{v}$. Then

$$\begin{aligned}B(P^{-1}\vec{v}) &= (P^{-1}AP)(P^{-1}\vec{v})\\ &= P^{-1}A\vec{v}\\ &= P^{-1}(\lambda\vec{v})\\ &= \lambda P^{-1}\vec{v}.\end{aligned}$$

Hence, $P^{-1}\vec{v}$ is an eigenvector of B associated to λ. $\square$

4.6. Diagonalizable Matrices

We begin this section by collecting some elementary facts about diagonal matrices:

Proposition 4.55. *Let D be an $n \times n$ diagonal matrix with diagonal elements $D_{ii} := \lambda_i$ for $i = 1, 2, \ldots, n$.*

(i) $p_D(x) = (x - \lambda_1)(x - \lambda_2)\cdots(x - \lambda_n)$.

(ii) The eigenvalues of D are $\lambda_1, \lambda_2, \ldots, \lambda_n$.

(iii) $D\vec{e}_i = \lambda_i \vec{e}_i$ where $\vec{e}_i$ is the ith standard basis vector.

Proof. (i): By definition,

$$\begin{aligned} p_D(x) &:= \det(xI_n - D) \\ &= \det \begin{pmatrix} x - \lambda_1 & 0 & \cdots & 0 \\ 0 & x - \lambda_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & x - \lambda_n \end{pmatrix} \\ &= (x - \lambda_1)(x - \lambda_2)\cdots(x - \lambda_n), \end{aligned}$$

where the last equality follows from Corollary 4.13.

(ii): This follows immediately from (i).

(iii): Immediate. $\square$

Here is the main definition for this section:

Definition 4.56. *Let A be an $n \times n$ matrix. A is called a* ***diagonalizable*** *matrix if it is similar to a diagonal matrix, that is, $P^{-1}AP = D$ for some diagonal matrix D and some invertible matrix P.*

The following result provides one answer to the question of when a matrix is diagonalizable.

Theorem 4.57. *Let A be a real (complex) $n \times n$ matrix. Let P be an $n \times n$ invertible matrix and let $\vec{p}_i$ be the ith column of P.*

(i) $P^{-1}AP$ is a diagonal matrix if and only if $\vec{p}_i$ is an eigenvector of A for $i = 1, 2, \ldots, n$. In other words, A is diagonalizable if and only if there exists a basis of $\mathbb{R}^n$ ($\mathbb{C}^n$) such that each basis vector is an eigenvector of A.

(ii) If $P^{-1}AP$ is a diagonal matrix whose ith diagonal element is λ_i, then $A\vec{p}_i = \lambda_i \vec{p}_i$.

Proof. (i) and (ii): Suppose

$$P^{-1}AP = D = \begin{pmatrix} \lambda_1 & 0 & \cdots & 0 \\ 0 & \lambda_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \lambda_n \end{pmatrix}. \tag{60}$$

Let $\{\vec{e}_1, \vec{e}_2, \ldots, \vec{e}_n\}$ denote the standard basis. Then D can be rewritten as

$$D = \begin{pmatrix} \lambda_1 \vec{e}_1 & \lambda_2 \vec{e}_2 & \cdots & \lambda_n \vec{e}_n \end{pmatrix}.$$

Multiplying both sides of (60) by P gives

$$\begin{aligned} AP &= PD \\ \begin{pmatrix} A\vec{p}_1 & A\vec{p}_2 & \cdots & A\vec{p}_n \end{pmatrix} &= \begin{pmatrix} \lambda_1 P\vec{e}_1 & \lambda_2 P\vec{e}_2 & \cdots & \lambda_n P\vec{e}_n \end{pmatrix} \\ \begin{pmatrix} A\vec{p}_1 & A\vec{p}_2 & \cdots & A\vec{p}_n \end{pmatrix} &= \begin{pmatrix} \lambda_1 \vec{p}_1 & \lambda_2 \vec{p}_2 & \cdots & \lambda_n \vec{p}_n \end{pmatrix}. \end{aligned} \tag{61}$$

Since the columns on both sides of (61) must match, we conclude that $A\vec{p}_i = \lambda_i \vec{p}_i$ for $i = 1, 2, \ldots, n$. Hence, each column of P is an eigenvector of A.

On the other hand, if each column $\vec{p}_i$ of P is an eigenvector of A, then the above calculation implies that $P^{-1}AP$ is a diagonal matrix whose ith diagonal element is the eigenvalue of A corresponding to $\vec{p}_i$. □

Example 4.58. *Consider the matrix A from Example 4.49:*

$$A = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}.$$

From Example 4.49, A has eigenvalues -1 and 3.

From Theorem 4.57, A is diagonalizable if and only if $\mathbb{R}^2$ has a basis which consists entirely of eigenvectors of A. Example 4.49 shows this to be the case with basis

$$\vec{p}_1 = (1, -1)^T, \qquad \vec{p}_2 = (1, 1)^T,$$

where $\vec{p}_1$ is an eigenvector associated to -1 and $\vec{p}_2$ is an eigenvector associated to 3.

By Theorem 4.57, the matrix

$$P = \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix}$$

will transform A into a diagonal matrix. Lets verify this:

$$\begin{aligned} P^{-1}AP &= \begin{pmatrix} 1/2 & -1/2 \\ 1/2 & 1/2 \end{pmatrix} \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix} \\ &= \begin{pmatrix} -1 & 0 \\ 0 & 3 \end{pmatrix} \end{aligned}$$

Example 4.59. *Consider the matrix A from Example 4.50:*

$$A = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

As in Example 4.50, we will regard A as a complex matrix. The eigenvalues of A are i and $-i$. In this case, we have a basis of $\mathbb{C}^2$ made up of the eigenvectors of A:

$$\vec{p}_1 = (i, -1)^T, \qquad \vec{p}_2 = (i, 1)^T,$$

where $\vec{p}_1$ is associated to i and $\vec{p}_2$ is associated to $-i$. The matrix which transforms A into a diagonal matrix is

$$P = \begin{pmatrix} i & i \\ -1 & 1 \end{pmatrix}.$$

Lets verify this:

$$\begin{aligned} P^{-1}AP &= \begin{pmatrix} -i/2 & -1/2 \\ -i/2 & 1/2 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} i & i \\ -1 & 1 \end{pmatrix} \\ &= \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}. \end{aligned}$$

There are two special classes of matrices which are always diagonalizable: real symmetric matrices and Hermitian matrices. We will work out the details for the real symmetric case explicitly. The results and proofs for the Hermitian case are similar. We will comment on this briefly.

Proposition 4.60. *Let A be a real symmetric matrix.*

(i) All eigenvalues of A are real.

(ii) If λ_1 and λ_2 are distinct eigenvalues of A and $\vec{v}_i \in E_{\lambda_i}$ for $i = 1, 2$, then $\vec{v}_1 \cdot \vec{v}_2 = 0$.

Proof. (i): Since $\mathbb{R} \subset \mathbb{C}$, lets regard A as a complex matrix. Suppose λ is an eigenvalue of A. Let $\vec{v}$ be an associated eigenvector. Then

$$\begin{aligned} \vec{v}^* A\vec{v} &= \vec{v}^*(\lambda\vec{v}) \\ &= \lambda\vec{v}^*\vec{v}. \end{aligned} \tag{62}$$

On the other hand, since A is real and symmetric, we have $A^* = A^T = A$. Hence,

$$\begin{aligned} \vec{v}^* A\vec{v} &= \vec{v}^* A^*\vec{v} \\ &= (A\vec{v})^*\vec{v} \\ &= (\lambda\vec{v})^*\vec{v} \\ &= \overline{\lambda}\vec{v}^*\vec{v}. \end{aligned} \tag{63}$$

Since $\vec{v} \neq \vec{0}$, we have $\vec{v}^*\vec{v} > 0$. Comparing (62) and (63), we conclude that $\lambda = \overline{\lambda}$. This implies that λ is real.

(ii): Suppose λ_1 and λ_2 are distinct eigenvalues. Let $\vec{v}_1$ and $\vec{v}_2$ be eigenvectors associated to λ_1 and λ_2 respectively. Since λ_1 and λ_2 are real, $\vec{v}_1$ and $\vec{v}_2$ can be taken to be **real** vectors. Then

$$\begin{aligned} \vec{v}_1^T A\vec{v}_2 &= \vec{v}_1^T(\lambda_2\vec{v}_2) \\ &= \lambda_2\vec{v}_1^T\vec{v}_2. \end{aligned} \tag{64}$$

Using the symmetry of A, we also have

$$\begin{aligned} \vec{v}_1^T A\vec{v}_2 &= \vec{v}_1^T A^T\vec{v}_2 \\ &= (A\vec{v}_1)^T\vec{v}_2 \\ &= \lambda_1\vec{v}_1^T\vec{v}_2. \end{aligned} \tag{65}$$

Since $\lambda_1 \neq \lambda_2$, (64) and (65) imply that $\vec{v}_1^T\vec{v}_2 = 0$. Of course, the latter can be rewritten as $\vec{v}_1 \cdot \vec{v}_2 = 0$. □

Corollary 4.61. *Let A be a real symmetric matrix. Then A has at least one eigenvalue.*

Proof. Let $p_A(x)$ be the characteristic polynomial of A. Clearly, $p_A(x)$ is a real polynomial, that is, its coefficients are all real numbers. Since $\mathbb{R} \subset \mathbb{C}$, we $p_A(x)$ is also a complex polynomial. There is a famous result from abstract algebra called the *Fundamental Theorem of Algebra* (which we will formally state in Chapter 5) which says that any complex polynomial always has a root. In particular, $p_A(x)$ has a root. However, from Proposition 4.60, any eigenvalue of A is always real. Since the roots of $p_A(x)$ and the eigenvalues of A are one and the same, we conclude that A has at least one eigenvalue. □

Theorem 4.62. *Let A be a real $n \times n$ matrix. Then A is a symmetric matrix if and only if there exists a real orthogonal matrix Q such that $Q^T AQ$ is a diagonal matrix. In particular, A is diagonalizable and $\mathbb{R}^n$ has an orthonormal basis which is made up of the eigenvectors of A.*

Proof. ($\Leftarrow$) Suppose there exists a real orthogonal matrix Q such that $Q^T AQ$ is diagonal. Let $D = Q^T AQ$. Then $A = QDQ^T$ and

$$\begin{aligned} A^T &= (QDQ^T)^T \\ &= (Q^T)^T D^T Q^T \\ &= QDQ^T \\ &= A. \end{aligned}$$

($\Rightarrow$) Now suppose that A is a real $n \times n$ symmetric matrix. We show by induction on n that there exists a real orthogonal matrix Q such that $Q^T AQ$ is a diagonal matrix. For $n = 1$, A is both symmetric and diagonal. Moreover, there are only two real 1×1 orthogonal matrices: 1 and -1. Taking $Q = 1$ or -1, we have $Q^T AQ = A$ which proves the result for $n = 1$. Now let us suppose that the result holds for all real $(n-1) \times (n-1)$ symmetric matrices for some $n \geq 2$.

Let A be a real $n \times n$ symmetric matrix. By Corollary 4.61, A has at least one eigenvalue (which must be real by Proposition 4.60). Let λ_1 be any eigenvalue of A. Let $\vec{q}_1 \in \mathbb{R}^n$ be any normalized eigenvector of A associated to λ_1. Using the Gram-Schmidt process, extend $\vec{q}_1$ to an orthonormal basis on $\mathbb{R}^n$

$$\vec{q}_1, \vec{v}_2, \ldots, \vec{v}_n.$$

Let P be the $n \times n$ matrix defined by

$$P := \begin{pmatrix} \vec{q}_1 & \vec{v}_2 & \cdots & \vec{v}_n \end{pmatrix}$$

and let P_1 be the $n \times (n-1)$ matrix given by

$$P_1 := \begin{pmatrix} \vec{v}_2 & \cdots & \vec{v}_n \end{pmatrix}.$$

Note that

$$\begin{aligned} \vec{q}_1^T A \vec{q}_1 &= \vec{q}_1^T A^T \vec{q}_1 \\ &= (A\vec{q}_1)^T \vec{q}_1 \\ &= \lambda_1 \vec{q}_1^T \vec{q}_1 \\ &= \lambda_1 \end{aligned} \tag{66}$$

and

$$\begin{aligned} \vec{v}_k^T (A\vec{q}_1) &= \vec{v}_k^T (\lambda_1 \vec{q}_1) \\ &= \lambda_1 \vec{v}_k^T \vec{q}_1 \\ &= \lambda_1 \vec{v}_k \cdot \vec{q}_1 \\ &= 0 \end{aligned} \tag{67}$$

for $k = 2, \ldots, n$. Using (66) and (67), we expand the matrix $P^T AP$:

$$\begin{aligned} P^T AP &= \begin{pmatrix} \vec{q}_1^T \\ \vec{v}_2^T \\ \vdots \\ \vec{v}_n^T \end{pmatrix} \begin{pmatrix} A\vec{q}_1 & A\vec{v}_2 & \cdots & A\vec{v}_n \end{pmatrix} \\ &= \begin{pmatrix} \lambda_1 & 0 \cdots & 0 \\ 0 & & \\ \vdots & P_1^T AP_1 & \\ 0 & & \end{pmatrix}. \end{aligned} \tag{68}$$

Note that the $(n-1) \times (n-1)$ real matrix $P_1^T AP_1$ is symmetric. Indeed,

$$(P_1^T AP_1)^T = P_1^T A^T (P_1^T)^T = P_1^T AP_1.$$

By the induction hypothesis, there exist an orthogonal matrix Q_1 such that

$$Q_1^T (P_1^T AP_1) Q_1 = D_1 \tag{69}$$

for some $(n-1) \times (n-1)$ diagonal matrix D_1. We can rewrite (69) as

$$(P_1 Q_1)^T A (P_1 Q_1) = D_1. \tag{70}$$

The matrix $P_1 Q_1$ is of size $n \times (n-1)$. Let $\vec{q}_2, \ldots, \vec{q}_n$ denote the $n-1$ columns of $P_1 Q_1$. Let

$$Q = \begin{pmatrix} \vec{q}_1 & \vec{q}_2 & \cdots & \vec{q}_n \end{pmatrix}. \tag{71}$$

Since the columns of P_1 are orthogonal to $\vec{q}_1$, it follows that

$$\vec{q}_1^T P_1 Q_1 = \begin{pmatrix} 0 & \cdots & 0 \end{pmatrix}.$$

Hence,

$$\vec{q}_1^T \vec{q}_k = 0, \qquad \text{for } k = 2, \ldots, n. \tag{72}$$

Also, note that

$$(P_1 Q_1)^T P_1 Q_1 = Q_1^T (P_1^T P_1) Q_1 = Q_1^T I_{n-1} Q_1 = Q_1^T Q_1 = I_{n-1}. \tag{73}$$

This implies that

$$\vec{q}_k^T \vec{q}_k = 1, \qquad \text{for } k = 2, \ldots, n \tag{74}$$

$$\vec{q}_k^T \vec{q}_j = 0, \qquad \text{for } k \neq j \tag{75}$$

From this, it follows that $Q^T Q = I_n$, that is, Q is an orthogonal matrix.

Lastly, let us compute $Q^T AQ$. From (72), we have

$$\vec{q}_1^T A\vec{q}_k = (A\vec{q}_1)^T \vec{q}_k = \lambda_1 \vec{q}_1^T \vec{q}_k = 0 \quad \text{for } k = 2, \ldots, n. \tag{76}$$

Using (76), we have

$$\begin{aligned} Q^T AQ &= \begin{pmatrix} \vec{q}_1^T \\ \vec{q}_2^T \\ \vdots \\ \vec{q}_n^T \end{pmatrix} \begin{pmatrix} A\vec{q}_1 & A\vec{q}_2 & \cdots & A\vec{q}_n \end{pmatrix} \\ &= \begin{pmatrix} \lambda_1 & 0 \cdots & 0 \\ 0 & & \\ \vdots & (P_1 Q_1)^T A (P_1 Q_1) & \\ 0 & & \end{pmatrix} \\ &= \begin{pmatrix} \lambda_1 & 0 \cdots & 0 \\ 0 & & \\ \vdots & D_1 & \\ 0 & & \end{pmatrix}, \end{aligned}$$

where the last equality follows from (70). Since D_1 is an $(n-1) \times (n-1)$ diagonal matrix, we conclude that $Q^T AQ$ is a diagonal matrix. This completes the induction step. □

Theorem 4.62 shows that any real symmetric matrix A is not only diagonalizable, but diagonalizable by an orthogonal matrix. Here is the general strategy for constructing the orthogonal matrix Q in Theorem 4.62 for a real symmetric matrix A:

1. Find all the eigenvalues of A. Let $\lambda_1, \lambda_2, \ldots, \lambda_k$ denote the **distinct** eigenvalues of A.
2. Find the corresponding eigenspace E_{λ_i} for $i = 1, 2, \ldots, k$.
3. Using Gram-Schmidt, construct an orthonormal basis $\mathcal{B}_i$ of E_{λ_i} for $i = 1, 2, \ldots, k$.
4. By Proposition 4.60, any element of $\mathcal{B}_i$ is orthogonal to any element of $\mathcal{B}_j$ for $i \neq j$.
5. The set $\mathcal{B} := \mathcal{B}_1 \cup \cdots \cup \mathcal{B}_k$ is an orthonormal basis of $\mathbb{R}^n$ made up of the eigenvectors of A.

6. The desired orthogonal matrix Q is the $n \times n$ matrix whose columns are the elements of $\mathcal{B}$.

Example 4.63. *Let*

$$A = \begin{pmatrix} 2 & 1 & -1 \\ 1 & 2 & 1 \\ -1 & 1 & 2 \end{pmatrix}.$$

The characteristic polynomial of A is $p_A(x) = x(x-3)^2$. Hence, the eigenvalues of A are 0 and 3. The eigenspace of A associated to 0 is

$$E_0 := \{(r, -r, r)^T \mid r \in \mathbb{R}\}.$$

The eigenspace of A associated to 3 is

$$E_3 := \{(r+s, s, -r)^T \mid r, s \in \mathbb{R}\}.$$

An orthonormal basis of E_0 is

$$\mathcal{B}_0 = \{(1/\sqrt{3}, -1/\sqrt{3}, 1/\sqrt{3})^T\}$$

and an orthonormal basis of E_3 is

$$\mathcal{B}_3 = \{(1/\sqrt{2}, 0, -1/\sqrt{2})^T. \ (1/\sqrt{6}, 2/\sqrt{6}, 1/\sqrt{6})^T\}.$$

The orthogonal matrix Q is

$$Q = \begin{pmatrix} \frac{1}{\sqrt{3}} & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{6}} \\ -\frac{1}{\sqrt{3}} & 0 & \frac{2}{\sqrt{6}} \\ \frac{1}{\sqrt{3}} & -\frac{1}{\sqrt{2}} & \frac{1}{\sqrt{6}} \end{pmatrix}.$$

Then

$$Q^T A Q =$$
$$\begin{pmatrix} \frac{1}{\sqrt{3}} & -\frac{1}{\sqrt{3}} & \frac{1}{\sqrt{3}} \\ \frac{1}{\sqrt{2}} & 0 & -\frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{6}} & \frac{2}{\sqrt{6}} & \frac{1}{\sqrt{6}} \end{pmatrix} \begin{pmatrix} 2 & 1 & -1 \\ 1 & 2 & 1 \\ -1 & 1 & 2 \end{pmatrix} \begin{pmatrix} \frac{1}{\sqrt{3}} & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{6}} \\ -\frac{1}{\sqrt{3}} & 0 & \frac{2}{\sqrt{6}} \\ \frac{1}{\sqrt{3}} & -\frac{1}{\sqrt{2}} & \frac{1}{\sqrt{6}} \end{pmatrix}$$
$$= \begin{pmatrix} 0 & 0 & 0 \\ 0 & 3 & 0 \\ 0 & 0 & 3 \end{pmatrix}.$$

Here is the complex version of the above story:

Proposition 4.64. *Let A be a Hermitian matrix.*

(i) All eigenvalues of A are real.

(ii) If λ_1 and λ_2 are distinct eigenvalues of A and $\vec{v}_i \in E_{\lambda_i}$ for $i = 1, 2$, then $(\vec{v}_1)^* \vec{v}_2 = 0$.

Theorem 4.65. *Let A be a complex $n \times n$ matrix. Then A is a Hermitian matrix if and only if there exists a unitary matrix U such that U^*AU is a diagonal matrix. In particular, A is diagonalizable and $\mathbb{C}^n$ has an orthonormal basis which is made up of the eigenvectors of A.*

The key point here is that for $\mathbb{C}^n$ and its subspaces, two vectors $\vec{u}$ and $\vec{v}$ in $\mathbb{C}^n$ are said to be orthogonal if $(\vec{u})^*\vec{v} = 0$. With this notion, the Gram-Schmidt process can be generalized to $\mathbb{C}^n$ and its subspaces. Unlike the real case, $(\vec{u})^*\vec{v} \neq (\vec{v})^*\vec{u}$ for $\vec{u}, \vec{v} \in \mathbb{C}^n$. Hence, some care has to be used in extending the Gram-Schmidt process to the complex case. The proofs of Proposition 4.64 and Theorem 4.65 are very similar to the real case given above. We leave the proofs as an exercise for the reader.

In Chapter 9, we will give alternate proofs of the diagonalizability of real symmetric matrices and Hermitian matrices in the general setting of inner product spaces. We conclude this section with the following observation:

Proposition 4.66. *Let A be an $n \times n$ diagonalizable matrix and let $\lambda_1, \lambda_2, \ldots, \lambda_n$ be the eigenvalues of A with multiplicities. Then $Tr(A) = \sum_{i=1}^n \lambda_i$.*

Proof. By definition, there exists an invertible matrix P such that $D := P^{-1}AP$ is a diagonal matrix. Let $\lambda_1, \lambda_2, \ldots, \lambda_n$ be the diagonal elements of D. By Proposition 4.55, these are the eigenvalues of D. Since D and A are similar matrices, it follows from Theorem 4.54 that the eigenvalues of A are also $\lambda_1, \lambda_2, \ldots, \lambda_n$ (counted with multiplicity). Once again, by Theorem 4.54, we have

$$\mathrm{Tr}(A) = \mathrm{Tr}(D) = \sum_{i=1}^{n} \lambda_i.$$

□

It turns out that the above result holds for all complex $n \times n$ matrices. We will prove this fact in Chapter 13.

Chapter 4 Exercises

1. Let
$$A = \begin{pmatrix} 1 & -2 & 3 & 1 \\ -1 & 4 & 2 & 1 \\ 0 & 6 & 8 & 1 \\ 0 & 0 & -2 & 5 \end{pmatrix}.$$
   (a) Compute $\det(A)$ by transforming A into upper triangular form using a suitable choice of elementary row operations.

(b) Compute $\det(A)$ by doing a cofactor expansion.

2. Let

$$A = \begin{pmatrix} 1 & -1 & 2 \\ 3 & 2 & 1 \\ 0 & 1 & 4 \end{pmatrix}$$

Calculate
(a) $\det(A)$
(b) $\det(A^T)$
(c) $\det(A^{-1})$

3. Let A, B, and C be 3×3 matrices such that $\det(AB) = 50$, $\det(-2B) = -80$, and $\det(-AC) = 15$. Find $\det(A)$, $\det(B)$, and $\det(C)$.

4. Find the adjugate matrix of

$$A = \begin{pmatrix} 1 & -3 & 3 \\ 2 & 3 & 1 \\ 1 & 1 & 1 \end{pmatrix}$$

Does the inverse of A exist? If so, compute it using $\mathrm{adj}(A)$.

5. Find the adjugate for each of the following matrices. Also, determine if the matrix is invertible. If so, compute it using the adjugate.

(a)

$$\begin{pmatrix} 0 & 1 & 2 \\ 1 & -5 & 4 \\ 2 & -1 & 0 \end{pmatrix}$$

(b)

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

6. Find a matrix A for a linear transformation from $\mathbb{R}^2$ to itself which first reflects a vector across the x-axis, then rotates it by 135° (counterclockwsie), and finally scales it by a factor of $\sqrt{2}/2$.

7. Find the matrix A associated to a linear transformation from $\mathbb{R}^2$ to itself which rotates a vector by 30° (counterclockwise) and then scales it by a factor of 2.

Also, what is A^6? (Hint: think geometrically.)

8. Let
$$A = \begin{pmatrix} 3 & -15 & 15 \\ -18 & 10 & -22 \\ -3 & 7 & -19 \end{pmatrix}.$$
Find the eigenvalues of A and their corresponding eigenspaces.

9. Let A be an $n \times n$ matrix and let λ be an eigenvalue of A. Let c be a scalar.
   (a) Show that $c\lambda$ is an eigenvalue of cA.
   (b) Show that if $\vec{v}$ is an eigenvector of A associated to λ, then $\vec{v}$ is also an eigenvector of cA associated to the eigenvalue $c\lambda$.

10. Let A be an $n \times n$ invertible matrix.
   (a) Show that if λ is an eigenvalue of A, then $\lambda \neq 0$.
   (b) Show that if λ is an eigenvalue of A, then $1/\lambda$ is an eigenvalue of A^{-1}.
   (c) Show that if $\vec{v}$ is an eigenvector of A associated to λ, then $\vec{v}$ is also an eigenvector of A^{-1} associated to $1/\lambda$.

11. Let
$$A = \begin{pmatrix} 3 & -1 & -1 \\ 0 & 2 & 0 \\ -1 & 1 & 3 \end{pmatrix}.$$
   (a) Find the eigenvalues of A and their corresponding eigenspaces.
   (b) Determine if A is diagonalizable. If so, find a matrix P for which $P^{-1}AP$ is a diagonal matrix.

12. Suppose A is a nonzero $n \times n$ matrix such that $A^k = 0$ for some positive integer k. Show that A is not diagonalizable. (Hint: consider the eigenvalues of A.)

13. Consider the symmetric matrix
$$A = \begin{pmatrix} 1 & 3 & 0 \\ 3 & 1 & 0 \\ 0 & 0 & -2 \end{pmatrix}.$$
   (a) Find the eigenvalues of A and their corresponding eigenspaces.
   (b) Find an orthogonal matrix Q for which Q^TAQ is a diagonal matrix.

14. Consider the symmetric matrix
$$A = \begin{pmatrix} -7 & 1 & 0 \\ 1 & -3 & 2 \\ 0 & 2 & -7 \end{pmatrix}.$$

(a) Find all the eigenvalues of A and their corresponding eigenspaces.
(b) Find an orthogonal matrix Q which diagonalizes A.

15. Suppose

$$A = \begin{pmatrix} a & 1 & 0 \\ b & 0 & 1 \\ c & 1 & 0 \end{pmatrix}$$

has three eigenvalues $0, 1, 2$. Find a, b, c.

16. Determine the values of λ for which the linear system

$$(1-\lambda)x + y = 0$$
$$x + (2-\lambda)y = 0$$

has nontrivial solutions, that is, solutions other than $x = 0$ and $y = 0$. What is the significance of these values?

17. The matrix

$$\begin{pmatrix} 2c^2 - 1 & 2cd \\ 2cd & 2d^2 - 1 \end{pmatrix}$$

is reflection of $\mathbb{R}^2$ about the line through (c, d) and $(0, 0)$ where

$$c^2 + d^2 = 1.$$

Find the eigenvalues and corresponding eigenspaces of the above matrix.

18. Let M be a square matrix.
(a) Show M and its transpose M^T have the same characteristic polynomial. Conclude that M and M^T have the same eigenvalues.
(b) Let λ be an eigenvalue of M (and hence also of M^T). Let E_λ and E'_λ be the eigenspace of M and M^T associated to λ respectively. Show that $\dim E_\lambda = \dim E'_\lambda$. Give an example to show that in general $E_\lambda \neq E'_\lambda$.

Chapter 5

The General View

In this chapter, we give the general definition of vector spaces and linear maps and recast the results of the previous chapters in this more general light. Hence, much of this chapter will feel like *déjà vu* and rightly so. Of course, several important concepts will be introduced along the way (so pay attention!). As discussed in Chapter 2, $\mathbb{R}^n$ and its subspaces are merely examples of vector spaces. In other words, not every vector space is $\mathbb{R}^n$ or one of its subspaces. This is the reason why linear algebra has numerous applications in science and engineering. Roughly speaking, a vector space is a set with an addition operation and a scalar multiplication whose algebraic properties are identical to those of $\mathbb{R}^n$ and its subspaces. We can think of general vector spaces as algebraic objects which have been modeled after the algebraic properties of $\mathbb{R}^n$ and its subspaces. Unlike $\mathbb{R}^n$ and its subspaces, general vector spaces do not come with a natural dot product. The dot product, as we recall, provides $\mathbb{R}^n$ and its subspaces with a geometric structure in the sense that one can compute the lengths of vectors, the distance between points, and the angle between pairs of vectors. For a general vector space to have its own geometric structure, one must supply the vector space with its own generalized dot product. This generalized dot product is called an *inner product* and will be discussed in Chapter 9.

5.1. A word on scalars

Before we give the general definition of a vector space, we need to comment on the scalars of a vector space. For $\mathbb{R}^n$ and its subspaces, the set of scalars is $\mathbb{R}$. $\mathbb{R}$ is an example of an algebraic object called a **field**.

Definition 5.1. *A **field** is a set $\mathbb{F}$ with an addition operation and a multiplication operation. Let $a, b \in \mathbb{F}$ and let $a+b$ denote the sum of a and b and ab denote the product of a and b. Then these operations satisfy the following conditions for all $a, b, c \in \mathbb{F}$:*

- $a + b = b + a$ *(additive commutativity)*
- $(a + b) + c = a + (b + c)$ *(additive associativity)*
- $ab = ba$ *(multiplicative commutativity)*
- $(ab)c = a(bc)$ *(multiplicative associativity)*
- $a(b + c) = ab + ac$ *(distributivity)*

*In addition, $\mathbb{F}$ contains a **zero element** (which we denote as 0) and a **unit element** (which we denote as 1) such that*

- $a + 0 = 0 + a = a$ *(additive identity)*
- $1a = a1 = a$ *(multiplicative identity)*

*Also, for every $a \in \mathbb{F}$, there exists an element $b \in \mathbb{F}$ such that $a+b = b+a = 0$. This element b is denoted $-a$ and is called the **additive inverse** of a. If a is nonzero, then there also exists an element $x \in \mathbb{F}$ such that $xa = ax = 1$. The element x is denoted as a^{-1} or $1/a$ and is called the **multiplicative inverse** of a.*

In linear algebra, there are two primary examples of fields: the field $\mathbb{R}$ of real numbers and the field $\mathbb{C}$ of complex numbers. Recall that

$$\mathbb{C} := \{a + ib \mid a, b \in \mathbb{R}\},$$

where $i = \sqrt{-1}$. The addition and multiplication on $\mathbb{C}$ are the obvious ones:

$$(a + ib) + (c + id) = (a + c) + i(b + d)$$

$$(a + ib)(c + id) = ac + iad + ibc + i^2 bd = (ac - bd) + i(ad + bc).$$

The zero element of $\mathbb{C}$ is obviously $0 + i0$ which we denote simply as 0 and the unit element is $1 + i0$ which we denote as 1. Following this simplified notation, the field $\mathbb{R}$ can be naturally regarded as a subset (or, to be more precise, a **subfield**) of $\mathbb{C}$ by identifying an element $a \in \mathbb{R}$ with the complex number $a + i0 \in \mathbb{C}$.

Exercise 5.2. *Check that $\mathbb{R}$ and $\mathbb{C}$ satisfy all the conditions of Definition 5.1.*

In this book, the only fields we work with are $\mathbb{R}$ or $\mathbb{C}$. **Hence, the symbol $\mathbb{F}$ will always be understood to mean $\mathbb{R}$ or $\mathbb{C}$.** As you might have guessed, there are other fields besides $\mathbb{R}$ and $\mathbb{C}$. For instance, there are fields with only a finite number of elements. A more detailed discussion of fields would take us into the realm of *abstract algebra*, and last we checked, this is a linear algebra book. For more on fields and other algebraic objects, we refer the curious reader to the classic reference [**1**].

We conclude this section by recalling an important result from abstract algebra which we will need later. The proof of this result is beyond the scope of this book so we omit it.

Theorem 5.3 (Fundamental Theorem of Algebra)**.** *Any polynomial in one variable with complex coefficients whose degree is at least* 1 *always has a root in* $\mathbb{C}$*.*

5.2. General Vector Spaces

Here at last is the general definition of a vector space.

Definition 5.4. *A* ***vector space over a field*** $\mathbb{F}$ *is a set* V *equipped with two operations: an addition operation*

$$+ : V \times V \to V, \quad (u, v) \mapsto u + v$$

and a scalar multiplication

$$\mathbb{F} \times V \to V, \quad (r, v) \mapsto rv$$

which satisfy the following conditions:

(1) $u + v = v + u$ *for all* $u, v \in V$ *(commutativity of addition)*
(2) $(u + v) + w = u + (v + w)$ *for all* $u, v, w \in V$ *(associativity of addition)*
(3) *there exists an element* $\mathbf{0} \in V$ *called the* ***zero vector*** *such that* $v + \mathbf{0} = v$ *for all* $v \in V$ *(identity element of addition)*
(4) *for all* $u \in V$*, there exists an element* $-u$ *such that* $u + (-u) = \mathbf{0}$ *(existence of the additive inverse of a vector)*
(5) $(r + s)u = ru + su$ *for all* $r, s \in \mathbb{F}$ *and* $u \in V$ *(distributivity of scalar multiplication with respect to field addition)*
(6) $r(u + v) = ru + rv$ *for all* $r \in \mathbb{F}$ *and* $u, v \in V$ *(distributivity of scalar multiplication with respect to vector addition)*
(7) $(rs)u = r(su)$ *for all* $r, s \in \mathbb{F}$ *and* $u \in V$ *(compatibility of scalar multiplication with field multiplication)*
(8) $1u = u$ *for all* $u \in V$ *(identity element of scalar multiplication)*

The elements of V *are called* ***vectors*** *and the elements of* $\mathbb{F}$ *are called* ***scalars****. A vector space over* $\mathbb{R}$ *is called* ***real vector space*** *and a vector space over* $\mathbb{C}$ *is called a* ***complex vector space****.*

Remark 5.5. *The astutue reader will notice that the properties (or axioms) of a general vector space in Definition 5.4 are virtually identical to the vector space properties of* $\mathbb{R}^n$ *in Proposition 2.3. As we stated previously, this is not accidental. The definition of a general vector space is modeled after the algebraic properties of* $\mathbb{R}^n$*.*

Notation 5.6. *For a point* $v \in \mathbb{R}^n$*, we used the arrow symbol* $\vec{v}$ *when we wanted to emphasize that* v *was to be regarded as a vector, that is, as an arrow in* $\mathbb{R}^n$ *whose tail was located at the origin and whose head was located at* v*. We will reserve this notation only for the vector space* $\mathbb{R}^n$ *and its subspaces.*

Notation 5.7. *The only special notation that we use for a general vector space* V *is with regard to its zero element which we denote as* $\mathbf{0}$ *to distinguish it from the zero element of the field of scalars* $\mathbb{F}$*. More advanced books do not bother with this additional notation and simply refer to the zero element of the vector space and the zero element of the field by the same symbol:* 0*. One determines whether* 0 *is an element of* V *or the field* $\mathbb{F}$ *by context alone. For example, if* $v \in V$*, then the zero in the expression* $v + 0$ *must be the zero vector since a vector and a scalar cannot be added together. On the other hand, the zero in the expression* $0v$ *must be the zero scalar since vectors cannot be multiplied together.*

Before giving examples of vector spaces which are different than $\mathbb{R}^n$ or its subspaces, we first prove some basic results about general vector spaces.

Proposition 5.8. *Let* V *be a vector space over* $\mathbb{F}$*. Then*

(i) *the zero vector* $\mathbf{0} \in V$ *is unique, that is, if* $u \in V$ *and* $u + v = v$ *for all* $v \in V$*, then* $u = \mathbf{0}$*.*

(ii) $0v = \mathbf{0}$

(iii) $-v = -1v$

(iv) $c\,\mathbf{0} = \mathbf{0}$

for all $v \in V$ *and* $c \in \mathbb{F}$*.*

Proof. (i): Suppose u is an element of V with the property that $u + v = v$ for all $v \in V$. Setting $v = \mathbf{0}$, we have $u + \mathbf{0} = \mathbf{0}$. However, from axiom (3) of Definition 5.4, we also have $u + \mathbf{0} = u$. From this, we conclude that $u = \mathbf{0}$.

(ii): Let $v \in V$ be arbitrary. Using axiom (5) of Definition 5.4, we have

$$0v = (0 + 0)v = 0v + 0v. \tag{77}$$

Adding the additive inverse of $0v$ to both sides of (77) and using axioms (2), (3), and (4) of Definition 5.4 gives

$$\begin{aligned} 0v + (-0v) &= (0v + 0v) + (-0v) \\ \mathbf{0} &= 0v + (0v + (-0v)) \\ \mathbf{0} &= 0v + \mathbf{0} \\ \mathbf{0} &= 0v, \end{aligned}$$

which proves (ii).

(iii): Using axioms (3), (5), and (8) of Definition 5.4 and part (ii) of Proposition 5.8, we have

$$\begin{aligned} v + (-1v) &= 1v + (-1v) \\ &= (1 + (-1))v \\ &= 0v \\ &= \mathbf{0}. \end{aligned}$$

Since we also have $v + (-v) = \mathbf{0}$ by axiom (4) of Definition 5.4, we have

$$\begin{aligned} v + (-1v) &= v + (-v) \\ (-v) + (v + (-1v)) &= (-v) + (v + (-v)) \\ ((-v) + v) + (-1v) &= ((-v) + v) + (-v) \\ \mathbf{0} + (-1v) &= \mathbf{0} + (-v) \\ -1v &= -v \end{aligned}$$

as required, where the third equality follows from axiom (2) of Definition 5.4 and the fourth and fifth equalities follow from axioms (4) and (3) of Definition 5.4 respectively.

(iv): Let $c \in \mathbb{F}$. If $c = 0$, then $c\mathbf{0} = \mathbf{0}$ by part (ii) of Proposition 5.8. So let us suppose that $c \neq 0$. Let $u = c\mathbf{0}$ and let $v \in V$ be arbitrary. Then

$$\begin{aligned} u + v &= c\mathbf{0} + v \\ &= c\mathbf{0} + 1v \\ &= c\mathbf{0} + (cc^{-1})v \\ &= c\mathbf{0} + c(c^{-1}v) \\ &= c(\mathbf{0} + c^{-1}v) \\ &= c(c^{-1}v) \\ &= (cc^{-1})v \\ &= 1v \\ &= v \end{aligned}$$

where the second and last equality follow from axiom (8) of Definition 5.4, the third equality follows from the fact that $c \neq 0$, the fourth and seventh equalities follow from axiom (7), the fifth equality follows from axiom (6), and the sixth equality follows from axiom (3). Hence, we have shown that $u+v = c\mathbf{0}+v = v$ for all $v \in V$. Part (i) of Proposition 5.8 now implies that $c\mathbf{0} = \mathbf{0}$. This completes the proof. □

At last, here are a few examples of vector spaces which are not $\mathbb{R}^n$ or one of its subspaces.

Example 5.9. *Let X be an arbitrary non-empty set and let $\mathbb{F} = \mathbb{R}$ or $\mathbb{C}$. (Choose a field and fix it!) Let $\mathbb{F}(X)$ be the set of all $\mathbb{F}$-valued functions on X. In other words, an element of $\mathbb{F}(X)$ is a map $f : X \to \mathbb{F}$. $\mathbb{F}(X)$ is naturally a vector space over $\mathbb{F}$. For vector addition, let $f, g \in \mathbb{F}(X)$. We define $f + g \in \mathbb{F}(X)$ pointwise:*

$$(f + g)(x) := f(x) + g(x) \in \mathbb{F}, \qquad \forall\, x \in X.$$

For scalar multiplication, let $c \in \mathbb{F}$. Then $cf \in \mathbb{F}(X)$ is defined again pointwise:

$$(cf)(x) := cf(x) \in \mathbb{F}, \qquad \forall\, x \in X.$$

The zero vector $\mathbf{0} \in \mathbb{F}(X)$ is the zero function, that is, the function $\mathbf{0} := f_0 : X \to \mathbb{F}$ defined by $f_0(x) := 0$ for all $x \in X$. The additive inverse of an arbitrary element $f \in \mathbb{F}(X)$ is the function $-f : X \to \mathbb{F}$ defined by $-f := -1f$. (See Proposition 5.8-(iii)).

Exercise 5.10. *Verify that the set $\mathbb{F}(X)$ with vector addition and scalar multiplication as defined in Example 5.9 is truly a vector space over $\mathbb{F}$, that is, it satisfies axioms (1)-(8) of Definition 5.4.*

Example 5.11. *Let $M_{m,n}(\mathbb{F})$ be the set of $m \times n$ matrices whose entries lie in $\mathbb{F}$. Then $M_{m,n}(\mathbb{F})$ equipped with the usual addition of matrices and scalar multiplication of matrices turns $M_{m,n}(\mathbb{F})$ into a vector space over $\mathbb{F}$. The zero vector $\mathbf{0}$ is just the $m \times n$ zero matrix. The additive inverse of $A \in M_{m,n}(\mathbb{F})$ is just $-A = -1A$. Note that the real vector space $\mathbb{R}^n = M_{1,n}(\mathbb{R})$ and the complex vector space $\mathbb{C}^n = M_{1,n}(\mathbb{C})$ are special cases of this.*

Exercise 5.12. *Verify that $M_{m,n}(\mathbb{F})$ in Example 5.11 is truly a vector space over $\mathbb{F}$, that is, it satisfies axioms (1)-(8) of Definition 5.4.*

Example 5.13. *Let* $\mathbb{F}[x]$ *be the set of all polynomials in the variable* x *whose coefficients lie in* $\mathbb{F}$. *In other words, an element of* $\mathbb{F}[x]$ *is a polynomial*

$$p(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$$

where $a_i \in \mathbb{F}$ *for* $i = 0, 1, \ldots, n$. $\mathbb{F}[x]$ *is naturally a vector space over* $\mathbb{F}$ *with vector addition given by the usual addition of polynomials and scalar multiplication given naturally by*

$$cp(x) = (ca_n)x^n + (ca_{n-1})x^{n-1} + \cdots + (ca_1)x + ca_0$$

for $c \in \mathbb{F}$. *The zero vector is the constant polynomial* $0 \in \mathbb{F}$. *The additive inverse of* $p(x)$ *is just* $-p(x) = -1p(x)$.

Exercise 5.14. *Verify that* $\mathbb{F}[x]$ *in Example 5.13 is truly a vector space over* $\mathbb{F}$, *that is, it satisfies axioms (1)-(8) of Definition 5.4.*

The following definition will no doubt be quite familiar to you. (As stated above, $\mathbb{F}$ is always understood to be $\mathbb{R}$ or $\mathbb{C}$.)

Definition 5.15. *Let* V *be a vector space over* $\mathbb{F}$. *A* ***subspace*** *of* V *is a non-empty subset* W *of* V *such that*

(a) $w + w' \in W$ *for all* $w, w' \in W$
(b) $cw \in W$ *for all* $c \in \mathbb{F}$, $w \in W$.

Proposition 5.16. *Let* V *be a vector space over* $\mathbb{F}$. *A subspace* W *of* V *is necessarily a vector space in its own right with vector addition and scalar multiplication inherited from* V.

Proof. Equip W with the vector addition and scalar multiplication from V. We now verify that W satisfies axioms (1)-(8) of Definition 5.4. Let $w, w', w'' \in W$ be arbitrary. Axioms (1) and (2) (the commutativity and associativity of vector addition) follows immediately from the fact that these axioms hold for V, the fact that $W \subset V$, and the fact that vector addition is closed on W (i.e. condition (a) of Definition 5.15).

For axioms (3) and (4) of Definition 5.4, let $w \in W$ be arbitrary. By condition (b) of Definition 5.15, $0w \in W$ and $-1w \in W$. However, by Proposition 5.8, $0w = \mathbf{0}$ and $-1w = -w$. Hence, W contains the zero vector and the additive inverse of all of its elements. This implies that W satisfies axioms (3) and (4) of Definition 5.4.

Axioms (5)-(8) follow immediately from the fact that these axioms hold for V, the fact that $W \subset V$, and from conditions (a) and (b) of Definition 5.15. $\square$

Example 5.17. *Let $\mathbb{F}[x]_d$ be the set of polynomials of degree d or less. Then $\mathbb{F}[x]_d$ is a subspace of the vector space of polynomials $\mathbb{F}[x]$ (see Example 5.13). Indeed, adding two polynomials of degree d or less gives another polynomial of degree d or less. In addition, multiplying a polynomial of degree d or less by a constant leaves the degree of the polynomial unchanged (unless the constant is zero in which case one obtains the zero polynomial). By Definition 5.15, $\mathbb{F}[x]_d$ is a subspace of $\mathbb{F}[x]$.*

Example 5.18. *Let $sl(n;\mathbb{F})$ be the set of all $n \times n$ matrices whose entries belong to $\mathbb{F}$ and have trace zero. Then $sl(n;\mathbb{F})$ is a subspace of the vector space $M_{n,n}(\mathbb{F})$ (see Example 5.11). Indeed, if $A, B \in sl(n;\mathbb{F})$, then*

$$Tr(A+B) = Tr(A) + Tr(B) = 0 + 0 = 0.$$

Also, for $c \in \mathbb{F}$, we have $Tr(cA) = c\,Tr(A) = c0 = 0$. By Definition 5.15, $sl(n;\mathbb{F})$ is a subspace of $M_{n,n}(\mathbb{F})$.

To make things a bit more concrete, we are going to work with real vector spaces until stated otherwise. Hence, when we say "V is a vector space ...", we understand this to be a vector space over $\mathbb{R}$. (We will be forced to work with complex vector spaces later in Chapter 9.) Even though we will be working with real vector spaces for much of this chapter, **all of the definitions and results of this chapter apply equally well to complex vector spaces**.

5.3. Linear Independence, Bases, & Dimension revisited

The notions of linear independence, bases, and dimension generalize quite naturally to general vector spaces. All of the definitions and results that we state in this section are essentially identical to those of Section 2.4. **More than that, the proofs given in Section 2.4 carry over to general vector spaces without modification**! The reason for this is that the proofs of Section 2.4 never relied on the fact that the vectors were elements of $\mathbb{R}^n$. They only relied on axioms (1)-(8) of Definition 5.4 (which are of course satisfied by the vector space structure on $\mathbb{R}^n$ given in Chapter 2). Hence, in this section, we will merely restate the definitions and results of Section 2.4 for general vector spaces. Some of the results (especially the lengthier ones) will be stated without proofs since the proofs can be found in Section 2.4. We will point this out when we do it. As usual, we will provide a number of examples along the way. We begin with the following (familiar) definition:

Definition 5.19. *Let V be a vector space. A vector $v \in V$ is a **linear combination** of vectors $v_1, \ldots, v_k \in V$ if there exists $a_1, \ldots, a_k \in \mathbb{R}$ such that*

$$v = a_1 v_1 + \cdots + a_k v_k.$$

Example 5.20. *Consider the vector space of real polynomials* $R[x]$ *and let* $f = x^2 - 2x + 1$, $g = 2x^2 + 1$, *and* $h = x^2 + 2x$. *Then* f *is a linear combination of* g *and* h *since* $f = g - h$.

Example 5.21. *Consider the vector space of real polynomials* $R[x]$ *and let* $f = -10x + 1$, $g = x^2 - 2x + 1$, *and* $h = 3x^2 + 4x + 2$. *Let us determine if* f *is a linear combination of* g *and* h. *Suppose then that*

$$f = ag + bh$$

for some $a, b \in \mathbb{R}$. *Since two polynomials are equal if and only if their coefficients are equal, the above equation implies the following system of linear equations:*

$$\begin{aligned} a + 3b &= 0 \\ -2a + 4b &= -10 \\ a + 2b &= 1 \end{aligned}$$

We express the above system as an augmented matrix and use the Gauss-Jordan method to solve it:

$$\begin{pmatrix} 1 & 3 & 0 \\ -2 & 4 & -10 \\ 1 & 2 & 1 \end{pmatrix}$$

Using Gauss Jordan, we solve the above system:

1. $2R_1 + R_2 \to R_2$, $-R_1 + R_3 \to R_3$

$$\begin{pmatrix} 1 & 3 & 0 \\ 0 & 10 & -10 \\ 0 & -1 & 1 \end{pmatrix}$$

2. $\frac{1}{10}R_2 \to R_2$

$$\begin{pmatrix} 1 & 3 & 0 \\ 0 & 1 & -1 \\ 0 & -1 & 1 \end{pmatrix}$$

3. $-3R_2 + R_1 \to R_1$, $R_2 + R_3 \to R_3$

$$\begin{pmatrix} 1 & 0 & 3 \\ 0 & 1 & -1 \\ 0 & 0 & 0 \end{pmatrix}$$

Hence, $a = 3$ *and* $b = -1$. *From this, we have* $f = 3g - h$.

Example 5.22. *Let*

$$A_1 = \begin{pmatrix} 1 & 2 \\ 0 & -1 \end{pmatrix}, \qquad A_2 = \begin{pmatrix} 1 & 1 \\ 3 & 4 \end{pmatrix}, \qquad A_3 = \begin{pmatrix} -1 & 2 \\ 2 & 1 \end{pmatrix}$$

Let us determine if

$$A = \begin{pmatrix} -2 & 9 \\ 3 & -3 \end{pmatrix}$$

is a linear combination of A_1, A_2, and A_3. So suppose then that

$$A = c_1 A_1 + c_2 A_3 + c_3 A_3.$$

Equating components on the left and right sides of the above equation we arrive at the following system of linear equations:

$$\begin{aligned} c_1 + c_2 - c_3 &= -2 \\ 2c_1 + c_2 + 2c_3 &= 9 \\ 3c_2 + 2c_3 &= 3 \\ -c_1 + 4c_2 + c_3 &= -3 \end{aligned}$$

We can solve the above system using the Gauss Jordan method. The augmented matrix is

$$\begin{pmatrix} 1 & 1 & -1 & -2 \\ 2 & 1 & 2 & 9 \\ 0 & 3 & 2 & 3 \\ -1 & 4 & 1 & -3 \end{pmatrix}$$

1. $-2R_1 + R_2 \to R_2$,$R_1 + R_4 \to R_4$

$$\begin{pmatrix} 1 & 1 & -1 & -2 \\ 0 & -1 & 4 & 13 \\ 0 & 3 & 2 & 3 \\ 0 & 5 & 0 & -5 \end{pmatrix}$$

2. $-R_2 \to R_2$

$$\begin{pmatrix} 1 & 1 & -1 & -2 \\ 0 & 1 & -4 & -13 \\ 0 & 3 & 2 & 3 \\ 0 & 5 & 0 & -5 \end{pmatrix}$$

3. $-R_2 + R_1 \to R_1$, $-3R_2 + R_3 \to R_3$, $-5R_2 + R_4 \to R_4$

$$\begin{pmatrix} 1 & 0 & 3 & 11 \\ 0 & 1 & -4 & -13 \\ 0 & 0 & 14 & 42 \\ 0 & 0 & 20 & 60 \end{pmatrix}$$

4. $\frac{1}{14}R_3 \to R_3$, $\frac{1}{20}R_4 \to R_4$

$$\begin{pmatrix} 1 & 0 & 3 & 11 \\ 0 & 1 & -4 & -13 \\ 0 & 0 & 1 & 3 \\ 0 & 0 & 1 & 3 \end{pmatrix}$$

5. $-3R_3 + R_1 \to R_1$, $4R_3 + R_2 \to R_2$, $-R_3 + R_4 \to R_4$

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

Hence, $c_1 = 2$, $c_2 = -1$, and $c_3 = 3$. From this, we conclude that $A = 2A_1 - A_2 + 3A_3$.

Definition 5.23. *Let V be a vector space. Vectors $v_1, \ldots, v_m \in V$* ***span*** *V if for all $v \in V$, there exists $c_1, \ldots, c_m \in \mathbb{R}$ such that*

$$v = c_1 v_1 + \cdots + c_m v_m$$

The set $\{v_1, \ldots, v_m\}$ is called a ***spanning set*** *of V.*

If $\{v_1, \ldots, v_m\}$ is a spanning set of V, one often denotes this by

$$V = \text{span } \{v_1, \ldots, v_m\}.$$

Proposition 5.24. *Let V be a vector space and let $v_1, \ldots, v_m$ be any vectors in V. Define*

$$W = \{c_1 v_1 + \cdots + c_m v_m \mid c_1, \ldots, c_m \in \mathbb{R}\}$$

Then W is a subspace of V and $W = span \{v_1, \ldots, v_m\}$.

Proof. Let $w_1,\ w_2 \in W$. We need to show that $w_1 + w_2 \in W$ and $rw_1 \in W$ for $r \in \mathbb{R}$. By definition of W, w_1 and w_2 can be expressed as

$$w_1 = c_1 v_1 + \cdots + c_m v_m$$

and

$$w_2 = d_1 v_1 + \cdots + d_m v_m$$

for some $c_i, d_j \in \mathbb{R}$, $1 \le i, j \le m$. From this, we have

$$w_1 + w_2 = (c_1 + d_1)v_1 + \cdots + (c_m + d_m)v_m$$

which is clearly in W. Likewise for $r \in \mathbb{R}$, we have

$$rw_1 = (rc_1)v_1 + \cdots + (rc_m)v_m$$

which is again in W. Lastly, from the definition of W, every element of W is a linear combination of $v_1, \dots, v_m$ and every linear combination of $v_1, \dots, v_m$ is in W. Hence, $W = \text{span}\{v_1, \dots, v_m\}$. This completes the proof. □

Here is the definition of linear independence (which is exactly the same as it was for $\mathbb{R}^n$ and its subspaces):

Definition 5.25. *Let V be a vector space. A set of vectors $v_1, \dots, v_k \in V$ are **linearly independent** if the condition*

$$c_1 v_1 + \cdots + c_k v_k = \mathbf{0}$$

*is satisfied **only if** $c_1 = c_2 = \cdots = c_k = 0$. If this condition is not satisfied, $v_1, \dots, v_k \in V$ is said to be **linearly dependent**.*

Example 5.26. *Let us determine if the polynomials $2x^2+1$, $5x+2$, $x+1$ are linearly independent. So let us suppose that*

$$c_1(2x^2+1) + c_2(5x+2) + c_3(x+1) = 0$$

for some $c_1, c_2, c_3 \in \mathbb{R}$. We need to show that c_1, c_2, and c_3 must be zero. The above equation implies the following system of linear equations

$$2c_1 = 0, \quad 5c_2 + c_3 = 0, \quad c_1 + 2c_2 + c_3 = 0$$

The above system has only one solution (as the reader can easily check): $c_1 = c_2 = c_3 = 0$. Hence, we conclude that $2x^2+1$, $5x+2$, $x+1$ are linearly independent.

Exercise 5.27. *Show that the polynomials $2x^2+1$, $5x+2$, $x+1$, and x^2 are linearly **dependent**.*

Example 5.28. *Let V be a vector space and suppose v_1, v_2 are linearly independent. Let $u_1 := v_1 + v_2$ and $u_2 := v_1 - v_2$. Let us show that u_1, u_2 is also linearly independent. Again, suppose that*

$$c_1 u_1 + c_2 u_2 = \mathbf{0}$$

for some $c_1, c_2 \in \mathbb{R}$. We must show that c_1 and c_2 are necessarily 0. From the definitions of u_1 and u_2, we have

$$c_1(v_1+v_2) + c_2(v_1-v_2) = (c_1+c_2)v_1 + (c_1-c_2)v_2 = \mathbf{0}.$$

Since v_1 and v_2 are linearly independent, we must have $c_1 + c_2 = 0$ and $c_1 - c_2 = 0$. The only solution to this system of linear equations is $c_1 = c_2 = 0$. This shows that u_1 and u_2 are linearly independent.

At this point, we can now give the definition of **basis** for general vector spaces:

Definition 5.29. *Let V be a vector space. A set $\{v_1, \ldots, v_n\}$ is a **basis** for V if the following two conditions are satisfied:*

(a) $\{v_1, \ldots, v_n\}$ is linearly independent
(b) $V = span\ \{v_1, \ldots, v_n\}$

Exercise 5.30. *Let $M_{m,n}(\mathbb{R})$ be the vector space of $m \times n$ real matrices. Let E_{ij} be the $m \times n$ matrix whose entries are all zero except for its (i, j)-entry which is 1. Show that $\{E_{ij} \mid 1 \leq i \leq m,\ 1 \leq j \leq n\}$ is a basis on $M_{m,n}(\mathbb{R})$.*

Proposition 5.31. *Let V be a vector space and let $\{v_1, \ldots, v_n\}$ be a subset of V. The following statements are equivalent:*

(a) $\{v_1, \ldots, v_n\}$ is a basis on V.
*(b) Every $v \in V$ can be expressed as a **unique** linear combination of $\{v_1, \ldots, v_n\}$.*

Proof. $(a) \Rightarrow (b)$. Suppose $\{v_1, \ldots, v_n\}$ is a basis on V and let $v \in V$. Since $\{v_1, \ldots, v_n\}$ is a basis, v can be expressed as a linear combination of these elements:

$$v = c_1 v_1 + \cdots + c_n v_n$$

for some $c_1, \ldots, c_n \in \mathbb{R}$. We would like to show that the above expression is unique. So let us suppose that we can also express v as

$$v = d_1 v_1 + \cdots + d_n v_n$$

for some $d_1, \ldots, d_n \in \mathbb{R}$. Equating these two expressions, we arrive at the following:

$$(c_1 - d_1)v_1 + \cdots + (c_n - d_n)v_n = \mathbf{0}.$$

Since $\{v_1, \ldots, v_n\}$ is linearly independent, we must have $c_i - d_i = 0$ for $i = 1, \ldots, n$. Hence, $c_i = d_i$ for $i = 1, \ldots, n$, which shows that the expression for v is unique.

$(a) \Leftarrow (b)$. Condition (b) implies that $V = \text{span}\ \{v_1, \ldots, v_n\}$. We only need to show that $\{v_1, \ldots, v_n\}$ is linearly independent. Suppose then that

$$c_1 v_1 + \cdots + c_n v_n = \mathbf{0}.$$

Since we also have $0v_1 + \cdots + 0v_n = \mathbf{0}$ and condition (b) implies that every element of V (including $\mathbf{0}$) can be expressed as a unique linear combination of $\{v_1, \ldots, v_n\}$, we conclude that $c_1 = c_2 = \cdots = c_n = 0$. $\square$

You might recall that the Replacement Theorem (Theorem 2.34) was one of the main theorems of Section 2.4. The theorem for the general case is virtually identical. The only difference is that the vector space is no longer limited to being $\mathbb{R}^n$ or one of its subspaces of $\mathbb{R}^n$. Without further adieu, here is the Replacement Theorem for general vector spaces:

Theorem 5.32 (Replacement Theorem)**.** *Let V be a vector space and let $\mathcal{B} = \{v_1, \ldots, v_n\}$ be a basis on V. Let $U = \{u_1, \ldots, u_m\}$ be a linearly independent set on V. Then $m \le n$ and there is a permutation σ of $\{1, 2, \ldots, n\}$ so that the set*

$$\mathcal{B}_{\sigma,m} := \{u_1, \ldots, u_m, v_{\sigma(m+1)}, \ldots, v_{\sigma(n)}\}$$

is also a basis of V.

Proof. The proof is identical to the proof of Theorem 2.34. □

As in Section 2.4, the Replacement Theorem leads to the following important result:

Theorem 5.33. *Let V be a vector space. Then every basis on V has the same number of elements.*

Proof. The proof is identical to the proof of Theorem 2.27 given in Section 2.4. □

The above theorem implies that the following definition is well defined:

Definition 5.34. *Let V be a vector space. The* ***dimension*** *of V is the number of elements in a basis of V. The dimension of V is denoted as* $\dim\ V$.

Example 5.35. *Let $M_{m,n}(\mathbb{R})$ be the vector space of $m \times n$ real matrices. Exercise 5.30 implies that* $\dim\ M_{m,n}(\mathbb{R}) = mn$.

Corollary 5.36. *Let V be a vector space of dimension n and let $\{v_1, \ldots, v_m\}$ be any set of m vectors of V where $m > n$. Then $\{v_1, \ldots, v_m\}$ must be linearly dependent.*

Proof. Suppose (for a moment) that $\{v_1, \ldots, v_m\}$ is linearly independent. Then certainly the subset $\{v_1, \ldots, v_n\}$ is also linearly independent. Let $\mathbb{B} := \{x_1, \ldots, x_n\}$ be any basis on V. By the Replacement Theorem, one can obtain a new basis by replacing n elements of $\mathbb{B}$ with $\{v_1, \ldots, v_n\}$. Since $\mathcal{B}$ has n elements, the new basis is simply $\{v_1, \ldots, v_n\}$. However, this means that v_{n+1} is a linear combination of $\{v_1, \ldots, v_n\}$ which is a contradiction. Hence, $\{v_1, \ldots, v_m\}$ must be linearly dependent. □

Exercise 5.37. *Let $Sym_n(\mathbb{R})$ be the set of $n \times n$ symmetric matrices. Recall that an $n \times n$ matrix A is symmetric if $A^T = A$.*

(i) Show that $Sym_n(\mathbb{R})$ is a subspace of $M_{n,n}(\mathbb{R})$.
(ii) Find the dimension of $Sym_n(\mathbb{R})$.

Theorem 5.38 (The Extension Theorem)**.** *Let V be a vector space of dimension n and let $\{v_1, \ldots, v_k\}$ be a linearly independent set of V with $k < n$. Then there exists vectors $v_{k+1}, \ldots, v_n$ of V such that $\{v_1, \ldots, v_k, v_{k+1}, \ldots, v_n\}$ is a basis on V.*

Proof. Let $\mathcal{B} := \{x_1, \ldots, x_n\}$ be any basis on V. By the Replacement Theorem (Theorem 5.32), there is a reordering of $\mathcal{B}$

$$\mathcal{B}_\sigma := \{x_{\sigma(1)}, \ldots, x_{\sigma(n)}\}$$

where σ is some permutation of $\{1, 2, \ldots, n\}$ such that a new basis can be formed by replacing the first k elements of $\mathcal{B}_\sigma$ with $v_1, \ldots, v_k$. In other words,

$$\{v_1, \ldots, v_k, x_{\sigma(k+1)}, \ldots, x_{\sigma(n)}\}$$

is a basis on V. Setting $v_i := x_{\sigma(i)}$ for $i = k+1, \ldots, n$ completes the proof. □

Example 5.39. *Let $\mathbb{R}[x]_3$ be the vector space of polynomials of degree 3 or less. Consider the elements $p_1(x) = x + 1$ and $p_2(x) = 5x + 3$. It is easy to see that $p_1(x)$ and $p_2(x)$ are linearly independent. By the Extension Theorem (Theorem 5.38), there exists a basis of $\mathbb{R}[x]_3$ which contains $p_1(x)$ and $p_2(x)$ as its first two elements. Let us find such a basis. Using the proof of Theorem 5.38 as a guide, let us start by choosing a basis of $\mathbb{R}[x]_3$. Clearly, $\{1, x, x^2, x^3\}$ is a basis on $\mathbb{R}[x]_3$. Since $p_1(x)$ and $p_2(x)$ are degree 1 polynomials, our intuition suggests that we should replace 1 and x with $p_1(x)$ and $p_2(x)$ to obtain a new basis. We leave it to the reader to verify that*

$$\{p_1(x), p_2(x), x^2, x^3\}$$

is also a basis on $\mathbb{R}[x]_3$.

We conclude this section with the following result:

Corollary 5.40. *Let V be a vector space of dimension $n > 0$ and let $\{v_1, v_2, \ldots, v_n\}$ be a subset of V which spans V. Then $\{v_1, v_2, \ldots, v_n\}$ is a basis of V.*

Proof. Let $S := \{v_1, v_2, \ldots, v_n\}$. We need to show that S is linearly independent. Let's suppose (for a moment) that S is not linearly independent and let's observe what happens. Let k be the maximum number of linearly independent elements in S. Since $1 \le \dim V = n$ and $V = \text{span } S$, we have $1 \le k < n$. Let us reorder the elements of S so that the first k elements of the reordering are linearly independent. In other words, we choose a permutation σ of $\{1, 2, \ldots, n\}$ such that

$$S_1 := \{v_{\sigma(1)}, \ldots, v_{\sigma(k)}\}$$

is linearly independent. Consider the set $S_1 \cup \{v_{\sigma(i)}\}$ where $i > k$. Since k is the maximum number of linearly independent elements in S, this set of $k+1$ elements cannot be linearly independent. Hence, there exists $c_1, \ldots, c_{k+1} \in \mathbb{R}$ (which are not all zero) such that

$$c_1 v_{\sigma(1)} + \cdots + c_k v_{\sigma(k)} + c_{k+1} v_{\sigma(i)} = \mathbf{0}.$$

If $c_{k+1} = 0$, then the linear independence of S_1 implies that $c_1, \ldots, c_k$ are zero as well. Hence, $c_{k+1} \neq 0$. This implies that $v_{\sigma(i)}$ can be expressed as a linear combination of the elements of S_1 for $i > k$. Now let $V_1 := \text{span } S_1$. Then V_1 is a subspace of V by Proposition 5.24. We have just seen that $v_{\sigma(i)} \in V_1$ for $i > k$. Since $v_{\sigma(i)} \in S_1$ for $i \le k$, we actually have $v_j \in V_1$ for $j = 1, \ldots, n$. Since $V = \text{span } S$, it follows that $V_1 = V$. Hence, S_1 is a linearly independent set which spans V. In other words, S_1 is a basis of V. By Theorem 5.33, every basis of V has the same number of elements and the dimension of V is simply the cardinality of any basis. Since $\dim\ V = n$ and S_1 has $k < n$ elements, we have a clear contradiction. This contradiction arose from our assumption that S was linearly dependent. From this, we conclude that S is actually linearly independent. □

5.4. Linear Maps

In Chapter 3, we considered maps from $\mathbb{R}^n$ to $\mathbb{R}^m$ that were defined in terms of matrix multiplication. Specifically, given an $m \times n$ matrix A, we expressed the vectors of $\mathbb{R}^n$ and $\mathbb{R}^m$ as *column* vectors (as opposed to the more usual row vectors as we did in Chapter 2). With this point of view, we obtain a map $A : \mathbb{R}^n \to \mathbb{R}^m$ which takes a (column) vector $\vec{v} \in \mathbb{R}^n$ to a (column) vector $A\vec{v} \in \mathbb{R}^m$ by multiplying the $m \times n$ matrix A by the $n \times 1$ matrix $\vec{v}$. We called this type of map a **linear transformation** and it has the following two properties:

(i) $A(\vec{u} + \vec{v}) = A\vec{u} + A\vec{v}$ for all $\vec{u}, \vec{v} \in \mathbb{R}^n$

(ii) $A(c\vec{v}) = cA\vec{v}$ for all $c \in \mathbb{R}$ and $\vec{v} \in \mathbb{R}^n$

Properties (i) and (ii) above motivate the more general notion of a **linear map** between general vector spaces.

Definition 5.41. *Let V and W be vector spaces. A **linear map** (or **linear homomorphism**) is a map $\varphi : V \to W$ which satisfies the following two conditions:*

(i) $\varphi(u+v) = \varphi(u) + \varphi(v)$ *for all* $u, v \in V$

(ii) $\varphi(cv) = c\varphi(v)$ *for all* $c \in \mathbb{R}$

Example 5.42. *A linear transformation from $\mathbb{R}^n$ to $\mathbb{R}^m$ is just a special case of a linear map.*

Example 5.43. *Let $\mathbb{R}[x]$ be the vector space of polynomials with real coefficients. Define $\varphi : \mathbb{R}[x] \to \mathbb{R}[x]$ be the map defined by differentiation:*

$$\varphi(p(x)) := \frac{d}{dx}p(x).$$

Then for any $p(x),\ q(x) \in \mathbb{R}[x]$ we have

$$\begin{aligned}\varphi(p(x)+q(x)) &= \frac{d}{dx}(p(x)+q(x)) \\ &= \frac{d}{dx}p(x) + \frac{d}{dx}q(x) \\ &= \varphi(p(x)) + \varphi(q(x)).\end{aligned}$$

Also, for $c \in \mathbb{R}$, we have

$$\begin{aligned}\varphi(cp(x)) &= \frac{d}{dx}cp(x) \\ &= c\frac{d}{dx}p(x) \\ &= c\varphi(p(x)).\end{aligned}$$

Hence, φ is a linear map.

Notation 5.44. *Given two vector spaces V and W, we will denote the zero vector in V and W using the same symbol: $\mathbf{0}$. Technically, one should use different symbols to denote the zero vectors of V and W. For example, one can denote the zero vector of V by $\mathbf{0}_V$ and the zero vector of W by $\mathbf{0}_W$. However, to keep the notation simple, we will avoid doing this. In fact, virtually all linear algebra books (and abstract algebra books) do not bother to use additional notation to distinguish the zero vector of one vector space from the zero vector of another. The reason for this is that the reader can easily distinguish the zero vector of one vector space from the zero vector of another by context alone.*

Proposition 5.45. *Let $\varphi : V \to W$ be a linear map. Then $\varphi(\mathbf{0}) = \mathbf{0}$.*

Proof. Using the linearity of φ, we have

$$\varphi(\mathbf{0}) = \varphi(\mathbf{0} + \mathbf{0}) = \varphi(\mathbf{0}) + \varphi(\mathbf{0}) = 2\varphi(\mathbf{0}).$$

The above equation implies that $\varphi(\mathbf{0}) = \mathbf{0}$. □

The following result is intuitively clear, but we prove it anyway for completeness.

Proposition 5.46. *Let $\varphi : V \to W$ be a linear map. Let $v_1, \dots, v_k \in V$ be a finite collection of vectors. Then*

$$\varphi(v_1 + \cdots + v_k) = \varphi(v_1) + \cdots + \varphi(v_k).$$

Proof. We prove this by induction on k. When $k = 2$, the result holds from the definition of a linear map. Suppose then that the result holds for a sum of k vectors. We now show that it holds for a sum of $k+1$ vectors. Let $v_1, \dots, v_k, v_{k+1} \in V$ and let $v = v_1 + \cdots + v_k$. Then

$$\begin{aligned}
\varphi(v_1 + \cdots + v_{k+1}) &= \varphi(v + v_{k+1}) \\
&= \varphi(v) + \varphi(v_{k+1}) \\
&= \varphi(v_1 + \cdots + v_k) + \varphi(v_{k+1}) \\
&= \varphi(v_1) + \cdots + \varphi(v_k) + \varphi(v_{k+1}),
\end{aligned}$$

where the second equality follows from the definition of a linear map and the last equality follows from the induction hypothesis. This completes the proof. □

Exercise 5.47. *Let $\mathbb{R}[x]$ be the vector space of polynomials of real coefficients. Fix a polynomial $g(x)$. Define $\varphi : \mathbb{R}[x] \to \mathbb{R}[x]$ by $\varphi(p(x)) = g(x)p(x)$. Show that φ is a linear map.*

The definition of a linear map implies that a linear map is completely determined once one specifies the values of the map on a basis of the domain. Specifically, one has the following:

Proposition 5.48. *Let V and W be vector spaces. Let $\{v_1, \dots, v_n\}$ be a basis on V and let $\{w_1, \dots, w_n\}$ be* ***any*** *vectors on W. Then there exists a unique linear map $\varphi : V \to W$ such that $\varphi(v_i) = w_i$ for $i = 1, 2, \dots, n$.*

Proof. Let $v \in V$. Then v can be expressed as a unique linear combination of the basis $\{v_1, \dots, v_n\}$:

$$v = c_1 v_1 + c_2 v_2 + \cdots + c_n v_n.$$

Define

$$\varphi(v) := \sum_{i=1}^{n} c_i w_i.$$

From the above definition, it follows that $\varphi(v_j) = w_j$ for $j = 1, \ldots, n$ since $x_j = \sum_{i=1}^{n} c_i v_i$ where $c_i = 0$ for $i \neq j$ and $c_j = 1$. Now we verify that φ satisfies the conditions of a linear map. With $v \in V$ as before, let $u \in V$ and express u as a linear combination of $\{v_1, \ldots, v_n\}$:

$$u = d_1 v_1 + d_2 v_2 + \cdots + d_n v_n.$$

Then

$$\varphi(u) := \sum_{i=1}^{n} d_i w_i.$$

Since

$$v + u = (c_1 + d_1)v_1 + \cdots + (c_n + d_n)v_n,$$

we have

$$\begin{aligned} \varphi(v+u) &= \sum_{i=1}^{n} (c_i + d_i) w_i \\ &= \sum_{i=1}^{n} c_i w_i + \sum_{i=1}^{n} d_i w_i \\ &= \varphi(v) + \varphi(u). \end{aligned}$$

Also, since $rv = \sum_{i=1}^{n} (rc_i) v_i$ for $r \in \mathbb{R}$, we have

$$\begin{aligned} \varphi(rv) &= \sum_{i=1}^{n} (rc_i) w_i \\ &= r \left(\sum_{i=1}^{n} c_i w_i \right) \\ &= r\varphi(v). \end{aligned}$$

This proves that φ is a linear map.

For the uniqueness part, suppose $\psi : V \to W$ is another linear map such that $\psi(v_i) = w_i$ for $i = 1, \ldots, n$. Let $v \in V$. Then $v = \sum_{i=1}^{n} c_i v_i$ for some $c_i \in \mathbb{R}$. Since

ψ is linear, we have

$$\begin{aligned}\psi(v) &= \psi\left(\sum_{i=1}^{n} c_i v_i\right)\\ &= \sum_{i=1}^{n} \psi(c_i v_i)\\ &= \sum_{i=1}^{n} c_i \psi(v_i)\\ &= \sum_{i=1}^{n} c_i w_i\\ &= \varphi(v).\end{aligned}$$

Hence, $\psi = \varphi$. This proves that there is exactly one linear map from V to W which maps the basis element v_i of V to an element w_i of W for $i = 1, \ldots, n$. □

Exercise 5.49. *Suppose one replaces* ***basis*** *in Proposition 5.48 by* ***spanning set****. Explain why the conclusion of Proposition 5.48 will fail in general.*

The condition of linearity is quite strong. Proposition 5.48 shows that given a basis $\mathcal{B} := \{v_1, \ldots, v_n\}$ of V and a map $\varphi : \mathcal{B} \to W$, there is only way to extend it to a linear map on all of V. From now on, when we have a map $\varphi : \mathcal{B} \to W$ and use the words *extend by linearity*, we are referring to the unique linear map from V to W whose restriction to the basis $\mathcal{B}$ is precisely the map $\varphi : \mathcal{B} \to W$. We will denote this unique linear map with the same symbol: $\varphi : V \to W$.

Example 5.50. *Let $\mathbb{R}[x]_d$ be the vector space of polynomials of degree d or less. Then $\{x^d, x^{d-1}, \ldots, x, 1\}$ is a basis of $\mathbb{R}[x]_d$. Let $\vec{v}_1, \ldots, \vec{v}_{d+1} \in \mathbb{R}^n$. By Proposition 5.48, there exists a unique linear map $\varphi : R[x]_d \to \mathbb{R}^n$ such that*

$$\varphi(x^{d+1-i}) = \vec{v}_i$$

for $i = 1, 2, \ldots, d+1$.

Next we introduce two natural subspaces associated to a linear map.

Definition 5.51. *Let $\varphi : V \to W$ be a linear map.*

(i) The ***kernel*** *(or* ***null space****) of φ is the subspace of V defined by*

$$\textit{ker } \varphi := \{v \in V \mid \varphi(v) = \mathbf{0}\}.$$

(ii) The ***image*** *(or* ***range****) of φ is the subspace of W defined by*

$$\textit{im } \varphi := \{w \in W \mid \exists\, v \in V \text{ such that } \varphi(v) = w\}.$$

The image of $\varphi : V \to W$ is also denoted as $\varphi(V)$ since

$$\text{im } \varphi = \{\varphi(v) \mid v \in V\}.$$

The next result shows that ker φ and im φ are indeed subspaces.

Proposition 5.52. *Let $\varphi : V \to W$ be a linear map. Then* ker φ *and im* φ *are subspaces.*

Proof. Let $v, v' \in \ker \varphi$ and let $c \in \mathbb{R}$. Then

$$\varphi(v + v') = \varphi(v) + \varphi(v') = \mathbf{0} + \mathbf{0} = \mathbf{0}$$

and

$$\varphi(cv) = c\varphi(v) = c\mathbf{0} = \mathbf{0}.$$

From the definition of ker φ, we conclude that $v + v'$ and cv are both elements of ker φ. This shows that ker φ is a subspace of V.

Next let $w, w' \in \text{im } \varphi$. By definition of im φ, there exists $v, v' \in \text{im } \varphi$ such that $\varphi(v) = w$ and $\varphi(v') = w'$. Hence,

$$w + w' = \varphi(v) + \varphi(v') = \varphi(v + v') \in \text{im } \varphi.$$

Also, for $c \in \mathbb{R}$, we have

$$cw = c\varphi(v) = \varphi(cv) \in \text{im } \varphi.$$

From this, we see that im φ is a subspace of W. □

For completeness, we also make the following definitions:

Definition 5.53. *Let $\varphi : V \to W$ be a linear map. Let V_1 be any subset of V and let W_1 be any subset of W. The* ***image of*** *V_1* ***under*** *φ is the set*

$$\varphi(V_1) := \{\varphi(v) \mid v \in V_1\}.$$

The ***preimage*** *(or* ***inverse image****)* ***of*** *W_1* ***under*** *φ is the set*

$$\varphi^{-1}(W_1) := \{v \in V \mid \varphi(v) \in W_1\}.$$

In Definition 5.53, note that $\varphi(V_1)$ is a subset of W and $\varphi^{-1}(W_1)$ is a subset of V.

Exercise 5.54. *Let $\varphi : V \to W$ be a linear map. Show that if V_1 is* ***subspace*** *of V and W_1 is a* ***subspace*** *of W, then $\varphi(V_1)$ is a subspace of W and $\varphi^{-1}(W_1)$ is a subspace of V.*

Example 5.55. *Let* $\pi : \mathbb{R}^2 \to \mathbb{R}$ *be the map defined by* $\pi(x, y) = x$*. It's easy to see that* π *is actually a linear map. The* ***preimage*** *of* $\pi^{-1}(1)$ *is the set of all* $(x, y) \in \mathbb{R}^2$ *such that* $\pi(x, y) = 1$*. From the definition of* π*, it's clear that*

$$\pi^{-1}(1) := \{(1, y) \mid y \in \mathbb{R}\}.$$

Example 5.56. *Let* $\mathbb{R}[x]$ *be the vector space of polynomials and let* $\varphi : \mathbb{R}[x] \to \mathbb{R}[x]$ *be the linear map defined by* $\varphi := \frac{d}{dx}$ *(see Example 5.43). The kernel of* φ *are all the polynomials* $p(x)$ *such that*

$$\varphi(p(x)) := \frac{d}{dx} p(x) = 0.$$

As we know from the Mean Value Theorem from calculus, a function which is differentiable on $(-\infty, \infty)$ *differentiates to zero if and only if the function is a constant. Hence, the kernel of* φ *consists of the constant polynomials, that is,*

$$\ker\ \varphi = \{p(x) \in \mathbb{R}[x] \mid p(x) = c \in \mathbb{R}\}.$$

The image of φ *is the subspace*

$$im\ \varphi := \{\frac{d}{dx} p(x) \mid p(x) \in \mathbb{R}[x]\} \subset \mathbb{R}[x].$$

Actually, from calculus, its quite clear that $im\ \varphi = \mathbb{R}[x]$*. Indeed, let* $p(x)$ *be any polynomial of* x *and let*

$$q(x) = \int p(x) dx$$

which is again a polynomial in x *(the constant of integration is not important). Then*

$$\varphi(q(x)) = \frac{d}{dx} q(x) = p(x).$$

This shows that $p(x) \in im\ \varphi$*. Since* $p(x)$ *was an arbitrary polynomial, it follows that* $im\ \varphi \supset \mathbb{R}[x]$*, which in turn implies that* $im\ \varphi = \mathbb{R}[x]$*.*
Hence, $\varphi := \frac{d}{dx}$ *is a linear map which is surjective, but not injective.*

Example 5.57. *Let* $T : \mathbb{R}^3 \to \mathbb{R}^3$ *be the linear map defined by*

$$T(x, y, z) := (x - y, y - z, x - z).$$

Let's find the kernel and the image of T*. The kernel of* T *is the set of all vectors* $(x, y, z) \in \mathbb{R}^3$ *such that* $T(x, y, z) = \vec{0}$*. In other words, the kernel is the solution to the linear system*

$$x - y = 0, \quad y - z = 0, \quad x - z = 0.$$

The solution to this system is easily found to be

$$\ker\ T = \{(a, a, a) \mid a \in \mathbb{R}\}.$$

From the definition of T, the image (or range) of T is

$$\text{im } T = \{(x - y, y - z, x - z) \mid x, y, z \in \mathbb{R}\}.$$

However, we can simplify the above expression by noting that $T(x, y, z)$ decomposes as

$$T(x, y, z) = x(1, 0, 1) + y(-1, 1, 0) + z(0, -1, -1).$$

Hence, im T is the span of the vectors $\vec{u}_1 = (1, 0, 1)$, $\vec{u}_2 = (-1, 1, 0)$, and $\vec{u}_3 = (0, -1, -1)$. Note that $\vec{u}_1$ and $\vec{u}_2$ are linearly independent and $\vec{u}_3$ is a linear combination of $\vec{u}_1$ and $\vec{u}_2$ (explicitly $\vec{u}_3 = -\vec{u}_1 - \vec{u}_2$). Hence, im T is the span of $\vec{u}_1$ and $\vec{u}_2$. More precisely, $\vec{u}_1$, and $\vec{u}_2$ is a basis for im T. This in turn implies that

$$\text{im } T = \{(x - y, y, x) \mid x, y \in \mathbb{R}\}.$$

In Example 5.57, we have the following relationship between the domain of T (i.e. $\mathbb{R}^3$), ker T, and im T:

$$\dim \mathbb{R}^3 = \dim \ker\ T + \dim \text{im } T$$

where we observe that $\dim \ker\ T = 1$ and $\dim \text{im } T = 2$. This is not a coincidence, but a consequence of a result called the *Rank-Nullity Theorem*, which we will state and prove in a moment. First, we need to define the terms rank and nullity.

Definition 5.58. *Let $\varphi : V \to W$ be a linear map. The* ***nullity*** *of φ is*

$$\textit{Nullity}(\varphi) := \dim \ker\ \varphi$$

and the ***rank*** *of φ is*

$$\textit{Rank}(\varphi) := \dim \textit{im } \varphi.$$

For convenience, we also prove the following result which we will use in the proof of the Rank-Nullity Theorem:

Proposition 5.59. *Let $\varphi : V \to W$ be a linear map. If $V = \textit{span}\{v_1, \ldots, v_m\}$, then*

$$\textit{im } \varphi = \textit{span}\{\varphi(v_1), \ldots, \varphi(v_m)\}.$$

Proof. By definition, im $\varphi := \{\varphi(v) \mid v \in V\}$. Since V is spanned by the vectors $v_1, \ldots, v_m$ and φ is linear, it follows that

$$\begin{aligned}\text{im } \varphi &= \{\varphi(a_1 v_1 + \cdots + a_m v_m) \mid a_1, \ldots, a_m \in \mathbb{R}\} \\ &= \{a_1 \varphi(v_1) + \cdots + a_m \varphi(v_m) \mid a_1, \ldots, a_m \in \mathbb{R}\}.\end{aligned}$$

The last equality means that im φ is spanned by the vectors $\varphi(v_1), \ldots, \varphi(v_m)$, which completes the proof. □

Theorem 5.60 (Rank-Nullity Theorem)**.** *Let $\varphi : V \to W$ be a linear map. Then*

$$\dim V = \textit{Nullity}(\varphi) + \textit{Rank}(\varphi).$$

Proof. By Proposition 5.52, ker φ and im φ are subspaces of V and W respectively. Let

$$n := \dim V, \quad k := \dim \ker\ \varphi.$$

Let $v_1, \ldots, v_k$ be a basis of ker φ. By the Extension Theorem, we extend $v_1, \ldots, v_k$ to a basis $v_1, \ldots, v_k, v_{k+1}, \ldots, v_n$ on V. By Proposition 5.59, im φ is spanned by the vectors

$$\varphi(v_1), \ldots, \varphi(v_k), \varphi(v_{k+1}), \ldots, \varphi(v_n).$$

Since $v_1, \ldots, v_k \in$ ker φ, we have $\varphi(v_1) = \cdots = \varphi(v_k) = \mathbf{0}$. Hence, the spanning set of im φ can be reduced to

$$\varphi(v_{k+1}), \ldots, \varphi(v_n).$$

We now show that these $n - k$ vectors is actually a basis on im φ. So suppose that

$$c_1\varphi(v_{k+1}) + \cdots + c_{n-k}\varphi(v_n) = \mathbf{0}$$

for some $c_1, \ldots, c_{n-k} \in \mathbb{R}$. By the linearity of φ, we can rewrite this as

$$\varphi(c_1v_{k+1} + \cdots + c_{n-k}v_n) = \mathbf{0}.$$

This implies that $c_1v_{k+1} + \cdots + c_{n-k}v_n \in$ ker φ. Let $v = c_1v_{k+1} + \cdots + c_{n-k}v_n$. Since $v \in \ker\varphi$ and $v_1, \ldots, v_k$ is a basis on $\ker\varphi$, we can express v as a linear combination of these vectors:

$$v = d_1v_1 + \cdots + d_kv_k.$$

Subtracting the two expressions for v gives

$$d_1v_1 + \cdots + d_kv_k - c_1v_{k+1} - \cdots - c_{n-k}v_n = \mathbf{0}.$$

Since $v_1, \ldots, v_k, v_{k+1}, \ldots, v_n$ is a basis on V, it follows that

$$d_1 = \cdots = d_k = c_1 = \cdots = c_{n-k} = 0,$$

which in turn proves that $\varphi(v_{k+1}), \ldots, \varphi(v_n)$ is a basis on im φ. In particular, this implies that

$$\dim\ \text{im}\ \varphi = n - k = \dim\ V - \dim! \ker\varphi.$$

Rewriting this expression gives

$$\dim V = \dim\ker\ \varphi + \dim\ \text{im}\ \varphi = \text{Nullity}(\varphi) + \text{Rank}(\varphi).$$

This completes the proof. □

5.5. Linear Isomorphisms

When are two vector spaces essentially the "same"? This is the question we will give a precise answer to in this section. We begin with the following definitions:

Definition 5.61. *Let $\varphi : V \to W$ be a linear map.*

*(i) φ is **injective** if it is one-to-one, that is, if $\varphi(v_1) = \varphi(v_2)$ for some $v_1, v_2 \in V$, then $v_1 = v_2$.*

*(ii) φ is **surjective** if it is onto, that is, for any $w \in W$, there exists $v \in V$ such that $\varphi(v) = w$*

*(iii) φ is **bijective** if it is both injective and surjective.*

Proposition 5.62. *Let $\varphi : V \to W$ be a linear map.*

(i) φ is injective if and only if $\ker \varphi = \{\mathbf{0}\}$.

(ii) φ is surjective if and only if $\text{im}\varphi = W$.

Proof. (i). Suppose φ is injective. Let $v \in \ker \varphi$. Then $\varphi(v) = \mathbf{0}$. However, since φ is linear, we also have $\varphi(\mathbf{0}) = \mathbf{0}$. Hence, $\varphi(v) = \varphi(\mathbf{0})$. The definition of injective map now implies that $v = \mathbf{0}$.

On the other hand, suppose that $\ker \varphi = \{\mathbf{0}\}$. If $\varphi(v_1) = \varphi(v_2)$ for some $v_1, v_2 \in V$, then

$$\begin{aligned} \mathbf{0} &= \varphi(v_1) - \varphi(v_2) \\ &= \varphi(v_1 - v_2). \end{aligned}$$

Hence, $v_1 - v_2 \in \ker \varphi$ and since $\ker \varphi = \{\mathbf{0}\}$, we have $v_1 - v_2 = \mathbf{0}$, which in turn implies that $v_1 = v_2$. This shows that φ is injective.

(ii). Immediate from the definition of surjective and $\text{im}\varphi$. □

The notion of an "identity map" is ubiquitous in mathematics. We will need this notion shortly in order to define when two vector spaces are "equivalent".

Definition 5.63. *Let X be a set. The **identity map** on X is the map $id_X : X \to X$ defined by $id_X(x) := x$ for all $x \in X$.*

Let X, Y, and Z be any sets and let $f : X \to Y$ and $g : Y \to Z$ be any maps. We denote the composition of g and f by $g \circ f$, that is, $g \circ f$ is the map from X to Z which sends $x \in X$ first to $f(x) \in Y$ and then sends $f(x)$ to $g(f(x)) \in Z$. As a diagram, one expresses $g \circ f$ as follows:

$$X \xrightarrow{f} Y \xrightarrow{g} Z$$

Exercise 5.64. *Let $f : X \to Y$ be any map between two sets. Verify that $id_Y \circ f = f$ and $f \circ id_X = f$ where $id_Y \circ f$ ($f \circ id_X$) denotes the composition of id_Y and f (f and id_X).*

Exercise 5.65. *Let V be a vector space. Show that the identity map on V, $id_V : V \to V$, is a bijective linear map.*

The following two definitions gives the precise meaning of what it means for two vector spaces to be the "same".

Definition 5.66. *A linear map $\varphi : V \to W$ is a **linear isomorphism** if there exists a map $\psi : W \to V$ such that $\psi \circ \varphi = id_V$ and $\varphi \circ \psi = id_W$. The map ψ is called the inverse of φ and is typically denoted by φ^{-1}.*

To emphasize that $\varphi : V \to W$ is a linear isomorphism, one often uses the following notaton:

$$\varphi : V \xrightarrow{\sim} W.$$

Definition 5.67. *Two vector spaces V and W are said to be **isomorphic** if there exists a linear isomorphism from V to W. The condition that V and W are isomorphic is denoted as $V \simeq W$.*

From the point of view of linear algebra, two vector spaces are the "same" if they are isomorphic. Naturally, this leads to the following question: *when are two vector spaces isomorphic?* The answer is actually quite simple. But before we answer this question, we take a moment to collect some basic facts about linear isomorphisms.

Proposition 5.68. *Let $\varphi : V \to W$ be a linear map. Then φ is a linear isomorphism if and only if φ is bijective.*

Proof. Suppose φ is a linear isomorphism. Let $\varphi^{-1} : W \to V$ denote the inverse of φ. Suppose $v_1, v_2 \in V$ such that $\varphi(v_1) = \varphi(v_2)$. This implies that

$$\begin{aligned} \varphi^{-1} \circ \varphi(v_1) &= \varphi^{-1} \circ \varphi(v_2) \\ id_V(v_1) &= id_V(v_2) \\ v_1 &= v_2. \end{aligned}$$

Hence, φ is injective. Now let $w \in W$ and let $v = \varphi^{-1}(w)$. Then

$$\varphi(v) = \varphi \circ \varphi^{-1}(w) = id_W(w) = w,$$

which shows that φ is also surjective. Hence, φ is bijective.

Conversely, suppose that φ is bijective. Define $\psi : W \to V$ as follows. Let $w \in W$. Since φ is both injective and surjective, there exists a **unique** element of V, which we will denote as v_w, such that $\varphi(v_w) = w$. Define $\psi(w) := v_w$. From the definition of ψ, we have

$$\begin{aligned}\varphi \circ \psi(w) &= \varphi(v_w) \\ &= w.\end{aligned}$$

From this, we conclude that $\varphi \circ \psi = id_W$.

Now let $v \in V$ and let $w := \varphi(v)$. Then

$$\begin{aligned}\psi \circ \varphi(v) &= \psi(w) \\ &= v_w\end{aligned}$$

In order to show that $\psi \circ \varphi = id_V$, we need to show that $v_w = v$. To do this, recall that $v_w \in V$ is the unique element of V which is defined by the condition $\varphi(v_w) = w$. At the same time, we also have $w = \varphi(v)$. Since φ is injective, we conclude that $v_w = v$, which proves that $\psi \circ \varphi = id_V$. By Definition 5.66, φ is a linear isomorphism. □

Proposition 5.69. *Let $\varphi : V \to W$ be a linear isomorphism. The inverse map $\varphi^{-1} : W \to V$ is unique and linear. In particular, φ^{-1} is also a linear isomorphism and the inverse of φ^{-1} is φ. In other words, $(\varphi^{-1})^{-1} = \varphi$.*

Proof. Suppose that $\psi_1 : W \to V$ and $\psi_2 : W \to V$ are both inverses to φ. Then

$$\begin{aligned}\psi_1 &= id_V \circ \psi_1 \\ &= (\psi_2 \circ \varphi) \circ \psi_1 \\ &= \psi_2 \circ (\varphi \circ \psi_1) \\ &= \psi_2 \circ id_W \\ &= \psi_2.\end{aligned}$$

This shows that inverse map is unique.

Next we show that $\varphi^{-1} : W \to V$ is linear. Let $w_1, w_2 \in W$. First, we show that

$$\varphi^{-1}(w_1 + w_2) = \varphi^{-1}(w_1) + \varphi^{-1}(w_2).$$

To do this, let $v_1 = \varphi^{-1}(w_1)$ and $v_2 = \varphi^{-1}(w_2)$. Since φ is linear, we have

$$\begin{aligned}\varphi(v_1 + v_2) &= \varphi(v_1) + \varphi(v_2) \\ &= \varphi \circ \varphi^{-1}(w_1) + \varphi \circ \varphi^{-1}(w_2) \\ &= id_W(w_1) + id_W(w_2) \\ &= id_W(w_1 + w_2) \\ &= \varphi \circ \varphi^{-1}(w_1 + w_2).\end{aligned}$$

Since φ is bijective (in particular injective) by Proposition 5.68, the above equality implies that

$$\begin{aligned}\varphi^{-1}(w_1 + w_2) &= v_1 + v_2 \\ &= \varphi^{-1}(w_1) + \varphi^{-1}(w_2)\end{aligned}$$

where we use the definition of v_1 and v_2 in the last equality. Now let $c \in \mathbb{R}$ and let $w \in W$. To complete the proof that φ^{-1} is linear, it remains to show that

$$\varphi^{-1}(cw) = c\varphi^{-1}(w).$$

Since φ is linear, we have

$$\begin{aligned}\varphi(c\varphi^{-1}(w)) &= c\varphi \circ \varphi^{-1}(w) \\ &= c id_W(w) \\ &= id_W(cw) \\ &= \varphi \circ \varphi^{-1}(cw).\end{aligned}$$

Again, using the fact that φ is bijective, the above equality implies that $\varphi^{-1}(cw) = c\varphi^{-1}(w)$. This completes the proof that φ^{-1} is linear.

Since $\varphi^{-1} : W \to V$ is a linear map and $\varphi : V \to W$ is a map which satisfies $\varphi^{-1} \circ \varphi = id_V$ and $\varphi \circ \varphi^{-1} = id_W$, it follows by Definition 5.66 that φ^{-1} is a linear isomorphism with inverse φ. This completes the proof. □

Exercise 5.70. *Recall that we write $V \simeq W$ if there exists a linear isomorphism from V to W. Use Proposition 5.69 to show that $V \simeq W$ is equivalent to $W \simeq V$.*

Here is the answer to the question posed above: *when are two vector spaces isomorphic?*

Theorem 5.71. *Two vector spaces are isomorphic if and only they have the same dimension.*

Proof. Let V and W be isomorphic vector spaces. By definiton, there exists a linear isomorphism from V to W (or equivalently from W to V). Let $\varphi : V \xrightarrow{\sim} W$ be any linear isomorphism. By Proposition 5.68, φ is bijective. Hence, $\ker \varphi = \{\mathbf{0}\}$ and $\operatorname{im} \varphi = W$. Let $n = \dim V$ and let $v_1, \ldots, v_n$ be a basis on V. Since $v_1, \ldots, v_n$ spans V, Proposition 5.59 implies that

$$\operatorname{span}\{\varphi(v_1), \ldots, \varphi(v_n)\} = \operatorname{im} \varphi = W.$$

Now suppose that

$$c_1\varphi(v_1) + \cdots + c_n\varphi(v_n) = \mathbf{0}$$

for some $c_1, \ldots, c_n \in \mathbb{R}$. Since φ is linear, the above equality can be rewritten as

$$\varphi(c_1v_1 + \cdots + c_nv_n) = \mathbf{0}.$$

Hence, $c_1v_1 + \cdots + c_nv_n \in \ker\ \varphi$. Since $\ker\ \varphi = \{\mathbf{0}\}$ and $v_1, \ldots, v_n$ is linearly independent, we conclude that $c_1 = \cdots = c_n = 0$. This shows that $\varphi(v_1), \ldots, \varphi(v_n)$ is also linearly independent. Since these vectors also span W, it follows that they form a basis on W. Hence, $\dim W = n = \dim V$.

Conversely, suppose that $\dim V = \dim W = n$. Let $\mathcal{B} := \{v_1, \ldots, v_n\}$ be a basis on V and let $\{w_1, \ldots, w_n\}$ be a basis on W. Define a map

$$\varphi : \mathcal{B} \to W$$

by $\varphi(v_i) := w_i$ for $i = 1, \ldots, n$. By Proposition 5.48, we can extend φ by linearity to a linear map from V to W. We now show that φ is bijective. Let $v \in \ker\ \varphi$ and express v in terms of the basis $\mathcal{B}$:

$$v = c_1v_1 + \cdots + c_nv_n.$$

Then

$$\begin{aligned} \varphi(v) &= c_1\varphi(v_1) + \cdots + c_n\varphi(v_n) \\ &= c_1w_1 + \cdots + c_nw_n. \end{aligned}$$

Since $\varphi(v) = \mathbf{0}$ and $w_1, \ldots, w_n$ is a basis on W, it follows that $c_1 = \cdots = c_n = 0$. This shows that $v = 0$, which implies that $\ker\ \varphi = \{\mathbf{0}\}$. Proposition 5.62 implies that φ is injective.

Now let $w \in W$ and express w in terms of the basis $w_1, \ldots, w_n$:

$$w = d_1w_1 + \cdots + d_nw_n.$$

Define $v \in V$ by

$$v = d_1v_1 + \cdots + d_nv_n.$$

Then

$$\begin{aligned} \varphi(v) &= d_1\varphi(v_1) + \cdots + d_n\varphi(v_n) \\ &= d_1w_1 + \cdots + d_nw_n \\ &= w. \end{aligned}$$

This shows that φ is surjective. We have now shown that φ is bijective. Proposition 5.68 implies that φ is a linear isomorphism. Hence, $V \simeq W$. This completes the proof. □

The following result follows directly from the proof of Theorem 5.71.

Corollary 5.72. *Let V and W be vector spaces of dimension n. A linear map from V to W is a linear isomorphism if and only if it maps a basis of V to a basis of W. In particular, if $v_1, \ldots, v_n$ is a basis on V and $w_1, \ldots, w_n$ is a basis on W, then the linear map $\varphi : V \to W$ which is (uniquely) determined by the conditions $\varphi(v_i) = w_i$ for $i = 1, \ldots, n$, is a linear isomorphism.*

Given two vector spaces V and W of the same dimension, Corollary 5.72 implies that there are infinitely many isomorphisms between V and W. An isomorphism between two arbitrary vector spaces V and W of the same dimension is determined by choosing a basis on both V and W and then pairing up each basis element of V with a basis element of W. In general, one does not have a natural or **canonical** isomorphism between two vector spaces of the same dimension. A canonical isomorphism between two vector spaces is one that does not depend on an arbitrary choices of bases.

On the other hand, if one has two vector spaces which are not arbitrary, but are related to one another in some way, one usually has a canonical (i.e. natural) linear map between the vector spaces. Moreover, if the vector spaces are related and of the same dimension, the canonical linear map is usually an isomorphism. We will study a special class of vector spaces called **quotient vector spaces** later in Chapter 11 which will provide us with some of the most common (and important) examples of canonical isomorphisms between vector spaces.

5.6. The Direct Sum Revisited

We conclude this chapter by generalizing the notion of the direct sum to arbitrary real vector spaces of finite dimension. At the same time, we stress that everything discussed in this chapter works equally well for complex vector spaces. The proof of every result in this section is identical to the proofs given in Section 2.7 for the vector space $\mathbb{R}^n$ and its subspaces. For this reason, we omit all proofs in this section. The only difference between Section 2.7 and the current one is that we make no mention of orthogonal complements. The reason for this, of course, is that in order to define the orthogonal complement of a subspace W of a vector space V, one requires that V has its own "dot product". An arbitrary vector space does not come equipped with a natural dot product. One must specify one first. Only then can one define orthogonal complements. A dot product for a general vector space is called an *inner product* and is the subject of Chapter 9.

Throughout this section, let V be a real vector space of dimension $n \geq 1$. We begin this section with the following definition:

Definition 5.73. *Let W_1 and W_2 be subspaces of V. The* ***sum*** *of W_1 and W_2 is the subspace of V defined by*

$$W_1 + W_2 := \{w_1 + w_2 \mid w_1 \in W_1,\ w_2 \in W_2\}.$$

Exercise 5.74. *Show that $W_1 + W_2$ is indeed a subspace of V.*

Proposition 5.75. *Let W_1 and W_2 be subspaces of V. Then*

(i) $W_1 \cap W_2$ *is also a subspace of* V

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

Proof. See the proof of Proposition 2.77. $\square$

Definition 5.76. *Let W_1 and W_2 be subspaces of V. V is a* ***direct sum*** *of W_1 and W_2 if the following conditions hold:*

(i) $V = W_1 + W_2$

(ii) $W_1 \cap W_2 = \{\mathbf{0}\}$

When V is a direct sum of W_1 and W_2, one replaces the "+" symbol with the direct sum symbol "$\oplus$" and writes $V = W_1 \oplus W_2$.

Proposition 5.77. *Let W_1 and W_2 be subspaces of V. The following statements are equivalent:*

(1) $V = W_1 \oplus W_2$

(2) Every $v \in V$ can be expressed ***uniquely*** *as $v = w_1 + w_2$ for some $w_1 \in W_1$ and $w_2 \in W_2$*

(3) $\dim V = \dim W_1 + \dim W_2$ *and* $W_1 \cap W_2 = \{\mathbf{0}\}$

Proof. See the proof of Proposition 2.79. $\square$

Example 5.78. *Let $M_2(\mathbb{R})$ denote the vector space of 2×2 matrices whose entires are real numbers. Let $\mathfrak{sl}_2(\mathbb{R})$ be the subspace of $M_2(\mathbb{R})$ consisting of all 2×2 real matrices whose trace is zero. Let*

$$E := \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \quad F := \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \quad H := \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Then $\{E, F, H\}$ is a basis on $\mathfrak{sl}_2(\mathbb{R})$. Indeed, an arbitrary element of $\mathfrak{sl}_2(\mathbb{R})$ decomposes uniquely as

$$\begin{pmatrix} c & a \\ b & -c \end{pmatrix} = aE + bF + cH.$$

Hence, $\dim \mathfrak{sl}_2(\mathbb{R}) = 3$. Let I_2 denote the 2×2 identity element and let $D :=$ span $\{I_2\}$. Then $\dim D = 1$ and $\mathfrak{sl}_2(\mathbb{R}) \cap D = \{\mathbf{0}\}$. Since

$$\dim \ M_2(\mathbb{R}) = 4 = \dim \mathfrak{sl}_2(\mathbb{R}) + \dim D,$$

Proposition 5.77 implies that $M_2(\mathbb{R}) = \mathfrak{sl}_2(\mathbb{R}) \oplus D$.

Chapter 5 Exercises

1. Let $\mathbb{R}[x]_2$ be the vector space of all real polynomials of degree 2 or less. Determine if the set
$$\{\, 1 + x + x^2,\, 3 - x^2,\, 2x + x^2 \,\}$$
is a basis of $\mathbb{R}[x]_2$.

2. Determine if the set of polynomials
$$\{\, 1, x, 1 - 2x^2, -3x + 2x^3 \,\}$$
is a basis of $\mathbb{R}[x]_3$ (the vector space of real polynomials of degree 3 or less).

3. Let $M_n(\mathbb{R})$ be the vector space of $n \times n$ matrices. Let $\mathrm{A}_n(\mathbb{R}) \subset M_n(\mathbb{R})$ be the subset of all skew-symmetric matrices. Recall than a matrix A is called skew-symmetric if $A^T = -A$.
   (a) Show that $\mathrm{A}_n(\mathbb{R})$ is a subspace of $M_n(\mathbb{R})$.
   (b) Find $\dim \mathrm{A}_n(\mathbb{R})$.

4. Find a basis for the subspace of all skew-symmetric 3×3 real matrices as a subspace of all real 3×3 matrices.

5. Express the polynomial $p(x) = x^3 + 3x^2 + 2x + 1$ as a linear combination of the polynomials
$$x^3 + 2, \qquad x^2 + x, \qquad 3x + 1, \qquad 2x + 1.$$

6. Let $M_3(\mathbb{R})$ be the vector space of real 3×3 matrices. Let $\mathrm{S}_3(\mathbb{R}) \subset M_3(\mathbb{R})$ be the subset consisting of all symmetric matrices.
   (a) Show that $\mathrm{S}_3(\mathbb{R})$ is a subspace of $M_3(\mathbb{R})$.
   (b) Give a basis for $\mathrm{S}_3(\mathbb{R})$. What is the dimension of $\mathrm{S}_3(\mathbb{R})$?
   (c) Extend the basis in part (b) to a basis on $M_3(\mathbb{R})$.

7. Let $M_n(\mathbb{R})$ be the vector space of real $n \times n$ matrices. Let $p(x) \in \mathbb{R}[x]$ be a real polynomial of degree k:
$$p(x) = c_n x^k + c_{k-1} x^{k-1} + \cdots + c_1 x + c_0.$$
For a matrix $A \in M_n(\mathbb{R})$, define a matrix $p(A) \in M_n(\mathbb{R})$ by
$$p(A) = c_n A^k + c_{k-1} A^{k-1} + \cdots + c_1 A + c_0 I_n.$$
Show that for any $A \in M_n(\mathbb{R})$, there exists a nonzero real polynomial $p(x) \in \mathbb{R}[x]$ such that $p(A) = \mathbf{0}$. (Hint: consider $\dim M_n(\mathbb{R})$.)

8. Show that the subset

$$\{\text{real polynomials } f(x) \text{ of degree } \le 3 \mid f(2) = 0\}$$

is a subspace of $\mathbb{R}[x]_4$, the vector space of real polynomials of degree 4 or less. Find a basis of this subspace and determine its dimension.

9. Is the line $y = 3x - 4$ a subspace of $\mathbb{R}^2$? Is the unit disk $\{(x, y) \mid x^2 + y^2 \le 1\}$ a subspace of $\mathbb{R}^2$? Justify your answers.

10. Let $\mathfrak{sl}_2(\mathbb{R})$ denote the subspace of all 2×2 real matrices whose trace is zero. Let

$$E = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \qquad F = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \qquad H = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Let $\varphi : \mathfrak{sl}_2(\mathbb{R}) \to \mathfrak{sl}_2(\mathbb{R})$ be a linear map which satisfies the following conditions:

$$\varphi(E - 2F) = H, \qquad \varphi(E + H) = F, \qquad \varphi(F - H) = E + F.$$

(a) Find $\varphi(E)$, $\varphi(F)$, and $\varphi(H)$.
(b) Find $\ker \varphi$.
(c) Find $\operatorname{im} \varphi$.
(d) Based on (b) and (c), is φ an isomorphism?

11. Let

$$A = \begin{pmatrix} 1 & 2 & -1 \\ 1 & -4 & 2 \end{pmatrix}$$

and let $T_A : \mathbb{R}^3 \to \mathbb{R}^2$ be the linear transformation associated to A, that is, $T_A(\vec{v}) := A\vec{v}$.
(a) Find $\ker T_A$ and give its dimension.
(b) Find $\operatorname{im} T_A$ and give its dimension.
(c) Verify the Rank-Nullity Theorem (Theorem 5.60) for T_A, that is, check that

$$\dim \mathbb{R}^3 = \dim \ker T_A + \dim \operatorname{im} T_A.$$

12. Find the nullity and rank of the linear map $T : \mathbb{R}^3 \to \mathbb{R}^2$ given by

$$T(a_1, a_2, a_3) = (a_1 + a_2, -a_3).$$

13. Let

$$A = \begin{pmatrix} 2 & 1 & 2 \\ 2 & -3 & 1 \\ -2 & -5 & -3 \end{pmatrix}$$

and let $T_A : \mathbb{R}^3 \to \mathbb{R}^3$ be the linear transformation associated to A.

(a) Find $\ker T_A$ and give its dimension.
(b) Find $\operatorname{im} T_A$ and give its dimension.
(c) Verify the Rank-Nullity Theorem (Theorem 5.60) for T_A.

(d) Is T_A is an isomorphism?

14. Suppose that $T : \mathbb{R}^2 \to \mathbb{R}^2$ is a linear transformation such that $T(-1,0) = (1,4)$ and $T(1,2) = (2,5)$. Determine $T(3,4)$. Is T one-to-one?

15. Let $M_n(\mathbb{R})$ be the vector space of all real $n \times n$ matrices.
    (a) Show that the trace
    $$\mathrm{Tr} : M_n(\mathbb{R}) \to \mathbb{R}$$
    is a linear map.
    (b) The kernel of Tr is simply the subspace of $M_n(\mathbb{R})$ consisting of all real $n \times n$ matrices with zero trace. This subspace is typically denoted as $\mathfrak{sl}_n(\mathbb{R})$. Apply the Rank-Nullity Theorem (Theorem 5.60) to determine the dimension of $\mathfrak{sl}_n(\mathbb{R})$.

16. Let $M_n(\mathbb{R})$ be the vector space of all real $n \times n$ matrices and let $\mathfrak{sl}_n(\mathbb{R})$ be the subspace of all real $n \times n$ matrices with zero trace. Suppose W is a subspace of $M_n(\mathbb{R})$ of dimension n such that
    $$M_n(\mathbb{R}) = \mathfrak{sl}_n(\mathbb{R}) + W.$$
    Find $\dim W \cap \mathfrak{sl}_n(\mathbb{R})$.

17. Let $M_n(\mathbb{R})$ be the vector space of all real $n \times n$ matrices and let
    $$F : M_n(\mathbb{R}) \to M_n(\mathbb{R})$$
    be the map defined by
    $$F(A) = \frac{1}{2}(A + A^T).$$
    (a) Show that F is linear.
    (b) Find $\mathrm{im}\, F$ and give its dimension. What type of matrices make up $\mathrm{im}\, F$?
    (c) Find $\ker F$ and give its dimension. What type of matrices make up $\ker F$?

18. Let $M_n(\mathbb{R})$ be the vector space of all real $n \times n$ matrices. Let $\mathrm{S}_n(\mathbb{R})$ and $\mathrm{A}_n(\mathbb{R})$ denote the subspaces of real $n \times n$ symmetric and skew-symmetric matrices respectively. Determine if
    $$M_n(\mathbb{R}) = \mathrm{S}_n(\mathbb{R}) \oplus \mathrm{A}_n(\mathbb{R}).$$
    Justify your answer.

19. Let V be a vector space and let $\varphi : V \to V$ be a linear map. A subspace W of V is called φ-invariant if $\varphi(W) \subset W$. Show $\ker \varphi$ and $\mathrm{im}\, \varphi$ are φ-invariant.

Chapter 6

Return to $\mathbb{R}^n$... Sort of

After Chapter 5, you might be nostalgic for the days when a vector was just an element of $\mathbb{R}^n$ (expressed either as a row or column vector) and a linear map was just a matrix which mapped column vectors of $\mathbb{R}^n$ to column vectors of $\mathbb{R}^m$ by matrix multiplication. It was so much simpler back then!

Well, it turns out that any (real) n-dimensional vector space can be *regarded* as the vector space $\mathbb{R}^n$ and any linear map between (finite dimensional) vector spaces can be *regarded* as a matrix. However, there's a catch. Before explaining what the catch is, let me explain what is meant by the word *regarded* here. Saying that we can regard any n-dimensional vector space V as $\mathbb{R}^n$ means that we have a way of representing each vector in V as a unique vector in $\mathbb{R}^n$. More precisely, we have a one-to-one correspondence between V and $\mathbb{R}^n$. Likewise, we have a way of representing any linear map between finite dimensional vector spaces as a matrix. The catch is that this representation is very far from being unique. The representation depends on a choice of basis or bases. Even so, the idea of representing general vectors as vectors in $\mathbb{R}^n$ or linear maps as matrices turns out to be mathematically fruitful. For example, the matrix representations of a linear map $\varphi : V \to V$ with respect to two different bases turn out to be related to one another in a very simple way. As we will see later, this simple form allows one to extend the idea of the determinant from square matrices to any linear map $\varphi : V \to V$ in a manner which is completely independent of a choice of basis on V. In addition, there is also a computational benefit from being able to express vectors as column vectors of $\mathbb{R}^n$ and linear maps as matrices.

For the sake of concreteness, we work with real vector spaces throughout this chapter. However, if we replace $\mathbb{R}^n$ with $\mathbb{C}^n$ and all real vector spaces by complex ones, all the definitions, results, and proofs of this chapter work exactly as before. In short, everything in this chapter applies equally well to the complex case.

6.1. Coordinate Vectors

Let V be a vector space of dimension n. For concreteness, we will also take V to be a real vector space, but we could just as easily take V to be a complex vector space. **For the rest of this chapter, we will always regard the vectors of $\mathbb{R}^n$ as column vectors**. We begin with the main definition of this section:

Definition 6.1. *Let $\mathcal{B} = \{v_1, \ldots, v_n\}$ be a basis on V. The* ***coordinate vector*** *of a vector $v \in V$* ***with respect to*** *$\mathcal{B}$ is the unique column vector*

$$[v]_{\mathcal{B}} := (a_1, a_2, \ldots, a_n)^T \in \mathbb{R}^n$$

where $a_1, a_2, \ldots, a_n$ are defined by the condition

$$v = a_1 v_1 + a_2 v_2 + \cdots + a_n v_n.$$

Example 6.2. *Consider the vector space $V = \mathbb{R}^2$. Let $\mathcal{B} = \{\vec{v}_1, \vec{v}_2\}$ be the basis on V with $\vec{v}_1 := (1,1)^T$ and $\vec{v}_2 = (0,1)^T$. Let $\vec{v} = (2,3)^T \in V$. Let us compute the coordinate vector $[\vec{v}]_B$ of $\vec{v}$ with respect to $\mathcal{B}$. By definition, $[\vec{v}]_B$ is the column vector*

$$[\vec{v}]_{\mathcal{B}} := \begin{pmatrix} a_1 \\ a_2 \end{pmatrix}$$

where a_1 and a_2 are uniquely defined by the condition

$$\vec{v} = a_1\vec{v}_1 + a_2\vec{v}_2.$$

The above equation is equivalent to the following linear system:

$$\begin{aligned} a_1 &= 2 \\ a_1 + a_2 &= 3. \end{aligned}$$

The solution to the above system is $a_1 = 2$ and $a_2 = 1$. Hence, $\vec{v} = 2\vec{v}_1 + \vec{v}_2$. From this, we conclude that

$$[\vec{v}]_{\mathcal{B}} := \begin{pmatrix} 2 \\ 1 \end{pmatrix}.$$

It is important to remember that a basis is an ordered set. Hence, changing the order of the vectors in a basis will result in a new basis. For instance, let $\mathcal{B}' = \{\vec{v}_2, \vec{v}_1\}$. Then $\mathcal{B}' \neq \mathcal{B}$ and the coordinate vector of $\vec{v}$ with respect to $\mathcal{B}'$ is

$$[\vec{v}]_{\mathcal{B}'} = \begin{pmatrix} 1 \\ 2 \end{pmatrix} \neq [\vec{v}]_{\mathcal{B}}.$$

The following result follows directly from the definition of the coordinate vector:

Proposition 6.3. *Let V be a vector space of dimension n and let $\mathcal{B} = \{u_1, \ldots, u_n\}$ be a basis on V. Then the coordinate vector of u_i with respect to $\mathcal{B}$ is $[u_i]_{\mathcal{B}} = \vec{e}_i$ where $\vec{e}_i$ is the i^{th} standard basis vector on $\mathbb{R}^n$.*

Proof. Let $u_j \in \mathcal{B}$. Then u_j, as a linear combination of the basis $\mathcal{B}$, is (of course)

$$u_j = \sum_{i=1}^{n} c_{ij} u_i$$

where $c_{ij} = 0$ for all $i \neq j$ and $c_{jj} = 1$. By definition, we have

$$[u_j]_{\mathcal{B}} = (c_{1j}, c_{2j}, \ldots, c_{nj})^T = \vec{e}_j.$$

□

Proposition 6.4. *Let $\mathcal{S} := \{\vec{e}_1, \ldots, \vec{e}_n\}$ denote the standard basis on $\mathbb{R}^n$. For any vector $\vec{v} \in \mathbb{R}^n$, the coordinate vector of $\vec{v}$ with respect to $\mathcal{S}$ is simply itself, that is, $[\vec{v}]_{\mathcal{S}} = \vec{v}$.*

Proof. Recall that $\vec{e}_i \in \mathbb{R}^n$ is the vector whose components are all zero except for the ith component which is 1. Let $\vec{v} = (v_1, \ldots, v_n)^T \in \mathbb{R}^n$. With respect to $\mathcal{S}$, $\vec{v}$ decomposes as

$$\vec{v} = v_1\vec{e}_1 + v_2\vec{e}_2 + \cdots + v_n\vec{e}_n.$$

It follows from this that the coordinate vector of $\vec{v}$ with respect to $\mathcal{S}$ is

$$[\vec{v}]_{\mathcal{S}} = (v_1, \ldots, v_n)^T = \vec{v}.$$

□

Example 6.5. *Let $\mathbb{R}[x]_2$ denote the vector space of polynomials of degree less than or equal to 2 whose coefficients are real numbers. A basis for $\mathbb{R}[x]_2$ is $\mathcal{B} = \{x^2, x, 1\}$. Hence, for a real polynomial $p = a_2x^2 + a_1x + a_0$, the associated coordinate vector with respect to $\mathcal{B}$ is*

$$[p]_{\mathcal{B}} = (a_2, a_1, a_0)^T.$$

Another basis on $\mathbb{R}[x]_2$ is

$$\mathcal{C} = \{x^2 - 1, x + 1, x - 1\}.$$

Let us compute the coordinate vector of p with respect to $\mathcal{C}$. This amounts to solving the following equation

$$p = b_1(x^2 - 1) + b_2(x + 1) + b_3(x - 1)$$

for $b_1, b_2, b_3 \in \mathbb{R}$. The above equation is equivalent to the linear system:

$$\begin{aligned} b_1 &= a_2 \\ b_2 + b_3 &= a_1 \\ b_2 - b_3 - b_1 &= a_0. \end{aligned}$$

The solution to this system is easily found to be

$$b_1 = a_2, \quad b_2 = \frac{a_0 + a_1 + a_2}{2}, \quad b_3 = \frac{a_1 - a_0 - a_2}{2}.$$

Hence,

$$[p]_{\mathcal{C}} = (a_2, \frac{a_0 + a_1 + a_2}{2}, \frac{a_1 - a_0 - a_2}{2})^T.$$

Example 6.6. *Consider the vector space $\mathbb{R}^3$ and let $\mathcal{B} = \{\vec{u}_1, \vec{u}_2, \vec{u}_3\}$ be the orthonormal basis on $\mathbb{R}^3$ defined by*

$$\vec{u}_1 := (1, 0, 0)^T, \quad \vec{u}_2 := (0, 5/13, 12/13)^T, \quad \vec{u}_3 := (0, 12/13, -5/13)^T.$$

Let $\vec{v} = (1, 2, 3)^T \in \mathbb{R}^3$. Since $\mathcal{B}$ is an orthonormal basis, it follows from Theorem 2.62 that

$$\begin{aligned} \vec{v} &= (\vec{v} \cdot \vec{u}_1)\vec{u}_1 + (\vec{v} \cdot \vec{u}_2)\vec{u}_2 + (\vec{v} \cdot \vec{u}_3)\vec{u}_3 \\ &= \vec{u}_1 + \frac{46}{13}\vec{u}_2 + \frac{9}{13}\vec{u}_3. \end{aligned}$$

Hence, $[\vec{v}]_{\mathcal{B}} = (1, 46/13, 9/13)^T$.

We conclude this section with another (basic) observation:

Proposition 6.7. *Let V be a vector space of dimension n and let $\mathcal{B} = \{u_1, \ldots, u_n\}$ be a basis on V. Let $v, w \in V$ and $c \in \mathbb{R}$. Then the following identities hold:*

(i) $[v + w]_{\mathcal{B}} = [v]_{\mathcal{B}} + [w]_{\mathcal{B}}$

(ii) $[cv]_{\mathcal{B}} = c[v]_{\mathcal{B}}$

Proof. Suppose that

$$[v]_{\mathcal{B}} = (a_1, \ldots, a_n)^T$$

and

$$[w]_{\mathcal{B}} = (b_1, \ldots, b_n)^T.$$

From the definition of the coordinate vector, we have

$$v = a_1u_1 + a_2u_2 + \cdots + a_nu_n$$

and

$$w = b_1u_1 + b_2u_2 + \cdots + b_nu_n.$$

This in turn implies that

$$v + w = (a_1 + b_1)u_1 + (a_2 + b_2)u_2 + \cdots + (a_n + b_n)u_n.$$

Hence,

$$[v + w]_{\mathcal{B}} = (a_1 + b_1, a_2 + b_2, \ldots, a_n + b_n)^T = [v]_{\mathcal{B}} + [w]_{\mathcal{B}}.$$

This proves (i). For (ii), we have

$$cv = (ca_1)u_1 + (ca_2)u_2 + \cdots + (ca_n)u_n,$$

which in turn implies that

$$[cv]_{\mathcal{B}} = (ca_1, ca_2, \ldots, ca_n)^T = c[v]_{\mathcal{B}}.$$

This completes the proof. □

6.2. The Transition Matrix

Let

$$\mathcal{B} = \{u_1, \ldots, u_n\}, \quad \mathcal{B}' = \{v_1, \ldots, v_n\}$$

be bases on V. Given any vector $v \in V$, we would like to determine how $\vec{v}_{\mathcal{B}}$ and $\vec{v}_{\mathcal{B}'}$ are related to one another. This will lead us to the notion of a **transition matrix**. Since $\mathcal{B}'$ is a basis, we can express every element of $\mathcal{B}$ as a (unique) linear combination of the elements of $\mathcal{B}'$:

$$u_j = \sum_{i=1}^{n} c_{ij} v_i, \quad \text{for } j = 1, \ldots, n. \tag{78}$$

Let $P_{\mathcal{B}'\mathcal{B}}$ be the $n \times n$ matrix

$$P_{\mathcal{B}'\mathcal{B}} = \begin{pmatrix} c_{11} & \cdots & c_{1n} \\ \vdots & \ddots & \vdots \\ c_{n1} & \cdots & c_{nn} \end{pmatrix} \tag{79}$$

The matrix $P_{\mathcal{B}'\mathcal{B}}$ is called the **transition matrix** or **change of basis matrix** from $\mathcal{B}$ to $\mathcal{B}'$. The motivation for this name will become clear in a moment. Now let $v \in V$ and suppose that

$$[v]_{\mathcal{B}} = (a_1, \ldots, a_n)^T, \qquad [v]_{\mathcal{B}'} = (b_1, \ldots, b_n)^T.$$

By definition, this means that

$$v = \sum_{i=1}^{n} a_i u_i \tag{80}$$

and

$$v = \sum_{i=1}^{n} b_i v_i. \tag{81}$$

Substituting (78) into (80) gives

$$v = \sum_{j=1}^{n} a_j \left(\sum_{i=1}^{n} c_{ij} v_i \right) = \sum_{i=1}^{n} \left(\sum_{j=1}^{n} c_{ij} a_j \right) v_i. \tag{82}$$

Since $\mathcal{B}'$ is a basis, the scalars appearing in (81) are unique. Hence, by comparing (81) and (82), we see that

$$b_i = \sum_{j=1}^{n} c_{ij} a_j. \tag{83}$$

However, the right side of (83) is simply the ith component of the column vector $P_{\mathcal{B}'\mathcal{B}}[v]_{\mathcal{B}}$. In other words, we have proven the following:

Theorem 6.8. *Let V be a vector space and let $\mathcal{B}$ and $\mathcal{B}'$ be any bases on V. For any $v \in V$, the coordinate vectors $[v]_{\mathcal{B}}$ and $[v]_{\mathcal{B}'}$ are related by the following equation:*

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

Theorem 6.8 justifies the name transition matrix (or change of base matrix) for the matrix $P_{\mathcal{B}'\mathcal{B}}$. Indeed, the transition matrix $P_{\mathcal{B}'\mathcal{B}}$ tells one how to transform a coordinate vector in the $\mathcal{B}$-coordinates to one in the $\mathcal{B}'$-coordinates.

The following result shows that the transition matrix can be conveniently expressed in terms of coordinate vectors:

Proposition 6.9. *Let V be a vector space of dimension n and let*

$$\mathcal{B} = \{u_1, \ldots, u_n\} \quad \text{and} \quad \mathcal{B}' = \{v_1, \ldots, v_n\}$$

be bases on V. Then the i^{th} column of the transition matrix $P_{\mathcal{B}'\mathcal{B}}$ is the coordinate vector of u_i with respect to the basis $\mathcal{B}'$. In other words,

$$P_{\mathcal{B}'\mathcal{B}} = ([u_1]_{\mathcal{B}'},\ [u_2]_{\mathcal{B}'}, \ldots, [u_n]_{\mathcal{B}'}) \tag{84}$$

Proof. For $j = 1, \ldots, n$, let us express the basis vector u_j as a linear combination of the basis $\mathcal{B}'$:

$$u_j = \sum_{i=1}^{n} c_{ij} v_i. \tag{85}$$

Equation (85) implies that the coordinate vector of u_j with respect to $\mathcal{B}'$ is

$$[u_j]_{\mathcal{B}'} = \begin{pmatrix} c_{1j} \\ c_{2j} \\ \vdots \\ c_{nj} \end{pmatrix}. \tag{86}$$

On the other hand, from the definition of the transition matrix (equations (78) and (79)), we have

$$P_{\mathcal{B}'\mathcal{B}} = \begin{pmatrix} c_{11} & \cdots & c_{1n} \\ \vdots & \ddots & \vdots \\ c_{n1} & \cdots & c_{nn} \end{pmatrix} \tag{87}$$

Comparing (86) and (87), we see that the j^{th} column of $P_{\mathcal{B}'\mathcal{B}}$ is precisely $[u_j]_{\mathcal{B}'}$. Hence, we can rewrite $P_{\mathcal{B}'\mathcal{B}}$ as

$$P_{\mathcal{B}'\mathcal{B}} = ([u_1]_{\mathcal{B}'},\ [u_2]_{\mathcal{B}'}, \ldots, [u_n]_{\mathcal{B}'}).$$

This completes the proof. □

Proposition 6.10. *Let $\mathcal{B} = \{\vec{v}_1, \ldots, \vec{v}_n\}$ be any basis on $\mathbb{R}^n$ and let $\mathcal{S} = \{\vec{e}_1, \ldots, \vec{e}_n\}$ denote the standard basis on $\mathbb{R}^n$. Then*

$$P_{\mathcal{S}\mathcal{B}} = (\vec{v}_1,\ \vec{v}_2,\ \ldots, \vec{v}_n).$$

Proof. From Proposition 6.4, we have $[\vec{v}]_{\mathcal{S}} = \vec{v}$ for any vector $\vec{v} \in \mathbb{R}^n$. By Proposition 6.9, we have

$$\begin{aligned} P_{\mathcal{S}\mathcal{B}} &= ([\vec{v}_1]_{\mathcal{S}},\ [\vec{v}_2]_{\mathcal{S}},\ \ldots,\ [\vec{v}_n]_{\mathcal{S}}) \\ &= (\vec{v}_1,\ \vec{v}_2,\ \ldots, \vec{v}_n). \end{aligned}$$

□

Example 6.11. *Let us consider a simple "test" of Theorem 6.8. Let* $\mathcal{B} = \{\vec{v}_1, \vec{v}_2\}$ *be the basis on* $\mathbb{R}^2$ *given by*

$$\vec{v}_1 = (1, -1)^T, \quad \vec{v}_2 = (4, -3)^T$$

and let $\mathcal{S} = \{\vec{e}_1, \vec{e}_2\}$ *be the standard basis on* $\mathbb{R}^2$*. By Proposition 6.10, we have*

$$P_{\mathcal{SB}} = (\vec{v}_1,\ \vec{v}_2) = \begin{pmatrix} 1 & 4 \\ -1 & -3 \end{pmatrix}.$$

Let $\vec{x} \in \mathbb{R}^n$ *be the vector whose coordinate representation with respect to* $\mathcal{B}$ *is*

$$[\vec{x}]_{\mathcal{B}} = (-2, 5)^T.$$

In other words, $\vec{x}$ *is given by*

$$\vec{x} = -2\vec{v}_1 + 5\vec{v}_2 = (-2, 2)^T + (20, -15)^T = (18, -13)^T.$$

By Proposition 6.4, $[\vec{x}]_{\mathcal{S}} = \vec{x}$*. By Theorem 6.8, we should obtain the same exact answer. Let us verify that this is indeed the case:*

$$P_{\mathcal{SB}}[\vec{x}]_{\mathcal{B}} = \begin{pmatrix} 1 & 4 \\ -1 & -3 \end{pmatrix} \begin{pmatrix} -2 \\ 5 \end{pmatrix} = \begin{pmatrix} 18 \\ -13 \end{pmatrix} = \vec{x} = [\vec{x}]_S.$$

The next result will prove useful for computing the transition matrix between two arbitrary bases $\mathcal{B}$ and $\mathcal{B}'$ on a vector space V.

Theorem 6.12. *Let* V *be a vector space of dimension* n *and let* $\mathcal{B}$*,* $\mathcal{C}$*, and* $\mathcal{D}$ *be bases on* V*. Then*

(a) $P_{\mathcal{BB}} = I_n$ *where* I_n *is the* $n \times n$ *identity matrix*
(b) $P_{\mathcal{DB}} = P_{\mathcal{DC}} P_{\mathcal{CB}}$
(c) $P_{\mathcal{CB}}^{-1} = P_{\mathcal{BC}}$

Proof. Let

$$\mathcal{B} = \{u_1, \ldots, u_n\}.$$

(a): By Proposition 6.3, we have $[u_i]_{\mathcal{B}} = \vec{e}_i$ for $i = 1, \ldots, n$. By Proposition 6.9, we have

$$\begin{aligned} P_{\mathcal{BB}} &= ([u_1]_{\mathcal{B}},\ [u_2]_{\mathcal{B}}, \ldots, [u_n]_{\mathcal{B}}) \\ &= (\vec{e}_1,\ \vec{e}_2,\ \ldots,\ \vec{e}_n) \\ &= I_n. \end{aligned}$$

(b): Let $v \in V$ be an arbitrary vector. Using Theorem 6.8, we have

$$[v]_{\mathcal{D}} = P_{\mathcal{DB}}[v]_{\mathcal{B}}$$

However, we also have

$$\begin{aligned}[v]_{\mathcal{D}} &= P_{\mathcal{DC}}[v]_{\mathcal{C}} \\ &= P_{\mathcal{DC}}\left(P_{\mathcal{CB}}[v]_{\mathcal{B}}\right) \\ &= \left(P_{\mathcal{DC}}P_{\mathcal{CB}}\right)[v]_{\mathcal{B}}.\end{aligned}$$

This shows that

$$P_{\mathcal{DB}}[v]_{\mathcal{B}} = \left(P_{\mathcal{DC}}P_{\mathcal{CB}}\right)[v]_{\mathcal{B}}. \tag{88}$$

Setting $v = u_i$ for any $i \in \{1, \ldots, n\}$ in (88), we obtain

$$P_{\mathcal{DB}}\vec{e}_i = \left(P_{\mathcal{DC}}P_{\mathcal{CB}}\right)\vec{e}_i \tag{89}$$

where we use the fact that $[u_i]_{\mathcal{B}} = \vec{e}_i$ (by Proposition 6.3). Equation (89) implies that the ith column of $P_{\mathcal{DB}}$ and $P_{\mathcal{DC}}P_{\mathcal{CB}}$ are equal for $i = 1, \ldots, n$. This in turn implies that

$$P_{\mathcal{DB}} = P_{\mathcal{DC}}P_{\mathcal{CB}}.$$

(c): Using (a) and (b), we find that

$$P_{\mathcal{BC}}P_{\mathcal{CB}} = P_{\mathcal{BB}} = I_n$$

and

$$P_{\mathcal{CB}}P_{\mathcal{BC}} = P_{\mathcal{CC}} = I_n.$$

This implies that $P_{\mathcal{CB}}^{-1} = P_{\mathcal{BC}}$. □

For convenience, we recall that for an invertible 2 matrix

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix},$$

its inverse is given explicitly by

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

Example 6.13. *Consider the vector space $\mathbb{R}^2$. Let $\mathcal{B}$ and $\mathcal{C}$ be the bases on $\mathbb{R}^2$ given by*

$$\mathcal{B} = \{(-1,2)^T,\ (2,5)\}$$

and

$$\mathcal{C} = \{(2,3)^T,\ (4,-1)^T\}.$$

Let us compute the transition matrix $P_{\mathcal{CB}}$ using Theorem 6.12. To do this, let $\mathcal{S} = \{\vec{e}_1, \vec{e}_2\}$ denote the standard basis on $\mathbb{R}^2$. By Proposition 6.10, we have

$$P_{\mathcal{SB}} = \begin{pmatrix} -1 & 2 \\ 2 & 5 \end{pmatrix}$$

and

$$P_{\mathcal{SC}} = \begin{pmatrix} 2 & 4 \\ 3 & -1 \end{pmatrix}.$$

Using Theorem 6.12, we have

$$\begin{aligned} P_{\mathcal{CB}} &= P_{\mathcal{CS}} P_{\mathcal{SB}} \\ &= P_{\mathcal{SC}}^{-1} P_{\mathcal{SB}} \\ &= \begin{pmatrix} 1/14 & 2/7 \\ 3/14 & -1/7 \end{pmatrix} \begin{pmatrix} -1 & 2 \\ 2 & 5 \end{pmatrix} \\ &= \begin{pmatrix} 1/2 & 11/7 \\ -1/2 & -2/7 \end{pmatrix}. \end{aligned}$$

Let's try a simple test of the above transition matrix. Let $\vec{v} \in \mathbb{R}^2$ be the vector whose coordinate vector with respect to $\mathcal{B}$ is

$$[\vec{v}]_{\mathcal{B}} = (2,3)^T.$$

By definition, this means that

$$\vec{v} = 2(-1,2)^T + 3(2,5)^T = (4,19)^T.$$

Using the transition matrix $P_{\mathcal{CB}}$, we compute $[\vec{v}]_{\mathcal{C}}$:

$$[\vec{v}]_{\mathcal{C}} = P_{\mathcal{CB}}[\vec{v}]_{\mathcal{B}} = (40/7, -13/7)^T.$$

Let us verify that this is indeed the coordinate vector of $\vec{v}$ with respect to the basis $\mathcal{C}$:

$$\frac{40}{7}(2,3)^T - \frac{13}{7}(4,-1)^T = (4,19)^T = \vec{v}.$$

Example 6.13 generalizes easily as follows:

Corollary 6.14. *Let $\mathcal{B}$ and $\mathcal{C}$ be any bases on $\mathbb{R}^n$. Then*

$$P_{\mathcal{CB}} = P_{\mathcal{SC}}^{-1} P_{\mathcal{SB}}.$$

Exercise 6.15. *Consider the following bases on* $\mathbb{R}^3$*:*

$$\mathcal{B} = \{(2,-1,1)^T,\ (0,-1,1)^T,\ (1,-1,0)^T\}$$

and

$$\mathcal{C} = \{(1,1,0)^T,\ (1,0,1)^T,\ (0,1,1)^T\}.$$

Compute the transition matrix $P_{\mathcal{CB}}$*.*

6.3. Matrix Representations of Linear Maps

In section 6.1, we showed that by fixing a basis on a vector space V, we were able to identify vectors of V with vectors of $\mathbb{R}^n$ (where $n = \dim V$). In this section, we apply the same idea to linear maps. This will allow us to represent a linear map $\varphi : V \to W$ as a matrix once we have fixed a basis on both V and W. With that said, we now introduce the main definition of this section:

Definition 6.16. *Let* $\varphi : V \to W$ *be a linear map. Let*

$$\mathcal{B} = \{v_1, \ldots, v_n\}$$

be a basis on V *and let*

$$\mathcal{C} = \{w_1, \ldots, w_m\}$$

be a basis on W*. The* ***matrix representation*** *of* φ *with respect to the bases* $\mathcal{B}$ *and* $\mathcal{C}$ *is the* $m \times n$ *matrix*

$$[\varphi]_{\mathcal{CB}} := \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix}$$

where the entries are a_{ij} *for* $1 \le i \le m$ *and* $1 \le j \le n$ *are defined as follows:*

$$\varphi(v_j) = \sum_{i=1}^{m} a_{ij} w_i.$$

The matrix representation of a linear map can also be expressed in terms of coordinate vectors:

Proposition 6.17. *Let $\varphi : V \to W$ be a linear map. Let*

$$\mathcal{B} = \{v_1, \ldots, v_n\}$$

be a basis on V and let

$$\mathcal{C} = \{w_1, \ldots, w_m\}$$

be a basis on W. Then the jth column of the matrix representation $[\varphi]_{\mathcal{CB}}$ is the coordinate vector $[\varphi(v_j)]_{\mathcal{C}}$, that is,

$$[\varphi]_{\mathcal{CB}} = ([\varphi(v_1)]_{\mathcal{C}},\ [\varphi(v_2)]_{\mathcal{C}}, \ldots, [\varphi(v_n)]_{\mathcal{C}}).$$

Proof. The proof follows directly from Definition 6.16. Indeed, the elements of the matrix representation $[\varphi]_{\mathcal{CB}}$ are the coefficients appearing in the equation

$$\varphi(v_j) = \sum_{i=1}^{m} a_{ij} w_i.$$

The above equation implies that the coordinate vector of the vector $\varphi(v_j) \in W$ with respect to the basis $\mathcal{C}$ is

$$[\varphi(v_j)]_{\mathcal{C}} = \begin{pmatrix} a_{1j} \\ a_{2j} \\ \vdots \\ a_{mj} \end{pmatrix}$$

which is simply the jth column of the matrix representation $[\varphi]_{\mathcal{CB}}$. □

Example 6.18. *Let $\mathbb{R}[x]_2$ be the vector space of polynomials of degree 2 or less and let $\mathbb{R}[x]_1$ be the vector space of polynomials of degree 1 or less. Let*

$$D : \mathbb{R}[x]_2 \to \mathbb{R}[x]_1$$

be the map which sends a polynomial $p(x) \in \mathbb{R}[x]_2$ to the polynomial

$$Dp(x) := \frac{dp}{dx}(x) \in \mathbb{R}[x]_1.$$

Example 5.43 implies that D is a linear map. Let $\mathcal{B} = \{x^2, x, 1\}$ and $\mathcal{C} = \{x, 1\}$. Then $\mathcal{B}$ is a basis on $\mathbb{R}[x]_2$ and $\mathcal{C}$ is a basis on $\mathbb{R}[x]_1$. Let us compute the matrix representation $[D]_{\mathcal{CB}}$. To do this, we apply D to each basis element of $\mathcal{B}$:

$$\begin{aligned} Dx^2 &= 2x = 2x + (0)1 \\ Dx &= 1 = 0x + 1 \\ D1 &= 0 = 0x + (0)1. \end{aligned}$$

Hence,

$$[Dx^2]_{\mathcal{C}} = \begin{pmatrix} 2 \\ 0 \end{pmatrix}, \quad [Dx]_{\mathcal{C}} = \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \quad [D1]_{\mathcal{C}} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}.$$

Proposition 6.17 implies that

$$[D]_{\mathcal{CB}} = \begin{pmatrix} 2 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}.$$

The next result shows that by fixing a basis on its domain and range, a linear map $\varphi : V \to W$ can be computed in terms of matrix multiplication involving its matrix representation and coordinate vectors on V:

Theorem 6.19. *Let $\varphi : V \to W$ be a linear map and let $\mathcal{B}$ and $\mathcal{C}$ be bases on V and W respectively. Then*

$$[\varphi]_{\mathcal{CB}}[v]_{\mathcal{B}} = [\varphi(v)]_{\mathcal{C}}, \qquad \forall\ v \in V.$$

Proof. Let

$$\mathcal{B} = \{v_1, \ldots, v_n\}$$

and let

$$\mathcal{C} = \{w_1, \ldots, w_m\}.$$

Let $v \in V$ and express v as a linear combination of the basis $\mathcal{B}$:

$$v = \sum_{j=1}^{n} \alpha_j v_j.$$

By definition, we have

$$[v]_{\mathcal{B}} = (\alpha_1, \alpha_2, \ldots, \alpha_n)^T.$$

Let $[\varphi]_{\mathcal{CB}}$ denote the matrix representation of φ with respect to the bases $\mathcal{B}$ and $\mathcal{C}$ and let a_{ij} denote the (i,j)-entry of $[\varphi]_{\mathcal{CB}}$. Let us now apply φ to the vector v:

$$\begin{aligned} \varphi(v) &= \sum_{j=1}^{n} \alpha_j \varphi(v_j) \\ &= \sum_{j=1}^{n} \sum_{i=1}^{m} \alpha_j a_{ij} w_i \\ &= \sum_{i=1}^{m} \left(\sum_{j=1}^{n} a_{ij} \alpha_j \right) w_i. \end{aligned}$$

The above equality implies that the ith component of the coordinate vector $[\varphi(v)]_{\mathcal{C}}$ is the sum $\sum_{j=1}^{n} a_{ij}\alpha_j$. At the same time, the sum $\sum_{j=1}^{n} a_{ij}\alpha_j$ is precisely the ith element of the column vector obtained by multiplying the matrix representation $[\varphi]_{\mathcal{CB}}$ with the coordinate vector $[v]_{\mathcal{B}}$. In other words, the sum $\sum_{j=1}^{n} a_{ij}\alpha_j$ is the ith element of the column vector $[\varphi]_{\mathcal{CB}}[v]_{\mathcal{B}}$. This implies that $[\varphi]_{\mathcal{CB}}[v]_{\mathcal{B}} = [\varphi(v)]_{\mathcal{C}}$, which completes the proof. □

Example 6.20. *Let $D : \mathbb{R}[x]_2 \to \mathbb{R}[x]_1$ be the linear map induced by ordinary differentiation from Example 6.18 and let $\mathcal{B} = \{x^2, x, 1\}$ and $\mathcal{C} = \{x, 1\}$ be bases on $[R][x]_2$ and $\mathbb{R}[x]_1$ respectively. From Example 6.18, we found that*

$$[D]_{\mathcal{CB}} = \begin{pmatrix} 2 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}.$$

Let us "test" Theorem 6.19. Consider the polynomial $p = 5x^2 - 3x + 2$. According to Theorem 6.19, we should find that

$$[D]_{\mathcal{CB}}[p]_{\mathcal{B}} = [Dp]_{\mathcal{C}}. \tag{90}$$

Let us verify that this is indeed the case. For the left side, we first note that

$$[p]_{\mathcal{B}} = \begin{pmatrix} 5 \\ -3 \\ 2 \end{pmatrix}.$$

Then the left side of (91) is

$$[D]_{\mathcal{CB}}[p]_{\mathcal{B}} = \begin{pmatrix} 10 \\ -3 \end{pmatrix}.$$

To compute the right side, we first note that $Dp = 10x - 3$. Given the basis $\mathcal{C}$, we immediately see that

$$[Dp]_{\mathcal{C}} = \begin{pmatrix} 10 \\ -3 \end{pmatrix}.$$

Hence, we conclude that $[D]_{\mathcal{CB}}[p]_{\mathcal{B}} = [Dp]_{\mathcal{C}}$ (as expected from Theorem 6.19).

Example 6.21. *Let V be a 2-dimensional vector space with basis $\mathcal{B} = \{v_1, v_2\}$ and let W be a 3-dimensional vector space with basis $\mathcal{C} = \{w_1, w_2, w_3\}$. Let $T : V \to W$ be the unique linear map whose values on the basis $\mathcal{B}$ is*

$$T(v_1) = 2w_1 + 3w_2 - w_3, \qquad T(v_2) = w_1 - w_2 + w_3.$$

From this, we see that

$$[T]_{\mathcal{CB}} = \begin{pmatrix} 2 & 1 \\ 3 & -1 \\ -1 & 1 \end{pmatrix}.$$

Let us try another test of Theorem 6.19. Let

$$v = 3v_1 + 5v_2$$

We now verify that

$$[T]_{\mathcal{CB}}[v]_{\mathcal{B}} = [T(v)]_{\mathcal{C}}. \tag{91}$$

For the left side of (91), we have

$$[T]_{\mathcal{CB}}[v]_{\mathcal{B}} = \begin{pmatrix} 2 & 1 \\ 3 & -1 \\ -1 & 1 \end{pmatrix} \begin{pmatrix} 3 \\ 5 \end{pmatrix} = \begin{pmatrix} 11 \\ 4 \\ 2 \end{pmatrix}.$$

To compute the right side of (91), we evaluate $T(v)$:

$$\begin{aligned} T(v) &= 3T(v_1) + 5T(v_2) \\ &= 3(2w_1 + 3w_2 - w_3) + 5(w_1 - w_2 + w_3) \\ &= 11w_1 + 4w_2 + 2w_3. \end{aligned}$$

This in turn implies that

$$[T(v)]_{\mathcal{C}} = \begin{pmatrix} 11 \\ 4 \\ 2 \end{pmatrix},$$

which shows that $[T]_{\mathcal{CB}}[v]_{\mathcal{B}} = [T(v)]_{\mathcal{C}}$.

Next, let $\varphi : V \to W$ be a linear map. Also, let $\mathcal{B}$ and $\mathcal{B}'$ be bases on V and let $\mathcal{C}$ and $\mathcal{C}'$ be bases on W. A natural question then is the following: *how are the matrix representations $[T]_{\mathcal{CB}}$ and $[T]_{\mathcal{C}'\mathcal{B}'}$ related to one another?* The answer is given by the next result:

Theorem 6.22. *Let $\varphi : V \to W$ be a linear map. Also, let $\mathcal{B}$ and $\mathcal{B}'$ be bases on V and let $\mathcal{C}$ and $\mathcal{C}'$ be bases on W. Then*

$$[\varphi]_{\mathcal{C}'\mathcal{B}'} = P_{\mathcal{C}'\mathcal{C}}[\varphi]_{\mathcal{CB}}P_{\mathcal{BB}'} \tag{92}$$

where $P_{\mathcal{BB}'}$ (resp. $P_{\mathcal{C}'\mathcal{C}}$) is the transition matrix from $\mathcal{B}'$ (resp. $\mathcal{C}$) to $\mathcal{B}$ (resp. $\mathcal{C}'$).

Proof. Let $v \in V$ be arbitrary and let $[v]_{\mathcal{B}}$ and $[v]_{\mathcal{B}'}$ be the coordinate vectors of v with respect to $\mathcal{B}$ and $\mathcal{B}'$. Also, let $[\varphi(v)]_{\mathcal{C}}$ and $[\varphi(v)]_{\mathcal{C}'}$ be the coordinate vectors of $\varphi(v)$ with respect to $\mathcal{C}$ and $\mathcal{C}'$. By Theorem 6.8, we have

$$[v]_{\mathcal{B}} = P_{\mathcal{BB}'}[v]_{\mathcal{B}'} \tag{93}$$

and

$$[\varphi(v)]_{\mathcal{C}'} = P_{\mathcal{C}'\mathcal{C}}[\varphi(v)]_{\mathcal{C}} \tag{94}$$

By Theorem 6.19, we have

$$[\varphi]_{\mathcal{CB}}[v]_{\mathcal{B}} = [\varphi(v)]_{\mathcal{C}} \tag{95}$$

and

$$[\varphi]_{\mathcal{C}'\mathcal{B}'}[v]_{\mathcal{B}'} = [\varphi(v)]_{\mathcal{C}'}. \tag{96}$$

Multiplying both sides of (95) from the left by $P_{\mathcal{C}'\mathcal{C}}$ and substituting (93) and (94) gives

$$P_{\mathcal{C}'\mathcal{C}}[\varphi]_{\mathcal{C}\mathcal{B}}P_{\mathcal{B}\mathcal{B}'}[v]_{\mathcal{B}'} = [\varphi(v)]_{\mathcal{C}'}. \tag{97}$$

Equations (96) and (97) imply

$$[\varphi]_{\mathcal{C}'\mathcal{B}'}[v]_{\mathcal{B}'} = P_{\mathcal{C}'\mathcal{C}}[\varphi]_{\mathcal{C}\mathcal{B}}P_{\mathcal{B}\mathcal{B}'}[v]_{\mathcal{B}'}. \tag{98}$$

Since $v \in V$ is arbitrary, equation (98) implies that

$$[\varphi]_{\mathcal{C}'\mathcal{B}'} = P_{\mathcal{C}'\mathcal{C}}[\varphi]_{\mathcal{C}\mathcal{B}}P_{\mathcal{B}\mathcal{B}'} \tag{99}$$

which completes the proof. □

Of particular interest to us is the special case of linear maps whose domain and range are the same vector space. A linear map

$$\varphi : V \to V$$

is commonly called an **endomorphism** of V. When computing the matrix representation of an endomorphism $\varphi : V \to V$, one typically chooses a single basis $\mathcal{B}$ of V and considers the matrix representation $[\varphi]_{\mathcal{B}\mathcal{B}}$. To simplify things a little, we will use the following notation:

$$[\varphi]_{\mathcal{B}} := [\varphi]_{\mathcal{B}\mathcal{B}}.$$

The next result is a special (yet important) case of Theorem 6.22:

Corollary 6.23. *Let $\varphi : V \to V$ be a linear map and let $\mathcal{B}$ and $\mathcal{B}'$ be bases on V. Then*

$$[\varphi]_{\mathcal{B}'} = P_{\mathcal{B}'\mathcal{B}}[\varphi]_{\mathcal{B}}P_{\mathcal{B}\mathcal{B}'} = P^{-1}_{\mathcal{B}\mathcal{B}'}[\varphi]_{\mathcal{B}}P_{\mathcal{B}\mathcal{B}'}.$$

Proof. Apply Theorem 6.22 to the linear map $\varphi : V \to V$ with $\mathcal{C} = \mathcal{B}$ and $\mathcal{C}' = \mathcal{B}'$. In the last equality, we use the fact that $P^{-1}_{\mathcal{B}\mathcal{B}'} = P_{\mathcal{B}'\mathcal{B}}$ by Theorem 6.12. □

Recall from Chapter 3 that two $n \times n$ matrices A and B are **similar** if there exists an invertible $n \times n$ matrix C such that $B = C^{-1}AC$. From Corollary 6.23, we see that $[\varphi]_{\mathcal{B}}$ and $[\varphi]_{\mathcal{B}'}$ are similar matrices. One can say more:

Corollary 6.24. *Let V be a vector space of dimension n and let $\varphi : V \to V$ be a linear map. Let $\mathcal{B}$ be any basis of V and let $A := [\varphi]_{\mathcal{B}}$. For any invertible $n \times n$ matrix C, there exists a basis $\mathcal{B}'$ of V such that $[\varphi]_{\mathcal{B}'} = C^{-1}AC$.*

Proof. Let $\mathcal{B} = \{u_1, u_2, \ldots, u_n\}$ be any basis on V and let $C = (c_{ij})$ be any invertible $n \times n$ matrix. Let

$$\mathcal{B}' := \{v_1, v_2, \ldots, v_n\}$$

be the basis on V defined by

$$v_j := \sum_{i=1}^{n} c_{ij} u_i$$

for $j = 1, 2, \ldots, n$. By the definition of the transition matrix, we have $P_{\mathcal{B}\mathcal{B}'} = C$. Corollary 6.23 then implies

$$[\varphi]_{\mathcal{B}'} = P_{\mathcal{B}\mathcal{B}'}^{-1} [\varphi]_{\mathcal{B}} P_{\mathcal{B}\mathcal{B}'} = C^{-1} AC.$$

This completes the proof. □

Example 6.25. *Let $T : \mathbb{R}^2 \to \mathbb{R}^2$ the linear map defined by*

$$T\vec{v} = \begin{pmatrix} 2y \\ x + y \end{pmatrix}$$

for $\vec{v} = (x, y)^T$. Let $\mathcal{S} = \{\vec{e}_1, \vec{e}_2\}$ denote the standard basis and let $\mathcal{B} = \{\vec{u}_1, \vec{u}_2\}$ where

$$\vec{u}_1 = (-2, 3)^T, \quad \vec{u}_2 = (1, -1)^T.$$

Let us compute $[T]_{\mathcal{B}}$. First, we compute the matrix representation of T with respect to $\mathcal{S}$ (i.e. $[T]_{\mathcal{S}} := [T]_{\mathcal{S}\mathcal{S}}$). This is easily computed using Proposition 6.17 and Proposition 6.4:

$$\begin{aligned} [T]_{\mathcal{S}} &= ([T(\vec{e}_1)]_{\mathcal{S}},\ [T(\vec{e}_2)]_{\mathcal{S}}) \\ &= \begin{pmatrix} 0 & 2 \\ 1 & 1 \end{pmatrix}. \end{aligned}$$

Next, we compute the transition matrix $P_{\mathcal{S}\mathcal{B}}$ with the help of Proposition 6.10:

$$P_{\mathcal{S}\mathcal{B}} = \begin{pmatrix} -2 & 1 \\ 3 & -1 \end{pmatrix}.$$

Using Corollary 6.23, we have

$$\begin{aligned} [T]_{\mathcal{B}} &= P_{\mathcal{S}\mathcal{B}}^{-1} [T]_{\mathcal{S}} P_{\mathcal{S}\mathcal{B}} \\ &= \begin{pmatrix} 1 & 1 \\ 3 & 2 \end{pmatrix} \begin{pmatrix} 0 & 2 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} -2 & 1 \\ 3 & -1 \end{pmatrix} \\ &= \begin{pmatrix} 7 & -2 \\ 20 & -6 \end{pmatrix}. \end{aligned}$$

Let's put the above result to the test. By Theorem 6.19 the following equality should hold for any vector $\vec{v} \in \mathbb{R}^2$

$$[T]_{\mathcal{B}} [\vec{v}]_{\mathcal{B}} = [T(\vec{v})]_{\mathcal{B}}. \tag{100}$$

For the test, let $\vec{v}$ be the vector whose coordinate representation with respect to $\mathcal{B}$ is

$$[\vec{v}]_{\mathcal{B}} = (2, 1)^T.$$

Hence, $\vec{v}$ is given by

$$\vec{v} = 2\vec{u}_1 + \vec{u}_2 = (-3, 5)^T.$$

Hence,

$$T(\vec{v}) = (10, 2)^T.$$

Let us first compute the right side of (100). Using the transition matrix $P_{\mathcal{BS}}$, we have

$$\begin{aligned}[T(\vec{v})]_{\mathcal{B}} &= P_{\mathcal{BS}}[T(\vec{v})]_{\mathcal{S}} \\ &= P_{\mathcal{BS}}T(\vec{v}) \\ &= \begin{pmatrix} 1 & 1 \\ 3 & 2 \end{pmatrix} \begin{pmatrix} 10 \\ 2 \end{pmatrix} \\ &= \begin{pmatrix} 12 \\ 34 \end{pmatrix}.\end{aligned}$$

For the left side of (100), we have

$$\begin{aligned}[T]_{\mathcal{B}}[\vec{v}]_{\mathcal{B}} &= \begin{pmatrix} 7 & -2 \\ 20 & -6 \end{pmatrix} \begin{pmatrix} 2 \\ 1 \end{pmatrix} \\ &= \begin{pmatrix} 12 \\ 34 \end{pmatrix},\end{aligned}$$

which is the desired result.

6.4. More on Matrix Representations

In this section, let V and W be any (real finite dimensional) vector spaces and define $\mathrm{Hom}(V, W)$ to be the set of all linear maps from V to W. It should be clear to the reader that $\mathrm{Hom}(V, W)$ has a natural vector space structure. Indeed, for any two linear maps φ, $\psi \in \mathrm{Hom}(V, W)$ and any scalar $c \in \mathbb{R}$, we simply define $\varphi + \psi \in \mathrm{Hom}(V, W)$ and $c\varphi \in \mathrm{Hom}(V, W)$ **pointwise**, that is,

$$(\varphi + \psi)(v) := \varphi(v) + \psi(v), \qquad \forall\ v \in V$$

and

$$(c\varphi)(v) := c\varphi(v), \qquad \forall\ v \in V.$$

Exercise 6.26. *Verify that the above operations turns Hom(V, W) into a vector space.*

The above vector space structure transforms very nicely when taking matrix representations:

Proposition 6.27. *Let $\varphi : V \to W$ and $\psi : V \to W$ be linear maps and let $\mathcal{B}$ and $\mathcal{C}$ be bases on V and W respectively. Then the following relations hold:*

(i) $[\varphi + \psi]_{\mathcal{C}\mathcal{B}} = [\varphi]_{\mathcal{C}\mathcal{B}} + [\psi]_{\mathcal{C}\mathcal{B}}$

(ii) $[r\varphi]_{\mathcal{C}\mathcal{B}} = r[\varphi]_{\mathcal{C}\mathcal{B}}$ *for all* $r \in \mathbb{R}$

Proof. (i): Let $v \in V$. Using Theorem 6.19 and Proposition 6.7, we have the following:

$$\begin{aligned}
[\varphi + \psi]_{\mathcal{C}\mathcal{B}}[v]_{\mathcal{B}} &= [(\varphi + \psi)(v)]_{\mathcal{C}} \\
&= [\varphi(v) + \psi(v)]_{\mathcal{C}} \\
&= [\varphi(v)]_{\mathcal{C}} + [\psi(v)]_{\mathcal{C}} \\
&= [\varphi]_{\mathcal{C}\mathcal{B}}[v]_{\mathcal{B}} + [\psi]_{\mathcal{C}\mathcal{B}}[v]_{\mathcal{B}} \\
&= \left([\varphi]_{\mathcal{C}\mathcal{B}} + [\psi]_{\mathcal{C}\mathcal{B}}\right)[v]_{\mathcal{B}}.
\end{aligned}$$

Since $v \in V$ is arbitrary, the above equation implies that

$$[\varphi + \psi]_{\mathcal{C}\mathcal{B}} = [\varphi]_{\mathcal{C}\mathcal{B}} + [\psi]_{\mathcal{C}\mathcal{B}}.$$

This completes the proof of (i).

(ii): Once again, using Theorem 6.19 and Proposition 6.7, we have the following:

$$\begin{aligned}
[r\varphi]_{\mathcal{C}\mathcal{B}}[v]_{\mathcal{B}} &= [r\varphi(v)]_{\mathcal{C}} \\
&= r[\varphi(v)]_{\mathcal{C}} \\
&= r[\varphi]_{\mathcal{B}\mathcal{C}}[v]_{\mathcal{B}}.
\end{aligned}$$

The above equation then implies

$$[r\varphi]_{\mathcal{C}\mathcal{B}} = r[\varphi]_{\mathcal{C}\mathcal{B}},$$

which completes the proof of (ii). ☐

Example 6.28. *Let $\mathbb{R}[x]_4$ denote the vector space of polynomials of degree 4 or less. Let*

$$\mathcal{B} := \{x^4, x^3, x^2, x, 1\}$$

and let D_1 and D_2 be the endomorphisms on $\mathbb{R}[x]_4$ given by

$$D_1 := 5\frac{d}{dx} + 1, \qquad D_1 p(x) := 5\frac{d}{dx}p(x) + p(x)$$

and

$$D_2 := \frac{d^2}{dx^2} - \frac{d}{dx}, \qquad D_2 p(x) = \frac{d^2}{dx^2}p(x) - \frac{d}{dx}p(x)$$

for all $p(x) \in \mathbb{R}[x]_4$. Its a simple matter to verify that D_1 and D_2 are indeed linear maps. Since

$$\begin{aligned} D_1 x^4 &= x^4 + 20x^3 \\ D_1 x^3 &= x^3 + 15x^2 \\ D_1 x^2 &= x^2 + 10x \\ D_1 x &= x + 5 \\ D_1 1 &= 1 \end{aligned}$$

and

$$\begin{aligned} D_2 x^4 &= -4x^3 + 12x^2 \\ D_2 x^3 &= -3x^2 + 6x \\ D_2 x^2 &= -2x + 2 \\ D_2 x &= -1 \\ D_2 1 &= 0, \end{aligned}$$

it follows that the matrix representation of D_1 and D_2 with respect to $\mathcal{B}$ is

$$[D_1]_{\mathcal{B}} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 20 & 1 & 0 & 0 & 0 \\ 0 & 15 & 1 & 0 & 0 \\ 0 & 0 & 10 & 1 & 0 \\ 0 & 0 & 0 & 5 & 1 \end{pmatrix}$$

and

$$[D_2]_{\mathcal{B}} = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ -4 & 0 & 0 & 0 & 0 \\ 12 & -3 & 0 & 0 & 0 \\ 0 & 6 & -2 & 0 & 0 \\ 0 & 0 & 2 & -1 & 0 \end{pmatrix}$$

where we recall that $[D_1]_{\mathcal{B}}$ and $[D_2]_{\mathcal{B}}$ are short for $[D_1]_{\mathcal{B}\mathcal{B}}$ and $[D_2]_{\mathcal{B}\mathcal{B}}$ respectively. By Proposition 6.27, we conclude that the matrix representation of $D_1 + D_2$ is

$$
\begin{aligned}
[D_1 + D_2]_{\mathcal{B}} &= [D_1]_{\mathcal{B}} + [D_2]_{\mathcal{B}} \\
&= \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 16 & 1 & 0 & 0 & 0 \\ 12 & 12 & 1 & 0 & 0 \\ 0 & 6 & 8 & 1 & 0 \\ 0 & 0 & 2 & 4 & 1 \end{pmatrix}.
\end{aligned}
$$

Let's try a simple test of our calculation. Let $p(x) = x^4 - x^3 + x^2 - x + 1$. Applying $D_1 + D_2$ to $p(x)$ gives

$$
\begin{aligned}
(D_1 + D_2)p(x) &:= D_1p(x) + D_2p(x) \\
&= (x^4 + 19x^3 - 14x^2 + 9x - 4) + (-4x^3 + 15x^2 - 8x + 3) \\
&= x^4 + 15x^3 + x^2 + x - 1.
\end{aligned}
$$

From this, we see that

$$[(D_1 + D_2)p(x)]_{\mathcal{B}} = (1, 15, 1, 1, -1)^T.$$

By Theorem 6.19, we have

$$[(D_1 + D_2)p(x)]_{\mathcal{B}} = [D_1 + D_2]_{\mathcal{B}}[p(x)]_{\mathcal{B}}.$$

Let us verify that the right side does indeed match the left side. Using our calculation for $[D_1 + D_2]_{\mathcal{B}}$, we have

$$
\begin{aligned}
[D_1 + D_2]_{\mathcal{B}}[p(x)]_{\mathcal{B}} &= \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 16 & 1 & 0 & 0 & 0 \\ 12 & 12 & 1 & 0 & 0 \\ 0 & 6 & 8 & 1 & 0 \\ 0 & 0 & 2 & 4 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ -1 \\ 1 \\ -1 \\ 1 \end{pmatrix} \\
&= \begin{pmatrix} 1 \\ 15 \\ 1 \\ 1 \\ -1 \end{pmatrix}
\end{aligned}
$$

which is the desired result.

The next result relates the composition of linear maps to matrix multiplication (and thus reveals the significance of matrix multiplication):

Proposition 6.29. *Let $\varphi : V \to W$ and $\psi : W \to U$ be linear maps. Let $\mathcal{B}$, $\mathcal{C}$, and $\mathcal{D}$ be bases on V, W, and U respectively. Then*

$$[\psi \circ \varphi]_{\mathcal{D}\mathcal{B}} = [\psi]_{\mathcal{D}\mathcal{C}}[\varphi]_{\mathcal{C}\mathcal{B}}$$

where the right side of the equation is matrix multiplication.

Proof. Let $v \in V$. By Theorem 6.19, we have

$$\begin{aligned}
[\psi \circ \varphi]_{\mathcal{DB}}[v]_{\mathcal{B}} &= [(\psi \circ \varphi)(v)]_{\mathcal{D}} \\
&= [\psi(\varphi(v))]_{\mathcal{D}} \\
&= [\psi]_{\mathcal{DC}}[\varphi(v)]_{\mathcal{C}} \\
&= [\psi]_{\mathcal{DC}}\left([\varphi]_{\mathcal{CB}}[v]_{\mathcal{B}}\right) \\
&= \left([\psi]_{\mathcal{DC}}[\varphi]_{\mathcal{CB}}\right)[v]_{\mathcal{B}}.
\end{aligned}$$

Since $v \in V$ is arbitrary, the above equation implies $[\psi \circ \varphi]_{\mathcal{DB}} = [\psi]_{\mathcal{DC}}[\varphi]_{\mathcal{CB}}$. This completes the proof. □

Example 6.30. *Let $\mathbb{R}[x]_4$ be the vector space of polynomials of degree 4 or less. Let D_1 and D_2 be the endomorphisms on $\mathbb{R}[x]_4$ defined by*

$$D_1 := 5\frac{d}{dx} + 1, \qquad D_1 p(x) := 5\frac{d}{dx}p(x) + p(x)$$

and

$$D_2 := \frac{d^2}{dx^2} - \frac{d}{dx}, \qquad D_2 p(x) = \frac{d^2}{dx^2}p(x) - \frac{d}{dx}p(x).$$

Consider the basis $\mathcal{B} = \{x^4, x^3, x^2, x, 1\}$ on $\mathbb{R}[x]_4$. Using the calculation from Example 6.28 and Proposition 6.29, we compute the matrix representation of $D_1 \circ D_2$ with respect to $\mathcal{B}$ (recall that $[D_1]_{\mathcal{B}}$ is short for $[D_1]_{\mathcal{BB}}$):

$$\begin{aligned}
[D_1 \circ D_2]_{\mathcal{B}} &= [D_1]_{\mathcal{B}}[D_2]_{\mathcal{B}} \\
&= \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 20 & 1 & 0 & 0 & 0 \\ 0 & 15 & 1 & 0 & 0 \\ 0 & 0 & 10 & 1 & 0 \\ 0 & 0 & 0 & 5 & 1 \end{pmatrix} \begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ -4 & 0 & 0 & 0 & 0 \\ 12 & -3 & 0 & 0 & 0 \\ 0 & 6 & -2 & 0 & 0 \\ 0 & 0 & 2 & -1 & 0 \end{pmatrix} \\
&= \begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ -4 & 0 & 0 & 0 & 0 \\ -48 & -3 & 0 & 0 & 0 \\ 120 & -24 & -2 & 0 & 0 \\ 0 & 30 & -8 & -1 & 0 \end{pmatrix}.
\end{aligned}$$

Let us put this calculation to the test. Let $p(x) = x^4 + x^3$. Then

$$\begin{aligned}(D_1 \circ D_2)p(x) &= D_1(D_2 p(x)) \\ &= D_1(-4x^3 + 9x^2 + 6x) \\ &= -4x^3 - 51x^2 + 96x + 30.\end{aligned}$$

Hence,

$$[(D_1 \circ D_2)p(x)]_{\mathcal{B}} = (0, -4, -51, 96, 30)^T.$$

We computed $[D_1 \circ D_2]_{\mathcal{B}}$ using Proposition 6.29. If our calculation of this matrix representation is correct, then by Theorem 6.19, we should observe

$$[(D_1 \circ D_2)p(x)]_{\mathcal{B}} = [D_1 \circ D_2]_{\mathcal{B}}[p(x)]_{\mathcal{B}}.$$

We now verify the above identity:

$$\begin{aligned}[D_1 \circ D_2]_{\mathcal{B}}[p(x)]_{\mathcal{B}} &= \begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ -4 & 0 & 0 & 0 & 0 \\ -48 & -3 & 0 & 0 & 0 \\ 120 & -24 & -2 & 0 & 0 \\ 0 & 30 & -8 & -1 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} \\ &= \begin{pmatrix} 0 \\ -4 \\ -51 \\ 96 \\ 30 \end{pmatrix}.\end{aligned}$$

This verifies the above identity (and suggests that our calculation of $[D_1 \circ D_2]_{\mathcal{B}}$ is indeed correct).

6.5. Determinants, Eigenvalues, and Eigenvectors for Linear Maps

Recall from Chapter 3 that the characteristic polynomial of an $n \times n$ matrix A is defined by

$$p_A(x) := \det(xI_n - A).$$

The eigenvalues of A are then defined to be the roots of its characteristic polynomial; an eigenvector of A associated to an eigenvalue λ of A was then defined to be a nonzero vector $\vec{v} \in \mathbb{R}^n$ satisfying $A\vec{v} = \lambda\vec{v}$.

Let V be a vector space over a field $\mathbb{F}$ (where $\mathbb{F}$, as usual, is understood to be $\mathbb{R}$ or $\mathbb{C}$). In order to generalize these ideas to an endomorphism $\varphi : V \to V$, we first need to generalize the notion of the determinant.

Definition 6.31. *Let $\mathcal{B}$ be* ***any*** *basis on V. The* ***determinant*** *of a linear map $\varphi : V \to V$ is defined as $det(\varphi) := det([\varphi]_{\mathcal{B}})$.*

For Definition 6.31 to be well defined, $\det(\varphi)$ cannot depend on the choice of basis $\mathcal{B}$. The next result shows that this is indeed the case.

Theorem 6.32. *Let $\varphi : V \to V$ be a linear map and let $\mathcal{B}$ and $\mathcal{C}$ be any bases on V. Then $\det([\varphi]_{\mathcal{B}}) = \det([\varphi]_{\mathcal{C}})$.*

Proof. By Corollary 6.23, we have

$$[\varphi]_{\mathcal{C}} = P_{\mathcal{BC}}^{-1}[\varphi]_{\mathcal{B}}P_{\mathcal{BC}}.$$

Using the multiplicative property of the determinant (see Chapter 3), we have

$$\begin{aligned}\det([\varphi]_{\mathcal{C}}) &= \det(P_{\mathcal{BC}}^{-1}[\varphi]_{\mathcal{B}}P_{\mathcal{BC}}) \\ &= \det(P_{\mathcal{BC}}^{-1})\det([\varphi]_{\mathcal{B}})\det(P_{\mathcal{BC}}) \\ &= \frac{1}{\det(P_{\mathcal{BC}})}\det([\varphi]_{\mathcal{B}})\det(P_{\mathcal{BC}}) \\ &= \det([\varphi]_{\mathcal{B}}).\end{aligned}$$

This completes the proof. □

Example 6.33. *Let A be an $n \times n$ matrix. Recall from Chapter 3 that A naturally defines a linear endomorphism of $\mathbb{R}^n$ via matrix multiplication. Explicitly, we associate to A the linear map $\varphi_A : \mathbb{R}^n \to \mathbb{R}^n$ which is defined by*

$$\varphi_A(\vec{v}) := A\vec{v}.$$

In Chapter 3, we used the term "linear transformation" for linear maps of this kind. Let $\mathcal{S}$ denote the standard basis on $\mathbb{R}^n$. Since the matrix representation $[\varphi_A]_{\mathcal{S}} = A$, it follows from Definition 6.31 that

$$\det(\varphi_A) = \det(A).$$

Hence, the determinant of the linear transformation associated to an $n \times n$ matrix A is precisely the determinant of A.

Example 6.34. *Let $\mathbb{R}[x]_2$ denote the vector space of real polynomials of degree 2 or less. Consider the linear map*

$$D : \mathbb{R}[x]_2 \to \mathbb{R}[x]_2, \quad p(x) \mapsto \frac{d}{dx}p(x).$$

Let $\mathcal{B} = \{x^2, x, 1\}$. Then the matrix representation of D with respect to $\mathcal{B}$ is

$$[D]_{\mathcal{B}} = \begin{pmatrix} 0 & 0 & 0 \\ 2 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}.$$

From this, we have

$$\det(D) = \det([D]_{\mathcal{B}}) = 0.$$

Using the notion of determinants for endomorphisms, we can now introduce the following definition:

Definition 6.35. *Let $\varphi : V \to V$ be a linear map. The **characteristic polynomial** of φ is the polynomial*

$$p_\varphi(x) := det(x \cdot id_V - \varphi),$$

where $id_V : V \to V$ is the identity map on V.

As the reader might have guessed, we have the following nice result:

Proposition 6.36. *Let $\varphi : V \to V$ be a linear map and let $\mathcal{B}$ be **any** basis on V. Then the characteristic polynomial of φ is exactly equal to the characteristic polynomial of the matrix representation $[\varphi]_{\mathcal{B}}$.*

Proof. Let $n = \dim V$. Using Proposition 6.27, we have

$$\begin{aligned} p_\varphi(x) &:= \det(x \cdot id_V - \varphi) \\ &:= \det([x \cdot id_V - \varphi]_{\mathcal{B}}) \\ &= \det(x[id_V]_{\mathcal{B}} - [\varphi]_{\mathcal{B}}) \\ &= \det(xI_n - [\varphi]_{\mathcal{B}}) \\ &:= p_{[\varphi]_{\mathcal{B}}}. \end{aligned}$$

This completes the proof. □

Example 6.37. *Let $D : \mathbb{R}[x]_2 \to \mathbb{R}[x]_2$ be the linear map defined in Example 6.34 and let $\mathcal{B} = \{x^2, x, 1\}$. From Example 6.34, we have*

$$[D]_{\mathcal{B}} = \begin{pmatrix} 0 & 0 & 0 \\ 2 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix},$$

Proposition 6.36 implies that the characteristic polynomial of D is simply the characteristic polynomial of $[D]_{\mathcal{B}}$. Using this fact, we find that

$$
\begin{aligned}
p_\varphi &= \det(xI_3 - [D]_\mathcal{B}) \\
&= \det\begin{pmatrix} x & 0 & 0 \\ -2 & x & 0 \\ 0 & -1 & x \end{pmatrix} \\
&= x^3.
\end{aligned}
$$

Using Definition 6.35, we can now generalize the notion of eigenvalues and eigenvectors to endomorphisms.

Definition 6.38. *Let $\varphi : V \to V$ be a linear map and let $p_\varphi(x)$ denote its characteristic polynomial. The* ***eigenvalues*** *of φ are the roots of p_φ. An* ***eigenvector*** *of φ associated to an eigenvalue λ of φ is a nonzero vector $v \in V$ satisfying*

$$\varphi(v) = \lambda v.$$

The subspace of V spanned by all the eigenvectors associated to λ is called the ***eigenspace*** *of λ. This subspace is denoted by E_λ^φ or by E_λ.*

Example 6.39. *Let $D : \mathbb{R}[x]_2 \to \mathbb{R}[x]_2$ be the linear map from Example 6.34. From Example 6.37, we found that the characteristic polynomial of D is $p_\varphi = x^3$. Hence, the eigenvalues of D are all zero. By inspection, the only eigenvectors of D are the constant polynomials:*

$$Dc = \frac{d}{dx}c = 0 = 0c$$

for all $c \in \mathbb{R} \subset \mathbb{R}[x]_2$.

In general, how does one go about finding the eigenvectors of a general endomorphism $\varphi : V \to V$. The next result says that this problem is equivalent to finding all the eigenvectors of any matrix representation of φ.

Theorem 6.40. *Let $\varphi : V \to V$ be a linear map and let $\mathcal{B}$ be* ***any*** *basis of V.*

(i) φ and $[\varphi]_\mathcal{B}$ have the same eigenvalues.

(ii) Let λ be any eigenvalue of φ and let v be an eigenvector of φ associated to λ. Then $[v]_\mathcal{B}$ is an eigenvector of $[\varphi]_\mathcal{B}$ associated to the eigenvalue λ.

(iii) Let λ be an eigenvalue of $[\varphi]_\mathcal{B}$ and let $\vec{x}$ be an eigenvector of $[\varphi]_\mathcal{B}$ associated to λ. Let $v_x \in V$ be the unique vector satisfying $[v_x]_\mathcal{B} = \vec{x}$. Then v_x is an eigenvector of φ associated to the eigenvalue λ.

Proof. (i): By Proposition 6.36, φ and $[\varphi]_{\mathcal{B}}$ have the same characteristic polynomial. Since the eigenvalues of φ and $[\varphi]_{\mathcal{B}}$ are just the roots of its characteristic polynomial, we conclude that φ and $[\varphi]_{\mathcal{B}}$ have the same eigenvalues.

(ii): Let $v \in V$. By Theorem 6.19, we have

$$[\varphi]_{\mathcal{B}}[v]_{\mathcal{B}} = [\varphi(v)]_{\mathcal{B}}. \tag{101}$$

Suppose now that v is an eigenvector of φ. By definition, $v \neq 0$ and $\varphi(v) = \lambda v$. This together with (101) implies

$$\begin{aligned}
[\varphi]_{\mathcal{B}}[v]_{\mathcal{B}} &= [\varphi(v)]_{\mathcal{B}} \\
&= [\lambda v]_{\mathcal{B}} \\
&= \lambda[v]_{\mathcal{B}},
\end{aligned}$$

where we have applied Proposition 6.27 in the last equality. This shows that $[v]_{\mathcal{B}}$ is an eigenvector of the matrix $[\varphi]_{\mathcal{B}}$. (Note that $[v]_{\mathcal{B}} \neq \vec{0}$ since $v \neq \mathbf{0}$.)

(iii): Suppose that $\vec{x}$ is an eigenvector of $[\varphi]_{\mathcal{B}}$ associated to an eigenvalue λ. Let $v_x \in V$ be the unique vector defined by $[v_x] = \vec{x}$. (Note that since $\vec{x} \neq \vec{0}$, we also have $v_x \neq \mathbf{0}$.) By Theorem 6.19, we have

$$\begin{aligned}
[\varphi(v_x)]_{\mathcal{B}} &= [\varphi]_{\mathcal{B}}[v_x]_{\mathcal{B}} \\
&= [\varphi]_{\mathcal{B}}\vec{x} \\
&= \lambda\vec{x} \\
&= \lambda[v_x]_{\mathcal{B}} \\
&= [\lambda v_x]_{\mathcal{B}}.
\end{aligned}$$

The last equality implies $\varphi(v_x) = \lambda v_x$. This completes the proof. □

We conclude this section by introducing the notion of diagonalizable linear maps, which turns out to be strongly related to the idea of diagonalizable matrices.

Definition 6.41. *A linear map $\varphi : V \to V$ is* ***diagonalizable*** *if there exists a basis of V such that every element of the basis is an eigenvector of φ.*

Example 6.42. *Let $\mathfrak{sl}(2;\mathbb{R})$ be the vector space consisting of 2×2 real matrices with trace zero. (See Example 5.18.) Let*

$$\varphi : \mathfrak{sl}(2;\mathbb{R}) \to \mathfrak{sl}(2;\mathbb{R})$$

be the linear map which sends a matrix

$$\begin{pmatrix} a & b \\ c & -a \end{pmatrix} \in \mathfrak{sl}(2;\mathbb{R})$$

to the matrix

$$\begin{pmatrix} 0 & 2b \\ -2c & 0 \end{pmatrix} \in \mathfrak{sl}(2;\mathbb{R}).$$

(It is a simple exercise to verify that φ is indeed linear.) The reader can verify that $\mathfrak{sl}(2;\mathbb{R})$ is a 3-dimensional vector space with basis

$$H := \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad E := \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \quad F := \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}.$$

Observe that

$$\varphi(H) = 0H, \quad \varphi(E) = 2E, \quad \varphi(F) = -2F.$$

Hence, φ is a diagonalizable linear map.

Theorem 6.43. *Let $\varphi : V \to V$ be a linear map and let $\mathcal{B}$ be* ***any*** *basis on V. Then the following statements are equivalent:*

(i) φ is diagonalizable.

(ii) The matrix representation $[\varphi]_{\mathcal{B}}$ is diagonalizable.

Proof. Let $n = \dim V$.

(i): Suppose that φ is diagonalizable. By definition, there exists a basis $\{v_1, \ldots, v_n\}$ of V such that v_i is an eigenvector of φ for $i = 1, \ldots, n$. Let λ_i be the eigenvalue of φ associated to v_i for $i = 1, \ldots, n$. Theorem 6.40 implies that

$$[v_1]_{\mathcal{B}}, \ldots, [v_n]_{\mathcal{B}}$$

are also eigenvectors on $[\varphi]_{\mathcal{B}}$. Note also that since $\{v_1, \ldots, v_n\}$ is a basis on V, it follows that $\{[v_1]_{\mathcal{B}}, \ldots, [v_n]_{\mathcal{B}}\}$ is a basis on $\mathbb{R}^n$. Let C be the matrix whose ith column is $[v_i]_{\mathcal{B}}$ for $i = 1, \ldots, n$. Then

$$C^{-1}[\varphi]_{\mathcal{B}}C = \begin{pmatrix} \lambda_1 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \ldots & \lambda_n \end{pmatrix}. \tag{102}$$

(ii): Now suppose that $[\varphi]_{\mathcal{B}}$ is diagonalizable. Then there exists an $n \times n$ matrix C satisfying (102). Let $\vec{x}_i$ denote the ith column of C. Equation (102) implies that $[\varphi]_{\mathcal{B}}\vec{x}_i = \lambda_i\vec{x}_i$. For $i = 1, \ldots, n$, let $u_i \in V$ be the unique vector defined by $[u_i]_{\mathcal{B}} = \vec{x}_i$. Theorem 6.40 implies that $\varphi(u_i) = \lambda_i u_i$. Moreover, since $\vec{x}_1, \ldots, \vec{x}_n$ is a basis on $\mathbb{R}^n$, it follows that $u_1, \ldots, u_n$ must be a basis on V. Hence, φ is diagonalizable. This completes the proof. □

Chapter 6 Exercises

1. Let $\mathbb{R}[x]_2$ be the vector space of real polynomials of degree 2 and let

$$\mathcal{B}_1 = \{x^2, x, 1\}, \qquad \mathcal{B}_2 = \{x^2 + x, 2x + 3, 1\}.$$

Compute the transition matrix $P_{\mathcal{B}_2\mathcal{B}_1}$. Use $P_{\mathcal{B}_2\mathcal{B}_1}$ to give the coordinate vector with respect to $\mathcal{B}_2$ for each of the polynomials given below:

(a) $5x^2 + 2x + 1$
(b) $-x^2 - 3x + 1$
(c) $2x - 7$
(d) $x^2 + 5x$

For (a)-(d) above, use the coordinate vector you computed to recover the original polynomial.

Lastly, what is the polynomial $p(x)$ whose coordinate vector with respect to $\mathcal{B}_2$ is $[p(x)]_{\mathcal{B}_2} = (1, -2, 2)^T$.

2. Consider the vector space $\mathbb{R}^2$. Let

$$\mathcal{B} = \{(1, 1),\ (1, -1)\}.$$

Let $\mathcal{S} = \{\vec{e}_1,\ \vec{e}_2\}$ denote the standard basis on $\mathbb{R}^2$. Compute the transition matrix $P_{\mathcal{B}\mathcal{S}}$. Use $P_{\mathcal{B}\mathcal{S}}$ to compute the coordinate vector with respect to $\mathcal{B}$ for each of the elements of $\mathbb{R}^2$ given below:

(a) $\vec{v} = (2, 1)$
(b) $\vec{u} = (1, 2)$
(c) $\vec{w} = (2, -3)$

For (a)-(c) above, use the coordinate vector you computed to recover the original vector.

Lastly, what is the element $\vec{v} \in \mathbb{R}^2$ whose coordinate vector with respect to $\mathcal{B}$ is $[\vec{v}]_{\mathcal{B}} = (2, 5)^T$.

3. Consider the vector space $\mathbb{R}^2$ and the following bases:

$$\mathcal{B}_1 = \{(1, 1),\ (1, -1)\}, \qquad \mathcal{B}_2 = \{(2, 1),\ (1, 2)\},$$

(a) Compute the transition matrix from $\mathcal{B}_1$ to $\mathcal{B}_2$: $P_{\mathcal{B}_2\mathcal{B}_1}$. (Hint: use the following relation:

$$P_{\mathcal{B}_2\mathcal{B}_1} = P_{\mathcal{B}_2\mathcal{S}}P_{\mathcal{S}\mathcal{B}_1} = P^{-1}_{\mathcal{S}\mathcal{B}_2}P_{\mathcal{S}\mathcal{B}_1},$$

where $\mathcal{S}$ is the standard basis on $\mathbb{R}^2$.)

(b) Compute the transition matrix from $\mathcal{B}_2$ to $\mathcal{B}_1$: $P_{\mathcal{B}_1\mathcal{B}_2}$ (Hint: $P_{\mathcal{B}_1\mathcal{B}_2} = P^{-1}_{\mathcal{B}_2\mathcal{B}_1}$

(c) Suppose $[\vec{v}]_{\mathcal{B}_1} = (5,1)^T$. Find $[\vec{v}]_{\mathcal{B}_2}$ using the appropriate transition matrix.

(d) Find $\vec{v}$ first using $[\vec{v}]_{\mathcal{B}_1}$ and then using $[\vec{v}]_{\mathcal{B}_2}$. (If your work is correct, both coordinate vectors will yield the same vector.)

4. Consider the vector space $\mathbb{R}^2$ and the following bases:

$$\mathcal{B}_1 = \{(2,3),\ (1,-1)\}, \qquad \mathcal{B}_2 = \{(1,3),\ (-2,4)\},$$

(a) Compute the transition matrix from $\mathcal{B}_1$ to $\mathcal{B}_2$: $P_{\mathcal{B}_2\mathcal{B}_1}$.

(b) Compute the transition matrix from $\mathcal{B}_2$ to $\mathcal{B}_1$: $P_{\mathcal{B}_1\mathcal{B}_2}$.

(c) Suppose $[\vec{v}]_{\mathcal{B}_1} = (1,2)^T$. Find $[\vec{v}]_{\mathcal{B}_2}$ using the appropriate transition matrix.

(d) Find $\vec{v}$ first using $[\vec{v}]_{\mathcal{B}_1}$ and then using $[\vec{v}]_{\mathcal{B}_2}$.

5. Find the matrix representation of the linear map $T : \mathbb{R}^2 \to \mathbb{R}^2$ defined by

$$T\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} -x \\ x+2y \end{pmatrix}$$

on $\mathbb{R}^2$ with respect to the standard basis $\vec{e}_1, \vec{e}_2$.

6. Find the matrix representation of the linear map $T : \mathbb{R}^3 \to \mathbb{R}^3$ defined by

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

with respect to the standard basis $\vec{e}_1, \vec{e}_2, \vec{e}_3$ of $\mathbb{R}^3$.

7. Let U be a vector space with basis $\mathcal{B} = \{u_1,\ u_2\}$ and let V be a vector space with basis $\mathcal{C} = \{v_1, v_2\}$. Let $T : U \to V$ be the linear map defined by

$$T(u_1) = 2v_1 + 3v_2\ , T(u_2) = v_1 - v_2\ .$$

Find the matrix representation $[T]_{\mathcal{C}\mathcal{B}}$.

8. Let U be a vector space with basis $\mathcal{B} = \{u_1, u_2, u_3\}$ and let V be a vector space with basis $\mathcal{C} = \{v_1, v_2\}$. Let $T : U \to V$ be the linear map defined by

$$T(u_1) = v_1 - 5v_2\ , T(u_2) = 2v_1 + v_2\ , T(u_3) = v_1 - v_2\ .$$

Find the matrix representation $[T]_{\mathcal{C}\mathcal{B}}$.

9. Let $M_2(\mathbb{R})$ be the vector space of real 2×2 matrices. Let

$$C = \begin{pmatrix} 2 & 1 \\ 0 & 1 \end{pmatrix}.$$

Let $L_C : M_2(\mathbb{R}) \to M_2(\mathbb{R})$ be the map defined by $L_C(A) := CA$ for $A \in M_2(\mathbb{R})$.

(a) Verify that L_C is linear.

(b) Let E_{ij} for $i, j \in \{1, 2\}$ be the 2×2 matrix which is 1 in the (i, j)-entry and zero everywhere else. Verify that

$$\mathcal{B} = \{E_{11}, E_{12}, E_{21}, E_{22}\}$$

is a basis of $M_2(\mathbb{R})$.

(c) Compute the matrix representation of L_C with respect to $\mathcal{B}$: $[L_C]_{\mathcal{B}}$.

(d) Verify that $L_C^{-1} = L_{C^{-1}}$.

(e) Compute $[L_{C^{-1}}]_{\mathcal{B}}$ and verify the following identity by direct calculation:

$$[L_{C^{-1}}]_{\mathcal{B}} = [L_C^{-1}]_{\mathcal{B}} = [L_C]_{\mathcal{B}}^{-1}.$$

In other words, check that $[L_{C^{-1}}]_{\mathcal{B}}[L_C]_{\mathcal{B}} = I_4$.

10. Let $\mathbb{R}[x]_2$ be the vector space of polynomials of degree 2 or less and let

$$D : \mathbb{R}[x]_2 \to \mathbb{R}[x]_2$$

be the linear map defined by

$$D(p(x)) = \frac{d^2}{dx^2}p(x) + 2\frac{d}{dx}p(x) + p(x).$$

Let $\mathcal{B} = \{x^2, x, 1\}$.

(a) Compute the matrix representation of D with respect to $\mathcal{B}$: $[D]_{\mathcal{B}}$.

(b) Use $[\mathcal{D}]_{\mathcal{B}}$ to compute the coordinate vector of

$$p(x) = x^2 - 2x + 1$$

with respect to $\mathcal{B}$.

(c) Compute the characteristic polynomial p_D of D.

(d) Find the eigenvalues of D and their corresponding eigenspaces.

11. Let V be a 3-dimensional vector space and let $\mathcal{B}_1$ and $\mathcal{B}_2$ be bases on V whose transition matrix is given by

$$P_{\mathcal{B}_2\mathcal{B}_1} = \begin{pmatrix} 1 & 2 & 2 \\ 0 & -1 & 1 \\ 2 & 1 & 1 \end{pmatrix}.$$

Suppose $\varphi : V \to V$ is an endomorphism of V whose matrix representation with respect to $\mathcal{B}_1$ is

$$[\varphi]_{\mathcal{B}_1} = \begin{pmatrix} 0 & 1 & 3 \\ 1 & 0 & 1 \\ 1 & 1 & 1 \end{pmatrix}.$$

Find the matrix representation of φ with respect to $\mathcal{B}_2$.

Chapter 7

More on Linear Systems

In Chapter 1, we introduced the Gauss Jordan method for solving systems of linear equations. We saw examples of systems with a unique solution, no solution, or multiple solutions. In this chapter, we apply the theory of vector spaces to determine which of the aforementioned three camps a given linear system falls into.

7.1. Row Space & Column Space

The following definitions will prove quite relevant towards the main goal of this chapter.

Definition 7.1. *Let A be an $m \times n$ matrix. Let $\vec{r}_i$ denote the ith row of A (expressed as a row vector) for $i = 1, \dots, m$ and let $\vec{c}_j$ denote the jth column of A (expressed as a column vector) for $j = 1, \dots, n$. The* ***row space*** *of A is defined by*

$$Row(A) := span\{\vec{r}_1, \dots, \vec{r}_m\} \subset \mathbb{R}^n.$$

The ***column space*** *of A is defined by*

$$Col(A) := span\{\vec{c}_1, \dots, \vec{c}_n\} \subset \mathbb{R}^m.$$

We would like to point out a small nuisance associated with this definition. For an $m \times n$ matrix A, $\mathrm{Row}(A)$ is a subspace of $\mathbb{R}^n$ and $\mathrm{Col}(A)$ is a subspace of $\mathbb{R}^m$. Since $\mathrm{Row}(A)$ is spanned by row vectors, we regard $\mathbb{R}^n$ as the vector space of row vectors. Similarly, since $\mathrm{Col}(A)$ is spanned by column vectors, $\mathbb{R}^m$ is regarded as the vector space of column vectors. If A is now a square matrix with $m = n$, then the elements of $\mathbb{R}^n$ are expressed as both row vectors and column vectors depending on the context. For convenience, we define

$$\text{Row}(A)^T := \{\vec{r}^{\,T} \mid \vec{r} \in \text{Row}(A)\} = \text{Col}(A^T)$$

and

$$\text{Col}(A)^T := \{\vec{c}^{\,T} \mid \vec{c} \in \text{Col}(A)\} = \text{Row}(A^T).$$

Example 7.2. *Let I_n denote the $n \times n$ identity matrix. The columns (and rows) of I_n consist of the standard basis $\{\vec{e}_1, \ldots, \vec{e}_n\}$ of $\mathbb{R}^n$. Hence,*

$$\mathit{Col}(I_n) = \mathit{Row}(I_n)^T = \mathit{span}\{\vec{e}_1, \ldots, \vec{e}_n\} = \mathbb{R}^n.$$

Example 7.3. *Let*

$$A = \begin{pmatrix} 2 & 3 & -1 \\ 1 & 4 & 6 \end{pmatrix}.$$

The column space of A is

$$\mathit{Col}(A) = \mathit{span}\left\{\begin{pmatrix} 2 \\ 1 \end{pmatrix}, \begin{pmatrix} 3 \\ 4 \end{pmatrix}, \begin{pmatrix} -1 \\ 6 \end{pmatrix}\right\} = \mathbb{R}^2$$

and the row space is

$$\mathit{Row}(A) = \mathit{span}\,\{(2,3,-1),\ (1,4,6)\}) \neq \mathbb{R}^3$$

7.2. Matrix Rank

The row space and column space of an $m \times n$ matrix A look quite different. After all, $\text{Row}(A)$ is a subspace of $\mathbb{R}^n$ while $\text{Col}(A)$ is a subspace of $\mathbb{R}^m$. Hence, the following result may seem a little surprising:

Theorem 7.4. *For any matrix A, $\dim \mathit{Row}(A) = \dim \mathit{Col}(A)$.*

Proof. Let A be an $m \times n$ matrix and let a_{ij} denote the (i, j) element of A. Let $\vec{r}_i \in \mathbb{R}^n$ for $i = 1, \ldots, m$ denote the ith row of A:

$$\vec{r}_i = (a_{i1}, \ldots, a_{in}). \tag{103}$$

Let $k = \dim \text{Row}(A)$. Let $\vec{v}_1, \ldots, \vec{v}_k \in \mathbb{R}^n$ be a basis of $\text{Row}(A)$. Let

$$\vec{v}_l = (b_{l1}, \ldots, b_{ln}), \quad l = 1, \ldots, k. \tag{104}$$

Express $\vec{r}_i$ for $i = 1, \ldots, m$ as a linear combination of $\vec{v}_1, \ldots, \vec{v}_k$:

$$\vec{r}_i = \alpha_{i1}\vec{v}_1 + \cdots + \alpha_{ik}\vec{v}_k. \tag{105}$$

Comparing the components of (103) and (104) to those of (105) leads to the following:

$$a_{ij} = \alpha_{i1}b_{1j} + \alpha_{i2}b_{2j} + \cdots + \alpha_{ik}b_{kj}. \tag{106}$$

Let $\vec{c}_j \in \mathbb{R}^m$ for $j = 1, \ldots, n$ denote the jth column of A. Then

$$\vec{c}_j = (a_{1j}, \ldots, a_{mj})^T. \tag{107}$$

Also, define $\vec{\alpha}_l \in \mathbb{R}^m$ for $l = 1, \ldots, n$ by

$$\vec{\alpha}_l := (\alpha_{1l}, \alpha_{2l}, \ldots, \alpha_{ml})^T. \tag{108}$$

Then (106) can be written more compactly as

$$\vec{c}_j = b_{1j}\vec{\alpha}_1 + b_{2j}\vec{\alpha}_2 + \cdots + b_{kj}\vec{\alpha}_k. \tag{109}$$

Since $\mathrm{Col}(A) := \mathrm{span}\{\vec{c}_1, \ldots, \vec{c}_n\}$, equation (109) implies

$$\mathrm{Col}(A) \subset \mathrm{span}\{\vec{\alpha}_1, \vec{\alpha}_2, \ldots, \vec{\alpha}_k\}. \tag{110}$$

This in turn implies that $\dim \mathrm{Col}(A) \leq k$. Since $k := \dim \mathrm{Row}(A)$, we have shown that

$$\dim \mathrm{Col}(A) \leq \dim \mathrm{Row}(A). \tag{111}$$

Now consider the matrix A^T. By the above argument, we have

$$\dim \mathrm{Col}(A^T) \leq \dim \mathrm{Row}(A^T). \tag{112}$$

However,

$$\mathrm{Col}(A^T) = \mathrm{span}\{\vec{r}_1^{\,T}, \ldots, \vec{r}_m^{\,T}\} = \mathrm{Row}(A)^T \tag{113}$$

and

$$\mathrm{Row}(A^T) = \mathrm{span}\{\vec{c}_1^{\,T}, \ldots, \vec{c}_n^{\,T}\} = \mathrm{Col}(A)^T. \tag{114}$$

Since the transpose operation does not alter the dimension of the subspace, the above two observations along with (112) gives

$$\dim \mathrm{Row}(A) \leq \dim \mathrm{Col}(A). \tag{115}$$

The inequalities (111) and (115) then imply $\dim \mathrm{Row}(A) = \dim \mathrm{Col}(A)$. This completes the proof. □

With Theorem 7.4 in hand, we now introduce the following definition:

Definition 7.5. *The **rank** of a matrix A (denoted Rank(A)) is defined to be the dimension of the column space of A or, equivalently, the dimension of the row space of A.*

Example 7.6. *Let*

$$A = \begin{pmatrix} 0 & 1 & 3 & -1 & 5 \\ -1 & 1 & 5 & 8 & -2 \end{pmatrix}.$$

Its clear that the rows of A are linearly independent. Hence, the row space of A has dimension 2. From this, we conclude that Rank(A) $= 2$.

We now prove two results which will be useful for calculating the rank of a matrix. For these results, recall that two matrices are row equivalent if one can be transformed into the other using nothing but elementary row operations.

Theorem 7.7. *Let A and B be row equivalent matrices. Then Row$(A) =$ Row(B). In particular, Rank$(A) =$ Rank(B).*

Proof. Let A and B be $m \times n$ matrices. Suppose that A can be transformed into B by a series of elementary row operations. Let N be the number of elementary row operations needed to transform A into B. Let $A_0 := A$ and let $A_1, A_2, \ldots, A_N := B$ denote the gradual transformation of A into B by elementary row operations. In other words, for $k = 0, 1, \ldots, N-1$, A_{k+1} is obtained from A_k by applying a single elementary row operation. Let us consider the effect on the row space of A_k after applying one of the three elementary row operations. Recall that the first row operation involves swapping two rows of a matrix; the second row operation involves scaling a row by a nonzero scalar; and the third row operation involves adding a scalar multiple of one row to that of a another row. Clearly, the new matrix obtained from A_k by applying any of these row operations has the same row space as A_k. Hence, $\text{Row}(A_k) = \text{Row}(A_{k+1})$ for $k = 0, 1, \ldots, N-1$. From this, we conclude that

$$\text{Row}(A) = \text{Row}(A_0) = \text{Row}(A_1) = \text{Row}(A_2) = \cdots = \text{Row}(A_N) = \text{Row}(B).$$

This completes the proof. □

Theorem 7.8. *Let A be a matrix and let E denote A in reduced row echelon form. Then the nonzero rows of E form a basis for Row(A). In particular, Rank(A) is equal to the number of nonzero rows of E.*

Proof. By Theorem 7.7, $\text{Row}(A) = \text{Row}(E)$. Let $\vec{r}_1, \ldots, \vec{r}_l$ denote the nonzero rows of E where $\vec{r}_i$ is the ith row of E. Since the zero rows of E contribute nothing to its row space, we have

$$\text{Row}(E) = \text{span}\{\vec{r}_1, \ldots, \vec{r}_l\}.$$

To complete the proof, we just need to show that $\vec{r}_1, \ldots, \vec{r}_l$ is linearly independent. We do this by induction on l. If $l = 1$, then we clearly have a linearly independent set. So suppose that linear independence holds for all matrices in reduced echelon form with exactly $l - 1$ non-zero rows, where $l \geq 2$.

Now let E be a matrix in row reduced echelon form with non-zero rows $\vec{r}_1, \ldots, \vec{r}_l$, where $\vec{r}_i$ is the ith row of E. Suppose that

$$c_1\vec{r}_1 + c_2\vec{r}_2 + \cdots + c_l\vec{r}_l = \vec{0}.$$

Since E is in reduced row echelon form, the leftmost non-zero component in $\vec{r}_1$ is a 1 and no other row has a non-zero number in this position. It follows from this that $c_1 = 0$. Let E' be the matrix with $l-1$ rows $\vec{r}_2, \ldots, \vec{r}_l$ (in this order). Then E' is in reduced row echelon form. By the induction hypothesis, $\vec{r}_2, \ldots, \vec{r}_l$ is linearly independent. This implies $c_2 = \cdots = c_l = 0$. Hence, $\vec{r}_1, \vec{r}_2, \ldots, \vec{r}_l$ is linearly independent. This completes the induction step. $\square$

Example 7.9. *Let*

$$A = \begin{pmatrix} 2 & 1 & 10 \\ 3 & 2 & 17 \\ 1 & 1 & 7 \end{pmatrix}$$

Let us find a basis for Row(A). By Theorem 7.8, a basis for Row(A) is simply the nonzero rows of A in reduced row echelon form. Applying the Gauss Jordan method to A, we obtain

$$\begin{pmatrix} 1 & 0 & 3 \\ 0 & 1 & 4 \\ 0 & 0 & 0 \end{pmatrix}.$$

Hence, a basis for Row(A) is

$$\{(1,0,3),\ (0,1,4)\}.$$

To find a basis for $\mathrm{Col}(A)$, we simply find a basis for $\mathrm{Row}(A^T)$ and use the fact that $\mathrm{Col}(A) = \mathrm{Row}(A^T)^T$.

Example 7.10. *Let*

$$A = \begin{pmatrix} 4 & 2 & 1 \\ -2 & 4 & 1 \\ -16 & 2 & -1 \end{pmatrix}$$

Let us find a basis for Col(A). The problem then is equivalent to finding a basis for the row space of

$$A^T = \begin{pmatrix} 4 & -2 & -16 \\ 2 & 4 & 2 \\ 1 & 1 & -1 \end{pmatrix}.$$

Using the Gauss Jordan method, we put A^T in reduced row echelon form:

$$\begin{pmatrix} 1 & 0 & -3 \\ 0 & 1 & 2 \\ 0 & 0 & 0 \end{pmatrix}.$$

Hence, a basis for Col(A) is

$$\{(1,0,-3)^T,\ (0,1,2)^T\}.$$

Example 7.11. *Let V be the subspace of $\mathbb{R}^4$ spanned by the vectors*

$$\vec{v}_1 := (1,2,3,4), \quad \vec{v}_2 = (1,-2,1,-3), \quad \vec{v}_3 = (1,10,7,18).$$

Let us find a basis for V. It is clear that $\vec{v}_1$ and $\vec{v}_2$ are linearly independent. However, is $\vec{v}_3$ a linear combination of $\vec{v}_1$ and $\vec{v}_2$? We can answer this question by regarding $\vec{v}_1$, $\vec{v}_2$, and $\vec{v}_3$ as the rows of the 3×4 matrix

$$A := \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & -2 & 1 & -3 \\ 1 & 10 & 7 & 18 \end{pmatrix}$$

and then computing a basis for the row space of this matrix using Theorem 7.8. If the reduced row echelon form of this matrix has exactly two non-zero rows, then $\vec{v}_3$ must be a linear combination of $\vec{v}_1$ and $\vec{v}_2$. Otherwise, $\vec{v}_1$, $\vec{v}_2$, and $\vec{v}_3$ are linearly independent and thus form a basis for V.
Using the Gauss Jordan method, we find that the reduced echelon form of A is given by

$$A := \begin{pmatrix} 1 & 0 & 2 & 1/2 \\ 0 & 1 & 1/2 & 7/4 \\ 0 & 0 & 0 & 0 \end{pmatrix}.$$

From this, we conclude that $\{\vec{v}_1,\ \vec{v}_2\}$ is a basis on V. Alternately, by Theorem 7.8, the first two rows of the above matrix also constitute a basis for V.

7.3. The null space of a matrix

Let V and W be vector spaces (over $\mathbb{R}$) and let $\varphi : V \to W$ be a linear map. Recall from Chapter 5 that the null space (or kernel) of φ is defined as

$$\ker\ \varphi := \{v \in V \mid \varphi(v) = \mathbf{0}\} \subset V$$

and the image of φ is

$$\mathrm{im}\ \varphi := \{\varphi(v) \in W \mid v \in V\} \subset W.$$

Also recall that the nullity of φ (denoted by $\mathrm{Nullity}(\varphi)$) is the dimension of $\ker\ \varphi$ and the rank of φ (denoted by $\mathrm{Rank}(\varphi)$) is the dimension of $\mathrm{im}\ \varphi$. The *Rank-Nullity Theorem* (Theorem 5.60) says that the rank and nullity of φ are related by

$$\mathrm{Nullity}(\varphi) + \mathrm{Rank}(\varphi) = \dim V.$$

We will now apply these ideas to the row and column space of an $m \times n$ matrix A.

As we saw in Chapter 3, A induces a natural linear map

$$\varphi_A : \mathbb{R}^n \to \mathbb{R}^m$$

by $\varphi_A(\vec{v}) := A\vec{v}$, where the right side is matrix multiplication. Let

$$\{\vec{c}_1, \ldots, \vec{c}_n\}$$

denote the columns of A and let $\vec{v} = (v_1, \ldots, v_n)^T \in \mathbb{R}^n$ be arbitrary. Then

$$\varphi_A(\vec{v}) = v_1\vec{c}_1 + v_2\vec{c}_2 + \cdots + v_n\vec{c}_n.$$

From this, we see that

$$\text{im } \varphi_A = \text{Col}(A),$$

which in turn implies

$$\text{Rank}(\varphi_A) = \text{Rank}(A).$$

This relationship is also the original motivation for the definition of the rank of a linear map. Also, the kernel or null space of φ_A is given by

$$\ker\ \varphi_A := \{\vec{v} \in \mathbb{R}^n \mid \varphi_A(\vec{v}) = \vec{0}\} = \{\vec{v} \in \mathbb{R}^n \mid A\vec{v} = \vec{0}\}.$$

This observation leads to the following definition:

Definition 7.12. *The* ***kernel*** *or* ***null space*** *of an $m \times n$ matrix A (denoted* $\ker(A)$ *or $N(A)$) is the subspace*

$$\{\vec{v} \in \mathbb{R}^n \mid A\vec{v} = \vec{0}\} \subset \mathbb{R}^n$$

The dimension of $\ker(A)$ *is denoted as Nullity(A).*

Applying the *Rank-Nullity Theorem* (Theorem 5.60) to the linear map φ_A gives

Corollary 7.13 (Rank-Nullity Theorem (matrix version))**.** *Let A be an $m \times n$ matrix. Then Rank(A) + Nullity$(A) = n$.*

Example 7.14. *Let*

$$A = \begin{pmatrix} 1 & 4 & 1 \\ 0 & 2 & 2 \\ -1 & -5 & -2 \end{pmatrix}.$$

Let us compute the null space of A. Let $\vec{v} = (v_1, v_2, v_3)^T$ and suppose that $A\vec{v} = \vec{0}$. Expanding this matrix equation, we obtain the homogeneous linear system:

$$\begin{aligned} v_1 + 4v_2 + v_3 &= 0 \\ 2v_2 + 2v_3 &= 0 \\ -v_1 - 5v_2 - 2v_3 &= 0. \end{aligned}$$

Solving the above linear system, we obtain the null space or kernel of A:

$$N(A) = \{(3r, -r, r)^T \mid r \in \mathbb{R}\}.$$

Since $\dim\ N(A) = 1$*, it follows from the matrix version of the Rank-Nullity Theorem that Rank$(A) = 2$.*

7.4. Solutions of linear systems: a closer look

In this section, we use the notion of rank to determine when a system of linear equations admits a unique solution, many solutions, or no solution.

Theorem 7.15. *Let A be an $m \times n$ matrix. For the matrix equation $A\vec{x} = \vec{b}$, let A' be the augmented matrix defined by*

$$A' := \begin{pmatrix} A & \vec{b} \end{pmatrix}.$$

(a) If Rank(A') = Rank$(A) = n$, then the solution to $A\vec{x} = \vec{b}$ is unique.
(b) If Rank(A') = Rank$(A) < n$, then there are many solutions to $A\vec{x} = \vec{b}$. In fact, there are infinitely many solutions.
(c) If Rank$(A') \neq$ Rank(A), then $A\vec{x} = \vec{b}$ has no solution.

Proof. Let $\vec{a}_i$ denote the ith column of A and let $\vec{x} = (x_1, \ldots, x_n)^T$. Then the matrix equation $A\vec{x} = \vec{b}$ expands as

$$x_1\vec{a}_1 + \cdots + x_n\vec{a}_n = \vec{b}. \tag{116}$$

Hence, $A\vec{x} = \vec{b}$ has a solution if and only if $\vec{b} \in \text{Col}(A)$. The question of whether the solution is unique then depends on whether $\vec{b}$ is a unique linear combination of $\vec{a}_1, \ldots, \vec{a}_n$.

For (a), let us suppose that $\text{Rank}(A') = \text{Rank}(A) = n$. From the definition of rank, we have

$$\dim\ \text{Col}(A) = \dim\ \text{Col}(A') = n.$$

This implies that $\vec{a}_1, \ldots, \vec{a}_n$ is linearly independent and hence a basis for Col(A). Also, since

$$\text{Col}(A') = \text{span}\{\vec{a}_1, \ldots, \vec{a}_n,\ \vec{b}\},$$

it follows that $\vec{b}$ is a linear combination of $\vec{a}_1, \ldots, \vec{a}_n$. (If not, then $\dim \text{Col}(A') = n + 1$ which would be a contradiction.) Since $\vec{a}_1, \ldots, \vec{a}_n$ is a basis of Col(A), it follows that $\vec{b}$ is a unique linear combination of $\vec{a}_1, \ldots, \vec{a}_n$ which (from the above remarks) implies that $A\vec{x} = \vec{b}$ has a unique solution. This completes the proof of (a).

For (b), let us suppose that $\text{Rank}(A') = \text{Rank}(A) < n$. As in (a), this implies that $\vec{b}$ is a linear combination of $\vec{a}_1, \ldots, \vec{a}_n$. Hence, $A\vec{x} = \vec{b}$ has a solution. By the matrix version of the Rank-Nullity Theorem (Corollary 7.13), we have

$$\text{Rank}(A) + \text{Nullity}(A) = n.$$

Since $\text{Rank}(A) < n$, it follows that $\text{Nullity}(A) > 0$. In particular, $N(A) \neq \{\vec{0}\}$. Let $\vec{x}_0$ be any solution to $A\vec{x} = \vec{b}$. Then $\vec{x}_0 + \vec{n}$ is also a solution for any $\vec{n} \in N(A)$. Indeed,

$$A(\vec{x}_0 + \vec{n}) = A\vec{x}_0 + A\vec{n} = \vec{b} + \vec{0} = \vec{b}.$$

Since $N(A) \neq \{0\}$, $N(A)$ has infinitely many elements. From the above observation, it follows that $A\vec{x} = \vec{b}$ has infinitely many solutions. This completes the proof of (b).

For (c), let us suppose that $\text{Rank}(A') \neq \text{Rank}(A)$. Since A' is spanned by the vectors $\vec{a}_1, \ldots, \vec{a}_n, \vec{b}$, it follows that $\text{Rank}(A') = \text{Rank}(A) + 1$. In particular, $\vec{b}$ cannot be a linear combination of the column vectors of A. From (116), it follows that $A\vec{x} = \vec{b}$ has no solution. This completes the proof of (c). □

Chapter 7 Exercises

1. Given

$$A = \begin{pmatrix} 1 & 2 & 4 \\ 3 & 8 & 4 \\ 2 & 6 & 3 \end{pmatrix},$$

   find $\dim Col(A)$ and $\dim Row(A)$. Then compare these two dimensions.

2. Let V be the subspace of $\mathbb{R}^4$ spanned by the vectors

$$\vec{v}_1 = (1, 0, 2, 3), \vec{v}_2 = (2, -1, 0, 4), \vec{v}_3 = (0, -1, -4, -2)$$

   Find a basis for V.

3. Find row space and column space of

$$A = \begin{pmatrix} 1 & -1 & 0 \\ 2 & -1 & 2 \end{pmatrix}$$

4. Calculate the rank of matrix

$$A = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 5 & 6 & 7 \\ 0 & 0 & 0 & 8 \\ 0 & 0 & 0 & 9 \end{pmatrix}$$

5. Find a basis for the null space of

$$\mathbf{A} = \begin{pmatrix} 1 & 4 & 2 \\ 0 & -3 & 4 \\ 1 & 1 & 6 \end{pmatrix}$$

6. Compute the null space of

$$A = \begin{pmatrix} 0 & 1 & 1 & -1 & 2 \\ 0 & 2 & -2 & -2 & 0 \\ 0 & 1 & 1 & -1 & -1 \\ 1 & 1 & 0 & 1 & -1 \end{pmatrix}$$

and use Rank-Nullity Theorem to evaluate the rank of A.

7. Suppose A is a $n \times n$ matrix, and $\text{rank}(A) = 1$. Show

(a) $A = \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix} \begin{pmatrix} b_1 & b_2 & \cdots & b_n \end{pmatrix}$

(b) $A^2 = kA$, where k is a scalar.

8. For any matrices $A_{n\times m}$ and $B_{m\times s}$, show

$$\text{rank}(AB) \leq \min(\text{rank}(A), \text{rank}(B))$$

9. Let A and B be $m \times n$ matrices. Show that

$$\text{rank}(A \pm B) \leq \text{rank}(A) + \text{rank}(B)$$

10. Let A and B be $n \times n$ square matrices. If $AB = 0$, show that

$$\text{rank}(A) + \text{rank}(B) \leq n$$

11. Let

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

(a) Find a basis for $\text{Row}(A)$. What is the dimension of $\text{Row}(A)$?
(b) Find a basis for $\text{Col}(A)$. What is the dimension of $\text{Col}(A)$?
(c) Find a basis for $\ker(A)$. What is the dimension of $\ker(A)$?
(d) Verify the matrix version of the Rank-Nullity Theorem.

12. Let
$$A = \begin{pmatrix} 2 & 2 & -1 & -1 & 0 \\ 1 & 1 & 1 & 0 & 1 \\ 1 & -2 & 1 & 0 & 0 \\ 0 & -3 & 0 & 0 & -1 \\ -1 & -1 & -4 & -1 & -3 \end{pmatrix}.$$
   (a) Find a basis for Row(A). What is the dimension of Row(A)?
   (b) Find a basis for Col(A). What is the dimension of Col(A)?
   (c) Find a basis for ker(A). What is the dimension of ker(A)?
   (d) Verify the matrix version of the Rank-Nullity Theorem.

13. Using your calculations from problem 11., determine if the following system has a solution. If the system has a solution, is it unique? Justify your answer.
$$\begin{aligned} w + 2x - y + 2z &= 2 \\ 3w + 7x - 2y + 5z &= 4 \\ x + y - z &= -2 \end{aligned}$$

14. Using your calculations from problem 12., determine if the following system has a solution. If the system has a solution, is it unique? Justify your answer.
$$\begin{aligned} 2v + 2w - x - y &= 1 \\ v + w + x + z &= 2 \\ v - 2w + x &= 1 \\ -3w - z &= 1 \\ -v - w - 4x - y - 3z &= 1 \end{aligned}$$

15. Determine how many solutions the following system has
   (a)
$$\begin{aligned} x_1 - 2x_2 + 3x_3 - 4x_4 &= 4 \\ x_2 - x_3 + x_4 &= 3 \\ x_1 + 3x_2 + x_4 &= 2 \\ -7x_2 + 3x_3 + 4x_4 &= 1 \end{aligned}$$
   (b)
$$\begin{aligned} -x_1 + 3x_2 - 3x_3 + 4x_4 &= -1 \\ 3x_1 - 2x_2 + 2x_3 - 3x_4 &= 2 \\ 2x_1 + 3x_2 - 3x_3 + 5x_4 &= -3 \\ 2x_1 - x_2 + x_3 - 3x_4 &= 4 \end{aligned}$$

Chapter 8

The Dual Space

In this very short chapter, we introduce the idea of the **dual space**, which turns out to be a very important idea in mathematics (especially in differential geometry which is the branch of mathematics which applies calculus to curved spaces). We will need the idea of the dual space later on in Chapter 9. Throughout this chapter, we let $\mathbb{F} = \mathbb{R}$ or $\mathbb{C}$ and every vector space is a **finite** dimensional vector space over $\mathbb{F}$ unless stated otherwise.

8.1. The Dual Space

The dual space is formally defined as follows:

Definition 8.1. *The **dual space** of a vector space V is the vector space V^* which consists of all linear maps from V into $\mathbb{F}$. The vector space structure on V^* is the natural one which is defined by pointwise addition and scalar multiplication. Explicitly, for $f, g \in V^*$ and $c \in \mathbb{F}$, vector addition and scalar multiplication are defined by*

$$(f + g)(v) := f(v) + g(v), \quad (cf)(v) := cf(v)$$

*for all $v \in V$. The elements of V^* are sometimes called **covectors** or **1-forms**.*

We now collect some basic facts about the dual space.

Theorem 8.2. *Let V be a (finite dimensional) vector space. Then* $\dim V^* = \dim V$.

Proof. Let $n = \dim V$ and let $\{b_1, b_2, \ldots, b_n\}$ be a basis on V. Let $\theta^i \in V^*$ for $i = 1, \ldots, n$ be the unique linear map from V to $\mathbb{F}$ defined by the condition:

$$\theta^i(b_j) = \begin{cases} 1 & \text{if } i = j \\ 0 & \text{if } i \neq j. \end{cases}$$

(Recall from Chapter 5 that any linear map is completely determined once its values on a basis are known.) We now show that $\{\theta^1, \ldots, \theta^n\}$ is a basis on V^*. Let $f \in V^*$ be arbitrary and let

$$f_\theta := \sum_{i=1}^{n} f(b_i)\theta^i.$$

From the definition of θ^i, we have

$$\begin{aligned} f_\theta(b_j) &= \left(\sum_{i=1}^{n} f(b_i)\theta^i \right)(b_j) \\ &= \sum_{i=1}^{n} f(b_i)\theta^i(b_j) \\ &= f(b_j)\theta^j(b_j) \\ &= f(b_j). \end{aligned}$$

Hence, f_θ and f agree on a basis of V. This implies that f_θ and f must be the same linear map, i.e., $f_\theta = f$. This shows that $\{\theta^1, \ldots, \theta^n\}$ spans V^*. We now show linear independence. Suppose that for some $c_1, \ldots, c_n \in \mathbb{F}$, we have

$$c_1\theta^1 + c_2\theta^2 + \cdots + c_n\theta^n = \mathbf{0}. \tag{117}$$

Evaluating the left and right sides at b_i gives

$$\begin{aligned} 0 &= (c_1\theta^1 + \cdots + c_n\theta^n)(b_i) \\ &= c_1\theta^1(b_i) + \cdots + c_n\theta^n(b_i) \\ &= c_i\theta^i(b_i) \\ &= c_i. \end{aligned}$$

This proves that $\{\theta^1, \ldots, \theta^n\}$ is a basis of V^*. From this, we conclude that $\dim V^* = n = \dim V$. □

The proof of Theorem 8.2 motivates the following definition:

Definition 8.3. *Let V be a vector space and let $\mathcal{B} = \{b_1, \ldots, b_n\}$ be a basis on V. The* ***dual basis*** *of $\mathcal{B}$ is the basis*

$$\mathcal{B}^* := \{\theta^1, \ldots, \theta^n\}$$

on V^* where $\theta^i : V \to \mathbb{F}$ is the unique linear map satisfying $\theta^i(b_i) = 1$ and $\theta^i(b_j) = 0$ for $j \neq i$.

Remark 8.4. *The notation for the dual basis varies greatly in the literature. If $\mathcal{B} = \{b_1, \ldots, b_n\}$ is a basis on V, the dual basis of $\mathcal{B}$ is sometimes denoted by*

$$\mathcal{B}^* = \{b_1^*, \ldots, b_n^*\}$$

or by

$$\mathcal{B}^* = \{b^1, \ldots, b^n\}.$$

For convenience, we record the following result:

Corollary 8.5. *Let V be a vector space and let $\mathcal{B} = \{b_1, \ldots, b_n\}$ be a basis on V. Also, let $\mathcal{B}^* = \{\theta^1, \ldots, \theta^n\}$ denote the dual basis. Then*

(i) $f = f(b_1)\theta^1 + \cdots + f(b_n)\theta^n$ for all $f \in V^*$

(ii) $v = \theta^1(v)b_1 + \cdots + \theta^n(v)b_n$ for all $v \in V$.

Proof. Statement (i) was already proved during the proof of Theorem 8.2. For statement (ii), let $v \in V$ and express v as (a unique) linear combination of the basis $\mathcal{B}$:

$$v = \alpha_1 b_1 + \cdots + \alpha_n b_n \tag{118}$$

Applying the dual basis element θ^i to both sides of (118) gives

$$\theta^i(v) = \alpha_1\theta^i(b_1) + \cdots + \alpha_n\theta^i(b_n) = \alpha_i\theta^i(b_i) = \alpha_i.$$

This proves (ii). □

Consider a vector space V. Since V^* is also a vector space, one can also take the dual of V^*. This new space is the vector space $(V^*)^*$ and is called the *double dual* of V. *So what do we get by taking the dual twice?* The next result provides an answer to this question (at least for the case of finite dimensional vector spaces).

Theorem 8.6. *Let V be a (finite dimensional) vector space. Then $(V^*)^*$ is canonically (i.e. naturally) isomorphic to V. Specifically, the isomorphism associates a vector $v \in V$ with the element $\varphi_v \in (V^*)^*$ defined by $\varphi_v(f) := f(v)$ for all $f \in V^*$.*

Proof. Let $v \in V$ and let $\varphi_v : V^* \to \mathbb{F}$ be the map which sends $f \in V^*$ to $f(v) \in \mathbb{F}$. We now quickly verify that φ_v is a linear map. Let $f, g \in V^*$ and let $c \in \mathbb{F}$. Then

$$\begin{aligned}\varphi_v(f+g) &:= (f+g)(v) \\ &= f(v) + g(v) \\ &= \varphi_v(f) + \varphi_v(g)\end{aligned}$$

and

$$\begin{aligned}\varphi_v(cf) &:= (cf)(v)\\ &= cf(v)\\ &= c\varphi_v(f).\end{aligned}$$

This proves that $\varphi_v : V^* \to \mathbb{F}$ is a linear map. In particular, this means that $\varphi_v \in (V^*)^*$.

Next, let $\varphi : V \to (V^*)^*$ be the map which sends $v \in V$ to $\varphi_v \in (V^*)^*$. In other words, $\varphi(v) := \varphi_v$. We now show that φ is a linear map. To do this, let $v, w \in V$ and $f \in V^*$. Then

$$\begin{aligned}\varphi_{v+w}(f) &:= f(v+w)\\ &= f(v) + f(w)\\ &= \varphi_v(f) + \varphi_w(f)\\ &= (\varphi_v + \varphi_w)(f), \end{aligned} \tag{119}$$

where the second equality follows from the fact that $f : V^* \to \mathbb{F}$ is a linear map (by definition) and the last equality is the definition of vector addition on $(V^*)^*$. For $c \in \mathbb{F}$, we also have

$$\begin{aligned}\varphi_{cv}(f) &:= f(cv)\\ &= cf(v)\\ &= c\varphi_v(f)\\ &= (c\varphi_v)(f)\end{aligned} \tag{120}$$

where the second equality again follows from the linearity of f. Since $f \in V^*$ was arbitrary, (119) and (120) then imply

$$\begin{aligned}\varphi(v+w) &:= \varphi_{v+w}\\ &= \varphi_v + \varphi_w\\ &= \varphi(v) + \varphi(w)\end{aligned}$$

and

$$\begin{aligned}\varphi(cv) &:= \varphi_{cv}\\ &= c\varphi_v\\ &c\varphi(v).\end{aligned}$$

This proves that $\varphi : V \to V^*$ is a linear map. Moreover, note that φ is canonical or natural since its construction does not depend on arbitrary choices such as a choice of basis on V for example.

Lastly, we prove that φ is an isomorphism. In other words, we have to show that φ is one-to-one and onto. First, we verify that φ is one-to-one, that is, $\dim \ker \varphi = 0$.

To do this, let $\{b_1, \ldots, b_n\}$ be any basis on V and let $\{\theta^1, \ldots, \theta^n\}$ denote the dual basis. By Corollary 8.5, any vector $v \in V$ decomposes as

$$v = \theta^1(v)b_1 + \theta^2(v)b_2 + \cdots + \theta^n(v)b_n.$$

Now let $v \in \ker \varphi$. Then for all $f \in V^*$, we have $\varphi_v(f) = f(v) = 0$. In particular, setting $f = \theta^i$, we have $\theta^i(v) = 0$ for $i = 1, \ldots, n$. From the above decomposition, this implies that $v = \mathbf{0}$. Hence, $\dim \ker \varphi = 0$.

For the onto part, first note that by Theorem 8.2, we have

$$\dim(V^*)^* = \dim V^* = \dim V.$$

Since $\dim \ker \varphi = 0$, the Rank Nullity Theorem (Theorem 5.60) implies

$$\dim V = \dim \ker \varphi + \dim \text{im } \varphi = \dim \text{im } \varphi.$$

This implies that im φ has the same dimension as $(V^*)^*$. However, im φ is also a subspace of $(V^*)^*$. From this, we conclude that im $\varphi = (V^*)^*$. Hence, φ is onto. This completes the proof. □

For the case of finite dimensional vector spaces (which is what we focus on in this book), most people simply blur the distinction between V and $(V^*)^*$ and simply regard them as being one and the same. In other words, one identifies the vector $v \in V$ with the element $\varphi_v \in (V^*)^*$ by setting $v(f) := f(v)$ for all $f \in V^*$. One emphasizes this point of view by writing $(V^*)^* = V$. This is the point of view we will adopt in this book. Strictly speaking, of course, what we really have is an isomorphism (albeit a natural one). Hence, the correct expression is $(V^*)^* \simeq V$ as opposed to $(V^*)^* = V$.

Here are some basic examples to consider.

Example 8.7. *Let $\mathfrak{sl}_2(\mathbb{R})$ be the vector space of 2×2 real matrices with zero trace. An arbitrary element $X \in \mathfrak{sl}_2(\mathbb{R})$ is of the form*

$$X = \begin{pmatrix} c & a \\ b & -c \end{pmatrix} \tag{121}$$

for $a, b, c \in \mathbb{R}$. As we have seen several times, a convenient basis for $\mathfrak{sl}_2(\mathbb{R})$ is

$$E = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \quad F = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \quad H = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Let $\{\delta_E, \delta_F, \delta_H\}$ denote the dual basis. Then

$$\begin{aligned}\mathfrak{sl}_2(\mathbb{R})^* &= \operatorname{span}\{\delta_E, \delta_F, \delta_H\} \\ &= \{\alpha_1\delta_E + \alpha_2\delta_F + \alpha_3\delta_H \mid a, b, c \in \mathbb{R}\}\end{aligned}$$

Let $f = \alpha_1\delta_E + \alpha_2\delta_F + \alpha_3\delta_H$ be an arbitrary 1-form and let $X \in \mathfrak{sl}_2(\mathbb{R})$ be an arbitrary element of the form (8.7). In other words, $X = aE + bF + cH$. Then

$$f(X) = \alpha_1 a + \alpha_2 b + \alpha_3 c.$$

Example 8.8. *Consider the vector space $\mathbb{R}^n$ with vectors expressed as column vectors. Let $\mathcal{S} = \{\vec{e}_1, \dots, \vec{e}_n\}$ denote the standard basis on $\mathbb{R}^n$ and let $f \in (\mathbb{R}^n)^*$ be an arbitrary element. Since f is a linear map from $\mathbb{R}^n$ to $\mathbb{R}$, it follows that f is just a linear transformation associated to some unique $1 \times n$ matrix A_f. In other words,*

$$f(\vec{v}) = A_f\vec{v} \in \mathbb{R}$$

for all $\vec{v} \in \mathbb{R}^n$, where the right side is evaluated by matrix multiplication. To compute A_f, let us apply f to some arbitrary vector $\vec{v} = v_1\vec{e}_1 + \cdots + v_n\vec{e}_n \in \mathbb{R}^n$:

$$\begin{aligned}f(\vec{v}) &= v_1 f(\vec{e}_1) + \cdots + v_n f(\vec{e}_n) \\ &= (f(\vec{e}_1), \dots, f(\vec{e}_n)) \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix}.\end{aligned}$$

From this, we see that

$$A_f = (f(\vec{e}_1), \dots, f(\vec{e}_n)).$$

Conversely, the linear transformation associated to any $1 \times n$ matrix A is also an element of the dual space $(\mathbb{R}^n)^*$. This shows that if we regard $\mathbb{R}^n$ as the vector space of ***column*** *vectors with n components, then $(\mathbb{R}^n)^*$ can be naturally identified with the vector space of* ***row*** *vectors with n components.*

8.2. The Dual of a Linear Map

Definition 8.9. *Let $\varphi : U \to V$ be a linear map. The* ***dual*** *of φ is the map $\varphi^* : V^* \to U^*$ defined by $\varphi^*(f) := f \circ \varphi \in U^*$ for $f \in V^*$.*

Before stating the next result, recall that the composition of two linear maps is again a linear map. This fact implies that $\varphi^*(f) : U \to \mathbb{F}$ in Definition 8.9 is a linear map. In other words, $\varphi^*(f)$ is indeed an element of U^*.

Proposition 8.10. *The dual of a linear map is also a linear map. Moreover, if $\varphi : U \to V$ and $\psi : V \to W$ are linear maps. Then $(\psi \circ \varphi)^* = \varphi^* \circ \psi^*$.*

Proof. Let $\varphi : U \to V$ be a linear map. To show that $\varphi^* : V^* \to U^*$ is linear, let $f, g \in V^*$ and let $c \in \mathbb{F}$. Then for all $u \in U$, we have

$$\begin{aligned} \varphi^*(f+g)(u) &:= (f+g) \circ \varphi(u) \\ &= f \circ \varphi(u) + g \circ \varphi(u) \\ &= (\varphi^*(f))(u) + (\varphi^*(g))(u) \\ &= (\varphi^*(f) + \varphi^*(g))(u) \end{aligned} \tag{122}$$

and

$$\begin{aligned} \varphi^*(cf)(u) &:= (cf) \circ \varphi(u) \\ &= c(f \circ \varphi(u)) \\ &= c(\varphi^*(f)(u)) \\ &= (c\varphi^*(f))(u). \end{aligned} \tag{123}$$

Since $u \in U$ is arbitrary, (122) and (123) imply

$$\varphi^*(f+g) = \varphi^*(f) + \varphi^*(g), \qquad \varphi^*(cf) = c\varphi^*(f).$$

This proves that φ^* is linear.

For the last part, let $\psi : V \to W$ be a linear map. Then for all $h \in W^*$, we have

$$\begin{aligned} (\psi \circ \varphi)^*(h) &= h \circ (\psi \circ \varphi) \\ &= (h \circ \psi) \circ \varphi \\ &= \varphi^*(h \circ \psi) \\ &= \varphi^*(\psi^*(h)) \\ &= (\varphi^* \circ \psi^*)(h). \end{aligned}$$

Since $h \in W^*$ is arbitrary, we conclude that $(\psi \circ \varphi)^* = \varphi^* \circ \psi^*$. This completes the proof. □

The next result concerns the matrix representation of the dual of a linear map:

Theorem 8.11. *Let $\varphi : V \to W$ be a linear map and let $\mathcal{B}$ be a basis on V and let $\mathcal{C}$ be a basis on W. Let $\mathcal{B}^*$ and $\mathcal{C}^*$ denote the dual bases of $\mathcal{B}$ and $\mathcal{C}$ respectively. Then the matrix representations $[\varphi^*]_{\mathcal{B}^*\mathcal{C}^*}$ and $[\varphi]_{\mathcal{C}\mathcal{B}}$ are related by $[\varphi^*]_{\mathcal{B}^*\mathcal{C}^*} = [\varphi]_{\mathcal{C}\mathcal{B}}^T$.*

Proof. Let $\mathcal{B} = \{v_1, \ldots, v_n\}$ be a basis on V and let $\mathcal{C} = \{w_1, \ldots, w_m\}$ be a basis on W. Also, let a_{ij} denote the (i, j)-element of the matrix representation $[\varphi]_{\mathcal{CB}}$. By definition, we have

$$\varphi(v_j) = \sum_{i=1}^{m} a_{ij} w_i. \tag{124}$$

Let $\mathcal{B}^* = \{\theta^1, \ldots, \theta^n\}$ and $\mathcal{C}^* = \{\delta^1, \ldots, \delta^m\}$ denote the dual bases of $\mathcal{B}$ and $\mathcal{C}$ respectively. Let b_{ij} denote the (i, j)-element of the matrix representation $[\varphi^*]_{\mathcal{B}^*\mathcal{C}^*}$. Once again, by definition, we have

$$\varphi^*(\delta^j) = \sum_{i=1}^{n} b_{ij} \theta^i. \tag{125}$$

From (125), we have

$$\begin{aligned} \varphi^*(\delta^j)(v_i) &= \sum_{k=1}^{n} b_{kj} \theta^i(v_i) \\ &= b_{ij}. \end{aligned} \tag{126}$$

On the other hand, using the definition of φ^*, we also have

$$\begin{aligned} \varphi^*(\delta^j)(v_i) &= \delta^j \left(\varphi(v_i)\right) \\ &= \delta^j \left(\sum_{k=1}^{m} a_{ki} w_k\right) \\ &= \sum_{k=1}^{m} a_{ki} \delta^j(w_k) \\ &= a_{ji}. \end{aligned} \tag{127}$$

(126) and (127) now imply $[\varphi^*]_{\mathcal{B}^*\mathcal{C}^*} = [\varphi]_{\mathcal{CB}}^T$. This completes the proof. $\square$

Theorem 8.11 is the reason why the dual of a linear map is also called the **transpose of a linear map** and the notation φ^T is used in place of φ^*.

Example 8.12. *Let $\mathbb{R}[x]_2$ denote the vector space of polynomials of degree 2 or less. Let $D : \mathbb{R}[x]_2 \to \mathbb{R}[x]_2$ be the linear map defined by*

$$Dp(x) := \frac{d^2}{dx^2}p(x) + 3\frac{d}{dx}p(x) + p(x), \qquad \forall\ p(x) \in \mathbb{R}[x]_2.$$

Let $\mathcal{B} := \{x^2, x, 1\}$. Then $\mathcal{B}$ is a basis on $\mathbb{R}[x]_2$ and the matrix representation of D with respect to $\mathcal{B}$ is

$$[D]_{\mathcal{B}} = \begin{pmatrix} 1 & 0 & 0 \\ 6 & 1 & 0 \\ 2 & 3 & 1 \end{pmatrix}.$$

Let $\mathcal{B}^*$ be the dual basis of $\mathcal{B}$. By Theorem 8.11, the matrix representation of D^* with respect to $\mathcal{B}^*$ is

$$[D^*]_{\mathcal{B}^*} = [D]_{\mathcal{B}}^T = \begin{pmatrix} 1 & 6 & 2 \\ 0 & 1 & 3 \\ 0 & 0 & 1 \end{pmatrix}.$$

Chapter 8 Exercises

In the problems below, let $\mathbb{F} = \mathbb{R}$ or $\mathbb{C}$ and assume all vector spaces are finite dimensional and over $\mathbb{F}$ unless stated otherwise.

1. Let $T : \mathbb{R}^3 \to \mathbb{R}^2$ be the linear map defined by

$$T(x, y, z) := (5x - 3y, y + z).$$

   Let $\mathcal{S}_3$ denote the standard basis on $\mathbb{R}^3$ and let $\mathcal{S}_2$ denote the standard basis on $\mathbb{R}^2$. Also, let $\mathcal{S}_3^*$ and $\mathcal{S}_2^*$ denote the corresponding dual bases. Compute the matrix representation $[T^*]_{\mathcal{S}_3^* \mathcal{S}_2^*}$ of the dual map $T^* : (\mathbb{R}^2)^* \to (\mathbb{R}^3)^*$ with respect to the aforementioned dual bases.

2. Let $\mathbb{R}[x]_2$ be the vector space of polynomials of degree 2 and let $\mathcal{B}$ denote the basis $\{x^2, x, 1\}$ on $\mathbb{R}[x]_2$. Let

$$D : \mathbb{R}[x]_2 \to \mathbb{R}[x]_2$$

   be the linear map defined by

$$Dp(x) := 3\frac{d^2}{dx^2}p(x) - 4\frac{d}{dx}p(x) - p(x).$$

   Let $\mathcal{B}^*$ denote the dual basis. Compute the matrix representation of the dual linear map D^* with respect to $\mathcal{B}^*$.

3. Let V be an **infinite** dimensional vector space over $\mathbb{F}$. Also, let $\varphi : V \to (V^*)^*$ be the linear map which sends $v \in V$ to the linear map $\varphi_v : V^* \to \mathbb{F}$ defined by $\varphi_v(f) := f(v)$. Show that φ is injective, but not surjective. In particular,

φ is not a vector space isomorphism.

4. Let $\varphi : V \to W$ be a vector space isomorphism. Show that $(\varphi^*)^{-1} = (\varphi^{-1})^*$.

5. Let V be a vector space of dimension n and let $f_1, f_2, \ldots, f_k \in V^*$ with $k \leq n$. Show that $f_1, f_2, \ldots, f_k$ is linearly independent if and only if

$$\dim(\ker f_1 \cap \ker f_2 \cap \cdots \cap \ker f_k) = n - k.$$

In particular, $f_1, \ldots, f_n \in V^*$ is a basis if and only if

$$\ker f_1 \cap \ker f_2 \cap \cdots \cap \ker f_n = \{\mathbf{0}\}.$$

Hints: Consider the map $\psi : V \to \mathbb{F}^k$ defined by $\psi(v) := (f_1(v), \ldots, f_k(v))$. Also, for a basis $\{b_1, \ldots, b_n\}$ on V, consider the $n \times k$ matrix

$$\begin{pmatrix} \psi(b_1) \\ \psi(b_2) \\ \vdots \\ \psi(b_n) \end{pmatrix}.$$

6. *Free Vector Spaces*. Let $\mathbb{F}$ be a field. Let A be a set. Define a vector space $F(A)$ to be the set of all functions $f : A \to \mathbb{F}$ that equal 0 almost everywhere in the sense that $f(a) = 0$ for all but finitely many $a \in A$. For $f, g \in F(A)$ and $c \in \mathbb{F}$, define

$$(f + g)(a) := f(a) + g(a), \qquad (cf)(a) := cf(a)$$

for all $a \in A$.
   (a) Show that $F(A)$ is a vector space over $\mathbb{F}$.
   (b) Show that for any vector space V over $\mathbb{F}$, the set of linear maps $F(A) \to V$ are in bijection with the set of functions $A \to V$.

7. Show that $\mathbb{R}^n$ is naturally isomorphic to the free real vector space $F(n)$ on a finite set n. Thus, for any real vector space V, linear maps $\mathbb{R}^n \to V$ are in bijection with functions $n \to V$.

8. Show that the polynomial vector space $\mathbb{F}[x]$ and the free vector space over a field $\mathbb{F}$ on the set of natural numbers $F(\mathbb{N})$ are isomorphic.

9. Show that the dual space $F(A)^*$ over a field $\mathbb{F}$ and the vector space of all functions $\mathbb{F}^A$ (not just those that equal 0 almost everywhere) are isomorphic. This example shows that a vector space and its dual are not necessarily isomorphic.

Chapter 9

Inner Product Spaces

In Chapter 2, we introduced the dot product on $\mathbb{R}^n$, which allows one to compute the length or norm of a vector as well as the angle between two vectors. The dot product, of course, is a byproduct of the natural (i.e. Euclidean) geometry on $\mathbb{R}^n$. In fact, the dot product is really much more than a byproduct. Since the dot product allows one to compute distances and angles, one can view the dot product as a clever, compact tool for encoding the Euclidean geometry of $\mathbb{R}^n$.

Now suppose that we have an arbitrary real vector space V. *What distinguishes* $\mathbb{R}^n$ *from* V? The answer is geometry. $\mathbb{R}^n$ comes with its own natural geometry (namely the familiar Euclidean geometry that we all learned about in grade school) whereas V does not. For example, let $C([0,1])$ be the set of all continuous real valued functions on the closed interval $[0,1]$. Note that $C([0,1])$ has a natural vector space structure with vector addition and scalar multiplication defined pointwise:

$$(f+g)(x) := f(x) + g(x)$$
$$(cf)(x) := cf(x)$$

for all $f, g \in C([0,1])$, $c \in \mathbb{R}$, and $x \in [0,1]$. Now here are some questions for the reader. *For continuous functions* $f, g \in C([0,1])$*, what is the angle between* f *and* g*? What is the length of* f*? How does one even define these concepts for functions?!* We can answer these questions rather easily for vectors in $\mathbb{R}^n$. However, when it comes to a vector space like $C([0,1])$, which is hard to visualize, these questions become more difficult to answer. Angles and lengths are geometric concepts and since $C([0,1])$ lacks a natural geometry, we do not know how to answer these questions. Put another way, we cannot answer these questions because $C([0,1])$ lacks its own dot product. On the other hand, if we could equip $C([0,1])$ with something like a dot product, then we would have a pretty good idea of how to answer these geometric questions. This line of thinking leads one to the notion of an *inner product*, which generalizes the notion of the dot product to general vector spaces.

In the next two sections, we will introduce two types of inner products: one for real vector spaces and one for complex vector spaces. We conclude our introductory remarks here by reminding the reader about the notion of **Cartesian products**:

Definition 9.1. *Let X_1, X_2, ..., X_n be any sets. The Cartesian product of X_1, X_2, ..., X_n is the set*

$$X_1 \times X_2 \times \cdots \times X_n := \{(x_1, x_2, \ldots, x_n) \mid x_i \in X_i \text{ for } i = 1, 2, \ldots, n\}.$$

The most important examples in this book is the real vector space $\mathbb{R}^n$ which is the Cartesian product of n copies of $\mathbb{R}$ and the complex vector $\mathbb{C}^n$ which is the Cartesian product of n copies of $\mathbb{C}$.

9.1. Real Inner Product Spaces

In this section, we define inner products for real vector spaces. The definition is modeled over the algebraic properties of the dot product.

Definition 9.2. *Let V be a real vector space. An* ***inner product*** *is a map*

$$\langle \cdot, \cdot \rangle : V \times V \to \mathbb{R}, \quad (u, v) \mapsto \langle u, v \rangle \in \mathbb{R}$$

which satisfies the following conditions:

(i) $\langle u, v \rangle = \langle v, u \rangle$ *for all* $u, v \in V$ *(symmetry)*
(ii) $\langle u + v, w \rangle = \langle u, w \rangle + \langle v, w \rangle$ *for all* $u, v, w \in V$ *(linearity condition 1)*
(iii) $\langle cu, v \rangle = c\langle u, v \rangle$ *for all* $c \in \mathbb{R}$ *and* $u, v \in V$ *(linearity condition 2)*
(iv) $\langle v, v \rangle \geq 0$ *for all* $v \in V$ *and* $\langle v, v \rangle = 0$ *iff* $v = \mathbf{0}$ *(positive definiteness)*

The pair $(V, \langle \cdot, \cdot \rangle)$ *is called a (real)* ***inner product space****.*

Let $w \in V$ be arbitrary and let $f_w : V \to \mathbb{R}$ be the map defined by

$$f_w(v) := \langle v, w \rangle.$$

Conditions (ii) and (iii) in Definition 9.2 then implies that $f_w : V \to \mathbb{R}$ is a linear map. Furthermore, the symmetry condition of $\langle \cdot, \cdot \rangle$ (condition (i)) also implies that $\langle \cdot, \cdot \rangle$ is linear in its second argument as well, that is,

$$\langle u, v + w \rangle = \langle u, v \rangle + \langle u, w \rangle, \qquad \langle u, cv \rangle = c\langle u, v \rangle$$

for all $u, v, w \in V$ and $c \in \mathbb{R}$.

Remark 9.3. *Let V and W be (real) vector spaces. A map*

$$\beta : V \times W \to \mathbb{R}, \quad (v, w) \mapsto \beta(v, w)$$

which is linear in each argument, that is,

$$\beta(v + v', w) = \beta(v, w) + \beta(v', w), \qquad \beta(cv, w) = c\beta(v, w)$$

and

$$\beta(v, w + w') = \beta(v, w) + \beta(v, w'), \qquad \beta(v, cw) = c\beta(v, w)$$

for all $v, v' \in V$, $w, w' \in W$, and $c \in \mathbb{R}$ is called a ***bilinear form****. An inner product is then an example of a bilinear form. Conditions (i)-(iii) of Definition 9.2 is simply the statement that an inner product is a* ***symmetric bilinear form*** *on V. If we thrown in condition (iv), Definition 9.2 is equivalent to the statement that $\langle \cdot, \cdot \rangle$ is a* ***positive definite, symmetric bilinear form****.*

Example 9.4. *The most well important example of an inner product space is, of course, the vector space $\mathbb{R}^n$ equipped with its dot product. For $\vec{u}, \vec{v} \in \mathbb{R}^n$, define*

$$\langle \vec{u}, \vec{v} \rangle := \vec{u} \cdot \vec{v}.$$

From the properties of the dot product, we immediately have

$$\langle \vec{u}, \vec{v} \rangle := \vec{u} \cdot \vec{v} = \vec{v} \cdot \vec{u} = \langle \vec{v}, \vec{u} \rangle$$

and

$$\begin{aligned} \langle \vec{u} + \vec{v}, \vec{w} \rangle &:= (\vec{u} + \vec{v}) \cdot \vec{w} \\ &= \vec{u} \cdot \vec{w} + \vec{v} \cdot \vec{w} \\ &= \langle \vec{u}, \vec{w} \rangle + \langle \vec{v}, \vec{w} \rangle \end{aligned}$$

and

$$\langle c\vec{u}, \vec{v} \rangle := (c\vec{u}) \cdot \vec{v} = c(\vec{u} \cdot \vec{v}) = c\langle \vec{u}, \vec{v} \rangle.$$

Also, $\langle \vec{u}, \vec{u} \rangle = \vec{u} \cdot \vec{u} \geq 0$ with equality only when $\vec{u} = \vec{0}$. Hence, we have shown that the dot product is an inner product.

Example 9.5. *Let $C([0, 1])$ be the set of all* ***continuous*** *real valued functions on the closed interval $[0, 1]$. Note that $C([0, 1])$ is naturally a real vector space with vector addition and scalar multiplication defined* ***pointwise****, i.e,*

$$(f + g)(x) := f(x) + g(x)$$

and $(cf)(x) := cf(x)$ for all $f, g \in C([0, 1])$ and $c \in \mathbb{R}$. Also, observe that $C([0, 1])$ is an ***infinite*** *dimensional vector space. Indeed, let $\mathbb{R}[x]_n$ denote the vector space of real polynomials of degree n or less. Since $\mathbb{R}[x]_n$ is a* subspace of $C([0,1])$ and $\dim \mathbb{R}[x]_n = n+1$, it follows that $\dim C([0,1]) = \infty$. We will now turn $C([0,1])$ into an inner product space. For $f, g \in C([0,1])$, define

$$\langle f, g\rangle := \int_0^1 f(x)g(x)dx.$$

From the above definition, we have

$$\langle f, g\rangle := \int_0^1 f(x)g(x)dx = \int_0^1 g(x)f(x)dx = \langle g, f\rangle.$$

Also, for $f, g, h \in C([0,1])$ and $c \in \mathbb{R}$, we have

$$\begin{aligned}\langle f+g, h\rangle &:= \int_0^1 (f+g)(x)h(x)dx \\ &= \int_0^1 f(x)g(x)dx + \int_0^1 f(x)h(x)dx \\ &= \langle f, g\rangle + \langle f, h\rangle\end{aligned}$$

and

$$\begin{aligned}\langle cf, g\rangle &:= \int_0^1 (cf)(x)g(x)dx \\ &= \int_0^1 cf(x)g(x)dx \\ &= c\int_0^1 f(x)g(x)dx \\ &= c\langle f, g\rangle.\end{aligned}$$

To show that $\langle \cdot, \cdot\rangle$ is an inner product, it only remains to show that it is positive definite. First, for any $f \in C([0,1])$, we have

$$\langle f, f\rangle := \int_0^1 f(x)f(x)dx = \int_0^1 f^2(x)dx \geq 0$$

since $f^2 \geq 0$. Now suppose $f \neq 0$. Then there exists an $x_0 \in [0,1]$ such that $f(x_0) \neq 0$. Moreover, since f is continuous, we can further assume that x_0 is neither 0 or 1. (A continuous function on $[0,1]$ which is nonzero cannot be nonzero at 0 and 1 while being zero for every $0 < x < 1$.) Since x_0 is neither 0 or 1 and f is continous, there must be an $\varepsilon > 0$ such that $[x_0 - \varepsilon, x_0 + \varepsilon] \subset [0,1]$ and f is never zero on $[x_0 - \varepsilon, x_0 + \varepsilon]$. By the Extreme Value Theorem, f attains an absolute minimum (which is nonzero) on $[x_0 - \varepsilon, x_0 + \varepsilon]$. Let m be the absolute minimum of f on $[x_0 - \varepsilon, x_0 + \varepsilon]$. Then

$$\begin{aligned}\langle f, f\rangle &:= \int_0^1 f^2(x)dx \\ &\geq \int_{x_0-\varepsilon}^{x_0+\varepsilon} f^2(x)dx \\ &\geq \int_{x_0-\varepsilon}^{x_0+\varepsilon} m^2 dx = 2m^2\varepsilon \neq 0.\end{aligned}$$

Hence, $\langle \cdot, \cdot\rangle$ is positive definite, which proves that it is indeed an inner product.

The inner product space constructed in Example 9.5 is infinite dimensional, which makes it quite different than the standard example given in Example 9.4. Our focus, however, will mainly be on **finite** dimensional inner product spaces. Hence, unless stated otherwise, every inner product space in this chapter is assumed to be finite dimensional.

Example 9.6. *Let $M_2(\mathbb{C})$ denote the set of 2×2 complex matrices. As we saw in Chapter 5, $M_2(\mathcal{C})$ is naturally a complex vector space. Indeed, vector addition is given by the usual additiion of matrices and scalar multiplication is just the ordinary scalar multiplication for matrices. Now any complex vector space is also a real vector space since $\mathbb{R} \subset \mathbb{C}$. In this example, we are going to view $M_2(\mathbb{C})$ as a **real** vector space. The reason for this will become clear in a moment. For a complex matrix*

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix},$$

let A^* denote its conjugate transpose, that is,

$$A^* = \begin{pmatrix} \overline{a} & \overline{c} \\ \overline{b} & \overline{d} \end{pmatrix},$$

where, for example, $\overline{a}$ denotes the conjugate of the complex number a.
*Now let $\mathfrak{su}(2)$ denote the **real** subspace of $M_2(\mathbb{C})$ consisting of all 2×2 complex matrices X whose trace is zero **and** satisfies $X^* = -X$. (A matrix which satisfies the second condition is called **skew-Hermitian**.) Note $\mathfrak{su}(2)$ is **not** a complex vector space! It is strictly a real vector space. Indeed, observe that if $X \in \mathfrak{su}(2)$, then*

$$(iX)^* = -iX^* = -i(-X) = iX \neq -iX.$$

Hence, $iX \notin \mathfrak{su}(2)$. This is why we chose to regard $M_2(\mathbb{C})$ as a real vector space for this particular example. We now define an inner product on $\mathfrak{su}(2)$ by

$$\langle X, Y\rangle := Tr(XY^*) = Tr(X(-Y)) = -Tr(XY).$$

We now verify that the above definition is indeed an inner product. From the properties of the trace, we immediately have $\langle X, Y\rangle = \langle Y, X\rangle$. We also have

$$\begin{aligned}\langle X+Y, Z\rangle &= -Tr((X+Y)Z) \\ &= -Tr(XZ+YZ) \\ &= -Tr(XZ) - Tr(YZ) \\ &= \langle X, Z\rangle + \langle Y, Z\rangle\end{aligned}$$

for all $X, Y, Z \in \mathfrak{su}(2)$. Also, we have $\langle cX, Y\rangle = -Tr(cXY) = -c\,Tr(XY) = c\langle X, Y\rangle$ for all $c \in \mathbb{R}$ and $X, Y \in \mathfrak{su}(2)$. Lastly, we need to verify that

$\langle\cdot,\cdot\rangle$ is positive definite. For this, we observe that every $X \in \mathfrak{su}(2)$ is of the form

$$X = \begin{pmatrix} \alpha i & z \\ -\overline{z} & -\alpha i \end{pmatrix}$$

for $\alpha \in \mathbb{R}$ and $z \in \mathbb{C}$. From the form of X, we deduce that $\dim \mathfrak{su}(2) = 3$. Now let us compute $\langle X, X\rangle$:

$$\begin{aligned}\langle X, X\rangle &= -\mathrm{Tr}(X^2) \\ &= -\mathrm{Tr}\begin{pmatrix} -(\alpha^2 + |z|^2) & 0 \\ 0 & -(\alpha^2 + |z|^2) \end{pmatrix} \\ &= 2(\alpha^2 + |z|^2) \\ &\geq 0.\end{aligned}$$

In particular, we see that $\langle X, X\rangle = 0$ if and only if $X = \mathbf{0}$.

We now ask the reader to think back to Chapter 2. Every idea or result associated to the dot product generalizes in a straightforward way to any real inner product space. In each case, the generalization is obtained by swapping out the dot product for an inner product. Consequently, all the proofs for the dot product case work equally well for the general case. In other words, all the hard work was already done in Chapter 2! We now run through a few of these ideas and results.

Definition 9.7. *Let $(V, \langle\cdot,\cdot\rangle)$ be a real inner product space. The norm or length of a vector $v \in V$ is defined by*

$$\|v\| := \sqrt{\langle v, v\rangle}.$$

Theorem 9.8. *Cauchy-Schwartz inequality (general case) Let $(V, \langle\cdot,\cdot\rangle)$ be a real inner product space. Then $|\langle u, v\rangle| \leq \|u\|\,\|v\|$ for all $u, v \in V$. Moreover, for u, v nonzero, $\langle u, v\rangle = \|u\|\,\|v\|$ if and only if $u = \lambda v$ for some positive $\lambda \in \mathbb{R}$.*

Proof. The proof is identical to the the dot product version (see Theorem 2.49). One simply replaces the dot product with the inner product and the proof still works. □

Definition 9.9. *Let $(V, \langle \cdot, \cdot \rangle)$ be a real inner product space. The angle $\theta \in [0, \pi]$ between two (nonzero) vectors $u, v \in V$ is defined by*

$$\cos \theta = \frac{\langle u, v \rangle}{\|u\| \, \|v\|}.$$

*u and v are said to be **orthogonal** if $\langle u, v \rangle = 0$.*

Definition 9.10. *Let $(V, \langle \cdot, \cdot \rangle)$ be a real inner product space and let $\{v_1, \ldots, v_k\}$ be a set of vectors in V. $\{v_1, \ldots, v_k\}$ is called an **orthogonal set** if $v_i \neq \mathbf{0}$ for $i = 1, \ldots, k$ and $\langle v_i, v_j \rangle = 0$ for all $1 \leq i < j \leq k$.*

In other words, a set of vectors in a real inner product space form an orthogonal set if they are all nonzero and mutually orthogonal to one another.

Proposition 9.11. *Let $(V, \langle \cdot, \cdot \rangle)$ be a real inner product space and let $\{v_1, \ldots, v_k\} \subset V$ be an orthogonal set. Then $\{v_1, \ldots, v_k\}$ is a linearly independent set.*

Proof. The proof is identical to the proof of Proposition 2.57. One simply replaces the dot product with the inner product $\langle \cdot, \cdot \rangle$ and the argument works as before. □

Definition 9.12. *Let $(V, \langle \cdot, \cdot \rangle)$ be a real inner product space. Let $v, u \in V$ with u nonzero. The **orthogonal projection** of v onto u is the vector*

$$proj_u v := \frac{\langle u, v \rangle}{\|u\|^2} u.$$

Recall from Chapter 2 that the notion of orthogonal projection was the critical ingredient in the Gram-Schmidt process which allows one to construct an orthogonal basis on any subspace of $\mathbb{R}^n$. Using Definition 9.12, the Gram-Schmidt process generalizes to any real inner product space as follows:

The Gram-Schmidt process for a real inner product space

Let $(V, \langle \cdot, \cdot \rangle)$ be a real inner product space. The Gram-Schmidt process generates an orthogonal basis from an existing basis on V. Once one obtains the orthogonal basis, one can normalize it to obtain an orthonormal basis. Let $\mathcal{B} = \{v_1, v_2, \ldots, v_n\}$ be **any** basis on V. We obtain an orthogonal basis

$$\mathcal{B}' := \{b_1, b_2, \ldots, b_n\}$$

as follows:

1. Define $b_1 := v_1$
2. For $k = 2, \ldots, n$, define

$$b_k := v_k - \sum_{i=1}^{k-1} \text{proj}_{b_i} v_k$$

Setting $u_i := b_i / \|b_i\|$, the set $\{u_1, u_2, \ldots, u_n\}$ is then an orthonormal basis.

At this point, the reader should be convinced that any dot product related result or idea from from Chapter 2 can be generalized to any real inner product space simply by replacing the dot product with an inner product. We conclude this section by mentioning one additional idea\result:

Definition 9.13. *Let $(V, \langle \cdot, \cdot \rangle)$ be a real inner product space and let W be a subspace of V. The* ***orthogonal complement*** *of W in V is the subspace*

$$W^{\perp} := \{w \in W \mid \langle w, v \rangle = 0 \ \forall \ v \in V\}.$$

Theorem 9.14. *Let $(V, \langle \cdot, \cdot \rangle)$ be a real inner product space and let W be a subspace of V. Then*

$$V = W \oplus W^{\perp}.$$

Proof. The proof is identical to the dot product version in Theorem 2.80. Specifically, one obtains the proof by replacing $\mathbb{R}^n$ with V and the dot product with $\langle \cdot, \cdot \rangle$ in the proof of Theorem 2.80. □

9.2. More on Real Inner Product Spaces

Let V be a (finite dimensional) real vector space. A natural question then is *how many inner products exist on V?* The answer is lots! We will see shortly that an inner product on V is equivalent to a choice of orthonormal basis on V. The following definition will prove essential to the problem at hand:

Definition 9.15. *Let $(V, \langle \cdot, \cdot \rangle)$ be a real inner product space and let*

$$\mathcal{B} = \{v_1, \ldots, v_n\}$$

*be any basis on V. The **matrix representation** of $\langle \cdot, \cdot \rangle$ with respect to the basis $\mathcal{B}$ is the $n \times n$ matrix whose (i, j) element is $\langle v_i, v_j \rangle$. The matrix representation of $\langle \cdot, \cdot \rangle$ with respect to $\mathcal{B}$ is denoted by $[\langle \cdot, \cdot \rangle]_{\mathcal{B}}$.*

The next result shows that a matrix representation of an inner product contains all the information about an inner product. This is analogous to a matrix representation of a linear map or the coordinate representation of a vector.

Proposition 9.16. *Let $(V, \langle \cdot, \cdot \rangle)$ be a real inner product space and let $\mathcal{B}$ be any basis on V.*

(i) $[\langle \cdot, \cdot \rangle]_{\mathcal{B}}$ is a symmetric matrix.
(ii) $\langle v, w \rangle = [v]_{\mathcal{B}}^T [\langle \cdot, \cdot \rangle]_{\mathcal{B}} [w]_{\mathcal{B}}$ for all $v, w \in V$.
(iii) If $\mathcal{B}$ is an orthonormal basis, then $\langle v, w \rangle = [v]_{\mathcal{B}} \cdot [w]_{\mathcal{B}}$ for all $v, w \in V$.

Proof. Let $\mathcal{B} = \{v_1, \ldots, v_n\}$ be any basis on V.

(i): The (i, j) and (j, i) entries of the matrix $[\langle \cdot, \cdot \rangle]_{\mathcal{B}}$ is $\langle v_i, v_j \rangle = \langle v_j, v_i \rangle$ (by the symmetry condition of the inner product). From this, we see that $[\langle \cdot, \cdot \rangle]_{\mathcal{B}}$ is a symmetric matrix.

(ii): Let $v, w \in V$ and write

$$[v]_{\mathcal{B}} = (\alpha_1, \ldots, \alpha_n)^T, \qquad [w]_{\mathcal{B}} = (\beta_1, \ldots, \beta_n)^T$$

for their coordinate representations with respect to $\mathcal{B}$. By definition, this means

$$v = \sum_{i=1}^{n} \alpha_i v_i, \qquad w = \sum_{j=1}^{n} \beta_j v_j. \tag{128}$$

Using (128), we expand $\langle v, w\rangle$ using the bilinearity of the inner product (which is a consequence of conditions (i)-(iii) of Definition 9.2)

$$\begin{aligned}\langle v, w\rangle &= \langle \sum_{i=1}^{n} \alpha_i v_i, \sum_{j=1}^{n} \beta_j v_j\rangle \\ &= \sum_{i=1}^{n}\sum_{j=1}^{n} \langle \alpha_i v_i, \beta_j v_j\rangle \\ &= \sum_{i=1}^{n}\sum_{j=1}^{n} \alpha_i \beta_j \langle v_i, v_j\rangle \\ &= \sum_{i=1}^{n}\sum_{j=1}^{n} \alpha_i \langle v_i, v_j\rangle \beta_j \\ &= [v]_{\mathcal{B}}^T [\langle \cdot, \cdot\rangle]_{\mathcal{B}} [w]_{\mathcal{B}}.\end{aligned}$$

(iii): Suppose now that $\mathcal{B} = \{v_1, \ldots, v_n\}$ is an orthonormal basis. Then

$$\langle v_i, v_j\rangle = \begin{cases} 1 & \text{if } i = j \\ 0 & \text{if } i \neq j \end{cases}$$

Hence, $[\langle \cdot, \cdot\rangle]_{\mathcal{B}} = I_n$ (the $n \times n$ identity matrix). Using (ii), we have

$$\begin{aligned}\langle v, w\rangle &= [v]_{\mathcal{B}}^T [\langle \cdot, \cdot\rangle]_{\mathcal{B}} [w]_{\mathcal{B}} \\ &= [v]_{\mathcal{B}}^T I_n [w]_{\mathcal{B}} \\ &= [v]_{\mathcal{B}}^T [w]_{\mathcal{B}} \\ &= [v]_{\mathcal{B}} \cdot [w]_{\mathcal{B}}.\end{aligned}$$

□

Theorem 9.17. *Let V be a (real) vector space. Let $\mathcal{B}$ be any basis on V and define*

$$\langle \cdot, \cdot\rangle^{\mathcal{B}} : V \times V \to \mathbb{R}$$

by $\langle u, v\rangle^{\mathcal{B}} := [u]_{\mathcal{B}} \cdot [v]_{\mathcal{B}}$ for all $u, v \in V$. Then $\langle \cdot, \cdot\rangle^{\mathcal{B}}$ is an inner product on V and $\mathcal{B}$ is an orthonormal basis with respect to this inner product. Moreover, ***every*** *inner product on V is of this form. In addition, if $\mathcal{C}$ is another basis on V, then $\langle \cdot, \cdot\rangle^{\mathcal{B}} = \langle \cdot, \cdot\rangle^{\mathcal{C}}$ if and only if the transition matrix $P_{\mathcal{CB}}$ is an orthogonal matrix, that is, $P_{\mathcal{CB}}^{-1} = P_{\mathcal{CB}}^T$.*

Proof. We now verify that $\langle \cdot, \cdot\rangle^{\mathcal{B}}$ satisfies all the conditions given in Definition 9.2. Condition (i) of Definition 9.2 follows from the fact that the dot product commutes:

$$\langle u, v\rangle^{\mathcal{B}} = [u]_{\mathcal{B}} \cdot [v]_{\mathcal{B}} = [v]_{\mathcal{B}} \cdot [u]_{\mathcal{B}} = \langle v, u\rangle^{\mathcal{B}}$$

for all $u, v \in V$. Conditions (ii) and (iii) are a consequence of Proposition 6.7 and the basic properties of the dot product:

$$\begin{aligned}\langle u+v, w\rangle^{\mathcal{B}} &= [u+v]_{\mathcal{B}} \cdot [w]_{\mathcal{B}} \\ &= ([u]_{\mathcal{B}} + [v]_{\mathcal{B}}) \cdot [w]_{\mathcal{B}} \\ &= [u]_{\mathcal{B}} \cdot [w]_{\mathcal{B}} + [v]_{\mathcal{B}} \cdot [w]_{\mathcal{B}} \\ &= \langle u, w\rangle^{\mathcal{B}} + \langle v, w\rangle^{\mathcal{B}}\end{aligned}$$

and

$$\begin{aligned}\langle cu, v\rangle^{\mathcal{B}} &= [cu]_{\mathcal{B}} \cdot [v]_{\mathcal{B}} \\ &= (c[u]_{\mathcal{B}}) \cdot [v]_{\mathcal{B}} \\ &= c([u]_{\mathcal{B}} \cdot [v]_{\mathcal{B}}) \\ &= c\langle u, v\rangle^{\mathcal{B}}\end{aligned}$$

for all $u, v, w \in V$ and $c \in \mathbb{R}$. For condition (iv), we have $\langle u, u\rangle = [u]_{\mathcal{B}} \cdot [u]_{\mathcal{B}} \geq 0$ for all $u \in V$. Moreover, since the coordinate vector $[u]_{\mathcal{B}} = \vec{0}$ if and only if $u = \mathbf{0}$, it follows that $\langle u, u\rangle = 0$ if and only if $u = 0$. This proves that $\langle \cdot, \cdot\rangle^{\mathcal{B}}$ is an inner product on V.

Now let $\langle \cdot, \cdot\rangle$ be any inner product on V. Using the Gram-Schmidt process for real inner product spaces (see Section 9.1), we can always construct an orthonormal basis on the real inner product space $(V, \langle \cdot, \cdot\rangle)$. Let $\mathcal{D}$ be any orthonormal basis for $(V, \langle \cdot, \cdot\rangle)$. By statement (iii) of Proposition 9.16, we have

$$\langle u, v\rangle = [u]_{\mathcal{D}} \cdot [v]_{\mathcal{D}}$$

for all $u, v \in V$. However, the right hand side is just $\langle u, v\rangle^{\mathcal{D}}$. Since $u, v \in V$ are arbitrary, we conclude that $\langle \cdot, \cdot\rangle = \langle \cdot, \cdot\rangle^{\mathcal{D}}$.

For the last part of Theorem 9.17, we need to determine when two bases $\mathcal{B}$ and $\mathcal{C}$ induce the same inner product on V. More precisely, we need to determine the necessary and sufficient conditions for $\langle \cdot, \cdot\rangle^{\mathcal{B}} = \langle \cdot, \cdot\rangle^{\mathcal{C}}$.

Suppose first that $\langle \cdot, \cdot\rangle^{\mathcal{B}} = \langle \cdot, \cdot\rangle^{\mathcal{C}}$ Let $u, v \in V$. Then

$$[u]_{\mathcal{B}} \cdot [v]_{\mathcal{B}} = [u]_{\mathcal{C}} \cdot [v]_{\mathcal{C}}. \tag{129}$$

Using Theorem 6.8 to express $[u]_{\mathcal{C}}$ and $[v]_{\mathcal{C}}$ in terms of $[u]_{\mathcal{B}}$ and $[v]_{\mathcal{B}}$ respectively, equation (129) can be rewritten as

$$\begin{aligned}[u]_{\mathcal{B}}^T [v]_{\mathcal{B}} &= [u]_{\mathcal{C}}^T [v]_{\mathcal{C}} \\ &= (P_{\mathcal{CB}}[u]_{\mathcal{B}})^T (P_{\mathcal{CB}}[v]_{\mathcal{B}}) \\ &= [u]_{\mathcal{B}}^T (P_{\mathcal{CB}}^T P_{\mathcal{CB}}) [v]_{\mathcal{B}}. \end{aligned} \tag{130}$$

Since the above relation holds for all $u, v \in V$, it follows that the coordinate vectors $[u]_{\mathcal{B}}$ and $[v]_{\mathcal{B}}$ can assume any element of $\mathbb{R}^n$ (where $n = \dim V$). From this, it follows that $P_{\mathcal{CB}}^T P_{\mathcal{CB}} = I_n$ (the $n \times n$ identity matrix). Hence, $P_{\mathcal{CB}}$ is orthogonal. To see this more explicitly, write $\mathcal{B} = \{b_1, \ldots, b_n\}$ and let $u = b_i$ and $v = b_j$. Then

$[u]_\mathcal{B} = \vec{e}_i$ and $[v]_\mathcal{B} = \vec{e}_j$, where $\vec{e}_i$ and $\vec{e}_j$ are the ith and $j$the standard basis vectors on $\mathbb{R}^n$ respectively. Equation (129) then reduces to

$$(I_n)_{ij} = \vec{e}_i^T(P_{\mathcal{CB}}^T P_{\mathcal{CB}})\vec{e}_j = (P_{\mathcal{CB}}^T P_{\mathcal{CB}})_{ij},$$

where $(I_n)_{ij}$ and $(P_{\mathcal{CB}}^T P_{\mathcal{CB}})_{ij}$ are the (i,j)-elements of I_n and $P_{\mathcal{CB}}^T P_{\mathcal{CB}}$ respectively.

On the other hand, if $P_{\mathcal{CB}}$ is orthogonal, then $P_{\mathcal{CB}}^T P_{\mathcal{CB}} = I_n$ and equation (130) implies that $[u]_\mathcal{B} \cdot [v]_\mathcal{B} = [u]_\mathcal{C} \cdot [v]_\mathcal{C}$, which in turn implies that $\langle \cdot, \cdot \rangle^\mathcal{B} = \langle \cdot, \cdot \rangle^\mathcal{C}$. This completes the proof. □

Example 9.18. *Consider the vector space $\mathbb{R}^2$ (with vectors expressed as column vectors) and let*

$$\vec{u}_1 = \begin{pmatrix} 1 \\ 1 \end{pmatrix}, \quad \vec{u}_2 = \begin{pmatrix} 1 \\ 2 \end{pmatrix}.$$

Then $\mathcal{B} = \{\vec{u}_1,\ \vec{u}_2\}$ is a basis on $\mathbb{R}^2$. Let $\langle \cdot, \cdot \rangle^\mathcal{B}$ denote the inner product on $\mathbb{R}^2$ induced by $\mathcal{B}$ from Theorem 9.17. Let $\mathcal{S} = \{\vec{e}_1, \vec{e}_2\}$ denote the standard basis on $\mathbb{R}^2$. Let us compute the matrix representation of $\langle \cdot, \cdot \rangle^\mathcal{B}$ with respect to $\mathcal{S}$. By definition, the (i,j) element of $[\langle \cdot, \cdot \rangle^\mathcal{B}]_\mathcal{S}$ is

$$\langle \vec{e}_i, \vec{e}_j \rangle^\mathcal{B} := [\vec{e}_i]_\mathcal{B} \cdot [\vec{e}_j]_\mathcal{B}.$$

In order to compute the above inner products, we first need to compute the coordinate vectors of $\vec{e}_1$ and $\vec{e}_2$ with respect to $\mathcal{B}$. Doing a small calculation, we find

$$[\vec{e}_1]_\mathcal{B} = \begin{pmatrix} 2 \\ -1 \end{pmatrix}, \quad [\vec{e}_2]_\mathcal{B} = \begin{pmatrix} -1 \\ 1 \end{pmatrix}.$$

The matrix representation of $\langle \cdot, \cdot \rangle^\mathcal{B}$ with respect to $\mathcal{S}$ is then

$$[\langle \cdot, \cdot \rangle^\mathcal{B}]_\mathcal{S} = \begin{pmatrix} 5 & -3 \\ -3 & 2 \end{pmatrix}.$$

Since $[\vec{v}]_\mathcal{S} = \vec{v}$ for all $\vec{v} \in \mathbb{R}^2$, Proposition 9.16 implies

$$\langle \vec{v}, \vec{w} \rangle^\mathcal{B} = \vec{v}^T \begin{pmatrix} 5 & -3 \\ -3 & 2 \end{pmatrix} \vec{u} \tag{131}$$

for all $\vec{v}, \vec{u} \in \mathbb{R}^2$. In particular, observe that $\langle \vec{u}_i, \vec{u}_i \rangle^\mathcal{B} = 1$ for $i = 1, 2$ and $\langle \vec{u}_1, \vec{u}_2 \rangle^\mathcal{B} = 0$ by evaluating the right side of (131). Also, note that

$$\langle \vec{e}_1, \vec{e}_2 \rangle^\mathcal{B} = -21 \neq 0.$$

Hence, the vectors $\vec{e}_1$ and $\vec{e}_2$ (which are orthogonal from the point of view of Euclidean geometry) fail to be orthogonal with respect to the inner product $\langle \cdot, \cdot \rangle^\mathcal{B}$.

9.3. Complex Inner Product Spaces

Whether you like complex vector spaces or not, complex vector spaces are ultimately "nicer" than real vector spaces. Specifically, linear endomorphisms of a complex vector space have more structure than endomorphisms on a real vector space. For instance, any linear endomorphism on a complex vector space always has at least one eigenvalue. This is not true for the real case. We will obtain a better view of this structure in Chapter 13. Furthermore, by studying complex vector spaces and their endomorphisms, we also learn more about linear endomorphisms on a real vector space. Hence, if you are not a fan of complex vector spaces, think of complex vector spaces as a tool or intermediary which we can use to learn more about real vector spaces and their linear maps. (Historically, complex numbers were not initially held in high regard. They were originally developed as a mere tool for finding **real** roots of cubic equations of the form $x^3 + ax - b$ with $a, b \in \mathbb{R}$.)

In this section, we introduce the notion of *complex inner product spaces*, which is a complex vector space equipped with a type of inner product, one that is similar to the real case, but not exactly the same. From a physics perspective, complex inner product spaces are of fundamental importance to the mathematical framework of quantum mechanics. While you may have some unease (or disdain) for complex numbers and the like, it seems that nature is rather fond of these mathematical curiosities. With that said, we now give the formal definition of a complex inner product space.

For the remainder of this chapter, we denote the conjugate of a complex number $z = a + bi$ ($i = \sqrt{-1}$) by $\overline{z} = a - bi$. The magnitude or **modulus** of a complex number z is $|z| := \sqrt{z\overline{z}}$. The conjugate transpose of an $n \times m$ complex matrix A will be denoted by A^*. Hence, if $z \in \mathbb{C}$, then $\overline{z} = z^*$.

Definition 9.19. *Let V be a complex vector space. A **Hermitian inner product** on V is a map*

$$\langle \cdot, \cdot \rangle : V \times V \to \mathbb{C}, \qquad (u, v) \mapsto \langle u, v \rangle \in \mathbb{C}$$

which satisfies the following conditions:

(i) $\langle u, v \rangle = \overline{\langle v, u \rangle}$ *for all* $u, v \in V$ *(conjugate symmetry)*
(ii) $\langle u, v + w \rangle = \langle u, v \rangle + \langle u, w \rangle$ *for all* $u, v, w \in V$ *(linearity condition 1)*
(iii) $\langle u, cv \rangle = c\langle u, v \rangle$ *for all* $u, v \in V$, $c \in \mathbb{C}$ *(linearity condition 2)*
(iv) $\langle v, v \rangle \geq 0$ *and* $\langle v, v \rangle = 0$ *iff* $v = \mathbf{0}$ *(positive definiteness)*

*The pair $(V, \langle \cdot, \cdot \rangle)$ is called a **complex inner product space**.*

We now make a few comments about Definition 9.19. Note that $\langle \cdot, \cdot \rangle$ is linear in the second slot by conditions (ii) and (iii). However, it is **not** quite linear in its first slot.

Proposition 9.20. *Let $u, v, w \in V$ and $c \in \mathbb{C}$. Then*

(i) $\langle u+v, w\rangle = \langle u, w\rangle + \langle v, w\rangle$

(ii) $\langle cv, w\rangle = \overline{c}\langle v, w\rangle$

Proof. For (i), we have

$$\begin{aligned}\langle u+v, w\rangle &= \overline{\langle w, u+v\rangle}\\ &= \overline{\langle w, u\rangle + \langle w, v\rangle}\\ &= \overline{\langle w, u\rangle} + \overline{\langle w, v\rangle}\\ &= \langle u, w\rangle + \langle v, w\rangle\end{aligned}$$

and for (ii) we have

$$\begin{aligned}\langle cv, w\rangle &= \overline{\langle w, cv\rangle}\\ &= \overline{c\langle w, v\rangle}\\ &= \overline{c}\overline{\langle w, v\rangle}\\ &= \overline{c}\langle v, w\rangle.\end{aligned}$$

□

Statement (ii) in Proposition 9.20 shows that $\langle cv, w\rangle \neq c\langle v, w\rangle$ in general. This is the reason why a complex inner product fails to be linear in its first slot.

Exercise 9.21. $\mathbb{C}^n$ *has a natural Hermitian inner product (which is analogous to the natural inner product (i.e. the dot product) that exists on* $\mathbb{R}^n$*). Let the vectors in* $\mathbb{C}^n$ *be expressed as column vectors. This inner product is defined by*

$$\langle \vec{u}, \vec{v}\rangle := (\vec{u})^*\vec{v}, \quad \forall\ \vec{u}, \vec{v} \in V. \tag{132}$$

If $\vec{u} = (u_1, \ldots, u_n)^T$ *and* $\vec{v} = (v_1, \ldots, v_n)^T$*, then the above inner product is given by*

$$\langle \vec{u}, \vec{v}\rangle = \sum_{i=1}^{n} \overline{u}_i v_i. \tag{133}$$

We will call this the ***standard Hermitian inner product*** *on* $\mathbb{C}^n$*. Verify that* $\langle \cdot, \cdot\rangle$ *is a Hermitian inner product on* $\mathbb{C}^n$*.*

Exercise 9.22. *Let $C([0,1];\mathbb{C})$ be the set of continuous complex valued functions on the closed interval $[0,1]$. Explicitly, an element f of $C([0,1];\mathbb{C})$ is of the form*

$$f(x) = f_1(x) + if_2(x)$$

where f_1 and f_2 are continuous real valued functions on $[0,1]$. $C([0,1];\mathbb{C})$ is naturally a complex vector space with vector addition and scalar multiplication defined pointwise:

$$(f+g)(x) := f(x) + g(x), \quad (cf)(x) := cf(x)$$

for $f, g \in C([0,1];\mathbb{C})$ and $c \in \mathbb{C}$. We now define a Hermitian inner product

$$\langle \cdot, \cdot \rangle : C([0,1];\mathbb{C}) \times C([0,1];\mathbb{C}) \to \mathbb{C}$$

by

$$\begin{aligned} \langle f, g \rangle &:= \int_0^1 \overline{f(x)} g(x) dx \\ &= \int_0^1 (f_1(x)g_1(x) + f_2(x)g_2(x)) + i \int_0^1 (f_1(x)g_2(x) - f_2(x)g_1(x)) dx \end{aligned}$$

for $f = f_1 + if_2$ and $g = g_1 + ig_2$ in $C([0,1];\mathbb{C})$. Show that $\langle \cdot, \cdot \rangle$ is a Hermitian inner product on $C([0,1];\mathbb{C})$. (The proof of this is similar to the one given in Example 9.5.

Using condition (iv) of Definition 9.19, we can define the length or norm of a vector just like in the real case:

Definition 9.23. *Let $(V, \langle \cdot, \cdot \rangle)$ be a complex inner product space. The **norm** of a vector $v \in V$ is $\|v\| := \sqrt{\langle v, v \rangle}$.*

Note that for a complex inner product space $(V, \langle \cdot, \cdot \rangle)$, we can no longer define an angle between two arbitrary vectors $v, w \in V$ since $\langle v, w \rangle$ is a complex number in general. Consequently, Definition 9.9 for a real inner product space simply does not work for the complex case. At best, we can generalize the notion of orthogonality to complex inner product spaces (which proves to be quite fruitful):

Definition 9.24. *Let $(V, \langle \cdot, \cdot \rangle)$ be a complex inner product space. Two vectors $v, w \in V$ are **orthogonal** if $\langle v, w \rangle = 0$.*

Using Definition 9.24, many of the results and ideas of real inner product spaces generalize to complex inner product spaces (although a little extra care is required due to the conjugate symmetry of Hermitian inner products). We begin with the complex version of the Cauchy-Schwartz inequality:

Theorem 9.25 (Cauchy-Schwartz inequality (complex version))**.** *Let* $(V, \langle\cdot,\cdot\rangle)$ *be a complex inner product space. Then* $|\langle v, w\rangle| \leq \|v\|\,\|w\|$ *for all* $v, w \in V$*. Moreover, for* v, w *nonzero,* $|\langle v, w\rangle| = \|v\|\,\|w\|$ *if and only if* $v = \lambda w$ *for some* $\lambda \in \mathbb{C}$*.*

Proof. First, observe that if $v = \mathbf{0}$ or $w = \mathbf{0}$, we immediately have $|\langle v, w\rangle| = \|v\|\,\|w\| = 0$. Hence, the Cauchy-Schwartz inequality holds for this case. So let us assume that v and w are nonzero vectors. Let

$$c := \frac{\langle w, v\rangle}{\|w\|^2} \in \mathbb{C} \tag{134}$$

and expand the quantity $\|v - cw\|^2$:

$$\begin{aligned}
\|v - cw\|^2 &= \langle v - cw, v - cw\rangle \\
&= \langle v, v\rangle - c\langle v, w\rangle - \overline{c}\langle w, v\rangle + |c|^2\langle w, w\rangle \\
&= \|v\|^2 - \frac{\langle w, v\rangle}{\|w\|^2}\langle v, w\rangle - \frac{\overline{\langle w, v\rangle}}{\|w\|^2}\langle w, v\rangle + \frac{|\langle w, v\rangle|^2}{\|w\|^4}\|w\|^2 \\
&= \|v\|^2 - \frac{|\langle v, w\rangle|^2}{\|w\|^2} - \frac{|\langle w, v\rangle|^2}{\|w\|^2} + \frac{|\langle w, v\rangle|^2}{\|w\|^2} \\
&= \|v\|^2 - \frac{|\langle v, w\rangle|^2}{\|w\|^2}
\end{aligned} \tag{135}$$

Since $\|v - cw\|^2 \geq 0$, (135) implies

$$|\langle v, w\rangle|^2 \leq \|v\|^2\,\|w\|^2\,,$$

which in turn implies the Cauchy-Schwartz inequality.

For the last part, observe that if $v = \lambda w$, then

$$\begin{aligned}
|\langle v, w\rangle| &= |\langle \lambda w, w\rangle| \\
&= |\lambda||\langle w, w\rangle| \\
&= |\lambda|\langle w, w\rangle \\
&= |\lambda|\,\|w\|^2 \\
&= (|\lambda|\,\|w\|)\,\|w\| \\
&= \|\lambda w\|\,\|w\| \\
&= \|v\|\,\|w\|\,.
\end{aligned}$$

On the other hand, suppose that $|\langle v,w\rangle| = \|v\|\,\|w\|$ with v,w nonzero. So let us assume that $w \neq \mathbf{0}$. Let $c \in \mathbb{C}$ be defined via (134). Then by (135), we have

$$\|v - cw\|^2 = \|v\|^2 - \frac{|\langle v,w\rangle|^2}{\|w\|^2} = \|v\|^2 - \frac{\|v\|^2\,\|w\|^2}{\|w\|^2} = 0,$$

which in turn implies that $v - cw = \mathbf{0}$. Hence, $v = cw$. This completes the proof. □

Definition 9.26. *Let $(V, \langle\cdot,\cdot\rangle)$ be a complex inner product space and let $\{v_1,\ldots,v_k\}$ be a set of vectors in V. $\{v_1,\ldots,v_k\}$ is called an* ***orthogonal set*** *if $v_i \neq \mathbf{0}$ for $i = 1,\ldots,k$ and $\langle v_i, v_j\rangle = 0$ for all $1 \leq i < j \leq k$.*

Proposition 9.27. *Let $(V, \langle\cdot,\cdot\rangle)$ be a complex inner product space and let $\{v_1,\ldots,v_k\} \subset V$ be an orthogonal set. Then $\{v_1,\ldots,v_k\}$ is a linearly independent set.*

Proof. Like the case of real inner products, the proof is identical to the proof of Proposition 2.57 for the dot product. One simply replaces the dot product with the Hermitian inner product $\langle\cdot,\cdot\rangle$ and the argument works as before. □

The definition of orthogonal projection for Hermitian inner products is essentially the same as the real case. However, due to the fact that a Hermitian inner product is only conjugate symmetric, we have to be careful with the order of the vectors which appear in the inner product:

Definition 9.28. *Let $(V, \langle\cdot,\cdot\rangle)$ be a complex inner product space. Let $v,u \in V$ with u nonzero. The* ***orthogonal projection*** *of v onto u is the vector*

$$\mathit{proj}_u v := \frac{\langle u,v\rangle}{\|u\|^2}u.$$

The Gram-Schmidt process (which we state below for convenience) can also be applied to a complex inner product space to produce an orthogonal basis. However, the order of the vectors u and v appearing in the inner product for the formula of $\mathrm{proj}_u v$ is critical for the Gram-Schmidt process to work as before. Of course it makes no difference for a real inner product space, but it does for a complex one.

The Gram-Schmidt process for a complex inner product space

Let $(V, \langle \cdot, \cdot \rangle)$ be a complex inner product space. The Gram-Schmidt process generates an orthogonal basis from an existing basis on V. Once one obtains the orthogonal basis, one can normalize it to obtain an orthonormal basis. Let $\mathcal{B} = \{v_1, v_2, \ldots, v_n\}$ be **any** basis on V. We obtain an orthogonal basis

$$\mathcal{B}' := \{b_1, b_2, \ldots, b_n\}$$

as follows:

1. Define $b_1 := v_1$
2. For $k = 2, \ldots, n$, define

$$b_k := v_k - \sum_{i=1}^{k-1} \operatorname{proj}_{b_i} v_k$$

Setting $u_i := b_i / \|b_i\|$, the set $\{u_1, u_2, \ldots, u_n\}$ is then an orthonormal basis.

The following result simply verifies that the Gram-Schmidt process still works for a complex inner product space provided that one follows Definition 9.28 **exactly** for the definition of orthogonal projection.

Theorem 9.29. *Any complex inner product space admits an orthogonal basis.*

Proof. Let $(V, \langle \cdot, \cdot \rangle)$ be a complex inner product space and let $n = \dim V$. Let $\mathcal{B} = \{v_1, \ldots, v_n\}$ be any basis on V and let $\mathcal{B}' = \{b_1, \ldots, b_n\}$ denote the set of vectors resulting from applying the Gram-Schmidt process to $\mathcal{B}$. By Proposition 9.27, it suffices to show that $\mathcal{B}'$ is an orthogonal set. Let $\mathcal{B}'_k =: \{b_1, \ldots, b_k\}$ for $k \le n$. We now show that $\mathcal{B}'_k$ is an orthogonal set for $k = 1, 2, \ldots, n$ by induction on k. First, observe that $\mathcal{B}'_1$ is trivially an orthogonal set. Now suppose that $\mathcal{B}'_k$ is an orthogonal set. To show that $\mathcal{B}'_{k+1}$ is an orthogonal set, we need to show that $\langle b_i, b_{k+1} \rangle = 0$ for $i = 1, 2, \ldots, k$ and $b_{k+1} \neq \mathbf{0}$. From the definition of b_{k+1}, we have

$$\begin{aligned}
\langle b_i, b_{k+1} \rangle &= \langle b_i, v_{k+1} \rangle - \sum_{j=1}^{k} \langle b_i, \operatorname{proj}_{b_j} v_{k+1} \rangle \\
&= \langle b_i, v_{k+1} \rangle - \sum_{j=1}^{k} \frac{\langle b_j, v_{k+1} \rangle}{\|b_j\|^2} \langle b_i, b_j \rangle \\
&= \langle b_i, v_{k+1} \rangle - \frac{\langle b_i, v_{k+1} \rangle}{\|b_i\|^2} \langle b_i, b_i \rangle \\
&= 0.
\end{aligned}$$

Note that if we were careless with the definition of $\operatorname{proj}_{b_i} v_{k+1}$ and used the inner product $\langle v_{k+1}, b_i \rangle$ instead of $\langle b_i, v_{k+1} \rangle$ in its definition, we would not obtain zero for $\langle b_i, b_{k+1}\rangle$. Rather, we would obtain

$$\langle b_i, v_{k+1}\rangle - \langle v_{k+1}, b_i\rangle = \langle b_i, v_{k+1}\rangle - \overline{\langle b_i, v_{k+1}\rangle} = 2\text{Im}\{\langle b_i, v_{k+1}\rangle\}$$

where $\text{Im}(z)$ denotes the imaginary part of a complex number z.

Lastly, to see that $b_{k+1} \neq \mathbf{0}$, observe that

$$\{b_1, \ldots, b_k\} \subset \text{span}\{v_1, \ldots, v_k\}.$$

Consequently, the condition $b_{k+1} = \mathbf{0}$ implies that $v_{k+1} \in \text{span}\{v_1, \ldots, v_k\}$; this contradicts the fact that $\{v_1, \ldots, v_n\}$ is a basis on V. From this, we conclude that $b_{k+1} \neq \mathbf{0}$. This along with the above calculation shows that $\mathcal{B}'_{k+1}$ is an orthogonal set. In particular, $\mathcal{B}'_n = \mathcal{B}'$ is an orthogonal set. This completes the proof. □

For the sake of completeness, we conclude this section with the following definition and result:

Definition 9.30. *Let $(V, \langle\cdot,\cdot\rangle)$ be a complex inner product space and let W be a subspace of V. The **orthogonal complement** of W in V is the subspace*

$$W^{\perp} := \{w \in W \mid \langle w, v\rangle = 0\ \forall\ v \in V\}.$$

Theorem 9.31. *Let $(V, \langle\cdot,\cdot\rangle)$ be a complex inner product space and let W be a subspace of V. Then*

$$V = W \oplus W^{\perp}.$$

Proof. The proof of Theorem 9.31 is identical to the dot product version given in Theorem 2.80. □

9.4. More on Complex Inner Product Spaces

As the reader might have guessed, the current section is simply the complex version of Section 9.2. The results and ideas of this section are naturally quite similar to those of Section 9.2, but not exactly the same. These slight differences are (again) due to the fact that a Hermitian inner product is not really symmetric, but only conjugate symmetric. The reader with a reasonable "math sense" will be able to guess how the results of Section 9.2 change for the complex case. Naturally, we begin with the following definition:

Definition 9.32. *Let $(V, \langle\cdot,\cdot\rangle)$ be a complex inner product space and let*

$$\mathcal{B} = \{v_1, \ldots, v_n\}$$

be any basis on V. The ***matrix representation*** *of $\langle\cdot,\cdot\rangle$ with respect to the basis $\mathcal{B}$ is the $n \times n$ (complex) matrix whose (i, j) element is $\langle v_i, v_j\rangle$. The matrix representation of $\langle\cdot,\cdot\rangle$ with respect to $\mathcal{B}$ is denoted by $[\langle\cdot,\cdot\rangle]_{\mathcal{B}}$.*

As in the real case, the matrix representation of a Hermitian inner product encodes all the information. Before stating the complex version of Proposition 9.16, we remind the reader that a complex matrix A is said to be **Hermitian** if $A^* = A$. A Hermitian matrix can be viewed as the complex version of a real symmetric matrix.

Proposition 9.33. *Let $(V, \langle\cdot,\cdot\rangle)$ be a complex inner product space and let $\mathcal{B}$ be any basis on V.*

(i) $[\langle\cdot,\cdot\rangle]_{\mathcal{B}}$ is a Hermitian matrix.
(ii) $\langle v, w\rangle = [v]^*_{\mathcal{B}}[\langle\cdot,\cdot\rangle]_{\mathcal{B}}[w]_{\mathcal{B}}$ for all $v, w \in V$.
(iii) If $\mathcal{B}$ is an orthonormal basis, then $\langle v, w\rangle = [v]^*_{\mathcal{B}}[w]_{\mathcal{B}}$ for all $v, w \in V$.

Proof. Let $\mathcal{B} = \{v_1, \ldots, v_n\}$ be any basis on V.

(i): The (i, j) and (j, i) entries of the matrix $[\langle\cdot,\cdot\rangle]_{\mathcal{B}}$ are $\langle v_i, v_j\rangle$ and $\langle v_j, v_i\rangle$ respectively. Since $\langle v_i, v_j\rangle = \overline{\langle v_j, v_i\rangle}$, it follows that $[\langle\cdot,\cdot\rangle]_{\mathcal{B}}$ is Hermitian.

(ii): Let $v, w \in V$ and write

$$[v]_{\mathcal{B}} = (\alpha_1, \ldots, \alpha_n)^T, \qquad [w]_{\mathcal{B}} = (\beta_1, \ldots, \beta_n)^T \in \mathbb{C}^n$$

for their coordinate representations with respect to $\mathcal{B}$. By definition, this means

$$v = \sum_{i=1}^{n} \alpha_i v_i, \qquad w = \sum_{j=1}^{n} \beta_j v_j. \tag{136}$$

Using (136), we expand $\langle v, w\rangle$ using conditions (i)-(iii) of Definition 9.19:

$$\begin{aligned}\langle v, w\rangle &= \langle \sum_{i=1}^{n} \alpha_i v_i, \sum_{j=1}^{n} \beta_j v_j\rangle \\ &= \sum_{i=1}^{n}\sum_{j=1}^{n} \langle \alpha_i v_i, \beta_j v_j\rangle \\ &= \sum_{i=1}^{n}\sum_{j=1}^{n} \overline{\alpha_i}\beta_j \langle v_i, v_j\rangle \\ &= \sum_{i=1}^{n}\sum_{j=1}^{n} \overline{\alpha_i}\langle v_i, v_j\rangle \beta_j \\ &= [v]^*_{\mathcal{B}}[\langle\cdot,\cdot\rangle]_{\mathcal{B}}[w]_{\mathcal{B}}.\end{aligned}$$

(iii): Suppose now that $\mathcal{B} = \{v_1, \dots, v_n\}$ is an orthonormal basis. Then

$$\langle v_i, v_j \rangle = \begin{cases} 1 & \text{if } i = j \\ 0 & \text{if } i \neq j \end{cases}$$

Hence, $[\langle \cdot, \cdot \rangle]_{\mathcal{B}} = I_n$ (the $n \times n$ identity matrix). Using (ii), we have

$$\begin{aligned} \langle v, w \rangle &= [v]_{\mathcal{B}}^* [\langle \cdot, \cdot \rangle]_{\mathcal{B}} [w]_{\mathcal{B}} \\ &= [v]_{\mathcal{B}}^* I_n [w]_{\mathcal{B}} \\ &= [v]_{\mathcal{B}}^* [w]_{\mathcal{B}}. \end{aligned}$$

□

Statement (i) of Proposition 9.33 is the reason why an inner product on a complex vector space is called *Hermitian*.

We conclude this section with the complex version of Theorem 9.17. This result shows that a Hermitian inner product on a complex vector is equivalent to a choice of orthonormal basis. Before stating the result, we remind the reader that an invertible complex matrix A is called **unitary** if $A^{-1} = A^*$. Hence, a unitary matrix can be viewed as the complex version of an orthogonal matrix.

Theorem 9.34. *Let V be a complex vector space. Let $\mathcal{B}$ be any basis on V and define*

$$\langle \cdot, \cdot \rangle^{\mathcal{B}} : V \times V \to \mathbb{C}$$

by $\langle u, v \rangle^{\mathcal{B}} := [u]_{\mathcal{B}}^* [v]_{\mathcal{B}}$ for all $u, v \in V$. Then $\langle \cdot, \cdot \rangle^{\mathcal{B}}$ is a Hermitian inner product on V and $\mathcal{B}$ is an orthonormal basis with respect to this inner product. Moreover, ***every*** *inner product on V is of this form. In addition, if $\mathcal{C}$ is another basis on V, then $\langle \cdot, \cdot \rangle^{\mathcal{B}} = \langle \cdot, \cdot \rangle^{\mathcal{C}}$ if and only if the transition matrix $P_{\mathcal{CB}}$ is a unitary matrix, that is, $P_{\mathcal{CB}}^{-1} = P_{\mathcal{CB}}^*$.*

Proof. We now verify that $\langle \cdot, \cdot \rangle^{\mathcal{B}}$ satisfies all the conditions given in Definition 9.19. For condition (i), we have

$$\langle u, v \rangle^{\mathcal{B}} = [u]_{\mathcal{B}}^* [v]_{\mathcal{B}} = \overline{([v]_{\mathcal{B}}^* [u]_{\mathcal{B}})} = \overline{\langle v, u \rangle^{\mathcal{B}}}$$

for all $u, v \in V$. Conditions (ii) and (iii) are a consequence of Proposition 6.7:

$$\begin{aligned} \langle u, v + w \rangle^{\mathcal{B}} &= [u]_{\mathcal{B}}^* \, [v + w]_{\mathcal{B}} \\ &= [u]_{\mathcal{B}}^* \left([v]_{\mathcal{B}} + [w]_{\mathcal{B}} \right) \\ &= [u]_{\mathcal{B}}^* [v]_{\mathcal{B}} + [u]_{\mathcal{B}}^* [w]_{\mathcal{B}} \\ &= \langle u, v \rangle^{\mathcal{B}} + \langle u, w \rangle^{\mathcal{B}} \end{aligned}$$

and

$$\begin{aligned}\langle u, cv\rangle^{\mathcal{B}} &= [u]_{\mathcal{B}}^*[cv]_{\mathcal{B}}\\ &= [u]_{\mathcal{B}}^*\left(c[v]_{\mathcal{B}}\right)\\ &= c([u]_{\mathcal{B}}^*[v]_{\mathcal{B}})\\ &= c\langle u, v\rangle^{\mathcal{B}}\end{aligned}$$

for all $u, v, w \in V$ and $c \in \mathbb{C}$. For condition (iv), let $u \in V$ and write

$$[u]_{\mathcal{B}} = (\alpha_1, \alpha_2, \ldots, \alpha_n)^T \in \mathbb{C}^n,$$

where $n := \dim V$. Then

$$\begin{aligned}\langle u, u\rangle^{\mathcal{B}} &= [u]_{\mathcal{B}}^*[u]_{\mathcal{B}}\\ &= \sum_{i=1}^{n} \overline{\alpha_i}\alpha_i\\ &= \sum_{i=1}^{n} |\alpha_i|^2.\end{aligned}$$

From this, we see that $\langle u, u\rangle \geq 0$. We also see that $\langle u, u\rangle = 0$ if and only if $[u]_{\mathcal{B}} = \vec{0}$ and the latter is equivalent to $u = \mathbf{0}$. Hence, $\langle\cdot,\cdot\rangle^{\mathcal{B}}$ is positive definite. We have thus proven that $\langle\cdot,\cdot\rangle^{\mathcal{B}}$ is a Hermitian inner product.

Now let $\langle\cdot,\cdot\rangle$ be any Hermitian inner product on V. Using the Gram-Schmidt process for complex inner product spaces (see Section 9.4), we can always construct an orthonormal basis on the complex inner product space $(V, \langle\cdot,\cdot\rangle)$. Let $\mathcal{D}$ be any orthonormal basis for $(V, \langle\cdot,\cdot\rangle)$. By statement (iii) of Proposition 9.33, we have

$$\langle u, v\rangle = [u]_{\mathcal{D}}^*[v]_{\mathcal{D}}$$

for all $u, v \in V$. However, the right hand side is just $\langle u, v\rangle^{\mathcal{D}}$. Since $u, v \in V$ are arbitrary, we conclude that $\langle\cdot,\cdot\rangle = \langle\cdot,\cdot\rangle^{\mathcal{D}}$.

For the last part of Theorem 9.34, we need to determine when two bases $\mathcal{B}$ and $\mathcal{C}$ induce the same Hermitian inner product on V. More precisely, we need to determine the necessary and sufficient conditions for $\langle\cdot,\cdot\rangle^{\mathcal{B}} = \langle\cdot,\cdot\rangle^{\mathcal{C}}$.

Suppose first that $\langle\cdot,\cdot\rangle^{\mathcal{B}} = \langle\cdot,\cdot\rangle^{\mathcal{C}}$ Let $u, v \in V$. Then

$$[u]_{\mathcal{B}}^*[v]_{\mathcal{B}} = [u]_{\mathcal{C}}^*[v]_{\mathcal{C}}. \tag{137}$$

Using Theorem 6.8 to express $[u]_{\mathcal{C}}$ and $[v]_{\mathcal{C}}$ in terms of $[u]_{\mathcal{B}}$ and $[v]_{\mathcal{B}}$ respectively, equation (137) can be rewritten as

$$\begin{aligned}[u]_{\mathcal{B}}^*[v]_{\mathcal{B}} &= [u]_{\mathcal{C}}^*[v]_{\mathcal{C}}\\ &= (P_{\mathcal{CB}}[u]_{\mathcal{B}})^*(P_{\mathcal{CB}}[v]_{\mathcal{B}})\\ &= [u]_{\mathcal{B}}^*(P_{\mathcal{CB}}^*P_{\mathcal{CB}})[v]_{\mathcal{B}}.\end{aligned} \tag{138}$$

Since the above relation holds for all $u, v \in V$, it follows that the coordinate vectors $[u]_{\mathcal{B}}$ and $[v]_{\mathcal{B}}$ can assume any element of $\mathbb{C}^n$ (where $n := \dim V$). From this, it follows that $P^*_{\mathcal{CB}} P_{\mathcal{CB}} = I_n$ (the $n \times n$ identity matrix). Hence, $P_{\mathcal{CB}}$ is unitary.

On the other hand, if $P_{\mathcal{CB}}$ is unitary, then $P^*_{\mathcal{CB}} P_{\mathcal{CB}} = I_n$ and equation (138) implies that $[u]^*_{\mathcal{B}}[v]_{\mathcal{B}} = [u]^*_{\mathcal{C}}[v]_{\mathcal{C}}$, which in turn implies that $\langle \cdot, \cdot \rangle^{\mathcal{B}} = \langle \cdot, \cdot \rangle^{\mathcal{C}}$. This completes the proof. ☐

Example 9.35. *Consider the vector space $\mathbb{C}^2$ (with vectors expressed as column vectors) and let*

$$\vec{u}_1 = \begin{pmatrix} i \\ 1 \end{pmatrix}, \qquad \vec{u}_2 = \begin{pmatrix} 2 \\ i \end{pmatrix}.$$

Then $\mathcal{B} = \{\vec{u}_1,\ \vec{u}_2\}$ is a basis on $\mathbb{C}^2$. Let $\langle \cdot, \cdot \rangle^{\mathcal{B}}$ denote the Hermitian inner product on $\mathbb{C}^2$ induced by $\mathcal{B}$ from Theorem 9.34. Let $\mathcal{S} = \{\vec{e}_1, \vec{e}_2\}$ denote the standard basis on $\mathbb{C}^2$. Let us compute the matrix representation of $\langle \cdot, \cdot \rangle^{\mathcal{B}}$ with respect to $\mathcal{S}$.
By definition, the (i, j) element of $[\langle \cdot, \cdot \rangle^{\mathcal{B}}]_{\mathcal{S}}$ is

$$\langle \vec{e}_i, \vec{e}_j \rangle^{\mathcal{B}} := [\vec{e}_i]^*_{\mathcal{B}} [\vec{e}_j]_{\mathcal{B}}.$$

In order to compute the above inner products, we first compute the coordinate vectors of $\vec{e}_1$ and $\vec{e}_2$ with respect to $\mathcal{B}$:

$$[\vec{e}_1]_{\mathcal{B}} = \begin{pmatrix} -i/3 \\ 1/3 \end{pmatrix}, \quad [\vec{e}_2]_{\mathcal{B}} = \begin{pmatrix} 2/3 \\ -i/3 \end{pmatrix}.$$

The matrix representation of $\langle \cdot, \cdot \rangle^{\mathcal{B}}$ with respect to $\mathcal{S}$ is then

$$[\langle \cdot, \cdot \rangle^{\mathcal{B}}]_{\mathcal{S}} = \begin{pmatrix} 2/9 & i/9 \\ -i/9 & 5/9 \end{pmatrix}.$$

Since $[\vec{v}]_{\mathcal{S}} = \vec{v}$ for all $\vec{v} \in \mathbb{C}^2$, Proposition 9.33 implies

$$\langle \vec{v}, \vec{w} \rangle^{\mathcal{B}} = \vec{v}^{\,*} \begin{pmatrix} 2/9 & i/9 \\ -i/9 & 5/9 \end{pmatrix} \vec{u} \tag{139}$$

for all $\vec{v}, \vec{u} \in \mathbb{C}^2$. In particular, observe that $\langle \vec{u}_i, \vec{u}_i \rangle^{\mathcal{B}} = 1$ for $i = 1, 2$ and $\langle \vec{u}_1, \vec{u}_2 \rangle^{\mathcal{B}} = 0$ by evaluating the right side of (139).

9.5. Inner Products and the Dual Space

For a finite dimensional vector space V, Theorem 8.6 shows that V and the double dual $(V^*)^*$ are essentially the same vector space. This view is a consequence of a canonical isomorphism from V to $(V^*)^*$ that allows one to naturally identify the elements of V with those of $(V^*)^*$. Naturally, one wonders if a similar relationship exists between V and V^*. The short answer to this question is no. However, if one is dealing with an inner product space, then the inner product itself can be used as a “bridge” to identify the elements of V with those of V^*. Since real inner products and Hermitian inner products are not quite the same (one is symmetric and the other is only conjugate symmetric), we will study the real and complex cases separately. We begin with the real case:

Theorem 9.36. *Let $(V, \langle\cdot,\cdot\rangle)$ be a real inner product space. Let $\psi : V \to V^*$ be the map which sends $u \in V$ to the 1-form $\psi_u \in V^*$ defined by $\psi_u := \langle\cdot, u\rangle$. In other words, $\psi_u(v) := \langle v, u\rangle$ for all $v \in V$. Then ψ is a vector space isomorphism. In particular, for any $f \in V^*$, there exists a $u \in V$ such that $f(v) = \langle v, u\rangle$ for all $v \in V$.*

Proof. Let $u \in V$. First, we need to verify that $\psi_u \in V^*$. In other words, we need to show that $\psi_u : V \to \mathbb{R}$ is a linear map. This can be seen by the following calculation:

$$\begin{aligned}\psi_u(v+w) &= \langle v+w, u\rangle \\ &= \langle v, u\rangle + \langle w, u\rangle \\ &= \psi_u(v) + \psi_u(w)\end{aligned}$$

and

$$\begin{aligned}\psi_u(rv) &= \langle rv, u\rangle \\ &= r\langle v, u\rangle \\ &= r\psi_u(v)\end{aligned}$$

for all $v, w \in V$ and $r \in \mathbb{R}$.

Next, we need to show that $\psi : V \to V^*$ itself is a linear map. Since $\psi(u) := \psi_u$, we need to show that

$$\psi_{u_1+u_2} = \psi_{u_1} + \psi_{u_2}, \qquad \psi_{ru_1} = r\psi_{u_1} \tag{140}$$

for all $u_1, u_2 \in U$ and $r \in \mathbb{R}$. To do this, let $v \in V$. Then

$$\begin{aligned}\psi_{u_1+u_2}(v) &= \langle v, u_1+u_2\rangle \\ &= \langle v, u_1\rangle + \langle v, u_2\rangle \\ &= \psi_{u_1}(v) + \psi_{u_2}(v) \\ &= (\psi_{u_1} + \psi_{u_2})(v) \end{aligned} \tag{141}$$

and

$$\begin{aligned}\psi_{ru_1}(v) &= \langle v, ru_1\rangle \\ &= r\langle v, u_1\rangle \\ &= r(\psi_{u_1}(v)) \\ &= (r\psi_{u_1})(v) \end{aligned} \tag{142}$$

(141) and (142) then imply (140).

Lastly, we need to show that ψ is a vector space isomorphism. In other words, we need to show that $\ker\psi = \{\mathbf{0}\}$ and $\text{im}\ \psi = V^*$. Let $u \in \ker\psi$. Then $\psi_u(v) := \langle v, u\rangle = 0$ for all $v \in V$. Since inner products are positive definite (by definition), it follows that $v = \mathbf{0}$. This proves that $\ker\psi = \{\mathbf{0}\}$. To show that $\text{im}\ \psi = V^*$, first observe from the Rank-Nullity Theorem (Theorem 5.60) that

$$\dim V = \dim\ker\psi + \dim\text{im}\ \psi = \dim\text{im}\ \psi.$$

Since $\dim V^* = \dim V$ (by Theorem 8.2) and $\text{im}\ \psi$ is a subspace of V^*, it follows readily that $\text{im}\ \psi = V^*$. This completes the proof. $\square$

We now turn to the complex case. For the complex case, we actually need a slight variation of the dual space. This variation is based on the notion of **antilinear maps**:

Definition 9.37. *Let V and W be complex vector spaces. A map $\varphi : V \to W$ is called* ***antilinear*** *if*

$$\varphi(v + w) = \varphi(v) + \varphi(w), \qquad \varphi(cv) = \bar{c}\varphi(v)$$

for all $v, w \in V$ and $c \in \mathbb{C}$, where $\bar{c}$ is the conjugate of c. An antilinear map is called an ***anitlinear isomorphism*** *if it is one-to-one and onto.*

Remark 9.38. *The properties of antilinear maps are similar to those of linear maps. However, for our present needs, we will not need this information (although we have provided several exercises at the end where you can work out some of these properties for yourself).*

We can now define our modified dual space:

Definition 9.39. *Let V be a complex vector space. The* ***antidual space*** *is the complex vector space $\overline{V^*}$ which consists of all antilinear maps from V to $\mathbb{C}$ with the usual pointwise vector addition and scalar multiplication:*

$$(f + g)(v) := f(v) + g(v), \quad \forall\ v \in V$$

$$(cf)(v) := cf(v), \quad \forall\ v \in V$$

for all $f, g \in \overline{V^*}$ and $c \in \mathbb{C}$. The element of $\overline{V^*}$ are called ***anti-covectors*** *or* ***anti-1-forms****.*

The relationship between V^* and $\overline{V^*}$ is given by the following result:

Theorem 9.40. *Let V be a complex vector space. Let $\rho : V^* \to \overline{V^*}$ be the map which sends $f \in V^*$ to its conjugate $\overline{f}$, where $\overline{f}(v) := \overline{f(v)}$ for all $v \in V$. Then ρ is an antilinear isomorphism. In particular,*

$$\dim \overline{V^*} = \dim V^* = \dim V.$$

Proof. We begin by verifying that ρ maps V^* into $\overline{V^*}$. To do this, let $f \in V^*$. Let us verify that $\rho(f) := \overline{f}$ is an antilinear map from V to $\mathbb{C}$ (i.e. an anti-covector). For $v, v' \in V$, we have

$$\begin{aligned} \overline{f}(v+v') &:= \overline{f(v+v')} \\ &= \overline{f(v)+f(v')} \\ &= \overline{f(v)} + \overline{f(v')} \\ &= \overline{f}(v) + \overline{f}(v'), \end{aligned}$$

where the last equality is simply the definition of $\overline{f}$. Also, for $c \in \mathbb{C}$, we have

$$\begin{aligned} \overline{f}(cv) &= \overline{f(cv)} \\ &= \overline{cf(v)} \\ &= \overline{c}\overline{f(v)} \\ &= \overline{c}\overline{f}(v) \end{aligned}$$

where the second equality follows from the fact that f is a linear map. This proves that $\overline{f} \in \overline{V^*}$.

Next, we show that ρ is an antilinear map. To do this, let $f, f' \in V^*$ and $c \in \mathbb{C}$. Also, let $v \in V$. Then

$$\begin{aligned} \rho(f+f')(v) &= \overline{f+f'}(v) \\ &= \overline{(f+f')(v)} \\ &= \overline{f(v)+f'(v)} \\ &= \overline{f}(v) + \overline{f'}(v) \\ &= \rho(f)(v) + \rho(f')(v) \\ &= [\rho(f)+\rho(f')](v) \end{aligned} \tag{143}$$

Also,

$$\begin{aligned} \rho(cf)(v) &= \overline{cf(v)} \\ &= \overline{c}\overline{f(v)} \\ &= \overline{c}\overline{f}(v) \\ &= \overline{c}\rho(f)(v) \\ &= [\overline{c}\rho(f)](v). \end{aligned} \tag{144}$$

(143) and (144) show that ρ is antilinear.

Lastly, we need to show that ρ is an (antilinear) isomorphism. For this, let $f \in \ker \rho$ and suppose that $\rho(f) := \overline{f} = \mathbf{0}$. In other words, $\overline{f}(v) := \overline{f(v)} = 0$ for all $v \in V$. Clearly, this implies that $f(v) = 0$ for all $v \in V$. In other words, $f = \mathbf{0}$. This proves that $\ker \rho = \{\mathbf{0}\}$. Hence, ρ is one-to-one.

To show that ρ is onto, let $g \in \overline{V^*}$. Define $f : V \to \mathbb{C}$ by $f(v) := \overline{g(v)}$ for all $v \in V$. Let $v, v' \in V$ and $c \in \mathbb{C}$. Since $g(v+v') = g(v)+g(v')$, the above calculation implies that

$$f(v + v') = f(v) + f(v').$$

On the other hand, since $g(cv) = \bar{c}g(v)$, the above calculation implies that $f(cv) = cf(v)$. This shows that $f \in V^*$. Since

$$\overline{f}(v) = \overline{f(v)} = \overline{\overline{g(v)}} = g(v)$$

for all $v \in V$, we see that $\rho(f) = g$. This proves that ρ is onto. Hence, ρ is an antilinear isomorphism. This in turn implies

$$\dim \overline{V^*} = \dim V^* = \dim V$$

where the last equality follows from Theorem 8.2. □

Remark 9.41. *Theorem 9.40 justifies the notation $\overline{V^*}$ for the antidual space. Every element of $\overline{V^*}$ is obtained by conjugating an element of V^*.*

Here is the complex version of Theorem 9.36:

Theorem 9.42. *Let $(V, \langle \cdot, \cdot \rangle)$ be a complex inner product space. Let*

$$\psi : V \to \overline{V^*}$$

be the map which sends $u \in V$ to the anti-1-form $\psi_u \in \overline{V^*}$ defined by $\psi_u := \langle \cdot, u \rangle$. In other words, $\psi_u(v) := \langle v, u \rangle$ for all $v \in V$. Then ψ is a vector space isomorphism. In particular, for any $f \in \overline{V^*}$, there exists a unique $u \in V$ such that $f(v) = \langle v, u \rangle$ for all $v \in V$.

Proof. The proof is quite similar to the proof of Theorem 9.36. However, there are some differences since the inner product here is conjugate symmetric. This is the reason why the image of ψ is in $\overline{V^*}$ as opposed to V^*.

Let $u \in V$. First, we verify that ψ_u is indeed an anti-1-form. To do this, let $v, v' \in V$ and $c \in \mathbb{C}$. Then

$$\begin{aligned} \psi_u(v + v') &= \langle v + v', u \rangle \\ &= \langle v, u \rangle + \langle v', u \rangle \\ &= \psi_u(v) + \psi_u(v') \end{aligned}$$

and

$$\begin{aligned}\psi_u(cv) &= \langle cv, u\rangle \\ &= \bar{c}\langle v, u\rangle \\ &= \bar{c}\psi_u(v),\end{aligned}$$

where the second equality follows from Proposition 9.20. This proves that $\psi_u \in \overline{V^*}$.

Next, we need to show that $\psi : V \to \overline{V^*}$ itself is a linear map. Since $\psi(u) := \psi_u$, we need to show that

$$\psi_{u_1+u_2} = \psi_{u_1} + \psi_{u_2}, \qquad \psi_{cu_1} = c\psi_{u_1} \tag{145}$$

for all $u_1, u_2 \in U$ and $c \in \mathbb{C}$. To do this, let $v \in V$. Then

$$\begin{aligned}\psi_{u_1+u_2}(v) &= \langle v, u_1 + u_2\rangle \\ &= \langle v, u_1\rangle + \langle v, u_2\rangle \\ &= \psi_{u_1}(v) + \psi_{u_2}(v) \\ &= (\psi_{u_1} + \psi_{u_2})(v)\end{aligned} \tag{146}$$

and

$$\begin{aligned}\psi_{cu_1}(v) &= \langle v, cu_1\rangle \\ &= c\langle v, u_1\rangle \\ &= c(\psi_{u_1}(v)) \\ &= (c\psi_{u_1})(v),\end{aligned} \tag{147}$$

where we recall that there is no conjugation when the scalar is pulled from the second argument of a Hermitian inner product. (146) and (147) then imply (145).

Lastly, we need to show that ψ is a vector space isomorphism. In other words, we need to show that $\ker\psi = \{\mathbf{0}\}$ and $\operatorname{im}\psi = \overline{V^*}$. Let $u \in \ker\psi$. Then $\psi_u(v) := \langle v, u\rangle = 0$ for all $v \in V$. Since all inner products (including Hermitian ones) are positive definite (by definition), it follows that $v = \mathbf{0}$. This proves that $\ker\psi = \{\mathbf{0}\}$. To show that $\operatorname{im}\psi = \overline{V^*}$, first observe from the Rank-Nullity Theorem (Theorem 5.60) that

$$\dim V = \dim\ker\psi + \dim\operatorname{im}\psi = \dim\operatorname{im}\psi.$$

Since $\dim\overline{V^*} = \dim V$ (by Theorem 9.40) and $\operatorname{im}\psi$ is a subspace of $\overline{V^*}$, it follows readily that $\operatorname{im}\psi = \overline{V^*}$. This completes the proof.

□

9.6. Adjoint Linear Maps

In this section, the term **inner product space** will refer to either a complex inner product space or a real inner product space. When we want to emphasize one over the other, we will do so explicitly. In this section, we introduce the idea of the adjoint map, which requires two ingredients for its construction: an existing linear map $\varphi : V \to V$ and an inner product on V.

Definition 9.43. *Let $(V, \langle \cdot, \cdot \rangle)$ be an inner product space (complex or real) and let $\varphi : V \to V$ be a linear map. The* ***adjoint*** *of φ is a linear map $\varphi^a : V \to V$ satisfying the condition $\langle \varphi(v), w \rangle = \langle v, \varphi^a(w) \rangle$ for all $v, w \in V$.*

Our goal now is to show that the adjoint map always **exists** and is **unique**. The following lemma is a key step towards this goal.

Lemma 9.44. *Let $(V, \langle \cdot, \cdot \rangle)$ be an inner product space and let $\varphi : V \to V$ be a linear map. Suppose $\widehat{\varphi} : V \to V$ is a map (not necessarily linear) which satisfies*

$$\langle \varphi(v), w \rangle = \langle v, \widehat{\varphi}(w) \rangle. \tag{148}$$

Then $\widehat{\varphi}$ is necessarily unique and linear. In other words, $\widehat{\varphi}$ is the adjoint map φ^a of φ with respect to the inner product $\langle \cdot, \cdot \rangle$.

Proof. Let $\mathbb{F} = \mathbb{C}$ or $\mathbb{R}$ and let $(V, \langle \cdot, \cdot \rangle)$ be an inner product space over $\mathbb{F}$.

Suppose that $\widehat{\varphi} : V \to V$ is a map (not necessarily linear) which satisfies (148). We first show that the map $\widehat{\varphi}$ is unique. So let us suppose that $\widetilde{\varphi} : V \to V$ is another map which satisfies

$$\langle \varphi(v), w \rangle = \langle v, \widetilde{\varphi}(w) \rangle$$

for all $v, w \in V$. This implies that

$$\langle v, \widehat{\varphi}(w) - \widetilde{\varphi}(w) \rangle = 0 \tag{149}$$

for all $v, w \in V$. Setting $v = \widehat{\varphi}(w) - \widetilde{\varphi}(w)$ gives

$$\langle \widehat{\varphi}(w) - \widetilde{\varphi}(w), \widehat{\varphi}(w) - \widetilde{\varphi}(w) \rangle = 0 \tag{150}$$

for all $w \in V$. The positive definiteness of the inner product then implies

$$\widehat{\varphi}(w) - \widetilde{\varphi}(w) = \mathbf{0} \tag{151}$$

for all $w \in V$. Hence, $\widehat{\varphi} = \widetilde{\varphi}$ which proves the uniqueness claim.

Lastly, we show that $\widehat{\varphi}$ is linear. Let $w_1, w_2 \in V$. Since $\widehat{\varphi}$ satisfies (148), we have

$$\begin{aligned} \langle v, \widehat{\varphi}(w_1 + w_2) \rangle &= \langle \varphi(v), w_1 + w_2 \rangle \\ &= \langle \varphi(v), w_1 \rangle + \langle \varphi(v), w_2 \rangle \\ &= \langle v, \widehat{\varphi}(w_1) \rangle + \langle v, \widehat{\varphi}(w_2) \rangle \\ &= \langle v, \widehat{\varphi}(w_1) + \widehat{\varphi}(w_2) \rangle \end{aligned} \tag{152}$$

for all $v \in V$. (152) thus implies

$$\langle v, \widehat{\varphi}(w_1 + w_2) - \widehat{\varphi}(w_1) - \widehat{\varphi}(w_2) \rangle = 0 \tag{153}$$

for all $v \in V$. The postive definiteness of the inner product implies

$$\widehat{\varphi}(w_1 + w_2) - \widehat{\varphi}(w_1) - \widehat{\varphi}(w_2) = \mathbf{0}. \tag{154}$$

In other words, we have $\widehat{\varphi}(w_1+w_2) = \widehat{\varphi}(w_1)+\widehat{\varphi}(w_2)$. Now let $w \in V$ and let $c \in \mathbb{F}$. Then

$$\langle \varphi(v), cw \rangle = \langle v, \widehat{\varphi}(cw) \rangle \tag{155}$$

for all $v \in V$. However, we also have

$$\begin{aligned} \langle \varphi(v), cw \rangle &= c\langle \varphi(v), w \rangle \\ &= c\langle v, \widehat{\varphi}(w) \rangle \\ &= \langle v, c\widehat{\varphi}(w) \rangle \end{aligned} \tag{156}$$

for all $v \in V$. (Note that from Definition 9.19, a Hermitian inner product is linear in its second argument. Hence, if $\langle \cdot, \cdot \rangle$ is Hermitian, there is no conjugation of c in the first and third equalities.) Equations (155) and (156) now imply

$$\langle v, \widehat{\varphi}(cw) - c\widehat{\varphi}(w) \rangle = 0 \tag{157}$$

for all $v \in V$. The positive definiteness of the inner product then implies that

$$\widehat{\varphi}(cw) - c\widehat{\varphi}(w) = \mathbf{0}. \tag{158}$$

In other words, $\widehat{\varphi}(cw) = c\widehat{\varphi}(w)$. This completes the proof that $\widehat{\varphi}$ is linear. □

Theorem 9.45. *Let $(V, \langle \cdot, \cdot \rangle)$ be an inner product space. Any linear map $\varphi : V \to V$ has a unique adjoint map with respect to $\langle \cdot, \cdot \rangle$.*

Proof. Let $\varphi : V \to V$ be a linear map.

We first consider the case where $(V, \langle \cdot, \cdot \rangle)$ is a real inner product space. Let $w \in V$ be arbitrary. Define a map $f_w : V^* \to \mathbb{R}$ by

$$f_w(v) := \langle \varphi(v), w \rangle$$

for all $v \in V$. Since φ is linear and a real inner product is linear in both arguments, it follows that f_w is linear. In other words, $f_w \in V^*$. By Theorem 9.36, there exists a unique element of V, which we denote as u_w, such that

$$f_w(v) = \langle v, u_w \rangle$$

for all $v \in V$. Define a map $\widehat{\varphi} : V \to V$ by $\widehat{\varphi}(w) := u_w$. From the definition of f_w and $\widehat{\varphi}$, we have

$$\langle \varphi(v), w \rangle = \langle v, \widehat{\varphi}(w) \rangle.$$

Lemma 9.44 now implies that $\widehat{\varphi}$ is both linear and unique. Hence, $\varphi^a := \widehat{\varphi}$ is the unique adjoint map of φ. This completes the proof of the real case.

The complex case is proved in a similar manner. Let $(V, \langle \cdot, \cdot \rangle)$ be a complex inner product space. As before, let $w \in V$ be arbitrary and define $f_w : V \to \mathbb{C}$ by

$$f_w(v) := \langle \varphi(v), w \rangle$$

Note that this time f_w is not linear, but antilinear. In other words, $f_w \in \overline{V^*}$. Indeed this follows from the linearity of φ and Proposition 9.20 which shows that a Hermitian inner product is antilinear in its first argument. By Theorem 9.42, there exists a unique element of V, which we (again) denote as u_w, such that

$$f_w(v) = \langle v, u_w \rangle$$

for all $v \in V$. As before, define a map $\widehat{\varphi} : V \to V$ by $\widehat{\varphi}(w) := u_w$. By construction, we again have

$$\langle \varphi(v), w \rangle = \langle v, \widehat{\varphi}(w) \rangle.$$

Lemma 9.44 once again implies that $\widehat{\varphi}$ is both linear and unique. Hence, $\varphi^a := \widehat{\varphi}$ is the unique adjoint map of φ. This completes the proof for the complex case. □

What happens if one takes the adjoint of the adjoint? The answer is given by the following result:

Corollary 9.46. *Let $(V, \langle \cdot, \cdot \rangle)$ be an inner product space and $\varphi : V \to V$ be a linear map. Then $(\varphi^a)^a = \varphi$.*

Proof. Let $\varphi^a : V \to V$ be the (unique) adjoint map of φ. From the definition of the adjoint map, we have

$$\langle \varphi(v), w \rangle = \langle v, \varphi^a(w) \rangle \tag{159}$$

for all $v, w \in V$.

First consider the case where $(V, \langle \cdot, \cdot \rangle)$ is a real inner product space. Since a real inner product is symmetric, we have

$$\langle w, \varphi(v) \rangle = \langle \varphi^a(w), v \rangle \tag{160}$$

for all $v, w \in V$. From the definition of the adjoint map, (160) shows that φ is an adjoint map of φ^a. However, by Theorem 9.45, the adjoint of a linear map is unique. From this, we conclude that $(\varphi^a)^a = \varphi$.

Now suppose that $(V, \langle \cdot, \cdot \rangle)$ is a complex inner product space. Taking the conjugate of both sides of (159) and then applying the conjugate symmetry of a Hermitian inner product once again gives (160). The same reasoning as in the real case implies that $(\varphi^a)^a = \varphi$. This completes the proof. □

The following results tells us how to compute the adjoint map practically:

Theorem 9.47. *Let $(V, \langle \cdot, \cdot \rangle)$ be a real inner product space and let $\mathcal{B}$ be an orthonormal basis on V. For a linear map $\varphi : V \to V$, the matrix representations of φ and φ^a with respect to $\mathcal{B}$ are related by $[\varphi^a]_{\mathcal{B}} = [\varphi]_{\mathcal{B}}^T$.*

Proof. Let $\mathcal{B} = \{x_1, \ldots, x_n\}$ be an orthonormal basis on V with respect to $\langle \cdot, \cdot \rangle$.

Let a_{ij} denote the (i, j)-element of the matrix representation $[\varphi]_{\mathcal{B}}$. Also, let b_{ij} denote the (i, j)-element of the matrix representation $[\varphi^a]_{\mathcal{B}}$. By definition,

$$\varphi(x_j) = \sum_{i=1}^{n} a_{ij} x_i$$

and

$$\varphi^a(x_j) = \sum_{i=1}^{n} b_{ij} x_i.$$

From this, we have

$$\begin{aligned} \langle \varphi(x_i), x_j \rangle &= \sum_{k=1}^{n} \langle a_{ki} x_k, x_j \rangle \\ &= \sum_{k=1}^{n} a_{ki} \langle x_k, x_j \rangle \\ &= a_{ji}, \end{aligned}$$

where the last equality follows from the fact that $\mathcal{B}$ is an orthonormal basis. Likewise, we have

$$\begin{aligned} \langle x_i, \varphi^a(x_j) \rangle &= \sum_{k=1}^{n} \langle x_i, b_{kj} x_k \rangle \\ &= \sum_{k=1}^{n} b_{kj} \langle x_i, x_k \rangle \\ &= b_{ij}. \end{aligned}$$

Since

$$\langle \varphi(x_i), x_j \rangle = \langle x_i, \varphi^a(x_j) \rangle,$$

we conclude that $b_{ij} = a_{ji}$. Hence, $[\varphi^a]_{\mathcal{B}} = [\varphi]_{\mathcal{B}}^T$. This completes the proof. □

Theorem 9.48. *Let $(V, \langle \cdot, \cdot \rangle)$ be a complex inner product space and let $\mathcal{B}$ be an orthonormal basis on V. For a linear map $\varphi : V \to V$, the matrix representations of φ and φ^a with respect to $\mathcal{B}$ are related by $[\varphi^a]_{\mathcal{B}} = [\varphi]_{\mathcal{B}}^*$, where $[\varphi]_{\mathcal{B}}^*$ denotes the conjugate transpose of $[\varphi]_{\mathcal{B}}$.*

Proof. Let $\mathcal{B} = \{x_1, \ldots, x_n\}$ be an orthonormal basis on V with respect to $\langle \cdot, \cdot \rangle$.

Let a_{ij} denote the (i, j)-element of the matrix representation $[\varphi]_{\mathcal{B}}$. Also, let b_{ij} denote the (i, j)-element of the matrix representation $[\varphi^a]_{\mathcal{B}}$. By definition,

$$\varphi(x_j) = \sum_{i=1}^{n} a_{ij} x_i$$

and

$$\varphi^a(x_j) = \sum_{i=1}^{n} b_{ij} x_i.$$

From this, we have

$$\begin{aligned} \langle \varphi(x_i), x_j \rangle &= \sum_{k=1}^{n} \langle a_{ki} x_k, x_j \rangle \\ &= \sum_{k=1}^{n} \overline{a}_{ki} \langle x_k, x_j \rangle \\ &= \overline{a}_{ji}, \end{aligned}$$

where the last equality follows from the fact that $\mathcal{B}$ is an orthonormal basis and by Proposition 9.20. Likewise, we have

$$\begin{aligned} \langle x_i, \varphi^a(x_j) \rangle &= \sum_{k=1}^{n} \langle x_i, b_{kj} x_k \rangle \\ &= \sum_{k=1}^{n} b_{kj} \langle x_i, x_k \rangle \\ &= b_{ij}. \end{aligned}$$

Since

$$\langle \varphi(x_i), x_j \rangle = \langle x_i, \varphi^a(x_j) \rangle,$$

we conclude that $b_{ij} = \overline{a}_{ji}$. Hence, $[\varphi^a]_{\mathcal{B}} = [\varphi]^*_{\mathcal{B}}$. This completes the proof. □

Example 9.49. *Let A be any $n \times n$ complex matrix and let $\langle \cdot, \cdot \rangle$ denote the standard Hermitian inner product on $\mathbb{C}^n$, that is,*

$$\langle \vec{u}, \vec{v} \rangle = (\vec{u})^* \vec{v}$$

for all $\vec{u}, \vec{v} \in \mathbb{C}^n$, where the elements of $\mathbb{C}^n$ are expressed as column vectors and $(\vec{u})^*$ denote the conjugate transpose of $\vec{u}$. Let $\mathcal{S} = \{\vec{e}_1, \ldots, \vec{e}_n\}$ denote the standard basis on $\mathbb{C}^n$. Then $\mathcal{S}$ is an orthonormal basis with respect to $\langle \cdot, \cdot \rangle$. Let $\varphi : \mathbb{C}^n \to \mathbb{C}^n$ be the matrix transformation associated to A, that is, $\varphi(\vec{v}) = A\vec{v}$. The matrix representation of φ with respect to $\mathcal{S}$ is simply $[\varphi]_{\mathcal{S}} = A$. By Theorem 9.48, we have $[\varphi^a]_{\mathcal{B}} = A^*$. This in turn implies that $\varphi^a(\vec{v}) = A^* \vec{v}$.

Example 9.50. *Let* $\mathbb{R}[x]_2$ *denote the vector space of real polynomials of degree* 2 *or less. Let* $\mathcal{B} = \{x^2, x, 1\}$ *and let*

$$\langle \cdot, \cdot \rangle := \langle \cdot, \cdot \rangle^{\mathcal{B}}$$

be the unique inner product on $\mathbb{R}[x]_2$ *for which* $\mathcal{B}$ *is an orthonormal basis. Let* D *be the linear map from* $\mathbb{R}[x]_2$ *to itself given by* $D = \frac{d}{dx} + 1$*. Then the matrix representation of* D *with respect to* $\mathcal{B}$ *is*

$$[D]_{\mathcal{B}} = \begin{pmatrix} 1 & 0 & 0 \\ 2 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}.$$

By Theorem 9.47, the matrix representation of the adjoint of D *with respect to* $\mathcal{B}$ *is*

$$[D^a]_{\mathcal{B}} = \begin{pmatrix} 1 & 2 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}.$$

Hence, D^a *acts on the basis elements as follows:*

$$D^a(x^2) = x^2, \qquad D^a(x) = 2x^2 + x, \qquad D^a(1) = x + 1.$$

As an additional check of Theorem 9.47, observe (for example) that

$$\langle D(x^2), x^2 \rangle = \langle x^2 + 2x, x^2 \rangle = \langle x^2, x^2 \rangle = \langle x^2, D^a(x^2) \rangle$$

and

$$\langle D(x^2), x \rangle = \langle x^2 + 2x, x \rangle = 2 = \langle x^2, 2x^2 + x \rangle = \langle x^2, D^a(x) \rangle.$$

9.7. Self-adjoint maps

As in the previous section, the term *inner product space* will refer to either a complex inner product space or a real one. When there is a need to single out one over the other, we will do so explicitly. We begin with our main definition:

Definition 9.51. *Let* $(V, \langle \cdot, \cdot \rangle)$ *be an inner product space. A* ***self-adjoint map*** *is a linear map* $\varphi : V \to V$ *such that* $\varphi^a = \varphi$*.*

Remark 9.52. *Self-adjoint maps turn out to play an important role in quantum mechanics. In quantum mechanics, a system is modeled by a certain type of complex inner product space and the observables of the system (i.e. the quantities that one measures like the position or momentum of an electron) are modeled by self-adjoint maps. Unlike the vector spaces that we deal with in this book, the complex inner product spaces in quantum mechanics are generally infinite dimensional.*

The matrix representations of self-adjoint maps are given by the following results:

Proposition 9.53. *Let $(V, \langle\cdot,\cdot\rangle)$ be a real inner product space and let $\mathcal{B}$ be an orthonormal basis on V. Then a linear map $\varphi : V \to V$ is self-adjoint if and only if $[\varphi]_{\mathcal{B}}$ is a symmetric matrix.*

Proof. Let $\varphi : V \to V$ be a linear map. By Theorem 9.47, we have $[\varphi]_{\mathcal{B}}^T = [\varphi^a]_{\mathcal{B}}$. Consequently, one obtains the following equivalence:

$$\varphi^a = \varphi \Longleftrightarrow [\varphi]_{\mathcal{B}}^T = [\varphi]_{\mathcal{B}}.$$

This completes the proof. □

Proposition 9.54. *Let $(V, \langle\cdot,\cdot\rangle)$ be a complex inner product space and let $\mathcal{B}$ be an orthonormal basis on V. Then a linear map $\varphi : V \to V$ is self-adjoint if and only if $[\varphi]_{\mathcal{B}}$ is a Hermitian matrix.*

Proof. Let $\varphi : V \to V$ be a linear map. By Theorem 9.48, we have $[\varphi]_{\mathcal{B}}^* = [\varphi^a]_{\mathcal{B}}$. Consequently, one obtains the following equivalence:

$$\varphi^a = \varphi \Longleftrightarrow [\varphi]_{\mathcal{B}}^* = [\varphi]_{\mathcal{B}}.$$

This completes the proof. □

Example 9.55. *Consider the complex vector space $\mathbb{C}^n$ where all vectors are expressed as column vectors and let $\langle\cdot,\cdot\rangle$ denote the standard Hermitian inner product on $\mathbb{C}^n$, that is, $\langle\vec{u},\vec{v}\rangle = (\vec{u})^*\vec{v}$ for $\vec{u},\vec{v} \in \mathbb{C}^n$. Let A be any Hermitian matrix and let $\psi : \mathbb{C}^n \to \mathbb{C}^n$ be the linear map defined via $\psi(\vec{v}) := A\vec{v}$. The standard basis $\mathcal{S}$ on $\mathbb{C}^n$ is then an orthonormal basis and $[\psi]_{\mathcal{S}} = A$. By Proposition 9.54, ψ is self-adjoint with respect to $\langle\cdot,\cdot\rangle$.*

We now prove our main result for self-adjoint maps on a complex inner product space. We will then use this result to deduce a similar result for real inner product spaces. This is a good example of how one can gain insight into real structures by first studying their complex counterparts.

Theorem 9.56. *Let $(V, \langle\cdot,\cdot\rangle)$ be a complex inner product space and let $\varphi : V \to V$ be a self-adjoint map.*

(i) Every eigenvalue of φ is real.

(ii) If λ and λ' are distinct eigenvalues of φ and v and v' are eigenvectors of φ associated to λ and λ' respectively, then $\langle v, v'\rangle = 0$.

(iii) There exists an orthogonal basis on V which consists entirely of eigenvectors of φ. In particular, φ is diagonalizable.

Proof. (i): Suppose λ is an eigenvalue of φ and v is an eigenvector of φ associated to λ. Since $\varphi^a = \varphi$, we have

$$\begin{aligned}\langle\varphi(v), v\rangle &= \langle v, \varphi(v)\rangle \\ \langle\lambda v, v\rangle &= \langle v, \lambda v\rangle \\ \overline{\lambda}\langle v, v\rangle &= \lambda\langle v, v\rangle.\end{aligned}$$

Since $v \neq \mathbf{0}$, we have $\langle v, v\rangle \neq 0$ which in turn implies that $\overline{\lambda} = \lambda$. From this, we conclude that $\lambda \in \mathbb{R}$.

(ii): Suppose that λ and λ' are distinct eigenvalues of φ and v and v' are their associated eigenvectors respectively. Then

$$\begin{aligned}\langle\varphi(v), v'\rangle &= \langle v, \varphi(v')\rangle \\ \langle\lambda v, v'\rangle &= \langle v, \lambda' v'\rangle \\ \lambda\langle v, v'\rangle &= \lambda'\langle v, v'\rangle,\end{aligned}$$

where we use the fact that λ is real in the third equality. Since $\lambda \neq \lambda'$, it follows immediately that $\langle v, v'\rangle = 0$.

(iii): We will prove this by induction on $\dim V$. For $\dim V = 1$, let $\vec{v}$ be any nonzero vector of V. Then $\{v\}$ is a basis of V which is also orthogonal (since any set consisting of a single nonzero vector is orthogonal in a trivial way). Since every element of V is a scalar multiple of v, we also have $\varphi(v) = \lambda v$ for some $\lambda \in \mathbb{C}$. Hence, $\{v\}$ is our desired basis. This proves (iii) for the 1-dimensional case.

Now let $(V, \langle\cdot,\cdot\rangle)$ be a complex inner product space of dimension n and assume that (iii) holds for all complex inner product spaces of dimension less than n. Here at last is where we really need to make use of the differences between the field of complex numbers and the field of real numbers. Let $p(x)$ denote the characteristic polynomial of φ. Since V is a complex vector space, $p(x)$ is then a complex polynomial (i.e. its coefficients are all elements of $\mathbb{C}$). Recall that the Fundamental Theorem of Algebra (Theorem 5.3) says that any complex polynomial has a zero or root which lies in $\mathbb{C}$. This implies that $p(x)$ has at least one root. However, the roots of $p(x)$ are simply the eigenvalues of φ. Hence, φ has at least one eigenvalue. Let E_λ denote the eigenspace of φ associated to λ, that is, E_λ is the subspace of V spanned by the eigenvectors of φ associated to λ. Since eigenvectors are nonzero by definition, it follows $\dim E_\lambda \geq 1$. If $\dim E_\lambda = \dim V$, then we are done. Indeed, in this case, we have $E_\lambda = V$ which immediately implies that **any** basis of V must consist entirely of eigenvectors of φ. Consequently, using the Gram-Schmidt process, we can construct an orthogonal basis on V which consists entirely of eigenvectors of φ. So let us instead suppose that $\dim E_\lambda < \dim V$. For this case, let

$$V' := E_\lambda^\perp$$

be the orthogonal complement of E_λ with respect to $\langle \cdot, \cdot \rangle$. By Theorem 9.31, we have

$$V = E_\lambda \oplus V'.$$

In particular, V' is a nonzero vector space with

$$\dim V' = \dim V - \dim E_\lambda = n - \dim E_\lambda < n.$$

We now show that $\varphi(V') \subset V'$. Let $v \in E_\lambda$ and let $v' \in V'$. Then

$$\begin{aligned}\langle \varphi(v'), v \rangle &= \langle v', \varphi(v) \rangle \\ &= \langle v', \lambda v \rangle \\ &= \lambda \langle v', v \rangle \\ &= 0.\end{aligned}$$

This shows that $\varphi(v') \in V' := E_\lambda^\perp$. Hence, φ maps V' into V'.

Let $\langle \cdot, \cdot \rangle'$ be the restriction of $\langle \cdot, \cdot \rangle$ to the subspace V' of V. Then $(V', \langle \cdot, \cdot \rangle')$ is a complex inner product space of dimension less than n. Let φ' be the restriction of φ to V'. Then $\varphi' : V' \to V'$ is a self-adjoint map on $(V', \langle \cdot, \cdot \rangle')$. By the induction hypothesis, there exists an orthogonal basis $\mathcal{B}'$ of V' which consists entirely of eigenvectors of φ'. Of course, any eigenvector of φ' is also an eigenvector of φ.

Next, let $\langle \cdot, \cdot \rangle_\lambda$ be the restriction of $\langle \cdot, \cdot \rangle$ to E_λ. Then $(E_\lambda, \langle \cdot, \cdot \rangle_\lambda)$ is also a complex inner product space. Hence, we can construct an orthogonal basis on E_λ. Let $\mathcal{B}_\lambda$ be any orthogonal basis on E_λ and let

$$\mathcal{B} := \mathcal{B}_\lambda \cup \mathcal{B}'.$$

Then $\mathcal{B}$ consists entirely of eigenvectors of φ. Moreover, since $V = E_\lambda \oplus V'$, it follows readily that $\mathcal{B}$ is also a basis of V. Also, observe that since $\mathcal{B}_\lambda \subset E_\lambda$ and $\mathcal{B}' \subset V' := (E_\lambda)^\perp$, it follows that every element of $\mathcal{B}$ is orthogonal to every element of $\mathcal{B}'$. In addition, since $\mathcal{B}_\lambda$ and $\mathcal{B}'$ are also orthogonal sets, it follows that $\mathcal{B}$ is also orthogonal. This completes the proof of (iii). □

Theorem 9.57. *Let A be an $n \times n$ Hermitian matrix.*

(i) The eigenvalues of A are real.

(ii) If λ_1 and λ_2 are distinct eigenvalues of A and $\vec{v}_1$ and $\vec{v}_2$ are eigenvectors of A associated to λ_1 and λ_2 respectively, then $(\vec{v}_1)^*\vec{v}_2 = 0$, where $\vec{v}_1, \vec{v}_2 \in \mathbb{C}^n$ are expressed as column vectors.

(iii) A is diagonalizable by a unitary matrix, that is, there exists a unitary matrix P such that P^*AP is a diagonal matrix.

Proof. Let $\langle \cdot, \cdot \rangle$ denote the standard Hermitian inner product on $\mathbb{C}^n$, that is,

$$\langle \vec{v}, \vec{w} \rangle = (\vec{v})^* \vec{w}$$

for all $\vec{v}, \vec{w} \in \mathbb{C}^n$, where the elements of $\mathbb{C}^n$ are expressed as column vectors. Let $\psi : \mathbb{C}^n \to \mathbb{C}^n$ be the linear map defined by $\psi(\vec{v}) := A\vec{v}$. From Example 9.55, $\psi : \mathbb{C}^n \to \mathbb{C}^n$ is a self-adjoint map on $(\mathbb{C}^n, \langle \cdot, \cdot \rangle)$.

Let $\mathcal{S}$ denote the standard basis on $\mathbb{C}^n$. Then the matrix representation $[\psi]_{\mathcal{S}} = A$. By Theorem 6.40, ψ and A have the same eigenvalues. Theorem 9.56 now implies that the eigenvalues of A are all real. This proves (i).

Suppose λ_1 and λ_2 are distinct eigenvalues of A and $\vec{v}_1$ and $\vec{v}_2$ are eigenvectors of A associated to λ_1 and λ_2 respectively. From the definition of ψ, $\vec{v}_1$ and $\vec{v}_2$ are also eigenvectors of ψ associated to distinct eigenvalues. By Theorem 9.56, we have

$$0 = \langle \vec{v}_1, \vec{v}_2 \rangle = (\vec{v}_1)^* \vec{v}_2.$$

This proves (ii).

Statement (iii) of Theorem 9.56 implies that $\mathbb{C}^n$ has an orthogonal basis which consists of the eigenvectors of ψ. Of course, from the definition of ψ, every eigenvector of ψ is also an eigenvector of A. Let

$$\mathcal{B} := \{\vec{v}_1, \ldots, \vec{v}_n\}$$

be this basis. Here, the term "orthogonal" means orthogonal with respect to the standard hermitian inner product on $\mathbb{C}^n$. Hence, for $\vec{v}_i$ and $\vec{v}_j$ with $i \neq j$, we have

$$\langle \vec{v}_i, \vec{v}_j \rangle = (\vec{v}_i)^* \vec{v}_j = 0.$$

Furthermore, by normalizing each of the basis vectors, we may further assume that $\mathcal{B}$ is an orthonormal basis. Hence,

$$\langle \vec{v}_i, \vec{v}_i \rangle = (\vec{v}_i)^* \vec{v}_i = 1$$

for $i = 1, \ldots, n$. Let P be the $n \times n$ matrix whose ith column is $\vec{v}_i$. Then it follows that $P^*P = I_n$. In other words, P is unitary. Let λ_i be the eigenvalue associated to the eigenvector $\vec{v}_i$. Then

$$\begin{aligned} AP &= (A\vec{v}_1, \ldots, A\vec{v}_n) \\ &= (\lambda_1\vec{v}_1, \ldots, \lambda_n\vec{v}_n) \\ &= PD, \end{aligned} \tag{161}$$

where D is the $n \times n$ diagonal matrix whose ith element is λ_i. (161) now implies $P^*AP = D$. This prove (iii). ☐

Example 9.58. *Consider the Hermitian matrix*

$$A = \begin{pmatrix} 1 & 2+i \\ 2-i & 3 \end{pmatrix}.$$

By Theorem 9.57, A has real eigenvalues and is diagonalizable by a unitary matrix. Let us verify this by direct calculation. The characteristic polynomial of A is found to be

$$p(x) = x^2 - 4x - 2.$$

The eigenvalues of A are then $2+\sqrt{6}$ *and* $2-\sqrt{6}$. *The eigenvectors associated to* $2+\sqrt{6}$ *and* $2-\sqrt{6}$ *are respectively*

$$\vec{v}_1 = \begin{pmatrix} 2+i \\ 1+\sqrt{6} \end{pmatrix}, \qquad \vec{v}_2 = \begin{pmatrix} 2+i \\ 1-\sqrt{6} \end{pmatrix}.$$

Clearly, this is a basis on $\mathbb{C}^2$. *Theorem 9.57 also states that the eigenvectors associated to distinct eigenvalues are orthogonal with respect to the standard Hermitian inner product. This is indeed the case:*

$$(\vec{v}_1)^*\vec{v}_2 = (2-i)(2+i) + (1+\sqrt{6})(1-\sqrt{6}) = 5 + (-5) = 0.$$

Let $\vec{u}_1 := \vec{v}_1/\|\vec{v}_1\|$ *and* $\vec{u}_2 := \vec{v}_2/\|\vec{v}_2\|$ *be the normalization of* $\vec{v}_1$ *and* $\vec{v}_2$ *respectively and let* P *be the* 2×2 *matrix whose first column is* $\vec{u}_1$ *and whose second column is* $\vec{u}_2$. *Then one has*

$$P^*AP = \begin{pmatrix} 2+\sqrt{6} & 0 \\ 0 & 2-\sqrt{6} \end{pmatrix}.$$

We now apply the results of the complex case to the real case.

Theorem 9.59. *Let* A *be a real* $n \times n$ *symmetric matrix.*

(i) The eigenvalues of A *are real.*

(ii) If λ_1 *and* λ_2 *are distinct eigenvalues of* A *and* $\vec{v}_1$ *and* $\vec{v}_2$ *are eigenvectors of* A *associated to* λ_1 *and* λ_2 *respectively, then* $\vec{v}_1 \cdot \vec{v}_2 = 0$.

(iii) A is diagonalizable by an orthogonal matrix, that is, there exists a (real) orthogonal matrix P *such that* P^TAP *is a diagonal matrix.*

Proof. Since $\mathbb{R} \subset \mathbb{C}$ and A is a real symmetric matrix, A is automatically a Hermitian matrix. By Theorem 9.57, all the eigenvalues of A are real. This proves (i).

For (ii), suppose that λ_1 and λ_2 are distinct eigenvalues of A and $\vec{v}_1$ and $\vec{v}_2$ are eigenvectors of A associated to λ_1 and λ_2 respectively. By statement (ii) of Theorem 9.57, we have

$$\begin{aligned}\vec{v}_1 \cdot \vec{v}_2 &= \vec{v}_1^T \vec{v}_2 \\ &= (\vec{v}_1)^* \vec{v}_2 \\ &= 0.\end{aligned}$$

where $\vec{v}_1$ and $\vec{v}_2$ are regarded as column vectors and we use the fact that $\vec{v}_1^T = (\vec{v}_1)^*$ since $\vec{v}_1 \in \mathbb{R}^n$. This proves (ii).

For (iii), let λ is an eigenvalue of A and let $\vec{v}$ be an eigenvector of A associated to λ. Since A is viewed as a Hermitian matrix, the eigenvectors of A (for the moment) should be regarded as elements of $\mathbb{C}^n$. We can decompose the eigenvector $\vec{v}$ into its and imaginary parts:

$$\vec{v} = \mathrm{Re}(\vec{v}) + i\ \mathrm{Im}(\vec{v}),$$

where $\mathrm{Re}(\vec{v})$ and $\mathrm{Im}(\vec{v})$ are elements of $\mathbb{R}^n$. Since $\vec{v}$ is an eigenvector of A associated to λ, we have

$$A\vec{v} = \lambda\vec{v}$$

$$A\mathrm{Re}(\vec{v}) + i\ A\mathrm{Im}(\vec{v}) = \lambda\mathrm{Re}(\vec{v}) + i\ \lambda\mathrm{Im}(\vec{v}) \tag{162}$$

Of course, the real parts on the left and right sides of (162) must be equal. Likewise, the imaginary parts on the left and right sides of (162) must be equal. Since A is a real matrix and $\lambda \in \mathbb{R}$, it follows that

$$A\mathrm{Re}(\vec{v}) = \lambda\mathrm{Re}(\vec{v}), \qquad A\mathrm{Im}(\vec{v}) = \lambda\mathrm{Im}(\vec{v}).$$

From this, we conclude that if $\vec{v} \in \mathbb{C}^n$ is an eigenvector of A, then $\mathrm{Re}(\vec{v})$ and $\mathrm{Im}(\vec{v})$ are also eigenvectors of A.

By statement (iii) of Theorem 9.57, there exists an $n \times n$ matrix P (possibly complex) such that $P^{-1} = P^*$ and P^*AP is diagonal. These two conditions imply that the columns of P form a basis on $\mathbb{C}^n$ which consists entirely of the eigenvectors of A. Let

$$\vec{v}_1, \vec{v}_2, \ldots, \vec{v}_n \tag{163}$$

denote the columns of P. Since each $\vec{v}_i$ is an eigenvector of A, the above argument implies that the following **real** vectors are also eigenvectors of A:

$$\mathcal{D} := \{\mathrm{Re}(\vec{v}_1),\ \mathrm{Re}(\vec{v}_2), \ldots, \mathrm{Re}(\vec{v}_n),\ \mathrm{Im}(\vec{v}_1),\ \mathrm{Im}(\vec{v}_2), \ldots, \mathrm{Im}(\vec{v}_n)\}. \tag{164}$$

Since (163) is a basis of $\mathbb{C}^n$ and $\vec{v}_j$ is a $\mathbb{C}$-linear combination of $\mathrm{Re}(\vec{v}_j)$ and $\mathrm{Im}(\vec{v}_j)$ for $j = 1, 2, \ldots, n$, it follows that (164) must span $\mathbb{C}^n$. This in turn implies that (164) must contain a basis of $\mathbb{C}^n$. Let $\mathcal{D}_1 \subset \mathcal{D}$ denote this basis. We have thus found a basis of $\mathbb{C}^n$ which consists of **real** eigenvectors of A. Since $\mathcal{D}_1$ is linearly independent over $\mathbb{C}$, it must also be linearly independent over $\mathbb{R} \subset \mathbb{C}$. Hence, $\mathcal{D}_1$ must also be a basis of the **real** vector space $\mathbb{R}^n$. Let $\lambda_1, \dots, \lambda_k$ be the distinct eigenvalues of A and let E_{λ_j} be the (real) eigenspace of A associated to λ_j. Statement (ii) of Theorem 9.59 combined with the fact that $\mathcal{D}_1$ is a basis of $\mathbb{R}^n$ implies that

$$\mathbb{R}^n = E_{\lambda_1} \oplus E_{\lambda_2} \oplus \cdots \oplus E_{\lambda_k}. \tag{165}$$

Let $\mathcal{B}_{\lambda_j}$ be any **orthonormal** basis of E_{λ_j} for $j = 1, \dots, k$. Then statement (ii) of Theorem 9.59 along with (165) implies that

$$\mathcal{B} := \mathcal{B}_{\lambda_1} \cup \cdots \cup \mathcal{B}_{\lambda_k}$$

is an orthonormal basis of $\mathbb{R}^n$ consisting of the eigenvectors of A. Denote the elements of $\mathcal{B}$ by

$$\mathcal{B} := \{\vec{x}_1, \dots, \vec{x}_n\}.$$

Let Q be the $n \times n$ matrix whose jth column is $\vec{x}_j$. Then the fact that $\mathcal{B}$ is orthonormal basis which consists of the eigenvectors of A implies that Q is an orthogonal matrix and $Q^T AQ$ is a diagonal matrix. This completes the proof of (iii). □

Example 9.60. *Consider the* 2×2 *real symmetric matrix*

$$A = \begin{pmatrix} -1 & 2 \\ 2 & 4 \end{pmatrix}.$$

By Theorem 9.59, A has real eigenvalues and is diagonalizable by an orthogonal matrix P. Let us verify this by direct calculation. The characteristic polynomial of A is then

$$p(x) = x^2 - 3x - 8.$$

The eigenvalues are then $(3+\sqrt{41})/2$ and $(3-\sqrt{41})/2$. The eigenvectors of A are found to be

$$\vec{v}_1 = \begin{pmatrix} 4 \\ 5+\sqrt{41} \end{pmatrix}, \qquad \vec{v}_2 = \begin{pmatrix} 4 \\ 5-\sqrt{41} \end{pmatrix}.$$

By inspection, we see that $\vec{v}_1 \cdot \vec{v}_2 = 0$. Let $\vec{u}_1 = \vec{v}_1 / \|\vec{v}_1\|$ and $\vec{u}_2 = \vec{v}_2 / \|\vec{v}_2\|$ be the normalization of $\vec{v}_1$ and $\vec{v}_2$ respectively and let P be the 2×2 matrix whose first column is $\vec{u}_1$ and whose second column is $\vec{u}_2$. Then P is orthogonal and

$$P^T AP = \begin{pmatrix} \frac{3+\sqrt{41}}{2} & 0 \\ 0 & \frac{3-\sqrt{41}}{2} \end{pmatrix}.$$

Theorem 9.61. *Let $(V, \langle\cdot,\cdot\rangle)$ be a real inner product space and let $\varphi : V \to V$ be a self-adjoint map.*

(i) Every eigenvalue of φ is real.

(ii) If λ and λ' are distinct eigenvalues of φ and v and v' are eigenvectors of φ associated to λ and λ' respectively, then $\langle v, v'\rangle = 0$.

(iii) There exists an orthogonal basis on V which consists entirely of eigenvectors of φ. In particular, φ is diagonalizable.

Proof. Let $\mathcal{B}$ be any orthonormal basis on V. Since φ is self-adjoint and $\mathcal{B}$ is orthonormal, Proposition 9.53 implies that the matrix representation $[\varphi]_{\mathcal{B}}$ is a symmetric matrix. Let $A := [\varphi]_{\mathcal{B}}$. By Theorem 9.59, the eigenvalues of A are all real. However, the eigenvalues of a linear map and its matrix representation are the same (see Theorem 6.40). From this, we conclude that the eigenvalues of φ are all real. This proves (i).

Now suppose that λ and λ' are distinct eigenvalues of φ and v and v' be eigenvectors of φ associated to λ and λ' respectively. Since $\mathcal{B}$ is an orthonormal basis, we have

$$\langle v, v'\rangle = [v]_{\mathcal{B}} \cdot [v']_{\mathcal{B}}$$

by Proposition 9.16. By Theorem 6.40, $[v]_{\mathcal{B}}$ and $[v']_{\mathcal{B}}$ are eigenvectors of $A := [\varphi]_{\mathcal{B}}$ associated to the eigenvalues λ and λ' respectively. Since A is (real) symmetric, Theorem 9.59 implies that $[v]_{\mathcal{B}} \cdot [v']_{\mathcal{B}} = 0$. Hence, $\langle v, v'\rangle = 0$. This proves (ii).

By statement (iii) of Theorem 9.59, there exists an orthogonal matrix P such that $P^T AP$ is diagonal. This simply implies that the columns of P form an orthonormal basis of $\mathbb{R}^n$ which consists entirely of eigenvectors of A. Let

$$\vec{v}_1, \ldots, \vec{v}_n$$

denote the columns of P. Let λ_i be the eigenvalue of A associated to $\vec{v}_i$ and let $v_i \in V$ be the unique vector whose coordinate representation with respect to $\mathcal{B}$ is $\vec{v}_i$, that is, $[v_i]_{\mathcal{B}} := \vec{v}_i$ for $i = 1, \ldots, n$. This implies that

$$v_1, \ldots, v_n$$

is a basis of V. By Theorem 6.40, v_i is also an eigenvector of φ associated to the eigenvalue λ_i for $i = 1, \ldots, n$. By Proposition 9.16, we have

$$\langle v_i, v_j\rangle = [v_i]_{\mathcal{B}} \cdot [v_j]_{\mathcal{B}} = \vec{v}_i \cdot \vec{v}_j. \tag{166}$$

Since $\vec{v}_1, \ldots, \vec{v}_n$ is an orthonormal basis on $\mathbb{R}^n$, (166) now implies $v_1, \ldots, v_n$ is an orthonormal basis on V. This proves (iii). $\square$

Chapter 9 Exercises

1. Consider the Hermitian matrix

$$A = \begin{pmatrix} 1 & 1+i \\ 1-i & 2 \end{pmatrix}.$$

   (a) Compute the eigenvalues of A and the corresponding eigenspaces.
   (b) Find a unitary matrix U for which U^*AU is a diagonal matrix.

2. Consider the Hermitian matrix

$$A = \begin{pmatrix} 1 & 1+i \\ 1-i & 1 \end{pmatrix}.$$

   (a) Compute the eigenvalues of A and the corresponding eigenspaces.
   (b) Find a unitary matrix U for which U^*AU is a diagonal matrix.

3. Test each matrix A below for diagonalizability. If A is diagonalizable, then find a non-singular matrix P such that $P^{-1}AP = D$, where D is diagonal.

$$A = \begin{pmatrix} 1 & 2 \\ 2 & -5 \end{pmatrix} \quad ; \quad A = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & -1 \\ 0 & 1 & 1 \end{pmatrix}.$$

4. Show that if a square matrix M is diagonalizable, then so is its transpose M^T.

5. Find an expression for A^n if

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

   Hint: diagonalize A.

6. Let $\langle \cdot, \cdot \rangle$ be an inner product on $\mathbb{R}^2$ for which the basis

$$\mathcal{B} = \{\vec{b}_1, \vec{b}_2\} = \{(1,1),\ (1,-1)\}$$

   is orthonormal with respect to $\langle \cdot, \cdot \rangle$. Let $\mathcal{S} = \{\vec{e}_1, \vec{e}_2\}$ denote the standard basis on $\mathbb{R}^2$.
   (a) Compute the matrix representation of $\langle \cdot, \cdot \rangle$ with respect to $\mathcal{S}$: $[\langle \cdot, \cdot \rangle]_{\mathcal{S}}$.
   (b) Let $\varphi : \mathbb{R}^2 \to \mathbb{R}^2$ be the linear map defined by

$$\varphi(\vec{e}_1) = 2\vec{e}_1 + \vec{e}_2, \qquad \varphi(\vec{e}_2) = \vec{e}_1 - 2\vec{e}_2.$$

   Compute the matrix representation of the adjoint map φ^a with respect to $\mathcal{S}$: $[\varphi^a]_{\mathcal{S}}$.

(c) As a test of your calculation, verify the following identity:

$$\langle \varphi(\vec{e}_1), \vec{e}_2 \rangle = \langle \vec{e}_1, \varphi^a(\vec{e}_2) \rangle.$$

7. Let $\langle \cdot, \cdot \rangle$ be an inner product on $\mathbb{R}^3$ for which the basis

$$\mathcal{B} = \{\vec{b}_1, \vec{b}_2, \vec{b}_3\} = \{(0, 1, -2),\ (2, -1, 0),\ (1, 0, 3)\}$$

is orthonormal with respect to $\langle \cdot, \cdot \rangle$. Let $\mathcal{S} = \{\vec{e}_1, \vec{e}_2, \vec{e}_3\}$ denote the standard basis on $\mathbb{R}^3$.

(a) Compute the matrix representation of $\langle \cdot, \cdot \rangle$ with respect to $\mathcal{S}$: $[\langle \cdot, \cdot \rangle]_{\mathcal{S}}$.

(b) Let $\varphi : \mathbb{R}^3 \to \mathbb{R}^3$ be the linear map defined by

$$\varphi(\vec{e}_1) = 2\vec{e}_1 + 2\vec{e}_3, \qquad \varphi(\vec{e}_2) = 2\vec{e}_1, \qquad \varphi(\vec{e}_3) = \vec{e}_1 + \vec{e}_2 + \vec{e}_3$$

Compute the matrix representation of the adjoint map φ^a with respect to $\mathcal{S}$: $[\varphi^a]_{\mathcal{S}}$.

(c) As a test of your calculation, verify the following identity:

$$\langle \varphi(\vec{e}_3), \vec{e}_2 \rangle = \langle \vec{e}_3, \varphi^a(\vec{e}_2) \rangle.$$

8. Let $\mathbb{R}[x]_2$ be the vector space of real polynomials of degree 2 or less. Let $\langle \cdot, \cdot \rangle$ be the inner product on $\mathbb{R}[x]_2$ defined by

$$\langle p(x), q(x) \rangle := \int_0^1 p(x)q(x)dx.$$

(a) Construct an orthonormal basis on $(\mathbb{R}[x]_2, \langle \cdot, \cdot \rangle)$ by applying the Gram-Schmidt process to the basis $\mathcal{B} := \{x^2, x, 1\}$ of $\mathbb{R}[x]_2$. Call the resulting orthonormal basis $\mathcal{C}$.

(b) Let $D : \mathbb{R}[x]_2 \to \mathbb{R}[x]_2$ be the linear map defined by

$$Dp(x) := 4\frac{d}{dx}p(x) + p(x).$$

Give the matrix representation of the adjoint map D^a of D with respect to $\mathcal{B}$ and the above inner product: $[D^a]_{\mathcal{B}}$.

(c) Let $\varphi : \mathbb{R}[x]_2 \to \mathbb{R}[x]_2$ be the linear map whose matrix representation with respect to $\mathcal{B}$ is

$$[\varphi]_{\mathcal{B}} = \begin{pmatrix} 6 & -15 & -60 \\ 0 & 18 & 48 \\ 0 & 0 & 6 \end{pmatrix}.$$

Calculate the following: $\langle \varphi(x^2), x \rangle$ and $\langle x^2, \varphi(x) \rangle$. What did you find?

(d) Determine conclusively if φ is self-adjoint. (Hint: calculate the matrix representation $[\varphi]_{\mathcal{C}}$.)

9. Let $C([0,1];\mathbb{C})$ be the vector space of continuous complex valued functions on the closed interval $[0,1]$. (See Example 9.22.) Define $\langle\cdot,\cdot\rangle$ by
$$\langle f,g\rangle := \int_0^1 \overline{f(x)}g(x)dx$$
for $f,g \in C([0,1];\mathbb{C})$. Show that $\langle\cdot,\cdot\rangle$ is a Hermitian inner product on $C([0,1];\mathbb{C})$. (The proof of this is similar to the one given in Example 9.5).

10. Suppose $\varphi : V \to W$ is an **antilinear** map.
   (i) Show that $\ker\varphi$ is a subspace of V and im φ is a subspace of W.
   (ii) As in the linear case, define
   $$\text{Nullity}(\varphi) := \dim\ker\varphi, \qquad \text{Rank}(\varphi) := \dim \text{im } \varphi.$$
   Show that the Rank-Nullity Theorem still holds for antilinear maps. In other words, show that
   $$\dim V = \text{Nullity}(\varphi) + \text{Rank}(\varphi)$$

11. Let $\varphi : U \to V$ and $\psi : V \to W$ be **antilinear** maps. Show that $\psi\circ\varphi : U \to W$ is a linear map.

Part 2

Advanced Topics

Chapter 10

The Determinant Revisited

The goal of this chapter is to prove the properties of the determinant which were introduced in Chapter 4. Along the way, we will encounter the explicit formula for the determinant and establish its equivalence to the recursive definition given in Chapter 4.

10.1. The Sign of a Permutation

Let S_n denote the set of permutations on the ordered set

$$\{1, 2, \ldots, n\}.$$

Recall that an element $\sigma \in S_n$ is simply a bijective map

$$\sigma : \{1, 2, \ldots, n\} \to \{1, 2, \ldots, n\}.$$

From σ, we obtain a reordering of the above set:

$$\{\sigma(1), \sigma(2), \ldots, \sigma(n)\}.$$

One can express the information contained in the permutation σ as a $2 \times n$ matrix:

$$\begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}.$$

The first row of the above matrix represents the inputs and the second row the corresponding outputs. Let e denote the identity map on $\{1, 2, \ldots, n\}$. e is called the **identity permutation**. Its matrix representation is then

$$\begin{pmatrix} 1 & 2 & \cdots & n \\ 1 & 2 & \cdots & n \end{pmatrix}.$$

Definition 10.1. *A permutation which simply swaps two elements i and j of the set $\{1, 2, \dots, n\}$ is a called a **transposition** and is denoted by (i, j).*

Example 10.2. *Consider the transposition $(2,5) \in S_5$ on the ordered $\{1, 2, 3, 4, 5\}$. Its matrix representation is*

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 5 & 3 & 4 & 2 \end{pmatrix}.$$

Intuitively, given any permutation $\sigma \in S_n$, one can obtain the permutation

$$\{\sigma(1), \sigma(2), \dots, \sigma(n)\}$$

by successively swapping pairs of elements of the set $\{1, 2, \dots, n\}$. In other words, σ can be expressed as a composition (or product) of transpositions. This intuitive fact is proven rigorously in any book on abstract algebra.

Example 10.3. *Consider the permutation $\sigma \in S_5$ whose matrix representation is*

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 2 & 3 & 1 \end{pmatrix}.$$

By scribbling away on paper, we see right away that σ is given by the composition

$$\sigma = (1,5)(1,2)(1,3)(1,4),$$

where we recall that $(i,j) : \{1,2,3,4,5\} \to \{1,2,3,4,5\}$ are maps (not points!) which maps i to j and j to i and leaves everything unchanged. Now one can ask, is this the only way to express σ as a product of compositions? The answer is no. We can also express σ as follows:

$$\sigma = (1,5)(1,2)(1,3)(1,4)(1,3)(1,2)(1,3)(2,3).$$

Example 10.4. *Consider the permutation $\beta \in S_5$ whose matrix representation is*

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 2 & 5 & 4 \end{pmatrix}.$$

With a little thought, we see that β is given by the product

$$\beta = (1,3)(2,3)(4,5).$$

We can also express β as the product

$$\beta = (1,3)(2,3)(4,5)(3,4)(2,4)(2,3)(2,4).$$

Examples 10.3 and 10.4 illustrate that the expression of a permutation as a product of transpositions is not unique. However, notice that both expressions for σ in

Example 10.3 consists of an even number of transpositions while the expressions for β in Example 10.4 consist of an odd number of transpositions. This is not a coincidence.

Theorem 10.5. *Let $\sigma \in S_n$ and suppose*

$$\sigma = \tau_1 \tau_2 \cdots \tau_r = \gamma_1 \gamma_2 \cdots \gamma_s, \tag{167}$$

where τ_i and γ_i are transpositions. Then r and s are either both even or both odd.

From (167), we have

$$e = \tau_1 \tau_2 \cdots \tau_r \gamma_s \cdots \gamma_2 \gamma_1.$$

Hence, Theorem 10.5 is equivalent to the following:

Theorem 10.6. *The identity permuation $e \in S_n$ is always expressed as an even number of transpositions.*

The proof of Theorem 10.6 is given in any book on abstract algebra and turns out to be somewhat lengthy. The point of all this is that one has a well defined notion of **even** and **odd** permutations:

Definition 10.7. *Let $\sigma \in S_n$ and let*

$$\sigma = \tau_1 \tau_2 \cdots \tau_r$$

*be any decomposition of σ into transpositions. σ is called **even** if r is even and **odd** if r is odd.*

*The **sign** of σ is then given by*

$$sgn(\sigma) := \begin{cases} 1 & \text{if } \sigma \text{ is even} \\ -1 & \text{if } \sigma \text{ is odd} \end{cases}$$

Example 10.8. *The permutation σ in Example 10.3 is even while the permutation β in Example 10.4 is odd. Hence, $sgn(\sigma) = 1$ and $sgn(\beta) = -1$.*

10.2. Multilinear Maps

The notion of a multilinear map is a simple generalization of a linear map. We have already encountered multilinear maps. For example, the inner product is a multilinear map and, later, we will see that the determinant is a multilinear map. Without loss of generality, we assume throughout this section that all vector spaces are real. Naturally, we begin with the following definition:

Definition 10.9. *Let W and V_i for $i = 1, \ldots, k$ be vector spaces. The map*

$$F : V_1 \times V_2 \times \cdots \times V_k \to W$$

is called a ***multilinear map*** *(or* ***k-linear map****) if F is linear in each of its k arguments.*

More explicitly, the map F in Definition 10.9 is k-linear if for any $i \in \{1, 2, \ldots, k\}$ and any fixed $x_j \in V_j$ for all $j \neq i$, F satisfies the following conditions:

$$F(x_1, \ldots, x_{i-1}, cv, x_{i+1}, \ldots, x_n) = cF(x_1, \ldots, x_{i-1}, v, x_{i+1}, \ldots, x_n)$$

and

$$F(x_1, \ldots, x_{i-1}, v + v', x_{i+1}, \ldots, x_n) \\ = F(x_1, \ldots, x_{i-1}, v, x_{i+1}, \ldots, x_n) + F(x_1, \ldots, x_{i-1}, v', x_{i+1}, \ldots, x_n)$$

for all $c \in \mathbb{R}$ and $v, v' \in V$.

Example 10.10. *Let V be a (real) vector space and let $\langle \cdot, \cdot \rangle$ be an inner product. Define*

$$F : V \times V \to \mathbb{R}$$

by $F(u, v) := \langle u, v \rangle$. Then

$$F(cu, v) = \langle cu, v \rangle = c\langle u, v \rangle = cF(u, v)$$

and

$$F(u + u', v) = \langle u + u', v \rangle = \langle u, v \rangle + \langle u', v \rangle = F(u, v) + F(u', v)$$

for all $c \in \mathbb{R}$ and $u, v \in V$. Likewise, we also have

$$F(u, cv) = cF(u, v), \quad F(u, v + v') = F(u, v) + F(u, v'), \quad \forall c \in \mathbb{R},\ v, v' \in V.$$

Hence, F is a 2-linear map.

Let V be any fixed real vector space. We are now going to specialize to k-linear maps of the form

$$F : \underbrace{V \times V \times \cdots \times V}_{k \text{ copies}} \to W.$$

Let $\{b_1, \ldots, b_n\}$ be a basis on V. Recall that for a linear map $\varphi : V \to W$, φ is completely determined by its values on the basis elements: $\varphi(b_i)$, $i = 1, \ldots, n$. Hence, if $\psi : V \to W$ is another linear map and $\psi(b_i) = \varphi(b_i)$ for $i = 1, \ldots, n$. then $\psi = \varphi$. A similar result applies to k-linear maps.

Theorem 10.11. *Let V be a vector space and let F and G be multilinear maps with the same range W and domain*

$$\underbrace{V \times V \times \cdots \times V}_{k \text{ copies}}.$$

Let $\{b_1, \ldots, b_n\}$ be a basis on V. Then $F = G$ if and only if

$$F(b_{i_1}, b_{i_2}, \ldots b_{i_k}) = G(b_{i_1}, b_{i_2}, \ldots b_{i_k}) \tag{168}$$

for all indices $i_1, i_2, \ldots, i_k \in \{1, 2, \ldots, n\}$.

Proof. We prove Theorem 10.11 explicitly for the case $k = 2$. The general case is proved in exactly the same way. The only difference is that the notation becomes more cumbersome.

($\Rightarrow$): This is immediate. If $F = G$, then certainly (168) is satisfied.

($\Leftarrow$): Suppose that

$$F(b_i, b_j) = G(b_i, b_j) \tag{169}$$

for all $b_i, b_j \in \{b_1, \ldots, b_n\}$. Let $u, v \in V$ be arbitrary. Then we can express each as a linear combination of the basis elements:

$$\begin{aligned} u &= \alpha_1 b_1 + \cdots + \alpha_n b_n \\ v &= \beta_1 b_1 + \cdots + \beta_n b_n, \end{aligned} \tag{170}$$

for some $\alpha_i, \beta_i \in \mathbb{R}$. Since F is multilinear, we have

$$\begin{aligned} F(u, v) &= \sum_{i=1}^{n} \alpha_i F(b_i, v) \\ &= \sum_{i=1}^{n} \sum_{j=1}^{n} \alpha_i \beta_j F(b_i, b_j). \end{aligned} \tag{171}$$

The same calculation applied to G gives

$$G(u, v) = \sum_{i=1}^{n} \sum_{j=1}^{n} \alpha_i \beta_j G(b_i, b_j). \tag{172}$$

Comparing (171) and (172) and using (169) implies $F(u, v) = G(u, v)$. □

We specialize even further with the following definition:

Definition 10.12. *Let*

$$F : \underbrace{V \times V \times \cdots \times V}_{k \text{ copies}} \to W$$

*be a k-linear map. F is **alternating** if swapping any two of its arguments changes the sign of F, that is,*

$$F(v_1, \ldots, v_i, \ldots, v_j, \ldots, v_k) = -F(v_1, \ldots, v_j, \ldots, v_i, \ldots, v_k).$$

*Moreover, if $W = \mathbb{R}$, then F is called a **k-form** on V.*

Example 10.13. *Consider the vector space $\mathbb{R}^2$ and define*

$$\omega_2 : \mathbb{R}^2 \times \mathbb{R}^2 \to \mathbb{R}$$

as follows: for

$$\vec{u} = \begin{pmatrix} a \\ b \end{pmatrix}, \qquad \begin{pmatrix} c \\ d \end{pmatrix},$$

$$\omega_2(\vec{u}, \vec{v}) := \det \begin{pmatrix} a & c \\ b & d \end{pmatrix} = ad - bc.$$

We now verify that ω_2 is a 2-form. First, we verify that ω_2 is alternating, that is, it changes sign if we swap any two of its arguments (in this case it only has two arguments):

$$\omega_2(\vec{v}, \vec{u}) = det \begin{pmatrix} c & a \\ d & b \end{pmatrix} = bc - ad = -(ad - bc) = -\omega_2(\vec{u}, \vec{v}).$$

Now we verify that ω_2 is linear in its first argument. To do this, let $r \in \mathbb{R}$ and let

$$\vec{x} = \begin{pmatrix} p \\ q \end{pmatrix}.$$

Then

$$\begin{aligned} \omega_2(\vec{u} + \vec{x}, \vec{v}) &= \det \begin{pmatrix} a+p & c \\ b+q & d \end{pmatrix} \\ &= (a+p)d - (b+q)c \\ &= (ad - bc) + (pd - qc) \\ &= \omega_2(\vec{u}, \vec{v}) + \omega_2(\vec{x}, \vec{v}) \end{aligned}$$

and

$$\begin{aligned} \omega_2(r\vec{u}, \vec{v}) &= \det \begin{pmatrix} ra & c \\ rb & d \end{pmatrix} \\ &= rad - rbc \\ &= r(ad - bc) \\ &= r\omega_2(\vec{u}, \vec{v}). \end{aligned}$$

To check the linearity of the second argument, we use the fact that ω_2 is alternating and the fact that ω_2 is linear in the first argument:

$$\begin{aligned}\omega_2(\vec{u}, \vec{v}+\vec{x}) &= -\omega_2(\vec{v}+\vec{x}, \vec{u}) \\ &= -\omega_2(\vec{v}, \vec{u}) - \omega_2(\vec{x}, \vec{u}) \\ &= \omega_2(\vec{u}, \vec{v}) + \omega_2(\vec{u}, \vec{x}).\end{aligned}$$

and

$$\begin{aligned}\omega_2(\vec{u}, r\vec{v}) &= -\omega_2(r\vec{v}, \vec{u}) \\ &= -r\omega_2(\vec{v}, \vec{u}) \\ &= r\omega_2(\vec{u}, \vec{v}).\end{aligned}$$

Hence, we have verified that ω_2 is a 2-form on $\mathbb{R}^2$.

Example 10.13 shows that the determinant on 2×2 matrices is really a 2-form on $\mathbb{R}^2$. In the next section, we will show that the determinant on $n \times n$ matrices for arbitrary n is an n-form on $\mathbb{R}^n$. Before we leave this section, we make a few more observations:

Proposition 10.14. *Let*

$$F : \underbrace{V \times V \times \cdots \times V}_{k \text{ copies}} \to W$$

be a k-linear map. For all $v_1, \ldots, v_k \in V$, the following statements are equivalent:

(1) F is alternating.
(2) Swapping two adjacent elements in $F(v_1, v_2, \ldots, v_k)$ results in a sign change, that is,

$$F(v_1, \ldots, v_i, v_{i+1}, \ldots, v_k) = -F(v_1, \ldots, v_{i+1}, v_i, \ldots, v_k)$$

for all $i < k$.
(3) If $v_i = v_{i+1}$ for all $i < k$, then $F(v_1, v_2, \ldots, v_k) = \mathbf{0}$.
(4) If $v_i = v_j$ for some $i \neq j$, then $F(v_1, v_2, \ldots, v_k) = \mathbf{0}$.

Proof. (1) $\Rightarrow$ (2). Immediate.

(2) $\Rightarrow$ (3). Suppose $v_i = v_{i+1}$ for some $i < k$. Then

$$F(v_1, \ldots, v_i, v_{i+1}, \ldots, v_k) = F(v_1, \ldots, v_{i+1}, v_i, \ldots, v_k) \quad = -F(v_1, \ldots, v_i, v_{i+1}, \ldots, v_k)$$

where the first equality follows from the fact that $v_i = v_{i+1}$ and the second equality follows from (2). This implies

$$F(v_1, v_2, \ldots, v_k) = \mathbf{0}.$$

(2) $\Leftarrow$ (3). Replace the ith and $(i+1)$th arguments of $F(v_1, v_2, \ldots, v_k)$ with $u := v_i + v_{i+1}$ and expand by multilinearity:

$$F(v_1, \ldots, u, u, \ldots, v_k) = F(v_1, \ldots, v_i, v_i, \ldots, v_k) + F(v_1, \ldots, v_i, v_{i+1}, \ldots, v_k) \\ + F(v_1, \ldots, v_{i+1}, v_i, \ldots, v_k) + F(v_1, \ldots, v_{i+1}, v_{i+1}, \ldots, v_k).$$

By (3), the term on the left side of the equation is zero and also the first and fourth terms on the right side. Hence, the above equation reduces to

$$F(v_1, \ldots, v_i, v_{i+1}, \ldots, v_k) + F(v_1, \ldots, v_{i+1}, v_i, \ldots, v_k) = \mathbf{0}.$$

From this, we conclude that $F(v_1, \ldots, v_i, v_{i+1}, \ldots, v_k) = -F(v_1, \ldots, v_{i+1}, v_i, \ldots, v_k)$.

(3) $\Rightarrow$ (4). Without loss of generality, take $i < j$. Suppose $v_i = v_j$. If $j = i+1$, then we have

$$F(v_1, v_2, \ldots, v_k) = \mathbf{0}$$

by (3). So let us suppose that $j > i+1$. Note that v_j can be moved to the $(i+1)$th spot by swapping adjacent pairs successively a total of $j - i - 1$ times. Since (3) implies (2), we have

$$F(v_1, v_2, \ldots, v_i, v_j, v_{i+1}, \ldots, v_k) = (-1)^{j-i-1} F(v_1, v_2, \ldots, v_k).$$

The left side of the equation is zero by (3). Hence, $F(v_1, v_2, \ldots, v_k) = \mathbf{0}$.

(4) $\Rightarrow$ (1). Without loss of generality, take $i < j$. Replace the ith and jth arguments of $F(v_1, v_2, \ldots, v_k)$ with $u := v_i + v_j$ and expand by multilinearity:

$$F(v_1, \ldots, u, \ldots, u, \ldots, v_k) = F(v_1, \ldots, v_i, \ldots, v_i, \ldots, v_k) + F(v_1, \ldots, v_i, \ldots, v_j, \ldots, v_k) \\ + F(v_1, \ldots, v_j, \ldots, v_i, \ldots, v_k) + F(v_1, \ldots, v_j, \ldots, v_j, \ldots, v_k).$$

By (4), the left side of the equation is zero and also the first and fourth terms on the right side. Hence,

$$F(v_1, \ldots, v_i, \ldots, v_j, \ldots, v_k) = -F(v_1, \ldots, v_j, \ldots, v_i, \ldots, v_k).$$

□

Proposition 10.15. *Let*

$$F : \underbrace{V \times V \times \cdots \times V}_{k \text{ copies}} \to W$$

be an alternating k-linear map. Let $v_1, \ldots, v_k \in V$ and let $\sigma \in S_k$ be a permutation. Then

$$F(v_{\sigma(1)}, v_{\sigma(2)}, \ldots, v_{\sigma(k)}) = sgn(\sigma) F(v_1, v_2, \ldots, v_k).$$

Proof. Let $\sigma \in S_k$ be a permutation. Express σ as a product of transpositions:

$$\sigma = \tau_r \cdots \tau_2 \tau_1.$$

To go from $F(v_1, v_2, \ldots, v_k)$ to $F(v_{\sigma(1)}, v_{\sigma(2)}, \ldots, v_{\sigma(k)})$, one needs to successively swap a total of r pairs of the arguments. Since each swap causes a sign change of $F(v_1, v_2, \ldots, v_k)$, it follows that

$$F(v_{\sigma(1)}, v_{\sigma(2)}, \ldots, v_{\sigma(k)}) = (-1)^r F(v_1, v_2, \ldots, v_k).$$

From the definition of the sign of a permutation, it follows that $\operatorname{sgn}(\sigma) = (-1)^r$. From this, we have

$$F(v_{\sigma(1)}, v_{\sigma(2)}, \ldots, v_{\sigma(k)}) = \operatorname{sgn}(\sigma) F(v_1, v_2, \ldots, v_k).$$

□

This is a refinement of Theorem 10.11 for alternating multilinear maps:

Theorem 10.16. *Let V be a vector space and let F and G be alternating k-linear maps with the same range W and domain*

$$\underbrace{V \times V \times \cdots \times V}_{k \text{ copies}}.$$

Let $\{b_1, \ldots, b_n\}$ be a basis on V. Then $F = G$ if and only if

$$F(b_{i_1}, b_{i_2}, \ldots b_{i_k}) = G(b_{i_1}, b_{i_2}, \ldots b_{i_k}) \tag{173}$$

for all indices

$$1 \leq i_1 < i_1 < i_2 < \cdots < i_k \leq n.$$

Proof. ($\Rightarrow$) If $F = G$, (173) is certainly satisfied.

($\Leftarrow$) Suppose (173) holds. Let

$$i_1, i_2, \ldots, i_k \in \{1, 2, \ldots, n\}$$

be arbitrary. Since F and G are both alternating, it follows from statement (4) of Proposition 10.14 that if $i_p = i_q$ for some $p \neq q$, then

$$F(b_{i_1}, b_{i_2}, \ldots b_{i_k}) = G(b_{i_1}, b_{i_2}, \ldots b_{i_k}) = \mathbf{0}.$$

Now consider the case where

$$i_1, i_2, \ldots, i_k \in \{1, 2, \ldots, n\}$$

are all distinct. Choose a permutation $\sigma \in S_k$ such that

$$i_{\sigma(1)} < i_{\sigma(2)} < \cdots < i_{\sigma(k)}. \tag{174}$$

(173) now implies

$$F(b_{i_{\sigma(1)}}, b_{i_{\sigma(2)}}, \ldots b_{i_{\sigma(k)}}) = G(b_{i_{\sigma(1)}}, b_{i_{\sigma(1)}}, \ldots b_{i_{\sigma(1)}}) \tag{175}$$

On the other hand, Proposition 10.15 implies that

$$F(b_{i_{\sigma(1)}}, b_{i_{\sigma(2)}}, \ldots b_{i_{\sigma(k)}}) = \operatorname{sgn}(\sigma) F(b_{i_1}, b_{i_2}, \ldots b_{i_k}) \tag{176}$$

$$G(b_{i_{\sigma(1)}}, b_{i_{\sigma(2)}}, \ldots b_{i_{\sigma(k)}}) = \operatorname{sgn}(\sigma) G(b_{i_1}, b_{i_2}, \ldots b_{i_k}). \tag{177}$$

(175), (176), and (177) now imply

$$F(b_{i_1}, b_{i_2}, \dots b_{i_k}) = G(b_{i_1}, b_{i_2}, \dots b_{i_k}) \tag{178}$$

for the case where the indices $i_1, i_2, \dots, i_k \in \{1, 2, \dots, n\}$ are all distinct. We have now proven that (177) holds for **all** possible values $i_1, i_2, \dots, i_k \in \{1, 2, \dots, n\}$. Theorem 10.11 now implies that $F = G$. □

Applying Theorem 10.16 to the case of n-forms on an n-dimensional vector space V immediately yields the following:

Corollary 10.17. *Let V be an n-dimensional vector space and let ω and μ be n-forms on V. Let $\{b_1, \dots, b_n\}$. Then $\omega = \mu$ if and only if*

$$\omega(b_1, b_2, \dots, b_n) = \mu(b_1, b_2, \dots, b_n).$$

10.3. The Determinant as an n-form

Let A be an $n \times n$ matrix. In Chapter 4, we defined the determinant as the cofactor expansion along the first row:

$$\det(A) := \sum_{k=1}^{n} (-1)^{1+k} a_{1k} \det(A[1, k]) \qquad \text{for } n \geq 2, \tag{179}$$

where we recall that $A[i, j]$ denotes the matrix obtained from A by deleting its ith row and jth column. The determinant of a 1×1 matrix (a) was defined to be itself: $\det(a) := a$. With this last ingredient, the determinant of any $n \times n$ matrix can be computed using (179). For the sake of calculation, this definition is just "ok". However, in order to get a deeper understanding of the determinant, the above definition is not very satisfactory.

In this section, we prove that the determinant is really an n-form on $\mathbb{R}^n$. This turns out to be the correct way to understand what a determinant really is. Once we establish that the determinant is an n-form, we will be able to derive the properties of the determinant relatively easily. To begin, let A be an $n \times n$ matrix with $n \geq 2$. Also, let $\vec{a}_1, \dots, \vec{a}_n \in \mathbb{R}^n$ denote the columns of A. For $i \in \{1, 2, \dots, n\}$, define

$$\omega_n^{(i)}(\vec{a}_1, \dots, \vec{a}_n) := \sum_{k=1}^{n} (-1)^{i+k} a_{ik} \det(A[i, k]) \tag{180}$$

Note that the right side of (180) is the cofactor expansion along the ith row of A. To simplify notation, we will also write

$$\omega_n^{(i)}(A) := \omega_n^{(i)}(\vec{a}_1, \dots, \vec{a}_n). \tag{181}$$

From (179), we have

$$\omega_n^{(1)}(A) = \det(A) \qquad n \geq 2. \tag{182}$$

The goal for this section is the following result:

Proposition 10.18. *For any $i \in \{1, 2, \ldots, n\}$, $\omega_n^{(i)}$ is an n-form on $\mathbb{R}^n$. In particular, the determinant is an n-form on $\mathbb{R}^n$.*

Proof. We will prove this by induction on n. For $n = 1$, there is nothing to prove. Consider the $n = 2$ case. Let

$$A = \begin{pmatrix} a & c \\ b & d \end{pmatrix}.$$

For the $n = 2$ case, we have two 2-forms: $\omega_2^{(1)}$ and $\omega_2^{(2)}$. By direct calculation, we find

$$\omega_2^{(1)}(A) = \omega_2^{(2)}(A) = ad - bc.$$

The calculation carried out in Example 10.13 shows that $\omega_2^{(1)}$ and $\omega_2^{(2)}$ are 2-forms on $\mathbb{R}^2$. Now let us suppose that the result holds for the $n-1$ case form some $n \geq 3$.

Now let A be an $n \times n$ matrix. By definition,

$$\omega_n^{(i)}(A) = \sum_{k=1}^{n} (-1)^{i+k} a_{ik} \det(A[i,k]).$$

Since the $A[i,k]$'s are $(n-1) \times (n-1)$ matrices, we can rewrite the above expression using (182):

$$\omega_n^{(i)}(A) = \sum_{k=1}^{n} (-1)^{i+k} a_{ik} \omega_{n-1}^{(1)}(A[i,k]).$$

Let $\vec{v} \in \mathbb{R}^n$ and let $r \in \mathbb{R}$. Let A' be the matrix obtained from A by replacing the jth column by $\vec{v}$ and let A'' be the matrix obtained from A by replacing the jth column by $\vec{a}_j + r\vec{v}$. To prove that $\omega_n^{(i)}$ is multilinear, we need to show that

$$\omega_n^{(i)}(A'') = \omega_n^{(i)}(A) + r\omega_n^{(i)}(A'). \tag{183}$$

Let v_k denote the kth component of $\vec{v}$. Also, let a'_{kl} and a''_{kl} denote the (k,l)-element of A' and A'' respectively. Note that for $k = 1, 2, \ldots, n$

$$a_{kl} = a'_{kl} = a''_{kl}, \qquad \text{for } l \neq j \tag{184}$$

and

$$a'_{kj} = v_k, \qquad a''_{kj} = a_{kj} + rv_k. \tag{185}$$

Also, observe that for $k = 1, 2, \ldots, n$

$$A[k,j] = A'[k,j] = A''[k,j]. \tag{186}$$

Expand $\omega_n^{(i)}(A'')$ as follows:

$$\begin{aligned}\omega_n^{(i)}(A'') &= \sum_{k=1}^{n}(-1)^{i+k}a''_{ik}\omega_{n-1}^{(1)}(A''[i,k]) \\ &= (-1)^{j+k}(a_{ij}+rv_i)\omega_{n-1}^{(1)}(A''[i,j]) + \sum_{k\neq j}(-1)^{i+k}a_{ik}\omega_{n-1}^{(1)}(A''[i,k]).\end{aligned} \tag{187}$$

Using (186), the first term in (187) can be rewritten as

$$(-1)^{j+k}a_{ij}\omega_{n-1}^{(1)}(A[i,j]) + (-1)^{j+k}rv_i\omega_{n-1}^{(1)}(A'[i,j]). \tag{188}$$

Given (185) and the fact that $\omega_{n-1}^{(1)}$ is an $(n-1)$-form by hypothesis implies that the summation term in (187) can be expanded as

$$\sum_{k\neq j}(-1)^{i+k}a_{ik}\omega_{n-1}^{(1)}(A[i,k]) + r\sum_{k\neq j}(-1)^{i+k}a_{ik}\omega_{n-1}^{(1)}(A'[i,k]). \tag{189}$$

Substituting (188) and (190) into (187) and using (182) gives

$$\begin{aligned}\omega_n^{(i)}(A'') &= \sum_{k=1}^{n}(-1)^{i+k}a_{ik}\omega_{n-1}^{(1)}(A[i,k]) + r\sum_{k=1j}^{n}(-1)^{i+k}a_{ik}\omega_{n-1}^{(1)}(A'[i,k]) \\ &= \sum_{k=1}^{n}(-1)^{i+k}a_{ik}\det(A[i,k]) + r\sum_{k=1j}^{n}(-1)^{i+k}a_{ik}\det(A'[i,k]) \\ &= \omega_n^{(i)}(A) + r\omega^{(i)}(A'),\end{aligned}$$

which is the desired result we seek.

Lastly, we verify that $\omega_n^{(i)}$ is alternating. By statement (3) of Proposition 10.14, it suffices to show that if $\vec{a}_j = \vec{a}_{j+1}$ for some $j < n$, then $\omega_n^{(i)}(A) = 0$. So let us suppose that $\vec{a}_j = \vec{a}_{j+1}$ for some $j < n$. Expanding $\omega_n^{(i)}(A)$ gives

$$\begin{aligned}\omega_n^{(i)}(A) &= \sum_{k=1}^{n}(-1)^{i+k}a_{ik}\det(A[i,k]) \\ &= \sum_{k=1}^{n}(-1)^{i+k}a_{ik}\omega_{n-1}^{(1)}(A[i,k]) \\ &= (-1)^{i+j}a_{ij}\omega_{n-1}^{(1)}(A[i,j]) + (-1)^{i+j+1}a_{i,j+1}\omega_{n-1}^{(1)}(A[i,j+1]) \\ &+ \sum_{k\neq j,j+1}(-1)^{i+k}a_{ik}\omega_{n-1}^{(1)}(A[i,k]).\end{aligned} \tag{190}$$

Since $\vec{a}_j = \vec{a}_{j+1}$, we have $A[i,j] = A[i,j+1]$ and $a_{ij} = a_{i,j+1}$. This implies that the first two terms in (190) sum to zero. For the summation in (190), note that $A[i,k]$ for $k \neq j, j+1$ contains two identical adjacent columns. By the induction hypothesis, $\omega_{n-1}^{(1)}$ is an $(n-1)$-form. This implies that $\omega_{n-1}^{(1)}(A[i,k]) = 0$ for $k \neq j, j+1$. Hence, the summation term in (190) is also zero. Hence, $\omega_n^{(i)}(A) = 0$ as desired. □

Corollary 10.19. $\omega_n^{(1)} = \omega_n^{(i)}$ *for* $i = 1, 2, \ldots, n$.

Proof. By Proposition 10.18, $\omega_n^{(i)}$ are n-forms on $\mathbb{R}^n$ for $i = 1, 2, \ldots, n$. Let

$$\vec{e}_1, \ldots, \vec{e}_n$$

be the standard basis on $\mathbb{R}^n$. By direct inspection, we have

$$\omega_n^{(i)}(\vec{e}_1, \ldots, \vec{e}_n) = 1 \tag{191}$$

for $i = 1, 2, \ldots, n$. Corollary 10.17 implies that

$$\omega_n^{(1)} = \omega_n^{(2)} = \cdots = \omega_n^{(n)}.$$

□

We can now prove half of the Cofactor Expansion Theorem (Theorem 4.10):

Corollary 10.20. *Let* A *be an* $n \times n$ *matrix with* $n \geq 2$. *Then for* $i = 1, 2, \ldots, n$

$$\det(A) = \sum_{k=1}^{n} (-1)^{k+i} a_{ik} \det(A[i,k]).$$

Proof. Using (182) and Corollary 10.19, we have

$$\begin{aligned} \det(A) &= \omega_n^{(1)}(A) \\ &= \omega^{(i)}{}_n(A) \\ &= \sum_{k=1}^{n} (-1)^{i+k} a_{ik} \det(A[i,k]). \end{aligned}$$

□

Let A be an $n \times n$ matrix with $n \geq 2$ and let $\vec{a}_i$ be the ith column of A. To emphasize that the determinant is really an n-form, we will occasionally write

$$\det(\vec{a}_1, \vec{a}_2, \ldots, \vec{a}_n) := \det(A).$$

We conclude this section with a proof of the behavior of the determinant under column operations (see Theorem 4.15):

Corollary 10.21. *Let A be an $n \times n$ matrix with $n \geq 2$ and let $\vec{a}_i$ denote the ith column of A.*

(i) Let A_1 be the matrix obtained from A by swapping columns $\vec{a}_i$ and $\vec{a}_j$ for $i \neq j$. Then $\det(A_1) = -\det(A)$.

(ii) Let A_2 be the matrix obtained from A by replacing $\vec{a}_i$ by $c\vec{a}_i$ for $c \in \mathbb{R}$. Then $\det(A_2) = c\det(A)$.

(iii) Let A_3 be the matrix obtained from A by replacing the jth column by $r\vec{a}_i + \vec{a}_j$ for $r \in \mathbb{R}$ and $i \neq j$. Then $\det(A_3) = \det(A)$.

Proof. For (i), take $i < j$ without loss of generality. Then we have

$$\begin{aligned}\det(A_1) &= \det(\vec{a}_1, \ldots, \vec{a}_j, \ldots, \vec{a}_i, \ldots, \vec{a}_k) \\ &= - = \det(\vec{a}_1, \ldots, \vec{a}_i, \ldots, \vec{a}_j, \ldots, \vec{a}_k) \\ &= -\det(A).\end{aligned}$$

For (ii), we have

$$\begin{aligned}\det(A_2) &= \det(\vec{a}_1, \vec{a}_2, \ldots, c\vec{a}_i, \ldots, \vec{a}_k) \\ &= c\det(\vec{a}_1, \vec{a}_2, \ldots, \vec{a}_i, \ldots, \vec{a}_k) \\ &= c\det(A).\end{aligned}$$

Lastly, for (iii), take $i < j$ without loss of generality. Then we have

$$\begin{aligned}\det(A_3) &= \det(\vec{a}_1, \ldots, \vec{a}_i, \ldots, c\vec{a}_i + \vec{a}_j, \ldots, \vec{a}_k) \\ &= c\det(\vec{a}_1, \ldots, \vec{a}_i, \ldots, \vec{a}_i, \ldots, \vec{a}_k) + \det(\vec{a}_1, \ldots, \vec{a}_i, \ldots, \vec{a}_j, \ldots, \vec{a}_k) \\ &= 0 + \det(\vec{a}_1, \ldots, \vec{a}_i, \ldots, \vec{a}_j, \ldots, \vec{a}_k) \\ &= \det(A).\end{aligned}$$

□

To use an old tired saying, understanding the determinant via (179) is a case of missing the forest for the trees. It is only after coming to the realization that the determinant is an n-form does the forest finally comes into view.

10.4. Explicit Formula

Let A be an $n \times n$ matrix with $n \geq 2$. Let $\vec{a}_i$ denote the ith column of A and let a_{ij} denote the (i, j)-element of A. Also, let $\vec{e}_i$ denote the ith standard basis. Then

$$\vec{a}_j = \sum_{i=1}^{n} a_{ij}\vec{e}_i.$$

In the last section, we showed that the determinant is an n-form on $\mathbb{R}^n$ which takes the value 1 on the standard basis. Let us expand $\det(A)$ using multilinearity:

$$\begin{aligned}\det(A) &= \det(\vec{a}_1, \vec{a}_2, \ldots, \vec{a}_n)\\ &= \sum_{i_1=1}^{n}\sum_{i_2=1}^{n}\cdots\sum_{i_n=1}^{n} a_{i_1 1}a_{i_2 2}\cdots a_{i_n n}\det(\vec{e}_{i_1}, \vec{e}_{i_2}, \ldots, \vec{e}_{i_n}). \qquad (192)\end{aligned}$$

Consider an arbitrary term in the sum:

$$a_{i_1 1}a_{i_2 2}\cdots a_{i_n n}\det(\vec{e}_{i_1}, \vec{e}_{i_2}, \ldots, \vec{e}_{i_n}). \qquad (193)$$

Each of the above indices i_k, $k = 1, 2, \ldots, n$, can take on any value from 1 to n. Since the determinant is an n-form, if there is any repetition in the set

$$i_1, i_2, \ldots, i_n, \qquad (194)$$

then (193) is exactly zero. Hence, the potentially nonzero terms in the sum (192) are those for which (194) is a permutation of $1, 2, \ldots, n$. Hence, for each of these terms, there is a unique permutation $\sigma \in S_n$ such that

$$i_k = \sigma(k) \qquad \text{for } k = 1, 2, \ldots, n. \qquad (195)$$

If (193) consists of entirely distinct indices, then by Proposition 10.15, we have

$$\operatorname{sgn}(\sigma)a_{\sigma(1)1}a_{\sigma(2)2}\cdots a_{\sigma(n)n}\det(\vec{e}_1, \vec{e}_2, \ldots, \vec{e}_n). \qquad (196)$$

Moreover, since the determinant takes the value 1 on the standard basis (in other words $\det(I_n) = 1$), (196) can be further simplified to

$$\operatorname{sgn}(\sigma)a_{\sigma(1)1}a_{\sigma(2)2}\cdots a_{\sigma(n)n}. \qquad (197)$$

Hence, every potentially nonzero term in (192) is of this form for some unique $\sigma \in S_n$. So by throwing out the terms with repeating indices in (192) (which are zero) and rewriting those with distinct indices in the form of (197) yields the explicit formula for the determinant:

Theorem 10.22. *Let A be an $n \times n$ matrix. Then*

$$\det(A) = \sum_{\sigma\in S_n} sgn(\sigma)a_{\sigma(1)1}a_{\sigma(2)2}\cdots a_{\sigma(n)n}.$$

We now give an alternate proof of Theorem 4.23 using the explicit formula for the determinant:

Theorem 10.23. *Let A be an $n \times n$ matrix. Then* $\det(A^T) = \det(A)$.

Proof. Let a_{ij} denote the (i,j)-element of A. Also, let $B = A^T$ and let b_{ij} denote the (i,j)-element of B. Using Theorem 10.22, we have

$$\begin{aligned}\det(A^T) &= \det(B) \\ &= \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) b_{\sigma(1)1} b_{\sigma(2)2} \cdots b_{\sigma(n)n} \\ &= \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) a_{1\sigma(1)} a_{2\sigma(2)} \cdots a_{n\sigma(n)}. \qquad (198)\end{aligned}$$

Consider an arbitrary term in the sum:

$$\operatorname{sgn}(\sigma) a_{1\sigma(1)} a_{2\sigma(2)} \cdots a_{n\sigma(n)}. \qquad (199)$$

Let σ^{-1} be the inverse map of σ. Note that $\operatorname{sgn}(\sigma^{-1}) = \operatorname{sgn}(\sigma)$. Using this fact, we can rewrite the above term as

$$\operatorname{sgn}(\sigma^{-1}) a_{\sigma^{-1}(\sigma(1))\sigma(1)} a_{\sigma^{-1}(\sigma(2))\sigma(2)} \cdots a_{\sigma^{-1}(\sigma(n))\sigma(n)} \qquad (200)$$

As sets, $\{\sigma(1), \sigma(2), \ldots, \sigma(n)\}$ and $\{1, 2, \ldots, n\}$ contain the same elements. (The only difference, of course, is the order of these sets.) So by simply rearranging the factors in (200), we see that (200) can be rewritten as

$$\operatorname{sgn}(\sigma^{-1}) a_{\sigma^{-1}1} a_{\sigma^{-1}(2)2} \cdots a_{\sigma^{-1}(n)n}. \qquad (201)$$

Using (201), we can rewrite (198) as

$$\det(A^T) = \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma^{-1}) a_{\sigma^{-1}1} a_{\sigma^{-1}(2)2} \cdots a_{\sigma^{-1}(n)n} \qquad (202)$$

Lastly, since the map from S_n to itself which sends σ to its inverse σ^{-1} is a bijection, it follows that the sum in (202) is equal to

$$\det(A^T) = \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) a_{\sigma(1)1} a_{\sigma(2)2} \cdots a_{\sigma(n)n} \qquad (203)$$

which is precisely the explicit formula for $\det(A)$. Hence, $\det(A^T) = \det(A)$. □

Corollary 10.24. *Let A be an $n \times n$ matrix for $n \geq 2$. Then for $j = 1, 2, \ldots, n$*

$$\det(A) = \sum_{k=1}^{n} (-1)^{k+j} a_{kj} \det(A[k,j]).$$

Proof. Let $B = A^T$. Using Corollary 10.20 and Theorem 10.23, we have

$$\begin{aligned}\det(A) &= \det(A^T)\\ &= \det(B)\\ &= \sum_{k=1}^{n}(-1)^{j+k} b_{jk} \det(B[j,k])\\ &= \sum_{k=1}^{n}(-1)^{j+k} a_{kj} \det(A^T[j,k])\\ &= \sum_{k=1}^{n}(-1)^{j+k} a_{kj} \det(A[k,j]^T)\\ &= \sum_{k=1}^{n}(-1)^{j+k} a_{kj} \det(A[k,j]).\end{aligned}$$

□

Remark 10.25. *Corollaries 10.20 and 10.24 prove the Cofactor Expansion Theorem (Theorem 4.10).*

The proof of Theorem 4.15 is obtained by combining Corollary 10.21 with the following result:

Corollary 10.26. *Let A be an $n \times n$ matrix with $n \geq 2$ and let R_i denote the ith row of A.*

(i) Let A_1 be the matrix obtained from A by swapping rows R_i and R_j for $i \neq j$. Then $\det(A_1) = -\det(A)$.

(ii) Let A_2 be the matrix obtained from A by replacing R_i by cR_i for $c \in \mathbb{R}$. Then $\det(A_2) = c\det(A)$.

(iii) Let A_3 be the matrix obtained from A by replacing the jth row by $cR_i + R_j$ for $c \in \mathbb{R}$ and $i \neq j$. Then $\det(A_3) = \det(A)$.

Proof. Let $B = A^T$ and let $\vec{b}_i$ denote the ith column of B. Then $\vec{b}_i = R_i^T$. To prove (i)-(iii), we apply Corollary 10.21 and Theorem10.23.

(i): Let $B_1 = A_1^T$. Then B_1 is the matrix obtained from B by swapping columns $\vec{b}_i$ and $\vec{b}_j$. Hence,

$$\det(A_1) = \det(A_1^T) = \det(B_1) = -\det(B) = -\det(A^T) = -\det(A).$$

(ii): Let $B_2 = A_2^T$. Then B_2 is the matrix obtained from B by scaling $\vec{b}_i$ by c. Hence,

$$\det(A_2) = \det(A_2^T) = \det(B_2) = c\det(B) = c\det(A^T) = c\det(A).$$

(iii): Let $B_3 = A_3^T$. Then B_3 is the matrix obtained from B by replacing column j by $c\vec{b}_i + \vec{b}_j$. Hence,

$$\det(A_3) = \det(A_3^T) = \det(B_3) = \det(B) = \det(A^T) = \det(A).$$

□

We conclude this chapter with a proof of the multiplicative property of the determinant (Theorem 4.19).

Theorem 10.27. *Let A and B be $n \times n$ matrices. Then* $\det(AB) = \det(A)\det(B)$.

Proof. The $n = 1$ case is trivial so let us assume $n \geq 2$. To prove Theorem 10.27, we make use of the fact that the determinant is an n-form on $\mathbb{R}^n$. Let $\vec{a}_i$ and $\vec{b}_i$ denote the ith columns of A and B respectively. Let a_{ij} and b_{ij} denote the (i, j)-elements of A and B respectively. Then

$$\det(AB) = \det(A\vec{b}_1, A\vec{b}_2, \ldots, A\vec{b}_n).$$

Expand the vector $A\vec{b}_i$:

$$A\vec{b}_i = b_{1i}\vec{a}_1 + b_{2i}\vec{a}_2 + \cdots + b_{ni}\vec{a}_n.$$

Since the determinant is an n-form (and hence multilinear), we have

$$\det(AB) = \sum_{i_1=1}^{n} \sum_{i_2=1}^{n} \cdots \sum_{i_n=1}^{n} b_{i_1 1} b_{i_2 2} \cdots b_{i_n n} \det(\vec{a}_{i_1}, \vec{a}_{i_2}, \ldots, \vec{a}_{i_n}). \tag{204}$$

Consider an arbitrary term in the sum:

$$b_{i_1 1} b_{i_2 2} \cdots b_{i_n n} \det(\vec{a}_{i_1}, \vec{a}_{i_2}, \ldots, \vec{a}_{i_n}). \tag{205}$$

Since the determinant is an n-form, if there is any repetition in the indices $i_1, i_2, \ldots, i_n$, the above term will be zero. Hence, the only terms which contribute to (204) are those for which $\{i_1, i_2, \ldots, i_n\}$ is equal to $\{1, 2, \ldots, n\}$ as **unordered** sets. In this case, there is a unique permutation $\sigma \in S_n$ such that

$$\sigma(k) = i_k.$$

So if $\{i_1, i_2, \ldots, i_n\}$ are all distinct, we can use Proposition 10.15 to rewrite (204) as

$$\operatorname{sgn}(\sigma) b_{\sigma(1)1} b_{\sigma(2)2} \cdots b_{\sigma(n)n} \det(\vec{a}_1, \vec{a}_2, \ldots, \vec{a}_n). \tag{206}$$

Since $\det(A) = \det(\vec{a}_1, \vec{a}_2, \ldots, \vec{a}_n)$, we can further simplify to

$$\operatorname{sgn}(\sigma) b_{\sigma(1)1} b_{\sigma(2)2} \cdots b_{\sigma(n)n} \det(A). \tag{207}$$

So discarding all the terms with repeating indices and rewriting those with distinct indices in the form of (207), we can rewrite (204) as

$$\begin{aligned}\det(AB) &= \sum_{\sigma\in S_n} \operatorname{sgn}(\sigma) b_{\sigma(1)1} b_{\sigma(2)2} \cdots b_{\sigma(n)n} \det(A) \\ &= \left(\sum_{\sigma\in S_n} \operatorname{sgn}(\sigma) b_{\sigma(1)1} b_{\sigma(2)2} \cdots b_{\sigma(n)n}\right) \det(A) \\ &= \det(B)\det(A) \\ &= \det(A)\det(B),\end{aligned}$$

where the second to last equality follows from the explicit formula for $\det(B)$. □

Chapter 10 Exercises

1. Let $\sigma \in S_6$ be the permutation given by
$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 5 & 1 & 4 & 6 \end{pmatrix}.$$
Write σ as a product of transpositions. What is the sign of σ?

2. A p-cycle in S_n is a permutation which is a generalization of a transposition. For example, the 3-cycle $(1, 3, 2)$ in S_5 is the permutation which maps 1 to 3, 3 to 2, and 2 to 1 and maps all other numbers to themselves. Explicitly, $(1, 3, 2)$ is given by
$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 2 & 4 & 5 \end{pmatrix}.$$
A transposition is then a 2-cycle. Write a p-cycle $(i_1, i_2, \ldots, i_p) \in S_n$ as a product of transpositions. What is the sign of a p-cycle?

3. Write every element of S_3 using the cycle notation introduced in Problem 2.. Also, determine the sign of each element in S_3.

4. Let V be a real vector space and suppose ω is a 2-form on V which satisfies the following condition:
$$\omega(u, v) = 0 \quad \forall\, v \in V \iff u = \mathbf{0}.$$
A 2-form which satisfies the above condition is called **nondegenerate** or **symplectic**. The pair (V, ω) is called a **symplectic vector space**. Show that if (V, ω) is a symplectic vector space, then there exists a basis of V of the form
$$\mathcal{B} = \{e_1, e_2, \ldots, e_n, f_1, f_2, \ldots, f_n\}$$
such that
$$\omega(e_i, f_j) = \begin{cases} 1 & \text{if } i = j \\ 0 & \text{if } i \neq j \end{cases}$$

and

$$\omega(e_i, e_j) = \omega(f_i, f_j) = 0, \qquad \text{for all } i, j.$$

The basis $\mathcal{B}$ is called a **symplectic vector space**. In particular, conclude that every symplectic vector space is necessarily even dimensional.

5. Let (V, ω) be a symplectic vector space (see Problem 4.). Let $W \subset V$ be a subspace. Define

$$W^\omega := \{v \in V \mid \omega(v, w) = 0 \ \forall \ w \in W\}.$$

W^ω is called the ω-orthogonal complement of W.

(a) Show that $\dim W + \dim W^\omega = \dim V$.

(b) Show that $(W^\omega)^\omega = W$.

(c) Construct a subspace L of V such that $\dim L = \frac{1}{2} \dim V$ and $L^\omega = L$. Such a subspace is called a **Lagrangian subspace** of (V, ω). (Hint: use Problem 4.).

(d) Show that in general V is not a direct sum of W and W^ω. (Hint: use (c)).

6. Consider the vector space $\mathbb{R}^2$ and define $\omega(\vec{u}, \vec{v}) := \det(\vec{u}, \vec{v})$ for all $\vec{u}, \vec{v} \in \mathbb{R}^2$.

(a) Show that $(\mathbb{R}^2, \omega)$ is a symplectic vector space (see Problem 4.).

(b) Let $\vec{e}_1, \vec{e}_2$ denote the standard basis on $\mathbb{R}^2$. Show that $\vec{e}_1, \vec{e}_2$ is a symplectic basis on $(\mathbb{R}^2, \omega)$.

(c) Let W_i be the subspace spanned by $\vec{e}_i$ for $i = 1, 2$. Show that W_i is a Lagrangian subspace of $(\mathbb{R}^2, \omega)$ for $i = 1, 2$ (see Problem 5.)

7. Let

$$A = \begin{pmatrix} 1 & -2 & 1 \\ 0 & 2 & 1 \\ 2 & 1 & 1 \end{pmatrix}.$$

(a) Compute $\det(A)$ using the explicit formula for the determinant. (Use Problem 3.)

(b) Check your answer in (a) by computing $\det(A)$ using a cofactor expansion.

8. Let $\vec{u}, \vec{v} \in \mathbb{R}^2$ be linearly independent. Show that $\det(\vec{u}, \vec{v})$ is the area of the parallelogram formed from $\vec{u}, \vec{v}$.

9. Let $\vec{u}, \vec{v}, \vec{w} \in \mathbb{R}^3$ be linearly independent. Show that $\det(\vec{u}, \vec{v}, \vec{w})$ is the volume of the parallelepiped formed by $\vec{u}, \vec{v}, \vec{w}$.

10. Let V be a real vector space. Let $\mathcal{B}_1$ and $\mathcal{B}_2$ be bases of V. $\mathcal{B}_1$ is said to have the same **orientation** as $\mathcal{B}_2$ if $\det(P_{\mathcal{B}_1\mathcal{B}_2}) > 0$, where $P_{\mathcal{B}_1\mathcal{B}_2}$ is the transition matrix from $\mathcal{B}_2$ to $\mathcal{B}_1$. We abbreviate the condition of vector space orientation by writing $\mathcal{B}_1 \sim \mathcal{B}_2$.

(a) Show that $\mathcal{B}_1 \sim \mathcal{B}_1$.
(b) Show that if $\mathcal{B}_1 \sim \mathcal{B}_2$, then $\mathcal{B}_2 \sim \mathcal{B}_1$.
(c) Show that if $\mathcal{B}_3$ is a basis of V and $\mathcal{B}_1 \sim \mathcal{B}_2$ and $\mathcal{B}_2 \sim \mathcal{B}_3$, then $\mathcal{B}_1 \sim \mathcal{B}_3$.

Conditions (a) through (c) prove that the idea of vector space orientation is an **equivalence relation**, a notion which we will introduce in Chapter 11.

Chapter 11

Quotient Vector Spaces

Quotient vector spaces are one of the most common and important constructions in mathematics for generating new vector spaces from existing vector spaces. Before we get to the business of actually defining and studying quotient vector spaces, we would like to take a moment to give some motivation for quotient vector spaces.

One of the most striking applications of quotient vector spaces occurs in a branch of mathematics called *algebraic topology.* First, *topology* is a branch of mathematics which regards spaces as being made of clay. In other words, in topology, spaces can be stretched, compressed, and deformed in a *continuous* manner. Two spaces are considered the same in topology if one space can be continuously deformed into the other without tearing the space in the process. For example, from the standpoint of topology, a cube is the same as a sphere since one can continuously deform the cube into the sphere without tearing the cube in the process. On the other hand, a donut or *torus* is not the same as a sphere (topologically speaking) since deforming the sphere into the torus would create tears in the sphere. The primary question in topology then is to determine when two spaces can be considered the same from the point of view of clay. In general, this is a very hard question to answer. It turns out to be somewhat easier to determine when two spaces are different. This question leads to algebraic topology, which is the application of *abstract* algebra to topology. One of the main tools of algebraic topology are certain objects called *cohomology groups.* Now the definition of cohomology groups is far outside the scope of a linear algebra textbook so we will make no effort to define them. However, the point of cohomology groups is this: *two spaces which produce different sets of cohomology groups cannot be topologically equivalent.* At this point, the reader is no doubt wondering what any of this has to do with quotient vector spaces. The answer is everything! At the end of the day, cohomology groups, at their most fundamental level, are nothing but quotient vector spaces! In essence then, quotient vector spaces can be used to distinguish one shape from that of another. Of course, the details of how this is done exactly is far outside the scope of this book. Even so, this example does highlight one of the most important applications of quotient vector spaces. With that said, we now turn to the business of actually defining and studying quotient vector spaces.

11.1. Quotient Vector Spaces

In this section, we will work our way towards the definition of a quotient vector space. We begin with the definition of an *equivalence relation* which generalizes the notion of equality between two elements in a set.

Definition 11.1. *Let S be a set. A* ***binary relation*** *on S is simply a subset $R \subset S \times S$. If $(a, b) \in R$, one writes $a \sim b$. One often suppresses any mention of R and simply refers to $\sim$ as the binary relation.*

An ***equivalence relation*** *on S is a binary relation $\sim$ which satisfies the following conditions:*

(i) $a \sim a$ for all $a \in S$ (reflexive property)
(ii) if $a \sim b$ for some $a, b \in S$, then $b \sim a$ (symmetric property)
(iii) if $a \sim b$ and $b \sim c$ for some $a, b, c \in S$, then $a \sim c$ (transitive property)

For $a \in S$, the set

$$[a] := \{b \in S \mid b \sim a\}$$

is called the **equivalence class** of a. The element a is said to be a **representative** of $[a]$. The set of all equivalence classes of S is denoted as $S/\sim$. $S/\sim$ is called the **quotient set** of the equivalence relation.

Remark 11.2. *Let V be a vector space and let $\mathcal{B}$ be a basis on V. Recall that we denote the coordinate representation of a vector $v \in V$ with respect to $\mathcal{B}$ by $[v]_{\mathcal{B}}$. While this notation is similar to the notation used for equivalence classes, coordinate representations have nothing to do with equivalence classes. Hence, the reader should not confuse these two ideas. Likewise, matrix representations have nothing to do with equivalence classes.*

Example 11.3. *Let S be any set and let $R \subset S \times S$ be the binary relation defined by*

$$R := \{(a, a) \mid a \in S\}.$$

Clearly, R satisfies the three conditions of Definition 11.1 and is thus an equivalence relation. Of course, the equivalence relation $\sim$ associated to R is none other than the usual notion of equality. In other words, $\sim$ is simply $=$ here. The equivalence class associated to $a \in S$ is simply the one element subset $[a] = \{a\}$. Hence, the quotient set $S/\sim$ is simply S in this case.

Theorem 11.4. *Let S be a set and let $\sim$ be an equivalence relation on S. For any $a, b \in S$, there are only two possibilities: $[a] \cap [b] = \emptyset$ or $[a] = [b]$. In particular, S is a (disjoint) union of its equivalence classes.*

Proof. Let $a, b \in S$. If $[a] = [b]$, we are done. So suppose that $[a] \neq [b]$. We need to show that $[a]$ and $[b]$ are disjoint sets. Let us suppose this is not the case, that is, $[a] \cap [b] \neq \emptyset$. Let $c \in [a] \cap [b]$. From the definition of equivalence classes, we have $c \sim a$ and $c \sim b$. By the symmetric property of equivalence relations, we also have $a \sim c$. The transitive property now implies that $a \sim b$, which means that $b \in [a]$. Now let $x \in [a]$ be any arbitrary element. By definition, we have $x \sim a$. Since $a \sim b$, we also have $x \sim b$ which in turn implies that $x \in [b]$. Since $x \in [a]$ was arbitrary, we conclude that $[a] \subset [b]$. A similar argument shows that $[a] \supset [b]$. From this, we conclude that $[a] = [b]$, which is a contradiction. Since we arrived at this contradiction by assuming $[a] \cap [b] \neq \emptyset$, we conclude that our assumption is wrong. In other words, $[a] \cap [b] = \emptyset$.

For the last statement, let $E := S/\sim$ denote the set of all equivalence classes of S. Let

$$X := \bigcup_{[a] \in E} [a].$$

This is a disjoint union by the first statement of Theorem 11.4, that is, given two distinct equivalence classes $[a]$ and $[b]$, we must have $[a] \cap [b] = \emptyset$. Clearly, we have $X \subset S$. Now, let $a \in S$ be arbitrary. By the reflexive property, we have $a \in [a]$. Since $[a] \in E$, it follows that $a \in X$, which in turn implies that $S \subset X$. From this, we conclude that $X = S$. This completes the proof. □

Remark 11.5. *The proof of Theorem 11.4 is an example of proof by contradiction. Proof by induction and proof by contradiction are two of the most powerful strategies used in mathematics for proving a claim.*

We now have the necessary background to define quotient vector spaces. Let V be a vector space and W a subspace of V. Let $R_W^V \subset V \times V$ be the binary relation given by

$$R_W^V := \{(v, v') \mid v, v' \in V \text{ and } v - v' \in W\}. \tag{208}$$

In other words, we write $v \sim v'$ if and only if $v - v' \in W$. The following result will prove to be essential to the definition of quotient vector spaces:

Theorem 11.6. *Let V be a vector space and W a subspace of V. Let $\sim$ be the binary relation determined by the set $R_W^V \subset V \times V$. Then $\sim$ is an equivalence relation.*

Proof. To prove the reflexive property, let $v \in V$. Since W is a subspace of V, W contains the zero element $\mathbf{0}$. Consequently, $v - v = \mathbf{0} \in W$. This shows that $v \sim v$.

For the symmetric property, let us suppose that $v \sim v'$ for some $v, v' \in V$. By definition, this means that $v - v' \in W$. Since W is a subspace of V, any scalar multiple of $v - v'$ is also in W. In particular, we have

$$-(v - v') = v' - v \in W.$$

From this, we have $v' \sim v$.

Lastly, for the transitive property, let us suppose that $v \sim v'$ and $v' \sim v''$ for some $v, v', v'' \in V$. Then $v - v'$ and $v' - v''$ are both in W. Since W is a subspace, the sum of any two elements of W is again in W. In particular, we have

$$(v - v') + (v' - v'') = v - v'' \in W.$$

From this, we have $v \sim v''$. This completes the proof. $\square$

Here (at last) is the definition of quotient vector spaces:

Definition 11.7. *Let V be a vector space over a field $\mathbb{F}$ and let W be a subspace of V. Let $R_W^V \subset V \times V$ be defined by (208) and let $\sim$ be the equivalence relation determined by R_W^V. The **quotient vector space** is the quotient set $V/\sim$ equipped with the following vector space structure:*

(i) (vector addition) $[u] + [v] := [u + v]$ for all $u, v \in V$
(ii) (scalar multiplication) $c[v] := [cv]$ for all $c \in \mathbb{F}$ and $v \in V$.

*The quotient vector space $V/\sim$ is denoted as V/W which one reads as "V mod W". The equivalence class $[v]$ represented by v is called the **coset** of u.*

Once again, we would like to stress to the reader that the element $[v] \in V/W$ is an equivalence class and not a coordinate representation of v. (This should be quite clear since we have not specified any basis and the notion of a coordinate representation is meaningless without fixing a basis on V.)

Now that we have defined the quotient vector space, we have to actually verify that V/W is indeed a vector space. However, before we can do that, we first have to show that the definition of vector addition and scalar multiplication appearing in Definition 11.7 is well-defined, that is, it is independent of the choice of equivalence class or coset representatives. The next result does just that.

Proposition 11.8. *Let V be a vector space over $\mathbb{F}$ and let W be a subspace of V. If $[u] = [u']$ and $[v] = [v']$ for some $u, u \in V$ and $v, v' \in V$, then*

(i) $[u + v] = [u' + v']$

(ii) $[cv] = [cv']$ *for all* $c \in \mathbb{F}$

Proof. Suppose that $[u] = [u']$ and $[v] = [v']$ for some $u, u' \in V$ and $v, v' \in V$. Let $\sim$ be the equivalence relation on V determined by R_W^V. In other words, for $x, y \in V$, we have $x \sim y$ if and only if $x - y \in W$.

By Theorem 11.6, $\sim$ is an equivalence relation. Hence, $u' \in [u']$ by the reflexive property. Since $[u'] = [u]$, we also have $u' \in [u]$ which implies that $u' \sim u$. In other words, $w_1 := u' - u \in W$. Likewise, since $[v] = [v']$, it follows that $w_2 := v' - v \in W$. From this, we have

$$u' = u + w_1, \qquad v' = v + w_2.$$

Consequently,

$$\begin{aligned} (u' + v') - (u + v) &= (u + w_1 + v + w_2) - (u + v) \\ &= w_1 + w_2 \\ &\in W, \end{aligned}$$

where the last equality follows from the fact that W is a subspace. Hence, $u' + v' \sim u + v$. From this, we have $u' + v' \in [u + v]$. Since we also have $u' + v' \in [u' + v']$, we see that $[u + v] \cap [u' + v'] \neq \emptyset$. Since $\sim$ is an equivalence relation, Theorem 11.4 implies that $[u + v] = [u' + v']$. This proves (i).

For (ii), let $c \in \mathbb{F}$. Then

$$\begin{aligned} cv' - cv &= c(v' - v) \\ &= c(v + w_2 - v) \\ &= cw_2 \\ &\in W, \end{aligned}$$

where the last equality follows from the fact that W is a subspace. Hence, $cv' \sim cv$. From this, we have $cv' \in [cv]$. Since we also have $cv' \in [cv']$, we see that $[cv] \cap [cv'] \neq \emptyset$. Since $\sim$ is an equivalence relation, Theorem 11.4 implies that $[cv] = [cv']$. This proves (ii). □

Now that we know that the vector addition and scalar multiplication operations are well-defined, it is a straightforward matter to check that the quotient vector space V/W satisfies all the axioms of a vector space given in Definition 5.4.

Exercise 11.9. *Let V be a vector space and let W be a subspace. Show that V/W with vector addition and scalar multiplication given by (i) and (ii) in Definition 11.7 satisfies all the axioms of a vector space (see Definition 5.4). In particular, show that the zero vector of V/W is simply the coset $[\mathbf{0}]$ and that the additive inverse of a coset $[v]$ is $[-v]$.*

For convenience, we record the following simple fact:

Proposition 11.10. *Let V be a vector space and let W be a subspace.*

(i) The coset of $v \in V$ in V/W is

$$[v] = \{w + v \mid w \in W\}. \tag{209}$$

(ii) $[v] = [\mathbf{0}]$ if and only if $v \in W$.

(209) is often denoted more concisely by writing $[v] = W + v$.

Proof. For (i), let $u \in [v]$ be arbitrary. It follows then that $u - v \in W$. Setting $w := u - v$, we have $u = w + v$. Hence, we have shown

$$[v] \subset \{w + v \mid w \in W\}.$$

For the reverse inclusion, let $w \in W$ be arbitrary and let $v' := w + v$. Clearly, we have $v' - v \in W$, which implies that $v' \in [v]$. Hence, we have

$$[v] \supset \{w + v \mid w \in W\}.$$

This proves (209).

For (ii), we simply observe that

$$[v] = [\mathbf{0}] \Longleftrightarrow v \in [\mathbf{0}] \Longleftrightarrow v - \mathbf{0} = v \in W.$$

This completes the proof. □

What is the dimension of V/W? What does a basis on V/W look like? These are some natural questions about the quotient vector space. The answers to these particular questions are given by the following result:

Theorem 11.11. *Let V be a vector space and let W be a subspace. Let $\mathcal{B} := \{w_1, \ldots, w_k\}$ be a basis on W and let $\mathcal{C} := \{w_1, \ldots, w_k, x_1, \ldots, x_{n-k}\}$ be any basis on V which extends $\mathcal{B}$, where $k := \dim W$ and $n := \dim V$. Then*

$$\{[x_1], \ldots, [x_{n-k}]\}$$

is a basis on V/W. In particular, $\dim V/W = \dim V - \dim W$.

Proof. Let $v \in V$ and express v as a (unique) linear combination of the basis $\mathcal{C}$:

$$v = a_1 w_1 + \cdots a_k w_k + b_1 x_1 + \cdots + b_{n-k} x_{n-k}.$$

From Definition 11.7, we have

$$\begin{aligned}
[v] &= [a_1 w_1 + \cdots a_k w_k + b_1 x_1 + \cdots + b_{n-k} x_{n-k}] \\
&= [a_1 w_1] + \cdots + [a_k w_k] + [b_1 x_1] + \cdots + [b_{n-k} x_{n-k}] \\
&= [\mathbf{0}] + \cdots + [\mathbf{0}] + b_1 [x_1] + \cdots + b_{n-k} [x_{n-k}] \\
&= b_1 [x_1] + \cdots + b_{n-k} [x_{n-k}]
\end{aligned}$$

where the third equality follows from statement (ii) of Proposition 11.10. Hence,

$$V/W = \operatorname{span}\{[x_1], \ldots, [x_{n-k}]\}.$$

To complete the proof, we we need to verify that the above vectors are linearly independent. So suppose that

$$c_1 [x_1] + \cdots c_{n-k} [x_{n-k}] = [\mathbf{0}]. \tag{210}$$

(210) can be rewritten as

$$[c_1 x_1 + \cdots + c_{n-k} x_{n-k}] = [\mathbf{0}].$$

Statement (ii) of Proposition 11.10 implies that

$$c_1 x_1 + \cdots + c_{n-k} x_{n-k} \in W. \tag{211}$$

Since $\mathcal{B} := \{w_1, \ldots, w_k\}$ is a basis on W and $\mathcal{C} := \{w_1, \ldots, w_k, x_1, \ldots, x_{n-k}\}$ is a basis on V, (211) implies that $c_i = 0$ for $i = 1, \ldots, n-k$, which proves that $[x_1], \ldots, [x_{n-k}]$ is also linearly independent. This completes the proof. □

Example 11.12. *Let $\mathbb{R}[x]_n$ denote the vector space of real polynomials of degree n or less. Consider the vector space $\mathbb{R}[x]_5$. Since $\mathbb{R}[x]_2$ is a subspace of $\mathbb{R}[x]_5$, we can form the quotient vector space $\mathbb{R}[x]_5/\mathbb{R}[x]_2$. The basis $\mathcal{B} = \{x^2, x, 1\}$ is a basis of $\mathbb{R}[x]_2$ and $\mathcal{C} = \{x^5, x^4, x^3, x^2, x, 1\}$ is a basis of $\mathbb{R}[x]_5$ which extends $\mathcal{B}$. By Theorem 11.11,*

$$\{[x^5],\ [x^4],\ [x^3]\}$$

is a basis of $\mathbb{R}[x]_5/\mathbb{R}[x]_2$. By Proposition 11.10, the elements $[x^2]$, $[x]$, and $[1]$ are all equal to the zero vector of $\mathbb{R}[x]_5/\mathbb{R}[x]_2$.

Example 11.13. *Let $M_2(\mathbb{R})$ be the vector space of 2×2 real matrices. Let $A_2(\mathbb{R})$ denote the susbpace of $M_2(\mathbb{R})$ consisting of 2×2 anti-symmetric (or skew-symmetric) matrices. Recall that a matrix A is anti-symmetric if $A^T = -A$. For a matrix,*

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix},$$

it is easy to see that A is anti-symmetric if and only if $a = 0$, $d = 0$, and $b = -c$. Hence, a basis for $A_2(\mathbb{R})$ is

$$W := \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

Let

$$X := \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \qquad Y := \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}, \qquad Z := \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Then $\{W, X, Y, Z\}$ is a basis on $M_2(\mathbb{R})$. By Theorem 11.11, a basis for $M_2(\mathbb{R})/A_2(\mathbb{R})$ is $[X]$, $[Y]$, and $[Z]$.

Let $S_2(\mathbb{R})$ denote the subspace of real 2×2 symmetric matrices. Observe that X, Y, and Z is a basis for $S_2(\mathbb{R})$. Let

$$\varphi : S_2(\mathbb{R}) \to M_2(\mathbb{R})/A_2(\mathbb{R})$$

be the natural map which sends a symmetric matrix A to its coset $[A]$ in $M_2(\mathbb{R})/A_2(\mathbb{R})$. This map is then a vector space isomorphism. Indeed, for $A, B \in \mathbb{S}_2(\mathbb{R})$ and $c \in \mathbb{R}$, we have

$$\varphi(A + B) := [A + B] = [A] + [B] = \varphi(A) + \varphi(B)$$

and

$$\varphi(cA) = [cA] = c[A] = c\varphi(A),$$

which proves that φ is linear. In particular, φ maps the basis X, Y, and Z on $\mathbb{S}_2(\mathbb{R})$ to the basis $[X]$, $[Y]$, and $[Z]$ on $M_2(\mathbb{R})/A_2(\mathbb{R})$, which implies that φ is an isomorphism. This shows that modding $M_2(\mathbb{R})$ by the subspace of anti-symmetric matrices yields a quotient space which is naturally isomorphic to the subspace of symmetric matrices. In the end of chapter exercises, you will generalize this result to the $n \times n$ case.

We conclude this section with the following definition:

Definition 11.14. *Let V be a vector space and let W be a subspace. The map $\pi : V \to V/W$ which sends a vector $v \in V$ to its coset $[v] \in V/W$ is called the* ***(canonical) projection map****.*

Proposition 11.15. *Let $\pi : V \to V/W$ be the projection map. Then*

(i) π *is linear*

(ii) $\ker \pi = W$

Proof. (i): This follows immediately from the definition of vector addition and scalar multiplication in V/W. Explicitly, for $v_1, v_2 \in V$ and $c \in \mathbb{F}$, we have

$$\begin{aligned}\pi(v_1 + v_2) &= [v_1 + v_2] \\ &= [v_1] + [v_2] \\ &= \pi(v_1) + \pi(v_2)\end{aligned}$$

and

$$\begin{aligned}\pi(cv_1) &= [cv_1] \\ &= c[v_1] \\ &= c\pi(v_1).\end{aligned}$$

(ii): Let $v \in V$. By Proposition 11.10, $\pi(v) = [v] = [\mathbf{0}]$ if and only if $v \in W$. Hence, $\ker \pi = W$. □

Remark 11.16. *The symbol π will **not** be reserved only for the projection map. We will typically use π to denote any canonical linear map between two vector spaces. (For example, see the Second and Third Isomorphism Theorems in the next section.)*

11.2. The Isomorphism Theorems

In this section, we present three *canonical* isomorphism theorems associated to quotient vector spaces. Throughout this section, we let $\mathbb{F} = \mathbb{R}$ or $\mathbb{C}$ and every vector space is over $\mathbb{F}$.

Theorem 11.17 (The First Isomorphism Theorem)**.** *Let $\varphi : V \to W$ be a linear map and let $\widetilde{\varphi} : V/\ker\varphi \to im\ \varphi$ be the map which sends $[v] \in V/ker\varphi$ to $\varphi(v) \in im\ \varphi$. Then $\widetilde{\varphi}$ is a vector space isomorphism. ($\widetilde{\varphi}$ is called the **induced map** associated to φ on the quotient vector space.)*

Proof. The first order of business is to show that $\widetilde{\varphi}$ is well-defined. In other words, we need to show that if $[v] = [v']$, then

$$\widetilde{\varphi}([v]) := \varphi(v) = \varphi(v') =: \widetilde{\varphi}([v']).$$

So let us suppose that $[v] = [v']$. From the definition of the quotient space $V/\ker\varphi$, this is equivalent to the statement that

$$v - v' \in \ker\varphi.$$

However, this implies that $\varphi(v - v') = \mathbf{0}$. Since φ is a linear map, we have

$$\varphi(v - v') = \varphi(v) - \varphi(v') = \mathbf{0},$$

which in turn implies that $\varphi(v) = \varphi(v')$. Hence, $\widetilde{\varphi}$ is indeed a well-defined map.

Next, we show that $\widetilde{\varphi}$ is linear. To do this, let $[v_1]$, $[v_2] \in V/\ker\varphi$ and let $c \in \mathbb{F}$. Then

$$\begin{aligned}\widetilde{\varphi}([v_1] + [v_2]) &= \widetilde{\varphi}([v_1 + v_2]) \\ &= \varphi(v_1 + v_2) \\ &= \varphi(v_1) + \varphi(v_2) \\ &= \widetilde{\varphi}([v_1]) + \widetilde{\varphi}([v_2])\end{aligned}$$

and

$$\begin{aligned}\widetilde{\varphi}(c[v_1]) &= \widetilde{\varphi}([cv_1]) \\ &= \varphi(cv_1) \\ &= c\varphi(v_1) \\ &= c\widetilde{\varphi}([v_1]).\end{aligned}$$

To show that $\widetilde{\varphi}$ is an isomorphism, we first verify that $\widetilde{\varphi}$ is injective. To do this, let $[v] \in \ker\widetilde{\varphi}$. Then

$$\begin{aligned}\widetilde{\varphi}([v]) &= \varphi(v) \\ &= \mathbf{0},\end{aligned}$$

which means that $v \in \ker\varphi$. By Proposition 11.10, this implies that $[v] = [\mathbf{0}]$. Hence, $\ker\widetilde{\varphi}$ is the zero subspace of $V/\ker\varphi$. From this, we conclude that $\widetilde{\varphi}$ is injective.

Lastly, since $\widetilde{\varphi}([v]) := \varphi(v)$ for all $v \in V$, it follows immediately that

$$\operatorname{im}\widetilde{\varphi} = \operatorname{im}\varphi.$$

This proves that $\widetilde{\varphi}$ is surjective, which completes the proof. □

Corollary 11.18. *Let $\varphi : V \to W$ be a surjective linear map and let*

$$\widetilde{\varphi} : V/\ker\varphi \to W, \quad [v] \mapsto \varphi(v)$$

be the induced map. Then $\widetilde{\varphi}$ is a vector space isomorphism.

Proof. Since φ is surjective, we have $\operatorname{im}\varphi = W$. Corollary 11.18 now follows from the First Isomorphism Theorem. □

Example 11.19. *Let* $\varphi : \mathbb{R}^3 \to \mathbb{R}^2$ *be the linear map defined by*

$$\varphi(x, y, z) := (x - y, z).$$

Clearly, φ *is surjective and the kernel of* φ *is*

$$\ker \varphi = \{(a, a, 0) \mid a \in \mathbb{R}\}.$$

By the First Isomorphism Theorem, the map

$$\widetilde{\varphi} : \mathbb{R}^3 / \ker \varphi \to \mathbb{R}^2, \quad [(x, y, z)] \mapsto (x - y, z)$$

is a vector space isomorphism.

Example 11.20. *Let* $M_n(\mathbb{R})$ *be the vector space of* $n \times n$ *real matrices and let* $S_n(\mathbb{R})$ *and* $A_n(\mathbb{R})$ *be the subspaces of* $n \times n$ *symmetric and anti-symmetric matrices respectively. Recall that a matrix* A *is anti-symmetric if* $A^T = -A$. *Define*

$$\varphi : M_n(\mathbb{R}) \to M_n(\mathbb{R}), \qquad A \mapsto \frac{1}{2}(A + A^T).$$

The map φ *is clearly linear. Moreover, the image of* φ *is* $\mathbb{S}_n(\mathbb{R})$. *Indeed, for any* $A \in M_n(\mathbb{R})$, $\varphi(A)^T = \varphi(A)$. *Also, if* A *is symmetric, then*

$$\varphi(A) := \frac{1}{2}(A + A^T) = \frac{1}{2} 2A = A.$$

Observe that $\ker \varphi = A_n(\mathbb{R})$. *Consequently, by the First Isomorphism Theorem, the map*

$$\widetilde{\varphi} : M_n(\mathbb{R})/A_n(\mathbb{R}) \to S_n(\mathbb{R}), \qquad [A] \mapsto \frac{1}{2}(A + A^T)$$

is a vector space isomorphism.

The Second and Third Isomorphism Theorems establish canonical isomorphisms between certain quotient vector spaces. In order to distinguish a coset of one quotient vector space from that of another, we will employ the notation of Proposition 11.10 where a coset $[v] \in V/W$ is denoted by $W + v$. Here is the **Second Isomorphism Theorem**:

Theorem 11.21 (Second Isomorphism Theorem)**.** *Let* V *be a vector space and let* U *and* W *be subspaces of* V. *For* $u \in U$, *denote its coset in* $U/U \cap W$ *by* $[u]$ *and for* $v \in U + W$, *denote its coset in* $(U + W)/W$ *by* $W + v$. *Let*

$$\pi : U/U \cap W \to (U + W)/W$$

be the map defined by $\pi([u]) := W + u$. *Then* π *is a vector space isomorphism.*

Proof. First, we need to check that π is well defined. In other words, if u and u' are elements of U which represent the same coset in $U/U \cap W$, we wish to show that

$$\pi([u]) = \pi([u']). \tag{212}$$

To do this, we simply note that since u and u' are representatives of the same coset in $U/U \cap W$, we have

$$u - u' \in U \cap W \subset W.$$

This implies that u and u' also represent the same coset in $(U+W)/W$, that is, $W + u = W + u'$. This proves (212). Hence, π is well defined.

Next, we check the linearity of π. To do this, let $u_1,\ u_2 \in U$ and let $c \in \mathbb{F}$. Then

$$\begin{aligned}\pi([u_1] + [u_2]) &= \pi([u_1 + u_2]) \\ &= W + (u_1 + u_2) \\ &= (W + u_1) + (W + u_2) \\ &= \pi([u_1]) + \pi([u_2])\end{aligned}$$

and

$$\begin{aligned}\pi(c[u_1]) &= \pi([cu_1]) \\ &= W + cu_1 \\ &= c(W + u_1) \\ &= c\pi([u_1]).\end{aligned}$$

To establish that π is an isomorphism, we first verify that π is injective. So let $[u] \in \ker \pi$. Then

$$\pi([u]) = W + u = W + \mathbf{0} = W$$

This implies that $u \in W$. However, since $[u]$ is an element of $U/(U \cap W)$, we also have $u \in U$. Hence, $u \in U \cap W$, which implies that $[u]$ is the zero vector in $U/U \cap W$. This proves that $\ker \pi = \{[\mathbf{0}]\}$, which implies that π is injective.

To show that π is surjective, we apply the Rank-Nullity Theorem (Theorem 5.60) to π, which gives

$$\dim U/(U \cap W) = \dim \ker \pi + \dim \text{im } \pi = \dim \text{im } \pi.$$

By Theorem 11.11, we have

$$\begin{aligned}\dim(U+W)/W &= \dim(U+W) - \dim W \\ &= \dim U + \dim W - \dim U \cap W - \dim W \\ &= \dim U - \dim U \cap W \\ &= \dim U/U \cap W,\end{aligned}$$

where the second equality follows from Proposition 5.75. The above calculation shows that im π has the same dimension as $\dim(U+W)/W$. Since im π is a subspace of $(U+W)/W$, it follows that

$$\text{im } \pi = (U+W)/W.$$

This completes the proof. □

Corollary 11.22. *Let V be a vector space and let U and W be subspaces of V such that $V = U \oplus W$ is a direct sum. Then the map*

$$\pi : U \to V/W$$

which sends $u \in U$ to the coset $[u] \in V/W$ is a vector space isomorphism.

Proof. Since V is a direct sum of U and W, we have $U \cap W = \{\mathbf{0}\}$ and $V = U + W$. In particular, $U/U \cap W = U$. Corollary 11.22 now follows from the Second Isomorphism Theorem. □

Example 11.23. *Consider the vector space $\mathbb{R}^3$ and let $\{\vec{e}_1, \vec{e}_2, \vec{e}_3\}$ denote the standard basis on $\mathbb{R}^3$. Let W be the subspace spanned by $\vec{e}_1 - \vec{e}_2$ and let U be the subspace spanned by $\vec{e}_1$ and $\vec{e}_3$. Then we have*

$$\mathbb{R}^3 = W \oplus U.$$

By the Second Isomorphism Theorem, the canonical map

$$\pi : U \xrightarrow{\sim} \mathbb{R}^3/W, \qquad \vec{u} \mapsto [\vec{u}]$$

is a vector space isomorphism.

Before we can state the third and final isomorphism theorem, we first need to know what the subspaces of a quotient vector space look like. The answer to this problem is given by the following result:

Proposition 11.24. *Let V be a vector space and let J be a subspace of V.*

(i) If W is a subspace of V such that $J \subset W$, then W/J is a subspace of V/J.
(ii) If X is a subspace of V/J, then there exists a unique subspace W_X of V such that $J \subset W_X$ and $X = W_X/J$.

Proof. (i): Let W be a subspace of V such that $J \subset W$. Then W is a vector space in its own right and J is also a subspace of W. Hence, it makes sense to consider the quotient space W/J. By Proposition 11.10, the coset of $w \in W$ in V/J and W/J are exactly the same; both are given by the set

$$[w] = \{j + w \mid j \in J\} = J + w.$$

This shows that W/J is a subset of V/J. Let $w_1, w_2 \in W$ and let $c \in \mathbb{F}$. Since W is a subspace of V, we have

$$[w_1] + [w_2] := [w_1 + w_2] \in W/J$$

and

$$c[w_1] := [cw_1] \in W/J.$$

This proves that W/J is a subspace of V/J.

(ii): Let X be a subspace of V/J and define

$$W_X := \{v \in V \mid [v] \in X\}.$$

Observe that $J \subset W_X$. Indeed, since X is a subspace of V/J, it necessarily contains the zero vector $[\mathbf{0}]$ of V/J. By Proposition 11.10, we have $[j] = [\mathbf{0}]$ for all $j \in J$. From the definition of W_X, we have $J \subset W_X$. Now let $w_1, w_2 \in W_X$. From the definition of W_X, we have $[w_1]$, $[w_2] \in X$. Since X is a subspace of V/J, we also have

$$[w_1] + [w_2] \in X.$$

However, $[w_1] + [w_2] := [w_1 + w_2]$. From the definition of W_X, we have $w_1 + w_2 \in W_X$. Likewise, for $c \in \mathbb{F}$, we have $c[w_1] \in X$. Since $c[w_1] := [cw_1]$, it follows that $cw_1 \in W_X$. This proves that W_X is a subspace of V. Moreover, it follows immediately from the definition of W_X that $X = W_X/J$.

For the uniqueness claim, suppose that there exists another subspace W'_X of V such that $J \subset W'_X$ and $X = W'_X/J$. Let $w \in W_X$. Since $W_X/J = X = W'_X/J$, we have $[w] \in W'_X/J$. Hence, there exists $w' \in W'_X$ such that $[w] = [w']$. This implies that $w' = w + j$ for some $j \in J$. Since $J \subset W_X$, it follows that $w + j \in W_X$. In particular, $w' \in W_X$ This shows that $W'_X \subset W_X$. An entirely similar argument shows that $W'_X \supset W_X$. This proves that $W'_X = W_X$ as desired. This completes the proof. □

We now state and prove the Third Isomorphism Theorem:

Theorem 11.25 (Third Isomorphism Theorem)**.** *Let V be a vector space and let W and J be subspaces of V such that $J \subset W$. For $v \in V$, denote its coset in V/W by $[v]$ and for $J + v \in V/J$, denote its coset in $(V/J)/(W/J)$ by $[J + v]$. Let*

$$\pi : V/W \to (V/J)/(W/J)$$

be the map defined by $\pi([v]) := [J+v]$. Then π is a vector space isomorphism.

Proof. Note that by Proposition 11.24, W/J is a subspace of V/J. Hence, it makes sense to consider the quotient vector space $(V/J)/(W/J)$.

As in the Second Isomorphism Theorem, the first order of business is to show that π is a well defined map. Hence, we must verify that if $[v] = [v']$, then

$$[J + v] = [J + v']. \tag{213}$$

So let us suppose that $[v] = [v']$ for some $v, v' \in V$. This implies that $v - v' \in W$. In particular, this mean that

$$J + (v - v') \in W/J. \tag{214}$$

(214) can be rewritten as

$$(J + v) - (J + v') \in W/J. \tag{215}$$

(215) then implies that their cosets in $(V/J)/(W/J)$ are equal. In other words, this implies (213). Hence, π is well defined.

Next, we verify that π is a linear map. To do this, let $[v_1],\ [v_2] \in V/W$ and let $c \in \mathbb{F}$. Then

$$\begin{aligned}\pi([v_1] + [v_2]) &= \pi([v_1 + v_2])\\ &= [J + (v_1 + v_2)]\\ &= [(J + v_1) + (J + v_2)]\\ &= [J + v_1] + [J + v_2]\\ &= \pi([v_1]) + \pi([v_2])\end{aligned}$$

and

$$\begin{aligned}\pi(c[v_1]) &= \pi([cv_1])\\ &= [J + cv_1]\\ &= [c(J + v_1)]\\ &= c[J + v_1]\\ &= c\pi([v_1]).\end{aligned}$$

To show that π is an isomorphism, let $[v] \in \ker \pi$. Since the zero vector of V/J is the coset $J + \mathbf{0} = J$, it follows that the zero vector of $(V/J)/(W/J)$ is $[J]$. Hence,

$$\pi([v]) = [J + v] = [J].$$

This implies that $J + v \in W/J$, which in turn implies that $v \in W$. Consequently, the coset of v in V/W is $[v] = [\mathbf{0}]$. This shows that $\ker \pi = \{[\mathbf{0}]\}$. Hence, π is injective.

For the surjectivity of π, we apply the Rank-Nullity Theorem (Theorem 5.60) to π. This gives

$$\dim V/W = \dim \ker \pi + \dim \operatorname{im}\, \pi = \dim \operatorname{im}. \tag{216}$$

(216) combined with Theorem 11.11 gives

$$\dim \operatorname{im}\, \pi = \dim V - \dim W. \tag{217}$$

On the other hand, by a few applications of Theorem 11.11, we also have

$$\begin{aligned}\dim(V/J)/(W/J) &= \dim V/J - \dim W/J \\ &= (\dim V - \dim J) - (\dim W - \dim J) \\ &= \dim V - \dim W. \end{aligned} \tag{218}$$

Since im π is a subspace of $(V/J)/(W/J)$, (217) and (218) imply that im $\pi = (V/J)/(W/J)$. This completes the proof. $\square$

Example 11.26. *Consider the vector space* $\mathbb{R}^5$ *and let* $\{\vec{e}_1, \vec{e}_2, \ldots, \vec{e}_5\}$ *denote the standard basis on* $\mathbb{R}^5$. *Let* W *be the subspace spanned by*

$$\{\vec{e}_2 - \vec{e}_4, \vec{e}_3 - \vec{e}_5, \vec{e}_5 - \vec{e}_1\}$$

and let J *be the subspace spanned by* $\vec{e}_3 - \vec{e}_1$. *Observe that* $J \subset W$. *By the Third Isomorphism Theorem, the map*

$$\pi : \mathbb{R}^5/W \to (\mathbb{R}^5/J)/(W/J)$$

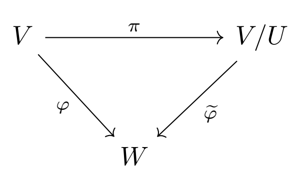
defined by $\pi([\vec{v}]) := [J + \vec{v}]$ *is a vector space isomorphism.*

11.3. Other Induced Maps

In this very short section, we introduce the following notion:

Definition 11.27. *Let* $\varphi : V \to W$ *be a linear map and let* U *be a subspace of* V. *Also, let* $\pi : V \to V/U$ *be the projection map.* φ *is said to* ***factor through*** V/U *if there exists a linear map* $\widetilde{\varphi} : V/U \to W$ *which satisfies* $\varphi = \widetilde{\varphi} \circ \pi$.

The condition that a linear map $\varphi : V \to W$ factors through a quotient vector space V/U is often expressed in the form of a **commutative diagram**:



The answer to when a linear map factors through a quotient vector space is given by the following result:

Theorem 11.28. *Let* $\varphi : V \to W$ *be a linear map and let* U *be a subspace of* V. *Then* φ *factors through* V/U *if and only if* $U \subset \ker \varphi$. *Moreover, the map* $\widetilde{\varphi} : V/U \to W$ *which satisfies* $\varphi = \widetilde{\varphi} \circ \pi$ *is unique.*

Proof. Suppose first that there exists a linear map $\widetilde{\varphi} : V/U \to W$ satisfying $\varphi = \widetilde{\varphi} \circ \pi$. From Proposition 11.15, the kernel of the projection map $\pi : V \to V/U$ is U. Hence, for any $u \in U$, we have

$$\begin{aligned}\varphi(u) &= \widetilde{\varphi} \circ \pi(u) \\ &= \widetilde{\varphi}([u]) \\ &= \widetilde{\varphi}([\mathbf{0}]) \\ &= \mathbf{0},\end{aligned}$$

where the last equality follows from the assumption that $\widetilde{\varphi}$ is linear. This shows that $U \subset \ker \varphi$.

On the other hand, let us suppose that $U \subset \ker \varphi$. Define a map $\widetilde{\varphi} : V/U \to W$ by the condition that

$$\widetilde{\varphi}([v]) := \varphi(v) \tag{219}$$

for all $v \in V$. Of course, we need to check that (219) produces a well defined map. So suppose that $v, v' \in V$ represent the same cosets in V/U. Then $v - v' \in U$ and since $U \subset \ker \varphi$, we have

$$\varphi(v - v') = \mathbf{0} \Longleftrightarrow \varphi(v) = \varphi(v'). \tag{220}$$

(220) then implies that $\widetilde{\varphi}([v]) = \widetilde{\varphi}([v'])$. This proves that $\widetilde{\varphi}$ is a well defined map. Since $\pi(v) := [v]$ for all $v \in V$, (219) can be rewritten as

$$\widetilde{\varphi} \circ \pi := \varphi, \tag{221}$$

which is none other than the factoring condition. To verify that $\widetilde{\varphi}$ is also linear, let $v_1, v_2 \in V$ and let $c \in \mathbb{F}$. Then

$$\begin{aligned}\widetilde{\varphi}([v_1] + [v_2]) &= \widetilde{\varphi}([v_1 + v_2]) \\ &= \varphi(v_1 + v_2) \\ &= \varphi(v_1) + \varphi(v_2) \\ &= \widetilde{\varphi}([v_1]) + \widetilde{\varphi}([v_2])\end{aligned}$$

and

$$\begin{aligned}\widetilde{\varphi}(c[v_1]) &= \widetilde{\varphi}([cv_1]) \\ &= \varphi(cv_1) \\ &= c\varphi(v_1) \\ &= c\widetilde{\varphi}([v_1]).\end{aligned}$$

This proves that $\widetilde{\varphi}$ is linear. To summarize, we have a constructed a linear map $\widetilde{\varphi} : V/U \to W$ satisfying $\varphi = \widetilde{\varphi} \circ \pi$. By definition, φ factors through V/U.

Lastly, for the uniqueness claim, suppose that $\psi : V/U \to W$ is another linear map satisfying $\varphi = \psi \circ \pi$. From this, we have

$$\widetilde{\varphi} \circ \pi = \psi \circ \pi.$$

Since the projection map π is surjective, it immediately follows that $\widetilde{\varphi} = \psi$. This proves the uniqueness claim. □

Example 11.29. *Let $\varphi : \mathbb{R}^4 \to \mathbb{R}^2$ be the linear map defined by*

$$\varphi(w, x, y, z) := (x - z, w - y).$$

The kernel of φ is then

$$\ker \varphi = \{(a, b, a, b) \mid a, b \in \mathbb{R}\}.$$

Let U be the subspace of $\mathbb{R}^4$ defined by

$$U := \{(a, 0, a, 0) \mid a \in \mathbb{R}\}.$$

Then $U \subset \ker \varphi$. By Theorem 11.28, φ factors through V/U. The unique "factoring map" is the map

$$\widetilde{\varphi} : V/U \to \mathbb{R}^2$$

given by

$$\widetilde{\varphi}([(w, x, y, z)]) = \varphi(x - z, w - y).$$

Theorem 11.30. *Let $\varphi : V \to V$ be a linear map and let $U \subset V$ be a subspace. The map*

$$\overline{\varphi} : V/U \to V/U, \qquad [v] \mapsto [\varphi(v)]$$

is a well defined linear map if and only if $\varphi(U) \subset U$. (The space U is said to be ***invariant*** *under φ.)*

Proof. $\overline{\varphi}$ is well defined if and only if

$$[\varphi(v + u)] = [\varphi(v)], \qquad \forall\ v \in V, \quad u \in U. \tag{222}$$

Since

$$[\varphi(v + u)] = [\varphi(v) + \varphi(u)] = [\varphi(v)] + [\varphi(u)], \tag{223}$$

it follows that (222) is equivalent to

$$[\varphi(v + u)] - [\varphi(v)] = [\varphi(u)] = [\mathbf{0}], \quad \forall\ u \in U. \tag{224}$$

Of course, (224) is equivalent to $\varphi(u) \in U$ for all $u \in U$. From this, we see that $\overline{\varphi}$ is well defined if and only if $\varphi(U) \subset U$.

Lastly, the linearity of $\overline{\varphi}$ follows easily from the linearity of φ. □

Chapter 11 Exercises

1. Let $M_n(\mathbb{R})$ denote the vector space of $n \times n$ real matrices. Also, let $\mathrm{S}_n(\mathbb{R})$ and $\mathrm{A}_n(\mathbb{R})$ denote the subspace of real symmetric and anti-symmetric matrices respectively. Recall that an $n \times n$ matrix A is anti-symmetric (or skew-symmetric) if $A^T = -A$.

(a) Show that $M_n(\mathbb{R}) = \mathrm{S}_n(\mathbb{R}) \oplus \mathrm{A}_n(\mathbb{R})$

(b) Let $\rho_s : \mathrm{S}_n(\mathbb{R}) \to M_n(\mathbb{R})/\mathrm{A}_n(\mathbb{R})$ be the map which sends an element A of $\mathrm{S}_n(\mathbb{R})$ to its coset $[A]$ in $M_n(\mathbb{R})/\mathrm{A}_n(\mathbb{R})$. Show that ρ_s is a vector space isomorphism.

(c) Let $\rho_a : \mathrm{A}_n(\mathbb{R}) \to M_n(\mathbb{R})/\mathrm{S}_n(\mathbb{R})$ be the map which sends an element A of $\mathrm{A}_n(\mathbb{R})$ to its coset $[A]$ in $M_n(\mathbb{R})/\mathrm{S}_n(\mathbb{R})$. Show that ρ_a is a vector space isomorphism.

2. Let $M_n(\mathbb{R})$ denote the vector space of $n \times n$ real matrices. Also, let $\mathrm{S}_n(\mathbb{R})$, $\mathrm{A}_n(\mathbb{R})$, and $\mathrm{D}_n(\mathbb{R})$ denote the subspace of real symmetric, anti-symmetric, and diagonal matrices respectively. Let

$$K_1 := M_n(\mathbb{R})/\mathrm{D}_n(\mathbb{R}), \qquad K_2 := \mathrm{S}_n(\mathbb{R})/\mathrm{D}_n(\mathbb{R}).$$

Show that $\mathrm{A}_n(\mathbb{R})$ is canoncially isomoprhic to the quotient vector space K_1/K_2. (Recall that a vector space isomorphism is canonical if it does not depend on an arbitrary choice of bases.)

3. A **short exact sequence** is a sequence of linear maps of the form

$$\mathbf{0} \to V_1 \xrightarrow{\iota} V_2 \xrightarrow{\pi} V_3 \to \mathbf{0}$$

where $\iota : V_1 \to V_2$ is an *injective* linear map and $\pi : V_2 \to V_3$ is a *surjective* linear map such that $\ker \pi = \mathrm{im}\ \iota$. The map $\mathbf{0} \to V_1$ is simply the linear map which sends the zero vector to the zero vector of V_1 and $V_3 \to \mathbf{0}$ is the linear map which maps every element of V_3 to the zero vector.

(a) Let V be a vector space and let W be any subspace of V. Show that the vector spaces W, V, and V/W naturally form a short exact sequence.

(b) For any short exact sequence

$$\mathbf{0} \to V_1 \xrightarrow{\iota} V_2 \xrightarrow{\pi} V_3 \to \mathbf{0},$$

show that there exists a linear map $\rho : V_3 \to V_2$ such that $\pi \circ \rho = id_{V_3}$. Given such a map ρ, also show that the map

$$\varphi : V_1 \times V_3 \to V_2, \qquad (v_1, v_3) \mapsto \iota(v_1) + \rho(v_3) \tag{225}$$

is a vector space isomorphism and that

$$V_2 = \ker \iota \oplus \mathrm{im}\ \rho.$$

In (225), $V_1 \times V_3$ is the Cartesian product of vector spaces, where vector addition and scalar multiplication are defined componentwise.

(c) Construct a linear map $\rho : V/W \to V$ for the short exact sequence in (a).

4. Let V be a real vector space and let $\mu \in V^*$ be a nonzero element of the dual space. Show that $V/\ker\mu \simeq \mathbb{R}$.

5. Let $M_n(\mathbb{R})$ be the vector space of $n \times n$ real matrices and let $\mathfrak{sl}_n(\mathbb{R})$ be the subspace of matrices with zero trace. Show that $M_n(\mathbb{R})/\mathfrak{sl}_n(\mathbb{R})$ is canonically isomorphic to $\mathbb{R}$.

6. Let $\varphi : V \to V$ be a diagonalizable linear map. Let $W \subset V$ be invariant under φ. Show that the induced map $\overline{\varphi} : V/W \to V/W$ is also diagonalizable.

7. Suppose that $V \subseteq \mathbb{R}^n$ is a subspace and let $V^\perp$ denotes the orthogonal complement of V with respect to the ordinary dot product. Show that the linear map
$$V^\perp \to \mathbb{R}^n/V, \qquad v \mapsto [v]$$
is an isomorphism. (This implies that every coset of V is represented by a unique element of $V^\perp$).

8. Consider the quotient vector space of $\mathbb{R}^3$ by the subspace W defined by $x - 2y + 2z = 0$. (Note that W is a plane through the origin.) Show that $\mathbb{R}^3/W$ is canonically isomorphic to $\mathbb{R}$. Use Problem 7. to interpret $\mathbb{R}^3/W$ geometrically.

9. Consider the quotient vector space of $\mathbb{R}^3$ by the subspace
$$W := \{(2t, -t, t) \mid t \in \mathbb{R}\}.$$
(Note that W is a line through the origin.) Use Problem 7. to interpret $\mathbb{R}^3/W$ geometrically.

Chapter 12

A Tour of Ring Theory

In this chapter, we venture into an area of *abstract algebra* called **ring theory**. The justification for doing this is that we will use ring theory later in Chapter 13 to prove some of the deepest results of linear algebra. Before we get to any precise definitions, lets take a moment to understand the basic idea of a **ring**, which is not at all complicated. Roughly speaking, a ring is a set with two binary operations: an addition operation and a multiplication operation which satisfy some natural conditions and are compatible with one another. For example, the set of all integers $\mathbb{Z}$ is a ring. Integers can be added together and they can be multiplied together and these operations have nice properties like associativity. Moreover, they are compatible with one another via the distributive property. However, this is a linear algebra book. For this reason, we are only interested in rings which are also *vector spaces*. So in this book, we will take a more **narrow** view of what a ring is. For us, a ring over a field $\mathbb{F}$ is a vector space over $\mathbb{F}$ with a vector multiplication operation which is compatible with the vector addition operation and the scalar multiplication operation on the vector space. Hence, a ring in this book is a set with three operations: scalar multiplication, vector addition, and vector multiplication; the latter allows two vectors to be multiplied together to produce a new vector. The type of rings that we focus on are more commonly called **$\mathbb{F}$-algebras**. However, we will not use this terminology. Instead, we will refer to this type of ring as a **ring over** $\mathbb{F}$. Hence, our terminology will differ a little from what you might find in an abstract algebra book. With that said, its time to be begin our study of rings.

12.1. Rings and their Homomorphisms

As far as this book is concerned, a ring is just a vector space with a vector multiplication. Of course, the vector multiplication on a ring cannot be arbitrary. It must also be compatible with vector addition and scalar multiplication. Here is the precise definition of a ring:

Definition 12.1. *A **ring** over $\mathbb{F}$ is a vector space R over $\mathbb{F}$ which is equipped with a vector multiplication*

$$R \times R \to R, \qquad (r, s) \mapsto rs \in R$$

which satisfies the following conditions for all $r, s, t \in R$ and $c \in \mathbb{F}$:

(i) $(rs)t = r(st)$ *(multiplicative associativity)*
(ii) $r(s + t) = rs + rt$ *(left distributivity)*
(iii) $(s + t)r = sr + tr$ *(right distributivity)*
(vi) $c(rs) = (cr)s = r(cs)$ *(scalar distributivity)*

*An element $\mathbf{1} \in R$ satisfying $\mathbf{1}r = r\mathbf{1} = r$ for all $r \in R$ is called an **identity element**. If R contains such an element (which is necessarily unique), then R is called a **ring with identity**.*

*Moreover, if $rs = sr$ for all $r, s \in R$, R is called a **commutative ring**.*

The following result is intuitively clear, but we will prove it all the same.

Proposition 12.2. *Let R be a ring over $\mathbb{F}$. Then $r\mathbf{0} = \mathbf{0}r = \mathbf{0}$ for all $r \in R$.*

Proof. Let $r \in R$ be arbitrary, then

$$\begin{aligned} r\mathbf{0} + r\mathbf{0} &= r(\mathbf{0} + \mathbf{0}) \\ &= r\mathbf{0} \end{aligned}$$

Adding the additive inverse $-(r\mathbf{0})$ to both sides of the above equation yields $r\mathbf{0} = \mathbf{0}$. A similar argument gives $\mathbf{0}r = \mathbf{0}$. □

At this point, we would like to discuss some of the differences between the vector addition and the vector multiplication operations on a ring. To do this, let R be a ring over $\mathbb{F}$. One of the differences concerns the idea of commutativity. Since R is also a vector space over $\mathbb{F}$, we have $r + s = s + r$ for any $r, s \in R$. Hence, the addition operation is commutative. However, in the case of the multiplication operation, commutativity is no longer required. In other words, a ring may contain elements u, v satisfying $uv \neq vu$.

Another key difference between vector addition and vector multiplication on a ring has to do with the notion of an inverse element. Once again, since R is also a vector space over $\mathbb{F}$, every element of $r \in R$ has an additive inverse element $-r$ such that $r + (-r) = \mathbf{0}$. This is not true for vector multiplication on a ring. More precisely, given an element $r \in R$, there may not exist a multiplicative inverse element $r^{-1} \in R$ such that $rr^{-1} = \mathbf{1}$. Certainly, if $r = \mathbf{0}$, then by Proposition 12.2, r cannot have a multiplicative inverse. On the other hand, even if $r \neq \mathbf{0}$, r may still lack a multiplicative inverse. In the language of abstract algebra, R equipped with its vector addition operation is an example of an **abelian group**. The subject of groups is a very interesting and massive subject in its own right. However, to stay on course for this chapter, we will not say anymore about groups.

At this point, its well past time for some concrete examples. All of the examples given below are vector spaces that possess a natural vector multiplication which is compatible with the vector space structure. Moreover, all of these examples have an identity element.

Example 12.3. *Any zero dimensional vector space $V = \{\mathbf{0}\}$ is naturally a ring. By Proposition 12.2, there is only one possibility for our vector multiplication: $\mathbf{00} := \mathbf{0}$. In this case, the identity element and the zero vector are one and the same. The ring consisting only of the zero vector is called the **zero ring**.*

Example 12.4. *The field of real numbers $\mathbb{R}$ is a ring over $\mathbb{R}$. In this particular case, the scalar multiplication and the vector multiplication on $\mathbb{R}$ are one and the same. Similarly, the field of complex numbers $\mathbb{C}$ is a ring over $\mathbb{C}$. Again, scalar multiplication and vector multiplication coincide here. Note that since $\mathbb{R} \subset \mathbb{C}$, we can also regard $\mathbb{C}$ as a ring over $\mathbb{R}$. In this case, the scalar multiplication and vector multiplication no longer coincide.*

Example 12.5. *Let $M_n(\mathbb{F})$ be the vector space of $n \times n$ matrices whose entries lie in $\mathbb{F}$. Then $M_n(\mathbb{F})$ is a ring over $\mathbb{F}$ if we take the usual matrix multiplication as our vector multiplication. Indeed, from our study of matrix operations in Chapter 3, we know that matrix multiplication satisfies the following relations for all $A, B, C \in M_n(\mathbb{F})$ and $c \in \mathbb{F}$:*

(i) $(AB)C = A(BC)$
(ii) $A(B + C) = AB + AC$
(iii) $(B + C)A = BC + CA$
(iv) $c(AB) = (cA)B = A(cB)$

By Definition 12.1, $M_n(\mathbb{F})$ is a ring over $\mathbb{F}$. In fact, the fields $\mathbb{R}$ and $\mathbb{C}$ are special cases of this ring since $\mathbb{R} = M_1(\mathbb{R})$ and $\mathbb{C} = M_1(\mathbb{C})$.

Example 12.6. *Let V be a vector space over $\mathbb{F}$ and let End(V) denote the set of linear endomorphisms of V. Again, recall that a linear endomorphism of V is simply a linear map from V to itself. End(V) is naturally a vector space over $\mathbb{F}$ with vector addition defined by*

$$(\varphi + \psi)(v) := \varphi(v) + \psi(v)$$

and scalar multiplication defined by

$$(c\varphi)(v) := c\varphi(v)$$

for all $\varphi, \psi \in$ End(V) and $c \in \mathbb{F}$. The vector multiplication that turns End(V) into a ring over $\mathbb{F}$ is (of course!) composition of linear maps:

$$\varphi\psi := \varphi \circ \psi.$$

The identity element on End(V) is (naturally) the identity map $id_V : V \to V$. The reader should verify that conditions (i)-(iv) of Definition 12.1 are indeed satisfied using composition of linear maps for vector multiplication. The vector space End(V) with this vector multiplication is called the ***endomorphism ring*** *of V.*

Example 12.7. *Let $\mathbb{F}[x]$ be the vector space of all polynomials in the variable x with coefficients in $\mathbb{F}$. $\mathbb{F}[x]$ is naturally a ring over $\mathbb{F}$ if we take the ordinary multiplication of polynomials for the vector multiplication on $\mathbb{F}[x]$. $\mathbb{F}[x]$ with this vector multiplication is called the* ***polynomial ring****.*

Of course, the polynomial ring $\mathbb{F}[x]$ naturally generalizes to the ***polynomial ring in n-variables****: $\mathbb{F}[x_1, x_2, \ldots, x_n]$.*

The endomorphism ring End(V) and the polynomial ring $\mathbb{F}[x]$ are the most important rings in this book. We will use these rings later in Chapter 13. Now that we have a reasonable idea of what a ring is, its time to define what a map between two rings should be. The definition is actually quite obvious:

Definition 12.8. *Let R and S be rings over $\mathbb{F}$. A* ***ring homomorphism*** *(or* ***ring map****) is a linear map $\varphi : R \to S$ which satisfies*

$$\varphi(r_1 r_2) = \varphi(r_1)\varphi(r_2)$$

for all $r_1,\ r_2 \in R$. In addition, if R and S both have identity elements, φ is also required to preserve the identity, that is, $\varphi(\mathbf{1}_R) = \mathbf{1}_S$ where $\mathbf{1}_R$ and $\mathbf{1}_S$ denote the identity elements on R and S respectively. If φ is also a vector space isomorphism, then φ is called a ***ring isomorphism****.*

Example 12.9. *For any ring R over $\mathbb{F}$, the identity map $id_R : R \to R$ is a ring isomorphism.*

Example 12.10. *Consider the ring of matrices $M_n(\mathbb{F})$. Let $P \in M_n(\mathbb{F})$ be any invertible matrix. Define*

$$\varphi : M_n(\mathbb{F}) \to M_n(\mathbb{F})$$

by $\varphi(A) := PAP^{-1}$. Then φ is a ring isomorphism. Let us verify this is indeed the case. First, we show that φ is a linear map. To do this, let $A, B \in M_n(\mathbb{F})$ and let $c \in \mathbb{F}$. Then

$$\begin{aligned} \varphi(A+B) &:= P(A+B)P^{-1} \\ &= PAP^{-1} + PBP^{-1} \\ &= \varphi(A) + \varphi(B) \end{aligned}$$

and

$$\begin{aligned} \varphi(cA) &:= P(cA)P^{-1} \\ &= c(PAP^{-1}) \\ &= c\varphi(A). \end{aligned}$$

Next, we show that φ preserves the vector multiplication

$$\begin{aligned} \varphi(AB) &= P(AB)P^{-1} \\ &= (PA)(PP^{-1})(BP^{-1}) \\ &= (PAP^{-1})(PBP^{-1}) \\ &= \varphi(A)\varphi(B). \end{aligned}$$

In addition, φ preserves the identity element on $M_n(\mathbb{F})$ (which is simply the identity matrix I_n):

$$\begin{aligned} \varphi(I_n) &:= PI_nP^{-1} \\ &= PP^{-1} \\ &= I_n. \end{aligned}$$

Lastly, φ has an inverse: $\varphi^{-1}(A) := P^{-1}AP$. Hence, φ is a ring isomorphism.

Example 12.11. *Let V be a vector space over $\mathbb{F}$ and fix a basis $\mathcal{B}$ on V. Define a map*

$$T : End(V) \to M_n(\mathbb{F})$$

which sends $\varphi \in End(V)$ to $[\varphi]_{\mathcal{B}}$, where $[\varphi]_{\mathcal{B}}$ is the matrix representation of φ with respect to $\mathcal{B}$. T is then a ring isomorphism. First, its clear that T is a bijective map. Indeed, two endomorphisms on V are equal if and only if their matrix representations with respect to $\mathcal{B}$ are equal. Also, given any $n \times n$ matrix A, there exists a (unique) endomorphism φ such that $[\varphi]_{\mathcal{B}} = A$. Let us verify that it is also a linear map. To do this, let $\varphi, \psi \in End(V)$ and let $c \in \mathbb{F}$. By Proposition 6.27, we have

$$\begin{aligned} T(\varphi + \psi) &:= [\varphi + \psi]_{\mathcal{B}} \\ &= [\varphi]_{\mathcal{B}} + [\psi]_{\mathcal{B}} \\ &= T(\varphi) + T(\psi) \end{aligned}$$

and

$$\begin{aligned} T(c\varphi) &:= [c\varphi]_{\mathcal{B}} \\ &= c[\varphi]_{\mathcal{B}} \\ &= cT(\varphi). \end{aligned}$$

This proves that φ is a vector space isomorphism. Note, however, that the isomorphism is not canonical as it depends on the basis $\mathcal{B}$.

Next, using Proposition 6.29, we verify that T also preserves the vector multiplication:

$$\begin{aligned} T(\varphi\psi) &= T(\varphi \circ \psi) \\ &= [\varphi \circ \psi]_{\mathcal{B}} \\ &= [\varphi]_{\mathcal{B}}[\psi]_{\mathcal{B}} \\ &= T(\varphi)T(\psi). \end{aligned}$$

Lastly, since $[id_V]_{\mathcal{B}} = I_n$ (where $n = \dim V$), it follows that T also preserves the identity element. This proves that T is a ring isomorphism.

As an immediate consequence of Example 12.11, we have the following:

Corollary 12.12. *Let V be a vector space over $\mathbb{F}$ of dimension n. Then* $\dim End(V) = n^2$.

Proof. From Example 12.11, $\mathrm{End}(V)$ and $M_n(\mathbb{F})$ are isomorphic as rings over $\mathbb{F}$. In particular, $\mathrm{End}(V)$ and $M_n(\mathbb{F})$ are isomorphic as vector spaces. Hence,

$$\dim \mathrm{End}(V) = \dim M_n(\mathbb{F}) = n^2.$$

$\square$

12.2. Subrings and Ideals

In this section, we introduce two subspaces associated to a ring: **subrings** and **ideals**.

Definition 12.13. *Let R be a ring over $\mathbb{F}$. A **subring** of R is a subspace S of R such that $s_1 s_2 \in S$ for all $s_1, s_2 \in S$.*

Proposition 12.14. *Let R and T be rings over $\mathbb{F}$ and let $\varphi : R \to T$ be a ring homomorphism. Then im φ is a subring of T.*

Proof. Since φ is also a linear map, im φ is a subspace of T. Let $t_1, t_2 \in \mathrm{im}\ \varphi$. Then there exists $r_1,\ r_2 \in R$ such that $\varphi(r_1) = t_1$ and $\varphi(r_2) = t_2$. Since φ preserves vector multiplicaton, we have

$$\begin{aligned} t_1 t_2 &= \varphi(r_1)\varphi(r_2) \\ &= \varphi(r_1 r_2) \\ &\in \mathrm{im}\ \varphi. \end{aligned}$$

This completes the proof. $\square$

Example 12.15. *Consider the ring $M_2(\mathbb{F})$. Let*

$$S := \{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \mid a, b, c \in \mathbb{F} \}$$

be the subsapce of 2×2 upper triangular matrices. Then S is a subring of $M_2(\mathbb{F})$. Indeed, consider two upper triangular matrices A and B:

$$A = \begin{pmatrix} a_1 & a_2 \\ 0 & a_3 \end{pmatrix}, \qquad B = \begin{pmatrix} b_1 & b_2 \\ 0 & b_3 \end{pmatrix}.$$

Then

$$AB = \begin{pmatrix} a_1 b_1 & a_1 b_2 + a_2 b_3 \\ 0 & a_3 b_3 \end{pmatrix} \in S.$$

The notion of an ideal comes in three different “flavors”: **left**, **right**, and **two-sided**. Here is the formal definition:

Definition 12.16. *Let R be a ring over $\mathbb{F}$.*

(i) A subspace J of R is called a ***left ideal*** *if $rj \in J$ for all $r \in R$ and $j \in J$.*

(ii) A subspace J of R is called a ***right ideal*** *if $jr \in J$ for all $r \in R$ and $j \in J$.*

(iii) A subspace J of R is called a ***two-sided ideal*** *(or simply* ***ideal****) if J is both a left and right ideal.*

Note that any left, right, or two-sided ideal of R is automatically a subring of R. The converse is not true. For example, the subring S in Example 12.15 is neither a left nor right ideal. Indeed, consider the matrix

$$\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \in M_2(\mathbb{F})$$

and multiply it from the left and right by an arbitrary element of S. Then

$$\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} = \begin{pmatrix} a & b+c \\ a & b+c \end{pmatrix} \notin M_2(\mathbb{F})$$

and

$$\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} a+b & a+b \\ c & c \end{pmatrix} \notin M_2(\mathbb{F})$$

whenever a and c are nonzero. For the sake of completeness, we state the following (obvious) result:

Proposition 12.17. *Let R be a commutative ring over $\mathbb{F}$. Then every ideal of R is a two-sided ideal.*

Proof. Let J be a left ideal of R. Then for any $r \in R$ and any $j \in J$, we have

$$jr = rj \in J.$$

Hence, J is also a right ideal and thus a two-sided ideal. Likewise, if J is a right ideal, it must also be a two-sided ideal. □

For the needs of this book, we will focus primarily on the polynomial ring $\mathbb{F}[x]$. Since $\mathbb{F}[x]$ is a commutative ring, the notions of left, right, and two-sided ideals all coincide. From now on, **the term "ideal" will always mean *two-sided* ideal**.

Example 12.18. *Let R be a ring over $\mathbb{F}$. The subspace of R consisting only of the zero vector $\mathbf{0}$ is an ideal of R since $r\mathbf{0} = \mathbf{0}r = \mathbf{0}$ for all $r \in R$. The ideal $\{\mathbf{0}\}$ is called the* ***trivial ideal****. Any ideal different that $\{\mathbf{0}\}$ is called* ***non-trivial****.*

The ring R itself is also an ideal of R. Any ideal of R different than R is called a ***proper ideal****.*

Example 12.19. *Consider the polynomial ring $\mathbb{F}[x]$ and let J denote the subspace of $\mathbb{F}[x]$ spanned by all polynomials of degree 2 or larger. Then J is an ideal of $\mathbb{F}[x]$. Indeed, let $a(x) \in J$ and let $p(x) \in \mathbb{F}[x]$. If either $a(x)$ or $p(x)$ is zero, we of course have $a(x)p(x) = \mathbf{0} \in J$ (since J is a subspace and thus contains the zero element). So let us suppose that $a(x)$ and $p(x)$ are both nonzero. Then*

$$\deg a(x)p(x) = \deg a(x) + \deg p(x) \geq \deg a(x) \geq 2.$$

Hence, $a(x)p(x) \in J$. This proves that J is an ideal of $\mathbb{F}[x]$. Moreover, since every nonzero element of J has degree at least 2, $J \neq \mathbb{F}[x]$, that is, J is a proper ideal of $\mathbb{F}[x]$. We will study the polynomial ring in more detail later in Section 12.4.

Here are some basic properties of ideals that we will make use of in Section 12.3:

Proposition 12.20. *Let R be a ring over $\mathbb{F}$ and let J and K be ideals of R. The subspaces $J + K$ and $J \cap K$ are both ideals of R.*

Proof. Let $r \in R$ and let $x \in J + K$. From the definition of $J + K$, $x = j + k$ for some $j \in J$ and $k \in K$. Since J and K are ideals of R, we have $rj, jr \in J$ and $rk, kr \in K$. Hence,

$$rx = r(j + k) = rj + rk \in J + K$$

and

$$xr = (j + k)r = jr + kr \in J + K.$$

This proves that $J + K$ is an ideal of R.

Let $a \in J \cap K$. Since a is an element of both J and K, it follows that ra and ar are elements of both J and K. In other words, $ra, ar \in J \cap K$. This proves that $J \cap K$ is an ideal of R. □

We conclude this section with the following result which shows that any ring homomorphism naturally gives rise to an ideal:

Theorem 12.21. *Let R and S be rings over $\mathbb{F}$ and let $\varphi : R \to S$ be a ring homomorphism. Then* $\ker \varphi$ *is an ideal of R.*

Proof. Let $a \in \ker \varphi$. Then for all $r \in R$, we have

$$\varphi(ra) = \varphi(r)\varphi(a) = \varphi(r)\mathbf{0} = \mathbf{0}.$$

LIkewise, $\varphi(ar) = \mathbf{0}$. This proves that ra and ar both lie in $\ker \varphi$. Hence, $\ker \varphi$ is an ideal of R. □

12.3. Quotient Rings and Isomorphism Theorems

Given a ring R over $\mathbb{F}$ and a subspace S of R, one can form the quotient vector space R/S. Given that we are dealing with rings, we can ask the following natural question: *What condition must be placed on S so that R/S is also a ring over $\mathbb{F}$, where the ring structure is induced from R?* The answer is given by the following result:

Theorem 12.22. *Let R be a ring over $\mathbb{F}$ and let J be a subspace of R. Then the quotient vector space R/J is a ring over $\mathbb{F}$ with vector multiplication defined by*

$$[r_1][r_2] := [r_1 r_2], \qquad \forall\ r_1, r_2 \in R \tag{226}$$

*if and only if J is an **ideal** of R. With J an ideal of R, the ring R/J is called the **quotient ring**. Moreover, if R is a ring with identity element $\mathbf{1}$, then its coset $[\mathbf{1}]$ is the identity element of R/J.*

Proof. Suppose first that R/J is a ring over $\mathbb{F}$ with vector multiplication given by (226). Let $j \in J$ and $r \in R$ be arbitrary. In the quotient vector space R/J, $[j] = [\mathbf{0}]$ is the zero vector. Since R/J is a ring, we have

$$[r][j] = [r][\mathbf{0}] = [\mathbf{0}] \tag{227}$$

On the other hand, by (226), we also have

$$[r][j] = [rj]. \tag{228}$$

(227) and (228) now imply that $rj \in J$. A similar argument shows that $jr \in J$. This proves that J is an ideal of R.

Now suppose that J is an ideal of R. We need to verify that the multiplication given by (226) is well defined. To do this, let $r_1, r_2 \in R$ and suppose that r_1' and r_2' are elements of R satisfying

$$[r_1] = [r_1'], \qquad [r_2] = [r_2']. \tag{229}$$

We need to verify that

$$[r_1][r_2] = [r_1'][r_2']. \tag{230}$$

Let $j_1 := r_1 - r_1'$ and $j_2 := r_2 - r_2'$. (229) implies that j_1 and j_2 are elements of J. Then

$$\begin{aligned} r_1 r_2 - r_1' r_2' &= (r_1' + j_1)(r_2' + j_2) - r_1' r_2' \\ &= r_1' r_2' + r_1' j_2 + j_1 r_2' + j_1 j_2 - r_1' r_2' \\ &= r_1' j_2 + j_1 r_2' + j_1 j_2. \end{aligned}$$

Since J is an ideal, every term in the last equality is an element of J. Hence, $r_1 r_2 - r_1' r_2' \in J$. This implies $[r_1 r_2] = [r_1' r_2']$, which in turn implies (230). This proves that the vector multiplication given by (226) is well defined.

Now suppose that R is a ring with identity element $\mathbf{1}$. Then for all $r \in R$, we have

$$[r][\mathbf{1}] = [r\mathbf{1}] = [r] = [\mathbf{1}r] = [\mathbf{1}][r]$$

This proves that $[\mathbf{1}]$ is the identity element of R/J.

To complete the proof, we need to show that R/J with vector multiplication given by (226) satisfies conditions (i)-(iv) in Definition 12.1. This is a very straightforward exercise which we leave to the reader. □

Exercise 12.23. *Let R be a ring over $\mathbb{F}$ and let J be an ideal of R. Verify that the vector multiplication on R/J satisfies conditions (i)-(iv) in Definition 12.1.*

We now apply the three isomorphism theorems for quotient vector spaces (Theorems 11.17, 11.21, and 11.25) to quotient rings and show that they yield ring isomorphisms.

Theorem 12.24 (First Isomorphism Theorem for Rings)**.** *Let R and S be rings over $\mathbb{F}$ and let $\varphi : R \to S$ be a ring homomorphism. Then the induced map*

$$\widetilde{\varphi} : R/\ker\varphi \to im\ \varphi$$

given by $\widetilde{\varphi}([r]) := \varphi(r)$ is a ring isomorphism.

Proof. By Theorem 12.21, $\ker\varphi$ is an ideal of R. Hence, $R/\ker\varphi$ is a quotient ring. By the First Isomorphism Theorem for quotient vector spaces (Theorem 11.17), $\widetilde{\varphi}$ is a vector space isomorphism. We now verify that $\widetilde{\varphi}$ preserves the vector multiplication. To do this, let $r_1, r_2 \in R$. Then

$$\begin{aligned} \widetilde{\varphi}([r_1][r_2]) &= \widetilde{\varphi}([r_1 r_2]) \\ &= \varphi(r_1 r_2) \\ &= \varphi(r_1)\varphi(r_2) \\ &= \widetilde{\varphi}([r_1])\widetilde{\varphi}([r_2]). \end{aligned}$$

Let us now suppose that R and S are rings with identity elements $\mathbf{1}_R$ and $\mathbf{1}_S$ respectively. Then $[\mathbf{1}_R]$ is the identity element of R/J and

$$\widetilde{\varphi}([\mathbf{1}_R]) = \varphi(\mathbf{1}_R) = \mathbf{1}_S.$$

This proves that $\widetilde{\varphi}$ preserves the identity element. □

Example 12.25. *Since $\mathbb{R} \subset \mathbb{C}$, let us regard $\mathbb{C}$ as a ring over $\mathbb{R}$. Define*

$$ev_i : \mathbb{R}[x] \to \mathbb{C}$$

to be the map which evaluates a real polynomial $p(x) \in \mathbb{R}[x]$ at $i := \sqrt{-1}$, that is, $ev_i(p(x)) := p(i)$. Clearly, ev_i is a ring homomorphism. Moreover, ev_i is surjective. Indeed, for $a, b \in \mathbb{R}$, we have

$$ev_i(a + bx) := a + bi \in \mathbb{C}.$$

By Theorem 12.24, the induced map

$$\widetilde{ev_i} : R[x]/\ker ev_i \to \mathbb{C}$$

given by $\widetilde{ev_i}([p(x)]) := p(i)$ is a ring isomorphism. Since

$$ev_i(x^2 + 1) := i^2 + 1 = -1 + 1 = 0,$$

we see that $x^2 + 1 \in ev_i$. Hence, $\ker \varphi \neq \{\mathbf{0}\}$. We will see later in Section 12.4 that $\ker ev_i$ consists of all real polynomials $p(x)$ which are divisible by the polynomial $x^2 + 1$.

This example shows that the field of complex numbers can be expressed as a quotient ring of the polynomial ring $R[x]$! We will generalize this example in Section 12.6.

Theorem 12.26 (Second Isomorphism Theorem for Rings)**.** *Let R be a ring over $\mathbb{F}$ and let J and K be ideals of R. Define*

$$\pi : J/J \cap K \to (J + K)/K$$

by $\pi([j]) := K + j$ (where the coset of j in $(J + K)/K$ is denoted by $K + j$). Then π is a ring isomorphism.

Proof. By Proposition 12.20, both $J \cap K$ and $J + K$ are ideals of R. Since $J \cap K \subset J$, it follows that $J \cap K$ is also an ideal of J (where J is regarded as a ring in its own right). Likewise, since $K \subset J + K$, it follows that K is also an ideal of $J + K$ (where $J + K$ is regarded as a ring). Hence, $J/J \cap K$ and $(J + K)/K$ are quotient rings.

By the Second Isomorphism Theorem for quotient vector spaces (Theorem 11.21), π is a vector space isomorphism. To complete the proof, we only need to show that π preserves the vector multiplication. To this, let $j_1, j_2 \in J$. Then

$$\begin{aligned}\pi([j_1][j_2]) &:= \pi([j_1 j_2])\\ &= K + j_1 j_2\\ &= (K + j_1)(K + j_2)\\ &= \pi([j_1])\pi([j_2]).\end{aligned}$$

This completes the proof. □

Example 12.27. *Let $\mathbb{R}[x, y]$ be the real polynomial ring in the variables x and y. For $p \in \mathbb{R}[x, y]$, define (p) to be the set of all polynomials of $\mathbb{R}[x, y]$ which are divisible by p. Hence, every polynomial $a \in (p)$ is of the form*

$$a = pq$$

for some polynomial $q \in \mathbb{R}[x, y]$. It is easy to see that (p) is in fact an ideal of $\mathbb{R}[x, y]$. Now consider the ideals (x) and (y) of $\mathbb{R}[x, y]$. Note that

$$(x) \cap (y) = (xy).$$

By Theorem 12.26, the quotient rings

$$(x)/(xy)$$

and

$$((x) + (y))/(y)$$

are canonically isomorphic.

For the last isomorphism theorem, we first need to know what the ideals of a quotient ring look like. The answer is given by the following result:

Proposition 12.28. *Let R be a ring over $\mathbb{F}$ and let J be an ideal of R.*

(i) If K is an ideal of R such that $J \subset K$, then K/J is an ideal of R/J.

(ii) If X is an ideal of R/J, then there exists a unique ideal K_X of R such that $X = K_X/J$.

Proof. (i): Since K is an ideal of R, it is also a subspace of R. It follows from Proposition 11.24 that K/J is a subspace of R/J. Let $[r] \in R/J$ and let $[k] \in K/J$, Since rk and kr are both elements of K (since K is an ideal), we have

$$[r][k] = [rk] \in K/J, \qquad [k][r] = [kr] \in K/J.$$

This proves that K/J is an ideal of R/J.

(ii): Let X be an ideal of R/J. Since X is also a subspace of R/J, it follows from Proposition 11.24 that there exists a unique subspace K_X of R such that $J \subset K_X$ and $X = K_X/J$. We need to show that K_X is also an ideal of R. To do this, let $r \in R$ and $k \in K_X$. Since $X = K_X/J$ is an ideal of R/J, we have

$$[r][k] = [rk] \in X = K_X/J.$$

This implies that $rk = j + k'$ for some $j \in J$ and $k' \in K_X$. Since $J \subset K_X$, it follows that $rk \in K_X$. A similar argument shows that $kr \in K_X$. This proves that K_X is an ideal of R. $\square$

Theorem 12.29 (Third Isomorphism Theorem for Rings)**.** *Let R be a ring over $\mathbb{F}$ and J and K be ideals of R with $J \subset K$. Let*

$$\pi : R/K \to (R/J)/(K/J)$$

be the natural map which sends $[r] \in R/K$ to $[J + r] \in (R/J)/(K/J)$. Then π is a ring isomorphism.

Proof. By Proposition 12.28, K/J is an ideal of R/J. Hence, we can form the quotient ring $(R/J)/(K/J)$. Proposition 11.24 implies that π is a vector space isomorphism. To prove the theorem, it only remains to show that π preserves the vector multiplication and the identity element if R is a ring with identity.

Let $r_1, r_2 \in R$. Then

$$\begin{aligned}\pi([r_1][r_2]) &= \pi([r_1 r_2]) \\ &= [J + r_1 r_2] \\ &= [J + r_1][J + r_2] \\ &= \pi([r_1])\pi([r_2]).\end{aligned}$$

Lastly, if R has an identity element $\mathbf{1}$, then we immediately have

$$\pi([\mathbf{1}]) = [J + \mathbf{1}].$$

Hence, π preserves the identity element. $\square$

Example 12.30. *Consider the polynomial ring $\mathbb{F}[x]$. For $p \in \mathbb{F}[x]$, let (p) denote the ideal of $\mathbb{F}[x]$ consisting of all polynomials divisible by p. Consider the ideals (x) and (x^2). Observe that $(x^2) \subset (x)$. By Theorem 12.29, the quotient rings*

$$\mathbb{F}[x]/(x)$$

and

$$(\mathbb{F}[x]/(x^2))/((x)/(x^2))$$

are canonically isomorphic.

12.4. More on the Polynomial Ring

In this section, we introduce a type of ring called a **principal ideal domain** over $\mathbb{F}$ (or **PID** over $\mathbb{F}$ for short) and then prove that the polynomial ring $\mathbb{F}[x]$ is a PID. To define a PID, we first need to introduce a few ideas.

Definition 12.31. *Let R be a ring over $\mathbb{F}$. A non-zero element $a \in R$ is called a **zero divisor** if there exists a nonzero element $b \in R$ such that $ab = \mathbf{0}$ or $ba = \mathbf{0}$.*

Example 12.32. *Consider the ring $M_2(\mathbb{R})$ consisting of all 2×2 real matrices. Then the matrix*

$$A = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$$

is zero divisor since for

$$B = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix},$$

we have $AB = \mathbf{0}$.

Definition 12.33. *An **integral domain** over $\mathbb{F}$ is a commutative ring R over $\mathbb{F}$ with identity which has no zero divisors.*

Example 12.34. *The polynomial ring $\mathbb{F}[x]$ is an integral domain over $\mathbb{F}$. Indeed, $\mathbb{F}[x]$ has an identity element (namely $1 \in \mathbb{F}$) and given two nonzero polynomials*

$$p_1 = \sum_{i=0}^{n} a_i x^i$$

and

$$p_2 = \sum_{i=0}^{m} b_i x^i,$$

their product is

$$p_1 p_2 = p_2 p_1 = \sum_{i=0}^{n} \sum_{j=0}^{m} a_i b_j x^{i+j} \neq 0$$

Definition 12.35. *Let R be a commutative ring over $\mathbb{F}$ with identity. An ideal J of R is said to be* ***prinicipal*** *if there exists an element $j_0 \in J$ such that*

$$J = \{rj_0 \mid r \in R\}.$$

The ideal J is said to be generated by j_0 and is denoted by $J = (j_0)$.

We can now state the definition of a **principal ideal domain over** $\mathbb{F}$:

Definition 12.36. *A* ***principal ideal domain over*** $\mathbb{F}$ *(or* ***PID over*** $\mathbb{F}$*) is an integral domain R over $\mathbb{F}$ with the property that every ideal of R is principal.*

We are now going to prove that $\mathbb{F}[x]$ is a PID. To do this, we need the following classic result:

Theorem 12.37 (Euclidean division of polynomials)**.** *Let $a(x), b(x) \in \mathbb{F}[x]$ with $b(x) \neq 0$. Then there exists $q(x), r(x) \in \mathbb{F}[x]$ with $\deg r(x) < \deg b(x)$ such that*

$$a(x) = b(x)q(x) + r(x).$$

Proof. First, consider the case where $\deg a(x) < \deg b(x)$. For this case, we simply set $q(x) = 0$ and $r(x) = a(x)$.

Now consider the case where $\deg a(x) \geq \deg b(x)$. Let

$$a(x) = a_n x^n + \cdots + a_1 x + a_0$$

and

$$b(x) = b_k x^k + \cdots + b_1 x + b_0.$$

Let $V \subset \mathbb{F}[x]$ the the vector space of polynomials of degree n or less. Set

$$f_j := \begin{cases} x^{j-k} b(x) & \text{for } j \geq k \\ x^j & \text{for } j < k \end{cases}$$

Since $\deg f_j = j$, it follows that

$$f_n, f_{n-1}, \ldots, f_1, f_0$$

is a basis for V. Since $a(x) \in V$, there exists $c_0, c_1, \ldots, c_n \in \mathbb{F}$ such that

$$\begin{aligned} a(x) &= \sum_{j=0}^{n} c_j f_j \\ &= \sum_{j=k}^{n} c_j x^{n-j} b(x) + \sum_{j=0}^{k-1} c_j x^j \\ &= \left(\sum_{j=k}^{n} c_j x^{n-j} \right) b(x) + \sum_{j=0}^{k-1} c_j x^j. \end{aligned}$$

Setting

$$q(x) = \sum_{j=k}^{n} c_j x^{n-j}$$

and

$$r(x) = \sum_{j=0}^{k-1} c_j x^j$$

proves the theorem for case where $\deg a(x) \geq \deg b(x)$. □

Theorem 12.38. *The polynomial ring $\mathbb{F}[x]$ is a PID. Moreover, if J is a nonzero ideal of $\mathbb{F}[x]$ and $b \in J$ is a nonzero polynomial of minimal degree in J, then $J = (b)$.*

Proof. We have already seen in Example 12.34 that $\mathbb{F}[x]$ is an integral domain over $\mathbb{F}$. We now show that every ideal of $\mathbb{F}[x]$ is principal. To do this, let J be an arbitrary ideal of $\mathbb{F}[x]$. If J is the zero ideal, then J is clearly principal (J is generated by $0 \in \mathbb{F}$). So let us assume that J is a nonzero ideal of $\mathbb{F}[x]$. Since J is nonzero, we can choose a nonzero polynomial $b \in J$ of minimal degree, that is,

$$\deg b \leq \deg a \qquad \forall \text{ nonzero } a \in J. \tag{231}$$

Let $a \in J$ be arbitrary. By Theorem 12.37, there exists $q, r \in \mathbb{F}[x]$ such that $\deg r < \deg b$ and $a = qb + r$. Since J is an ideal and $b \in J$, we also have $bq \in J$. This implies that

$$r = a - bq \in J.$$

If $r \neq 0$, then J contains a nonzero polynomial of degree less than b; this contradicts (231). Consequently, we must have $r = 0$, which in turn implies that $a = qb$. This proves that J is generated by the polynomial b, that is, $J = (b)$. This completes the proof. □

Example 12.39. *Let us consider the ring homomorphism from Example 12.25:*

$$ev_i : \mathbb{R}[x] \to \mathbb{C}, \quad p(x) \mapsto p(i).$$

As we noted in Example 12.25, the kernel of ev_i, $\ker ev_i$, is not zero as it contains the polynomial x^2+1. If p is a polynomial of degree 1 or 0 (recall that a degree 0 polynomial is a constant polynomial where the constant is required to be nonzero), then we clearly have $p(i) \neq 0$. Hence, x^2+1 is a polynomial of minimal degree in $\ker ev_i$. Since $\ker ev_i$ is an ideal of $\mathbb{R}[x]$, Theorem 12.38 shows that $\ker ev_i = (x^2+1)$. Hence, every element of $\ker ev_i$ is of the form $(x^2+1)q(x)$ for $q \in \mathbb{F}[x]$.

12.5. The Chinese Remainder Theorem

In this section, we prove a result called the **Chinese Remainder Theorem** for the polynomial ring $\mathbb{F}[x]$. Before doing this, we first cover some basic preliminaries. We begin by introducing some common notation associated to $\mathbb{F}[x]$:

Notation 12.40. *Let $a, b \in \mathbb{F}[x]$ be polynomials with b nonzero. If b divides a, that is, there exists a polynomial $q \in \mathbb{F}[x]$ such that $a = qb$, one expresses this condition by writing*

$$b \mid a \tag{232}$$

(232) reads as "b divides a". If b does not divide a, one writes $b \nmid a$.

Example 12.41. *For the polynomial ring $\mathbb{R}[x]$, $x+1 \mid x^2-1$.*

Definition 12.42. *Two polynomials $p_1, p_2 \in \mathbb{F}[x]$ are said to be **coprime** (or **relatively prime**) if they have no common factors. In other words, if $b \in \mathbb{F}[x]$ is a nonzero polynomial such that $b \mid p_1$ and $b \mid p_2$, then b must be an element of $\mathbb{F}$.*

*A finite set of polynomials $p_1, p_2, \ldots, p_n$ are said to be **pairwise coprime** if any two polynomials p_i, p_j with $i \neq j$ are coprime.*

Example 12.43. *For the polynomial ring $\mathbb{R}[x]$, the polynomials*

$$x+1, \; 5x+2, \; x^2+1$$

are pairwise coprime.

Given a finite number of rings over $\mathbb{F}$, $R_1, R_2, \ldots, R_n$, we can easily produce a new ring over $\mathbb{F}$ by taking the cartesian product of these rings. Moreover, the new ring naturally contains subrings which are isomorphic to $R_1, R_2, \ldots, R_n$.

Definition 12.44 (Direct Product of Rings)**.** *Let $R_1, R_2, \ldots, R_n$ be rings over $\mathbb{F}$. The cartesian product*

$$R := R_1 \times R_2 \cdots \times R_n.$$

is naturally a ring over $\mathbb{F}$ with ring structure. Formally, its vector space structure is defined by

$$(a_1, a_2, \ldots, a_n) + (b_1, b_2, \ldots, b_n) := (a_1 + b_1, a_2 + b_2, \ldots, a_n + b_n)$$

and

$$c(a_1, a_2, \ldots, a_n) := (ca_1, ca_2, \ldots, ca_n)$$

for $a_i, b_i \in R_i$ for $i = 1, \ldots, n$ and $c \in \mathbb{F}$. The vector multiplication on R is given by

$$(a_1, a_2, \ldots, a_n)(b_1, b_2, \ldots, b_n) := (a_1b_1, a_2b_2, \ldots, a_nb_n)$$

*R equipped with the above ring structure is called a **direct product of rings**.*

Moreover, if $R_1, R_2, \ldots, R_n$ has identity element $\mathbf{1}_1, \mathbf{1}_2, \ldots, \mathbf{1}_n$, then R has the identity element

$$(\mathbf{1}_1, \mathbf{1}_2, \ldots, \mathbf{1}_n).$$

*The direct product of rings is also called an **external direct sum**.*

Remark 12.45. *Definition 12.44 can be generalized to an infinite number of rings. However, in the infinite case, the terms "direct product of rings" and "external direct sum" no longer coincide. We will not discuss the precise meaning of these terms in this book.*

The following is a very simple exercise that the reader should carry out if there is any doubt that Definition 12.44 yields a ring over $\mathbb{F}$:

Exercise 12.46. *Verify that Definition 12.44 satisfies all the conditions of a ring over $\mathbb{F}$ given in Definition 12.1.*

Here is a consequence of Theorem 12.38 that we will make use of shortly:

Proposition 12.47. *Let* $b_1, b_2 \in \mathbb{F}[x]$ *be coprime. Then there exists* $q_1, q_2 \in \mathbb{F}[x]$ *such that*

$$q_1 b_1 + q_2 b_2 = 1. \tag{233}$$

Proof. Let

$$J := \{a_1 b_1 + a_2 b_2 \mid a_1, a_2 \in \mathbb{F}[x]\}.$$

Then its easy to see that J is an ideal of $\mathbb{F}[x]$. Since all ideals of $\mathbb{F}[x]$ are principal by Theorem 12.38, there exists a polynomial $\alpha \in \mathbb{F}[x]$ such that $J = (\alpha)$. Since $b_1, b_2 \in J$, we have

$$\alpha \mid b_1, \qquad \alpha \mid b_2.$$

However, since b_1 and b_2 are coprime, it follows that $\alpha \in \mathbb{F} - \{0\}$. However, if J contains a nonzero element of $\mathbb{F}$, it follows that $J = \mathbb{F}[x]$. Hence, in particular, $1 \in J = \mathbb{F}[x]$. From the definition of J, it follows that there exists polynomials $q_1, a_2 \in \mathbb{F}[x]$ satisfying (233). This completes the proof. □

We are now in a position to state the **Chinese Remainder Theorem**. We will actually state two versions of the theorem. The first version is easier to understand:

Theorem 12.48 (Chinese Remainder Theorem-I)**.** *Let* $b_1, b_2, \ldots, b_k \in \mathbb{F}[x]$ *be a finite set of pairwise coprime polynomials. Let* $r_1, r_2, \ldots, r_k \in \mathbb{F}[x]$ *be arbitrary polynomials. Then there exists a polynomial* $a \in \mathbb{F}[x]$ *such that*

$$a - r_i \in (b_i)$$

for $i = 1, \ldots, k$. *In other words,* a *can be expressed as*

$$a = q_i b_i + r_i$$

for some $q_i \in \mathbb{F}[x]$ *for* $i = 1, \ldots, k$.

Here is the second version:

Theorem 12.49 (Chinese Remainder Theorem-II). *Let* $b_1, b_2, \ldots, b_k \in \mathbb{F}[x]$ *be a finite set of pairwise coprime polynomials. Let*

$$\pi_k : \mathbb{F}[x] \to \mathbb{F}[x]/(b_1) \times \mathbb{F}[x]/(b_2) \times \cdots \times \mathbb{F}[x]/(b_k)$$

be the map defined by

$$\pi(a) := ([a]_1, [a]_2, \ldots, [a]_k)$$

for $a \in \mathbb{F}[x]$*, where* $[a]_i$ *denotes the coset of* a *in* $\mathbb{F}[x]/(b_i)$ *for* $i = 1, \ldots, k$*. Then*

(i) π_k *is a ring homomorphism*

(ii) π_k *is surjective*

(iii) $\ker \pi_k = (b_1 b_2 \cdots b_k)$

(iv) The induced map

$$\widetilde{\pi}_k : \mathbb{F}[x]/(b_1 b_2 \cdots b_k) \to \mathbb{F}[x]/(b_1) \times \mathbb{F}[x]/(b_2) \times \cdots \times \mathbb{F}[x]/(b_k)$$

defined by $\widetilde{\pi}_k([a]) := \pi_k(a)$ *is a ring isomorphism for* $a \in \mathbb{F}[x]$.

Our plan now is to prove the second version of the Chinese Remainder Theorem and then show how the second version implies the first version. Here is the proof of the second version:

Proof. (i): Let $a, a' \in \mathbb{F}[x]$ and $c \in \mathbb{F}$, we have

$$\begin{aligned}
\pi_k(a + a') &:= ([a + a']_1, [a + a']_2, \ldots, [a + a']_k) \\
&= ([a]_1 + [a']_1, [a]_2 + [a']_2, \ldots, [a]_k + [a']_k) \\
&= ([a]_1, [a]_2, \ldots, [a]_k) + ([a']_1, [a']_2, \ldots, [a']_k) \\
&= \pi_k(a) + \pi_k(a')
\end{aligned}$$

and

$$\begin{aligned}
\pi_k(ca) &:= ([ca]_1, [ca]_2, \ldots, [ca]_k) \\
&= (c[a]_1, c[a]_2, \ldots, c[a]_k) \\
&= c([a]_1, [a]_2, \ldots, [a]_k) \\
&= c\pi_k(a).
\end{aligned}$$

This proves that π_k is linear. In addition, we also have

$$\begin{aligned}
\pi_k(aa') &= ([aa']_1, [aa']_2, \ldots, [aa']_k) \\
&= ([a]_1[a']_1, [a]_2[a']_2, \ldots, [a]_k[a']_k) \\
&= ([a]_1, [a]_2, \ldots, [a]_k)([a']_1, [a']_2, \ldots, [a']_k) \\
&= \pi_k(a)\pi_k(a').
\end{aligned}$$

This proves that π_k is a ring homomorphism.

(ii)-(iv): For $k = 1$, the theorem clearly holds. Let us consider the $k = 2$ case:

$$\pi_2 : \mathbb{F}[x] \to \mathbb{F}[x]/(b_1) \times \mathbb{F}[x]/(b_2).$$

Since $b_1, b_2 \in \mathbb{F}[x]$ are coprime, it follows from Proposition 12.47 that there exists $q_1, q_2 \in \mathbb{F}[x]$ such that

$$q_1 b_1 + q_2 b_2 = 1. \tag{234}$$

Let $f_1, f_2 \in \mathbb{F}[x]$ be arbitrary and let

$$a = f_1 q_2 b_2 + f_2 q_1 b_1. \tag{235}$$

From (234), we have

$$f_1 = f_1 q_1 b_1 + f_1 q_2 b_2 \tag{236}$$

and

$$f_2 = f_2 q_1 b_1 + f_2 q_2 b_2. \tag{237}$$

Then

$$a - f_1 = (f_2 q_1 - f_1 q_1) b_1 \tag{238}$$

and

$$a - f_2 = (f_2 q_2 - f_2 q_2) b_2 \tag{239}$$

(238) and (239) imply that

$$a - f_1 \in (b_1), \qquad a - f_2 \in (b_2). \tag{240}$$

(240) implies

$$[a]_1 = [f_1]_1, \qquad [a]_2 = [f_2]_2. \tag{241}$$

From (241), we have

$$\pi_2(a) = ([a]_1, [a]_2) = ([f_1]_1, [f_2]_2), \tag{242}$$

which proves that π_2 is surjective.

Observe that $a \in \ker \pi_2$ if and only if $a \in (b_1) \cap (b_2)$. However, since b_1, b_2 are coprime, we have

$$\ker \pi_2 = (b_1) \cap (b_2) = (b_1 b_2). \tag{243}$$

Using (243) and applying the First Isomorphism Theorem for rings (Theorem 12.24) yields the ring isomorphism:

$$\widetilde{\pi}_2 : \mathbb{F}[x]/(b_1 b_2) \to \mathbb{F}[x]/(b_1) \times \mathbb{F}[x]/(b_2).$$

This proves (ii)-(iv) for the $k = 2$ case.

We now prove (ii)-(iv) for the general case by induction on k. Now suppose the theorem holds for $k - 1$ pairwise polynomials where $k \geq 3$. Let $b_1, b_2, \ldots, b_k \in \mathbb{F}[x]$ be pairwise coprime. Let

$$\widetilde{b} := b_1 b_2 \cdots b_{k-1}.$$

Since $\widetilde{b}$ and b_k are also coprime, the $k = 2$ case implies that

$$\pi_2 : \mathbb{F}[x] \to \mathbb{F}[x]/(\widetilde{b}) \times \mathbb{F}[x]/(b_k)$$

is surjective and

$$\ker \pi_2 = (\widetilde{b} b_k) = (b_1 b_2 \cdots b_k). \tag{244}$$

By induction, we also have that the map

$$\pi_{k-1} : \mathbb{F}[x] \to \mathbb{F}[x]/(b_1) \times \mathbb{F}[x]/(b_2) \times \cdots \times \mathbb{F}[x]/(b_{k-1})$$

is a surjective ring homomorphism with $\ker \pi_{k-1} = (b_1 b_2 \cdots b_{k-1}) = (\widetilde{b})$ and that the induced map

$$\widetilde{\pi}_{k-1} : \mathbb{F}[x]/(\widetilde{b}) \to \mathbb{F}[x]/(b_1) \times \mathbb{F}[x]/(b_2) \times \cdots \times \mathbb{F}[x]/(b_{k-1})$$

is a ring isomorphism. Let $id_k : \mathbb{F}[x]/(b_k) \to \mathbb{F}[x]/(b_k)$ denote the identity map and let

$$\widetilde{\pi}_{k-1} \times id_k : \mathbb{F}[x]/(\widetilde{b}) \times \mathbb{F}[x]/(b_k) \to: \mathbb{F}[x]/(\widetilde{b}) \times \mathbb{F}[x]/(b_k)$$

be the map defined by

$$\begin{aligned} \widetilde{\pi}_{k-1} \times id_k([f], [g]_k) &:= (\widetilde{\pi}_{k-1}([f]), [g]_k) \\ &= (\pi_{k-1}(f), [g]_k) \\ &= ([f]_1, [f]_2, \ldots, [f]_{k-1}, [g]_k). \end{aligned}$$

Since $\widetilde{\pi}_{k-1}$ and id_k are both ring isomorphisms, it follows that $\widetilde{\pi}_{k-1} \times id_k$ is also a ring isomorphism.

Now observe that the map

$$\pi_k : \mathbb{F}[x] \to \mathbb{F}[x]/(b_1) \times \mathbb{F}[x]/(b_2) \times \cdots \times \mathbb{F}[x]/(b_{k-1}) \times \mathbb{F}[x]/(b_k)$$

is in fact given by the composition

$$\pi_k = (\widetilde{\pi}_{k-1} \times id_k) \circ \pi_2.$$

Since π_2 is a surjective ring homomorphism and $\widetilde{\pi}_{k-1} \times id_k$ is a ring isomorphism, it follows that π_k is surjective with kernel

$$\ker \pi_k = \ker(\widetilde{\pi}_{k-1} \times id_k) \circ \pi_2 = \ker \pi_2 = (b_1 b_2 \cdots b_k),$$

where the last equality follows from (244). This proves (ii) and (iii) for π_k. Applying the First Isomorphism Theorem for rings (Theorem 12.24) to π_k proves (iv). This completes the proof. □

Here is the proof of the first version of the Chinese Remainder Theorem (Theorem 12.48):

Proof. Let $b_1, \ldots, b_k \in \mathbb{F}[x]$ be pairwise coprime. By Theorem 12.49, the map

$$\pi_k : \mathbb{F}[x] \to \mathbb{F}[x]/(b_1) \times \mathbb{F}[x]/(b_2) \times \cdots \times \mathbb{F}[x]/(b_k)$$

given by $\pi_k(a) = ([a]_1, [a]_2, \ldots, [a]_k)$ is a surjective ring homomorphism, where $[a]_i$ denotes the coset of a in $\mathbb{F}[x]/(b_i)$. Hence, for $r_1, \ldots, r_k \in \mathbb{F}[x]$ arbitrary, there exists $a \in \mathbb{F}[x]$ such that

$$\pi(a) = ([r_1]_1, [r_2]_2, \ldots, [r_k]_k).$$

This implies that $[a]_i = [r_i]_i$ for $i = 1, \ldots, k$. This in turn is equivalent to $a_i - r_i \in (b_i)$ for $i = 1, \ldots, k$. This completes the proof. □

12.6. † Other Fields

The notion of a field was defined way back in Chapter 5 in Definition 5.1. In linear algebra, the fields of greatest interest are the field of real numbers $\mathbb{R}$ and the field of complex numbers $\mathbb{C}$. In addition to $\mathbb{R}$ and $\mathbb{C}$, another common field is the field of rational numbers

$$\mathbb{Q} := \{\frac{a}{b} \mid a, b \in \mathbb{Z},\ b \neq 0\},$$

where $\mathbb{Z} := \{0, \pm 1, \pm 2, \pm 3, \ldots, \}$ are the set of integers. Of course, there are other fields besides $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$. In this section, we are going to broaden our knowledge of fields (slightly) by proving a simple result that will provide us with a mechanism to generate other fields. This short section is only needed for Chapter 14, which focuses on less conventional applications of linear algebra. In this section, $\mathbb{F}$ will denote any field. (In fact, all the general results of this chapter work for any field.) We now introduce some definitions which will be needed later in Chapter 14.

Definition 12.50. *Let $p \in \mathbb{F}[x]$. p is said to be an* ***irreducible polynomial*** *if $\deg p \geq 1$ and there does not exist polynomials $a, b \in \mathbb{F}[x]$ with $\deg a \geq 1$ and $\deg b \geq 1$ such that $p = ab$. A polynomial of positive degree which is not irreducible is said to be* ***reducible****.*

Example 12.51. *Consider the polynomial $p(x) = x^2 + 1$. In $\mathbb{R}[x]$, p is irreducible. However, in $\mathbb{C}[x]$, p is reducible since*

$$p = (x + i)(x - i)$$

and $x + i$ and $x - i$ are both elements of $\mathbb{C}[x]$.

We now introduce the notion of a **field extension**:

Definition 12.52. *A field $\mathbb{K}$ is said to be a* ***field extension*** *of a field $\mathbb{F}$ if $\mathbb{F} \subset \mathbb{K}$ and the restriction of the field operations of $\mathbb{K}$ to $\mathbb{F}$ coincide with the field operations of $\mathbb{F}$ as a field.*

Example 12.53. *The field $\mathbb{R}$ is a field extension of $\mathbb{Q}$ and $\mathbb{C}$ is a field extension of both $\mathbb{Q}$ and $\mathbb{R}$.*

We conclude this very brief section with the following result which can be viewed as a generalization of Example 12.25:

Theorem 12.54. *Let $p(x) \in \mathbb{F}[x]$. Then the quotient ring $\mathbb{F}[x]/(p)$ is a field if and only if $p(x)$ is irreducible.*

Moreover, $\mathbb{F}[x]/(p)$ is a field extension of $\mathbb{F}$, where the field $\mathbb{F}$ is identified with its image under the projection map $\pi : \mathbb{F}[x] \to \mathbb{F}[x]/(p)$. In other words, each element $\lambda \in \mathbb{F}$ is uniquely identified with its coset $[\lambda]$ in $\mathbb{F}[x]/(p)$.

Proof. Suppose first that $p(x)$ is irreducible. Since $\mathbb{F}[x]/(p)$ is a commutative ring, we only need to show that every nonzero element of $\mathbb{F}[x]/(p)$ has an inverse. So let $[a] \in \mathbb{F}[x]/(p)$ be a nonzero element. This implies that $a \notin (p)$. Moreover, since p is irreducible, it follows that a and p are coprime. Proposition 12.47 implies that there exists $q_1, q_2 \in \mathbb{F}[x]$ such that

$$q_1 a + q_2 p = 1 \tag{245}$$

Hence, taking the coset of both sides of (245) in $\mathbb{F}[x]/(p)$ gives

$$\begin{aligned} [q_1 a + q_2 p] &= [1] \\ [q_1 a] + [q_2 p] &= [1] \\ [q_1 a] + [0] &= [1] \\ [q_1][a] &= [1]. \end{aligned}$$

Hence, $[a]$ has an inverse.

Lastly, since $\deg p \geq 1$, it follows that $c \notin (p)$ for all nonzero $c \in \mathbb{F}$. Hence, the image of $\mathbb{F}$ under the projection map

$$\pi : \mathbb{F}[x] \to \mathbb{F}[x]/(p)$$

is naturally isomorphic to $\mathbb{F}$ itself. Hence, by identifying $\mathbb{F}$ with its isomorphic image

$$\pi(\mathbb{F}) \subset \mathbb{F}[x]/(p),$$

we can regard the field $\mathbb{F}[x]/(p)$ as a field extension of $\mathbb{F}$.

Now suppose that $\mathbb{F}[x]/(p)$ is a field, but p is not irreducible. Then $p = p_1 p_2$ for some polynomials $p_1, p_2 \in \mathbb{F}[x]$ of positive degree. Since $\deg p > p_i$ for $I = 1, 2$, it follows that $p_i \not| (p)$ for $i = 1, 2$. In particular, $[p_1]$ and $[p_2]$ are nonzero elements in $\mathbb{F}[x]/(p)$. Since $\mathbb{F}[x]/(p)$ is a field, the product of any two nonzero elements can never be zero. However, we have

$$[p_1][p_2] = [p_1 p_2] = [p] = [0],$$

which is a contradiction. Hence, p must be irreducible. □

Example 12.55. *Consider the polynomial ring* $\mathbb{Q}[x]$. *Since* $\sqrt{2} \notin \mathbb{Q}$, *it follows that the polynomial* $x^2 - 2$ *is irreducible in* $\mathbb{Q}[x]$. *By Theorem 12.54, the quotient ring*

$$\mathbb{Q}[x]/(x^2 - 2)$$

is a field extension of $\mathbb{Q}$. *Moreover, since* $[x^2 - 2] = [0]$, *it follows that*

$$[x]^2 = [2].$$

Hence, the coset $[x]$ *of* x *in* $\mathbb{Q}[x]/(x^2 - 2)$ *can be identified with* $\sqrt{2}$. *So* $\mathbb{Q}[x]/(x^2 - 2)$ *is essentially the field* $\mathbb{Q}$ *with* $\sqrt{2}$ *tacked on. For this reason, we can denote this field extension by* $\mathbb{Q}(\sqrt{2})$. *You will revisit this idea in Chapter 14.*

Chapter 12 Exercises

1. Let $C(\mathbb{R})$ be the ring of continuous real valued functions on $\mathbb{R}$. Let

$$J := \{f \in C(\mathbb{R}) \mid f(0) = 0\}.$$

   Show that $J$is an ideal of $C(\mathbb{R})$.

2. Let $M_n(\mathbb{R})$ be the ring of real $n \times n$ matrices. Let R be the set of real $n \times n$ matrices whose first column is entirely zero. Show that R is a subring of $M_n(\mathbb{R})$, but not an ideal of $M_n(\mathbb{R})$. (By ideal, we always mean a 2-sided ideal.)

3. Let $M_n(\mathbb{R})$ be the ring of real $n \times n$ matrices. Let $B_n(\mathbb{R})$ be the subspace of $M_n(\mathbb{R})$ consisting of all real $n \times n$ upper triangular matrices.
   (a) Show that $B_n(\mathbb{R})$ is a subring of $M_n(\mathbb{R})$, but not an ideal of $M_n(\mathbb{R})$.

   (b) Let $N_n(\mathbb{R})$ be the subspace of all real $n \times n$ strictly upper triangular matrices. Show that $N_n(\mathbb{R})$ is an ideal of $B_n(\mathbb{R})$.

4. Let $a \in \mathbb{F}$ and let $\rho_a : \mathbb{F}[x, y] \to \mathbb{F}[x]$ be the map which sends the polynomial $p(x, y)$ in 2-variables to the polynomial $p(x, a) \in \mathbb{F}[x]$ in 1-variable.
   (a) Show that φ is a surjective ring homomorphism.
   (b) Show that $\ker \varphi = (y - a)$. Conclude that $\mathbb{F}[x, y]/(y - a)$ and $\mathbb{F}[x]$ are isomorphic as rings.

5. Let $p(x, y) \in \mathbb{F}[x, y]$. Show that $p(x, x) = 0$ if and only if $(x - y) \mid p(x, y)$. Hint: rewrite $p(x, y)$ in the form

$$p(x, y) = c_n(y)x^n + c_{n-1}(y)x^{n-1} + \cdots + c_1(y)x + c_0(y),$$

where $c_i(y)$ is a polynomial in y only for $i = 0, 1, \ldots, n$. Use this to show that $\mathbb{F}[x, y]/(x - y)$ and $\mathbb{F}[x]$ are isomorphic as rings.

6. Let $M_n(\mathbb{R})$ be the ring of real $n \times n$ matrices and let A be an $n \times n$ matrix. Define
$$\mathrm{ev}_A : \mathbb{R}[x] \to M_n(\mathbb{R})$$
to the map which sends the real polynomial $p(x) = c_n x^n + \cdots + c_1 x + c_0$ to the real matrix
$$p(A) := c_n A^n + \cdots + c_1 A + c_0 I_n.$$
   (a) Show that ev_A is a ring homomorphism.
   (b) Show that $\ker \mathrm{ev}_A \neq \{0\}$.
   (c) Show that there exists a unique nonzero monic polynomial $m_A(x)$ such that $p(A) = 0$ if and only if $m_A(x) \mid p(x)$. (This polynomial is called the **minimal polynomial** of A; we will study this idea in greater detail in Chapter 13.)

7. The Chinese Remainder Theorem implies that there exists a real polynomial $p(x)$ which satisfies the following conditions:
$$\begin{aligned} x^2 &\mid (p(x) - x^3) \\ (x^2 + 1) &\mid (p(x) - x^4) \\ (x - 1) &\mid (p(x) - x^2). \end{aligned}$$
Find $p(x)$.

8. Let R be a ring and let I and J be ideals of R. Show that the (left, right, or two-sided) ideal $I + J$ is the smallest ideal containing I and J.

9. Prove what is commonly known as the Chinese Remainder Theorem for the integers $\mathbb{Z}$: if m and n are coprime, then for any integers a, b there exists an integer k such that $m \mid (k - a)$ and $n \mid (k - b)$. Said differently, the the system of modular equations $x \equiv a \pmod{m}$ and $x \equiv b \pmod{n}$ has a simultaneous solution.

10. An ideal $M \subseteq R$ of a commutative ring R is said to be maximal if for any ideal J of R such that $M \subseteq J$, then either $M = J$ or $J = R$.
   (a) Show that an ideal $(p(x))$ of $\mathbb{F}[x]$ is maximal if and only if $p(x)$ is an irreducible polynomial.
   (b) Prove a general version of Theorem 12.54: for a commutative ring R and an ideal J of R, R/J is a field if and only if J is a maximal ideal.

11. Prove that two integers a and b are coprime if and only if there are integers s, t such that $sa + tb = 1$

Chapter 13

The Minimal Polynomial and its Consequences

In this chapter, we state and prove some of the more advanced results of linear algebra. All of the results in this chapter revolve around a polynomial called the *minimal polynomial*, which is intimately related to the characteristic polynomial of a linear endomorphism. (Recall that a linear endomorphism is simply a linear map from a vector space V to itself.) To prove the main results of this chapter, we will need to make use of the basic ring theory that we developed in Chapter 12. Hence, the reader should study Chapter 12 before starting the current chapter. In addition to its use of ring theory, the current chapter differs from the preceding chapters because of its greater emphasis on complex vector spaces. Indeed, we must rely heavily on the power of complex numbers to prove some of the main results of this chapter.

13.1. The Minimal Polynomial

Throughout this section, we let $\mathbb{F} = \mathbb{R}$ or $\mathbb{C}$ and we let V be a vector space over $\mathbb{F}$. For a polynomial

$$p(x) = c_n x^n + c_{n-1} x^{n-1} + \cdots + c_1 x + c_0 \in \mathbb{F}[x]$$

and a linear endomorphism $\varphi \in \text{End}(V)$, we define a linear endomorphism $p(\varphi) \in \text{End}(V)$ via

$$p(\varphi) := c_n \varphi^n + c_{n-1} \varphi^{n-1} + \cdots + c_1 \varphi + c_0 id_V. \tag{246}$$

The following result will prove to be a stepping stone to the minimal polynomial:

Lemma 13.1. *For $\varphi \in End(V)$, there exists a nonzero polynomial $p \in \mathbb{F}[x]$ such that $p(\varphi) = \mathbf{0}$.*

Proof. Let $N := (\dim V)^2$ and consider the set

$$\varphi^N,\ \varphi^{N-1},\ \ldots, \varphi,\ id_V. \tag{247}$$

From Corollary 12.12, the endomorphism ring $\mathrm{End}(V)$ is a vector space of dimension N. Hence, the above set (which consists of $N+1$ elements of $\mathrm{End}(V)$) must be linearly dependent. Consequently, there exists some scalars $c_i \in \mathbb{F}$, $i = 0, 1, \ldots, N$ (not all zero) such that

$$c_N\varphi^N + c_{N-1}\varphi^{N-1} + \cdots + c_1\varphi + c_0 id_V = \mathbf{0}. \tag{248}$$

Setting

$$p(x) := c_N x^N + c_{N-1}x^{N-1} + \cdots + c_1 x + c_0$$

(which is nonzero since not all of the c_i's are zero), it follows from (248) that $p(\varphi) = \mathbf{0}$. This completes the proof. □

For $\varphi \in \mathrm{End}(V)$, let

$$\mathrm{ev}_\varphi : \mathbb{F}[x] \to \mathrm{End}(V) \tag{249}$$

be the map defined by

$$\mathrm{ev}_\varphi(p) := p(\varphi). \tag{250}$$

Theorem 13.2. *Let $\varphi \in End(V)$. Then*

(i) ev_φ is a ring homomorphism.
(ii) $\ker ev_\varphi \neq \{0\}$
(iii) Let $m_\varphi(x) \in \mathbb{F}[x]$ be a monic polynomial of minimal degree satisfying $m_\varphi(\varphi) = \mathbf{0}$. Then m_φ is unique and has the following property: if $p(x) \in \mathbb{F}[x]$ satisfies $p(\varphi) = \mathbf{0}$, then $m_\varphi(x) \mid p(x)$.

The polynomial m_φ in statement (iii) is called the ***minimal polynomial*** *of φ.*

Proof. (i): Let $p_1, p_2 \in \mathbb{F}[x]$ and let $c \in \mathbb{F}$. Let $K := \deg p_1$ and $L := \deg p_2$. Write

$$p_1(x) = \sum_{i=0}^{K} a_i x^i, \qquad p_2(x) = \sum_{i=0}^{L} b_i x^i.$$

Without loss of generality, assume $K \geq L$. If $K > L$, set $b_j := 0$ for $j = L{+}1, \ldots, K$. Then

$$(p_1 + p_2)(x) = \sum_{i=0}^{K} (a_i + b_i)x^i, \qquad cp_1(x) = \sum_{i=0}^{K} ca_i x^i$$

From this, we have

$$\begin{aligned}
\mathrm{ev}_\varphi(p_1 + p_2) &:= \sum_{i=0}^{K} (a_i + b_i)\varphi^i \\
&= \sum_{i=0}^{K} a_i \varphi^i + \sum_{i=0}^{K} b_i \varphi^i \\
&= \sum_{i=0}^{K} a_i \varphi^i + \sum_{i=0}^{L} b_i \varphi^i \\
&= p_1(\varphi) + p_2(\varphi) \\
&= \mathrm{ev}_\varphi(p_1) + \mathrm{ev}_\varphi(p_2)
\end{aligned}$$

and

$$\begin{aligned}
\mathrm{ev}_\varphi(cp_1) &:= \sum_{i=0}^{K} ca_i \varphi^i \\
&= c(\sum_{i=0}^{K} a_i \varphi^i) \\
&= cp_1(\varphi) \\
&= c\mathrm{ev}_\varphi(p_1),
\end{aligned}$$

where we set $\varphi^0 := id_V$. This proves that ev_φ is linear.

To verify that ev_φ preserves the ring multiplication, we first write

$$p_1 p_2 = \sum_{i=0}^{K} \sum_{j=0}^{L} a_i b_j x^{i+j}.$$

Then

$$\begin{aligned}
\mathrm{ev}_\varphi(p_1 p_2) &= \sum_{i=0}^{K} \sum_{j=0}^{L} a_i b_j \varphi^{i+j} \\
&= \sum_{i=0}^{K} \sum_{j=0}^{L} a_i b_j \varphi^i \varphi^j \\
&= \left(\sum_{i=0}^{K} a_i \varphi^i \right) \left(\sum_{j=0}^{L} b_j \varphi^j \right) \\
&= p_1(\varphi) p_2(\varphi) \\
&= \mathrm{ev}_\varphi(p_1)\mathrm{ev}_\varphi(p_2).
\end{aligned}$$

Also, from (246), we see that for the constant polynomial $p(x) = 1$, we have

$$\mathrm{ev}_\varphi(p) = p(\varphi) = id_V.$$

Hence, ev_φ preserves the identity element. This completes the proof that ev_φ is a ring homomorphism.

(ii): From the definition of ev_φ, $\ker \mathrm{ev}_\varphi$ consists of all polynomials p satisfying $p(\varphi) = \mathbf{0}$. Lemma 13.1 shows that there exists a nonzero polynomial $p \in \mathbb{F}[x]$ satisfying $p(\varphi) = \mathbf{0}$. Hence, $p \in \ker \mathrm{ev}_\varphi$ and we conclude that $\ker \mathrm{ev}_\varphi \neq \{0\}$.

(iii): Since $\ker \mathrm{ev}_\varphi \neq \{0\}$, there exists a monic polynomial m_φ of minimal degree satisfying $m_\varphi(\varphi) = \mathbf{0}$. (Recall that a nonzero polynomial in one variable is monic if its highest power term has coefficient 1.) Since ev_φ is a ring homomorphism, it follows from Theorem 12.21 that $\ker \mathrm{ev}_\varphi$ is an ideal of $\mathbb{F}[x]$. Theorem 12.38 now implies that $\ker \mathrm{ev}_\varphi$ is generated by m_φ:

$$\ker \mathrm{ev}_\varphi = (m_\varphi) := \{m_\varphi q \mid q \in \mathbb{F}[x]\}.$$

Consequently, if $p \in \mathbb{F}[x]$ is any polynomial satisfying $p(\varphi) = \mathbf{0}$, we have $m_\varphi(x) \mid p(x)$. Hence, m_φ has the desired property.

For the uniqueness of m_φ, let $\widehat{m}_\varphi$ be another monic polynomial of minimal degree satisfying $\widehat{m}_\varphi(\varphi) = \mathbf{0}$. Then $m_\varphi \mid \widehat{m}_\varphi$, and since m_φ and $\widehat{m}_\varphi$ are both of minimal degree, we have $\deg \widehat{m}_\varphi = \deg m_\varphi$. This implies that $\widehat{m}_\varphi(x) = cm_\varphi(x)$ for some $c \in \mathbb{F}$. Since m_φ and $\widehat{m}_\varphi$ are both monic, it follows that $c = 1$, which proves the uniqueness of m_φ. This completes the proof. □

Example 13.3. *Consider the vector space $\mathbb{R}^2$ and let $\vec{e}_1$ and $\vec{e}_2$ denote the standard basis on $\mathbb{R}^2$. Let $\varphi \in End(\mathbb{R}^2)$ be the endomorphism on $\mathbb{R}^2$ defined by*

$$\varphi(\vec{e}_1) = \vec{e}_2, \qquad \varphi(\vec{e}_2) = -\vec{e}_1.$$

Consider the monic polynomial $p(x) = x + a$ for $a \in \mathbb{R}$. Then the endomorphism $p(\varphi) : \mathbb{R}^2 \to \mathbb{R}^2$ is given by

$$p(\varphi)(\vec{e}_1) = a\vec{e}_1 + \vec{e}_2, \qquad p(\varphi)(\vec{e}_2) = -\vec{e}_1 + a\vec{e}_2.$$

Hence, $p(\varphi) \neq \mathbf{0}$. This implies that the minimal polynomial of φ must be of degree 2 or higher. Now consider the monic polynomial $q = x^2 + ax + b$ for $a, b \in \mathbb{R}$. Then

$$p(\varphi)(\vec{e}_1) = (b-1)\vec{e}_1 + a\vec{e}_2, \qquad p(\varphi)(\vec{e}_2) = -a\vec{e}_1 + (b-1)\vec{e}_2$$

Hence, $p(\varphi) = \mathbf{0}$ if and only if $a = 0$ and $b = 1$. We conclude that $m_\varphi = x^2 + 1$ is the minimal polynomial of φ.

Theorem 13.2 shows that the map ev_φ defined by (250) is a ring homomorphism. The proof of Theorem 13.2 shows that the kernel of ev_φ is the ideal generated by the minimal polynomial $m_\varphi(x)$ of φ. Applying the First Isomorphism Theorem for rings (Theorem 12.24) to ev_φ yields the following result:

Corollary 13.4. *Let $\varphi \in End(V)$ and let $\mathbb{F}[\varphi]$ denote the image of the ring homomorphism $ev_\varphi : \mathbb{F}[x] \to End(V)$. Then the induced map*

$$\widetilde{ev}_\varphi : \mathbb{F}[x]/(m_\varphi) \to \mathbb{F}[\varphi]$$

given by $[p] \mapsto ev_\varphi(p) := p(\varphi)$ is a ring isomorphism.

The notion of the minimal polynomial of a linear map can be defined for square matrices in a natural way:

Definition 13.5. *Let A be an $n \times n$ matrix whose entries lie in $\mathbb{F}$ and let $T_A : \mathbb{F}^n \to \mathbb{F}^n$ be the linear map defined by $T_A(\vec{v}) := A\vec{v}$. The **minimal polynomial** associated to A is $m_A(x) := m_{T_A}(x)$, where $m_{T_A}(x)$ is the minimal polynomial of the linear map T_A.*

Definition 13.5 is natural in the following sense:

Proposition 13.6. *Let A be an $n \times n$ matrix whose entries lie in $\mathbb{F}$. Let*

$$q(x) = x^k + c_{k-1}x^{k-1} + \cdots c_1 x + c_0 \in \mathbb{F}[x]$$

be the monic polynomial of minimal degree such that

$$q(A) := A^k + c_{k-1}A^{k-1} + \cdots + c_1 A + c_0 I_n = \mathbf{0}.$$

Then $m_A(x) = q(x)$.

Proof. Let $T_A : \mathbb{F}^n \to \mathbb{F}^n$ be the natural linear map associated to A. Let

$$p(x) = a_m x^m + a_{m-1}x^{m-1} + \cdots + a_1 x + a_0 \in \mathbb{F}[x]$$

be any polynomial. Since $(T_A)^r$ is just the natural linear map associated to the matrix A^r, that is,

$$(T_A)^r = T_{A^r},$$

it follows that

$$p(T_A)\vec{v} = (a_m A^m + a_{m-1}A^{m-1} + \cdots + a_1 A + a_0 I_n)\vec{v}.$$

In other words,

$$p(T_A) = T_{p(A)}.$$

Hence, $p(T_A)$ is the zero map if and only if $p(A)$ is the zero matrix. From this, we conclude that the minimal polynomial of T_A is the monic polynomial $q(x)$ of smallest degree for which $q(A)$ is the zero matrix. By Definition 13.5, $m_A(x) = q(x)$. □

Example 13.7. *Let*

$$A = \begin{pmatrix} 2 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & -3 \end{pmatrix}.$$

In this case, its easy to see that the minimal polynomial of A is

$$m_A(x) = (x-2)(x+3) = x^2 + x - 6.$$

13.2. The Primary Decomposition Theorem

In this section, the field $\mathbb{F}$ is again $\mathbb{R}$ or $\mathbb{C}$ and V is a vector space over $\mathbb{F}$. The following result is a special case of the **Primary Decomposition Theorem**. This result will serve as a key step in the proof of the Primary Decomposition Theorem.

Lemma 13.8. *Let $\varphi \in End(V)$. Suppose $p_1, p_2 \in \mathbb{F}[x]$ are coprime and $p_1(\varphi)p_2(\varphi) = \mathbf{0}$. Then*

(i) $\varphi(\ker p_i(\varphi)) \subset \ker p_i(\varphi)$ *for* $i = 1, 2$

(ii) $V = \ker p_1(\varphi) \oplus \ker p_2(\varphi)$

(iii) *im* $p_1(\varphi) = \ker p_2(\varphi)$ *and im* $p_2(\varphi) = \ker p_1(\varphi)$

Proof. (i): Let $v \in \ker p_1(\varphi)$. Since $p_1(\varphi)\varphi = \varphi p_1(\varphi)$, we have

$$\begin{aligned} p_1(\varphi)\varphi(v) &= \varphi p_1(\varphi)(v) \\ &= \varphi(\mathbf{0}) \\ &= \mathbf{0}. \end{aligned}$$

Hence, $\varphi(v) \in \ker p_1(\varphi)$, which proves that $\varphi(\ker p_1(\varphi)) \subset \ker p_1(\varphi)$. A similar argument shows that $\varphi(\ker p_2(\varphi)) \subset \ker p_2(\varphi)$.

(ii): Since p_1 and p_2 are coprime, Proposition 12.47 shows that there exists $q_1, q_2 \in \mathbb{F}[x]$ such that

$$1 = q_1(x)p_1(x) + q_2(x)p_2(x). \tag{251}$$

By Theorem 13.2, the map

$$\mathrm{ev}_\varphi : \mathbb{F}[x] \to \mathrm{End}(V), \qquad \mathrm{ev}_\varphi(p) := p(\varphi)$$

is a ring homomorhpism. Applying ev_φ to both sides of (251) yields

$$\begin{aligned} \mathrm{ev}_\varphi(1) &= \mathrm{ev}_\varphi(q_1p_1 + q_2p_2) \\ id_V &= \mathrm{ev}_\varphi(q_1)\mathrm{ev}_\varphi(p_1) + \mathrm{ev}_\varphi(q_2)\mathrm{ev}_\varphi(p_2) \\ id_V &= q_1(\varphi)p_1(\varphi) + q_2(\varphi)p_2(\varphi). \end{aligned} \tag{252}$$

Let $v \in \ker p_1(\varphi) \cap \ker p_2(\varphi)$. Using (252), we have

$$\begin{aligned} v &= (q_1(\varphi)p_1(\varphi) + q_2(\varphi)p_2(\varphi))\, v \\ &= q_1(\varphi)p_1(\varphi)v + q_2(\varphi)p_2(\varphi)v \\ &= q_1(\varphi)\mathbf{0} + q_2(\varphi)\mathbf{0} \\ &= \mathbf{0}. \end{aligned}$$

Hence,

$$\ker p_1(\varphi) \cap \ker p_2(\varphi) = \{\mathbf{0}\}. \tag{253}$$

Now let $v \in V$ be arbitrary. Using (252) again and noting that $a(\varphi)b(\varphi) = b(\varphi)a(\varphi)$ for all $a, b \in \mathbb{F}[x]$, we have

$$\begin{aligned} v &= q_1(\varphi)p_1(\varphi)v + q_2(\varphi)p_2(\varphi)v \\ &= p_1(\varphi)q_1(\varphi)v + p_2(\varphi)q_2(\varphi)v. \end{aligned} \tag{254}$$

Since $p_1(\varphi)p_2(\varphi) = p_2(\varphi)p_1(\varphi) = \mathbf{0}$ by hypothesis, it follows that

$$p_1(\varphi)q_1(\varphi)v \in \ker p_2(\varphi), \qquad p_2(\varphi)q_2(\varphi)v \in \ker p_1(\varphi). \tag{255}$$

(253), (254), and (255) now imply

$$V = \ker p_1(\varphi) \oplus \ker p_2(\varphi).$$

This proves (i).

(iii): Let $v_1 \in \ker p_1(\varphi)$. From (252), we have

$$\begin{aligned} v_1 &= (q_1(\varphi)p_1(\varphi) + q_2(\varphi)p_2(\varphi))v_1 \\ &= q_2(\varphi)p_2(\varphi)v_1 \\ &= p_2(\varphi)q_2(\varphi)v_1 \\ &\in \text{im } p_2(\varphi). \end{aligned}$$

Hence, $\ker p_1(\varphi) \subset \text{im } p_2(\varphi)$. Now let $u_2 \in \text{im } p_2(\varphi)$. Then $u_2 = p_2(\varphi)v$ for some $v \in V$. This implies that

$$p_1(\varphi)u_2 = p_1(\varphi)p_2(\varphi)v = \mathbf{0},$$

where we have used the fact that $p_1(\varphi)p_2(\varphi)$ is the zero map. This shows that $u_2 \in \ker p_1(\varphi)$. Hence, $\ker p_1(\varphi) \supset \text{im } p_2(\varphi)$. Combining the previous result gives $\ker p_1(\varphi) = \text{im } p_2(\varphi)$. A similar argument shows that $\ker p_2(\varphi) = \text{im } p_1(\varphi)$. This completes the proof. □

Theorem 13.9 (Primary Decomposition Theorem)**.** *Let $\varphi \in End(V)$. Suppose $p_1, p_2, \ldots, p_k \in \mathbb{F}[x]$ are pairwise coprime and*

$$p_1(\varphi)p_2(\varphi)\cdots p_k(\varphi) = \mathbf{0}.$$

Then

(i) $\varphi(\ker p_i(\varphi)) \subset \ker p_i(\varphi)$ *for* $i = 1, \ldots, k$

(ii) $V = \ker p_1(\varphi) \oplus \ker p_2(\varphi) \oplus \cdots \oplus \ker p_k(\varphi)$

Proof. (i): The proof is identical to the proof of (i) in Lemma 13.8. Once again, it follows from the fact that $p_i(\varphi)$ and φ commute:

$$p_i(\varphi)\varphi = \varphi p_i(\varphi)$$

for $i = 1, 2, \ldots, k$.

(ii): We prove this by induction on k. For $k = 1$, we simply have $p_1(\varphi) = \mathbf{0}$. Hence, $\ker p_1(\varphi) = V$. The case of $k = 2$ is statement (ii) of Lemma 13.8. So let us assume that the result is true for any k pairwise coprime polynomials where $k \geq 2$. Let $p_1, p_2, \ldots, p_{k+1} \in \mathbb{F}[x]$ be $k + 1$ pairwise coprime polynomials such that

$$p_1(\varphi)p_2(\varphi)\cdots p_{k+1}(\varphi) = \mathbf{0}. \tag{256}$$

Let $g(x) := p_1(x)p_2(x)\cdots p_k(x)$. Then g and p_{k+1} are coprime and $g(\varphi)p_{k+1}(\varphi) = \mathbf{0}$. By Lemma 13.8, we have

$$V = \ker g(\varphi) \oplus \ker p_{k+1}(\varphi) \tag{257}$$

and $\varphi(\ker g(\varphi)) \subset \ker g(\varphi)$ and $\varphi(\ker p_{k+1}(\varphi)) \subset \ker p_{k+1}(\varphi)$.

Let

$$\varphi_1 := \varphi|_{\ker g(\varphi)} : \ker g(\varphi) \to \ker g(\varphi)$$

be the restriction of φ to the subspace $\ker g(\varphi) \subset V$. Since $p_1, \ldots, p_k$ are coprime and $\varphi(\ker g(\varphi)) \subset \ker g(\varphi)$

$$\begin{aligned}
\mathbf{0} &= g(\varphi)|_{\ker g(\varphi)} \\
&= g\left(\varphi_{\ker g(\varphi)}\right) \\
&= g(\varphi_1) \\
&= p_1(\varphi_1)p_2(\varphi_1)\cdots p_k(\varphi_1).
\end{aligned}$$

By the induction hypothesis applied to the endomorphism $\varphi_1 \in \mathrm{End}(\ker g(\varphi))$ and the k pairwise coprime polynomials $p_1, \ldots, p_k$, we have

$$\ker g(\varphi) = \ker p_1(\varphi_1) \oplus \ker p_2(\varphi_1) \oplus \cdots \oplus \ker p_k(\varphi_1). \tag{258}$$

We now show that $\ker p_i(\varphi_1) = \ker p_i(\varphi)$ for $i = 1, 2, \ldots, k$. To do this, let $v \in \ker p_i(\varphi_1) \subset \ker g(\varphi)$. Then

$$\begin{aligned} p_i(\varphi)v &= \left(p_i(\varphi)|_{\ker g(\varphi)}\right) v \\ &= p_i\left(\varphi|_{\ker g(\varphi)}\right) v \\ &= p_i(\varphi_1)v \\ &= \mathbf{0}. \end{aligned}$$

Hence, $\ker p_i(\varphi_1) \subset \ker p_i(\varphi)$. On the other hand, for $v \in \ker p_i(\varphi)$, we have

$$\begin{aligned} g(\varphi)v &= p_1(\varphi)p_2(\varphi)\cdots p_i(\varphi)\cdots p_k(\varphi)v \\ &= p_1(\varphi)p_2(\varphi)\cdots \widehat{p_i(\varphi)}\cdots p_k(\varphi)p_i(\varphi)v \\ &= \mathbf{0} \end{aligned}$$

where $\widehat{p_i(\varphi)}$ denotes the omission of $p_i(\varphi)$. This implies that $v \in \ker g(\varphi)$. Hence, v is in the domain of $p_i(\varphi_1)$. Applying $p_i(\varphi_1)$ to v gives

$$\begin{aligned} p_i(\varphi_1)v &= p_i\left(\varphi|_{\ker g(\varphi)}\right) v \\ &= \left(p_i(\varphi)|_{\ker g(\varphi)}\right) v \\ &= p_i(\varphi)v \\ &= \mathbf{0}. \end{aligned}$$

Hence, $\ker p_i(\varphi_1) \supset \ker p_i(\varphi)$ for $i = 1, 2, \ldots, k$. We have thus proved that

$$\ker p_i(\varphi_1) = \ker p_i(\varphi) \tag{259}$$

for $i = 1, \ldots, k$. Equations (257), (258), and (259) now imply

$$V = \ker p_1(\varphi) \oplus \ker p_2(\varphi) \oplus \cdots \oplus \ker p_k(\varphi) \oplus \ker p_{k+1}(\varphi).$$

This completes the proof. □

Example 13.10. *Consider the vector space* $\mathbb{R}^4$ *and let* $\vec{e}_1, \vec{e}_2, \vec{e}_3, \vec{e}_4$ *denote the standard basis on* $\mathbb{R}^4$. *Let* $\varphi : \mathbb{R}^4 \to \mathbb{R}^4$ *be the linear map defined by*

$$\varphi(\vec{e}_1) = \vec{e}_3, \quad \varphi(\vec{e}_2) = \vec{e}_4, \quad \varphi(\vec{e}_3) = -\vec{e}_1, \quad \varphi(\vec{e}_4) = \vec{e}_2$$

Let $p_1 = x^2 + 1$ *and* $p_2 = x^2 - 1$. *Then* p_1 *and* p_2 *are coprime. By direct calculation, one finds that*

$$p_1(\varphi)p_2(\varphi) = \mathbf{0}.$$

Theorem 13.9 (or Lemma 13.8 in this case) implies that

$$\mathbb{R}^4 = \ker p_1(\varphi) \oplus \ker p_2(\varphi).$$

By a straightforward calculation, we find that

$$\ker p_1(\varphi) = span\{\vec{e}_1, \vec{e}_3\}, \qquad \ker p_2(\varphi) = span\{\vec{e}_2, \vec{e}_4\}.$$

In this case, one finds that there are no monic polynomials p *in degrees 1,2, and 3 satisfying* $p(\varphi) = \mathbf{0}$. *From this, we deduce that the minimal polynomial of* φ *is* $m_\varphi = (x^2 + 1)(x^2 - 1) = x^4 - 1$.

13.3. Diagonalizable Linear Maps

In this section, we study the minimal polynomial associated to diagonalizable linear maps and prove a well known theorem about *simultaneously diagonalizable* linear maps (a notion which we will define precisely a bit later). Throughout this section, the field $\mathbb{F}$ is either $\mathbb{R}$ or $\mathbb{C}$ and V is a vector space over $\mathbb{F}$. We being with some basic observations:

Proposition 13.11. *Let* $\varphi : V \to V$ *be a linear map and let* $\lambda_1, \ldots, \lambda_k$ *be distinct eigenvalues of* φ. *Let* v_i *be an eigenvector of* φ *associated to* λ_i *for* $i = 1, \ldots, k$. *Then* $\{v_1, \ldots, v_k\}$ *is linearly independent.*

Proof. For $l \leq k$, let

$$E_l := \{v_1, v_2, \ldots, v_l\}.$$

For $l = 1$, $E_l = \{v_1\}$ is a linear independent set (since eigenvectors are nonzero by definition). We now prove that E_l is linearly independent for $l = 1, 2, \ldots, k$ by induction on l. Suppose then that E_l is linearly independent. Let us suppose that

$$v_1, v_2, \ldots, v_{l+1}$$

is linearly dependent. This implies that

$$v_{l+1} \in \operatorname{span}\{v_1, \ldots, v_l\}.$$

Let us express v_{l+1} as a linear combination of the elements of E_l:

$$v_{l+1} = \sum_{i=1}^{l} \alpha_i v_i. \tag{260}$$

Applying φ to both sides of (260) gives

$$\begin{aligned}\varphi(v_{l+1}) &= \sum_{i=1}^{l} \alpha_i \varphi(v_i) \\ \lambda_{l+1} v_{l+1} &= \sum_{i=1}^{l} \alpha_i \lambda_i v_i. \end{aligned} \tag{261}$$

On the other hand, multiplying both sides of (260) by λ_l gives

$$\lambda_{l+1} v_{l+1} = \sum_{i=1}^{l} \alpha_i \lambda_{l+1} v_i. \tag{262}$$

Subtracting (261) from (262) gives

$$\sum_{i=1}^{l} \alpha_i (\lambda_{l+1} - \lambda_i) v_i = \mathbf{0}.$$

Since $v_1, \ldots, v_l$ are linearly independent, it follows that $\alpha_i(\lambda_{l+1} - \lambda_i) = 0$ for $i = 1, \ldots, l$. Since $\lambda_i \neq \lambda_j$ for $i \neq j$, it follows that $\alpha_i = 0$ for $i = 1, \ldots, l$. From (260), this implies that $v_{l+1} = \mathbf{0}$, which is a contradiction since eigenvectors are nonzero by definition. Hence, we conclude that E_{l+1} is linearly independent. In particular, $E_k := \{v_1, \ldots, v_k\}$ is linearly independent. This completes the proof. □

Proposition 13.12. *Let $\varphi : V \to V$ be a linear map and let $\lambda_1, \ldots, \lambda_k$ denote all the distinct eigenvalues of φ. Also, let E_i denote the eigenspace of φ associated to λ_i for $i = 1, \ldots, k$. Then φ is diagonalizable if and only if*

$$V = E_1 \oplus E_2 \oplus \cdots \oplus E_k.$$

Proof. Since φ is diagonalizable, V has a basis $\{v_1, \ldots, v_n\}$ which consists of eigenvectors of φ. Hence, each v_i lies in some E_j. This implies that

$$V = E_1 + E_2 + \cdots + E_k.$$

We now show that this sum is actually a direct sum. To do this, let $u_i \in E_i$ for $i = 1, \ldots, k$ and suppose that

$$u_1 + u_2 + \cdots + u_k = \mathbf{0}.$$

Let $S := \{u_i \mid u_i \neq \mathbf{0}\}$. If $S \neq \emptyset$, then S is a linearly dependent set consisting of eigenvectors associated to distinct eigenvalues. However, this contradicts Proposition 13.11. From this, we conclude that $u_1 = u_2 = \cdots = u_k = \mathbf{0}$. This implies that V is a direct sum of the E_i's.

Now suppose that V is a direct sum of the eigenspaces E_i, $i = 1, \dots, k$. Let $\mathcal{B}_i$ be any basis on E_i for $i = 1, \dots, k$. Then

$$\mathcal{B} = \mathcal{B}_1 \cup \mathcal{B}_2 \cup \cdots \cup \mathcal{B}_k$$

is a basis of V consisting of the eigenvectors of φ. Hence, φ is diagonalizable. $\square$

The following result expresses the condition of diagonalizability in terms of the minimal polynomial.

Theorem 13.13. *Let $\varphi : V \to V$ be a linear map and let $\lambda_1, \dots, \lambda_k$ denote the distinct eigenvalues of φ. Then φ is diagonalizable if and only if its minimal polynomial is*

$$m_\varphi(x) = (x - \lambda_1)(x - \lambda_2) \cdots (x - \lambda_k). \tag{263}$$

Proof. Suppose first that $\varphi : V \to V$ is diagonalizable. Let $m_\varphi(x)$ denote the minimal polynomial of φ. Also, let $p_i(x) = x - \lambda_i$ for $i = 1, \dots, k$ and let

$$p(x) = p_1(x)p_2(x) \cdots p_k(x).$$

Note that $p(x)$ is a monic polynomial.

Let E_i be the eigenspace associated to λ_i for $i = 1, \dots, k$. By Proposition 13.12,

$$V = E_1 \oplus E_2 \oplus \cdots \oplus E_k.$$

Let $u_i \in E_i$. Since $\varphi(u_i) = \lambda_i u_i$, we have

$$p_i(\varphi)u_i = (\varphi - \lambda_i id_V)u_i = \varphi(u_i) - \lambda_i u_i = \lambda_i u_i - \lambda_i u_i = \mathbf{0}.$$

Hence,

$$\begin{aligned} p(\varphi)u_i &= p_1(\varphi)p_2(\varphi) \cdots p_k(\varphi)u_i \\ &= p_1(\varphi)p_2(\varphi) \cdots \widehat{p_i(\varphi)} \cdots p_k(\varphi)p_i(\varphi)u_i \\ &= p_1(\varphi)p_2(\varphi) \cdots \widehat{p_i(\varphi)} \cdots p_k(\varphi)\mathbf{0} \\ &= \mathbf{0} \end{aligned}$$

where $\widehat{p_i(\varphi)}$ denotes omission of $p_i(\varphi)$. Since V is a direct sum of the E_i's, it follows that $p(\varphi) = \mathbf{0}$. Theorem 13.2 implies that

$$m_\varphi(x) \mid p(x).$$

Since $p_1, p_2, \dots, p_k$ are distinct linear factors (and hence irreducible and pairwise coprime - see Definitions 12.50 and 12.42), it follows that m_φ must be a product of some subset of $\{p_1, p_2, \dots, p_k\}$. So let us suppose that for some integers

$$1 \leq a_1 < a_2 < \cdots < a_l \leq k,$$

we have

$$m_\varphi = p_{a_1} p_{a_2} \cdots p_{a_l}.$$

Suppose now that some linear factor p_j is missing from m_φ. Then for $u_j \in E_j$, we have

$$p_{a_i}(\varphi)u_j = (\lambda_j - \lambda_{a_i})u_j \neq \mathbf{0}$$

for $i = 1, 2, \ldots, l$. Hence

$$\begin{aligned} m_\varphi(\varphi)u_j &= p_{a_1}(\varphi)p_{a_2}(\varphi)\cdots p_{a_l}(\varphi)u_j \\ &= (\lambda_{a_1} - \lambda_j)(\lambda_{a_2} - \lambda_j)\cdots(\lambda_{a_l} - \lambda_j)u_j \\ &\neq \mathbf{0}, \end{aligned}$$

which is a contradiction. Hence, m_φ must be a product of **all** the p_i's:

$$m_\varphi = p = p_1 p_2 \cdots p_k = (x - \lambda_1)(x - \lambda_2)\cdots(x - \lambda_k).$$

This proves the first half of the theorem.

Now let us suppose that the minimal polynomial m_φ of φ is given by (263). Since the factors $(x - \lambda_i)$ for $i = 1, \ldots, k$ are pairwise coprime, the Primary Decomposition Theorem (Theorem 13.9) implies that

$$V = \ker(\varphi - \lambda_1 id_V) \oplus \ker(\varphi - \lambda_2 id_V) \oplus \cdots \oplus \ker(\varphi - \lambda_k id_V).$$

However, $\ker(\varphi - \lambda_i id_V)$ is simply the eigenspace of φ associated to λ_i for $i = 1, \ldots, k$. By Proposition 13.12, φ is diagonalizable. □

Definition 13.14. *Let $\varphi_1, \ldots, \varphi_m \in End(V)$ be diagonalizable linear maps. The linear maps $\varphi_1, \ldots, \varphi_m$ are **simultaneously diagonalizable** if there exists a basis $\mathcal{B}$ of V such that each element of $\mathcal{B}$ is an eigenvector of φ_i for $i = 1, \ldots, m$.*

Example 13.15. *Consider the vector space $\mathbb{R}^2$ and let $\vec{e}_1$ and $\vec{e}_2$ be the standard basis on $\mathbb{R}^2$. Let $\varphi_1, \varphi_2 \in End(\mathbb{R}^2)$ be the linear maps defined by*

$$\varphi_1(\vec{e}_1) = \vec{e}_1 + 2\vec{e}_2, \qquad \varphi_1(\vec{e}_2) = 2\vec{e}_1 + \vec{e}_2$$

and

$$\varphi_2(\vec{e}_1) = 3\vec{e}_1 - \vec{e}_2, \qquad \varphi_2(\vec{e}_2) = -\vec{e}_1 + 3\vec{e}_2.$$

With a little work, one finds that φ_1 and φ_2 are diagonalizable with eigenvectors

$$\vec{e}_1 + \vec{e}_2, \qquad \vec{e}_1 - \vec{e}_2.$$

Indeed,

$$\varphi_1(\vec{e}_1 + \vec{e}_2) = 3(\vec{e}_1 + \vec{e}_2), \qquad \varphi_1(\vec{e}_1 - \vec{e}_2) = -(\vec{e}_1 - \vec{e}_2),$$

and

$$\varphi_2(\vec{e}_1 + \vec{e}_2) = 2(\vec{e}_1 + \vec{e}_2), \qquad \varphi_2(\vec{e}_1 - \vec{e}_2) = 4(\vec{e}_1 - \vec{e}_2),$$

Since the vectors $\vec{e}_1 + \vec{e}_2$ and $\vec{e}_1 - \vec{e}_2$ form a basis on $\mathbb{R}^2$, we conclude that φ_1 and φ_2 are simultaneously diagonalizable.

We conclude this section by proving a well known theorem about simultaneously diagonalizable linear maps. Before doing this, we need the following result:

Lemma 13.16. *Let $\varphi : V \to V$ be diagonalizable linear maps. If U is a subspace of V which is* ***invariant*** *under φ, that is, $\varphi(U) \subset U$. Then the restriction to U*

$$\varphi|_U : U \to U$$

is also diagonalizable.

Proof. Let $\lambda_1, \ldots, \lambda_k$ be the distinct eigenvalues of φ. Let $\rho := \varphi|_U$. Since φ is diagonalizable, Theorem 13.13 implies that the minimal polynomial of φ is

$$m_\varphi = (x - \lambda_1)(x - \lambda_2) \cdots (x - \lambda_k).$$

Let m_ρ be the minimal polynomial of ρ. Since $m_\varphi(\varphi) = \mathbf{0}$, we also have

$$\begin{aligned} m_\varphi(\rho)(U) &= m_\varphi(\varphi|_U)(U) \\ &= m_\varphi(\varphi)(U) \\ &= \mathbf{0}. \end{aligned}$$

Theorem 13.2 implies that $m_\rho \mid m_\varphi$. Since m_φ consists of distinct linear factors $(x - \lambda_i)$, $i = 1, \ldots, k$, it follows that m_ρ must be a product of some subset of the factors $\{x - \lambda_i \mid i = 1, \ldots, k\}$. Theorem 13.13 implies that $\rho := \varphi|_U$ is diagonalizable. □

Theorem 13.17. *Let $\varphi_1, \ldots, \varphi_m \in End(V)$ be diagonalizable linear maps. Then the linear maps $\varphi_1, \ldots, \varphi_m$ are simultaneously diagonalizable if and only if they commute with one another, that is, $\varphi_i \varphi_j = \varphi_j \varphi_i$ for all $i, j \in \{1, \ldots, m\}$.*

Proof. ($\Leftarrow$): Suppose $\varphi_1, \ldots, \varphi_m$ are commuting diagonalizable linear maps. We show that they are simultaneously diagonalizable by induction on m. For $m = 1$, we have a single diagonalizable linear map $\{\varphi_1\}$, which is simultaneously diagonalizable in a trivial way. Now suppose that the result is true for m commutating diagonalizable linear maps.

Let $\varphi_1, \ldots, \varphi_m, \varphi_{m+1}$ be any $m+1$ commuting diagonalizable linear maps. Let $\lambda_1, \ldots, \lambda_k$ be the distinct eigenvalues of $\varphi_{m+1} : V \to V$ and let E_i be the eigenspace of φ_{m+1} associated to λ_i for $i = 1, \ldots, k$. Let $e_i \in E_i$. Then for $j \leq m$, we have

$$\begin{aligned} \varphi_{m+1}\varphi_j(e_i) &= \varphi_j \varphi_{m+1}(e_i) \\ &= \lambda_i \varphi_j(e_i). \end{aligned}$$

Hence $\varphi_j(e_i)$ is an eigenvector of φ_{m+1} associated to λ_i. Hence, $\varphi_j(E_i) \subset E_i$ for $j = 1, \ldots, m$. By Lemma 13.16, the restricted linear map

$$\varphi_j|_{E_i} : E_i \to E_i$$

is diagonalizable for $j = 1, \ldots, m$. By the induction hypothesis, the m commuting diagonalizable linear maps

$$\varphi_1|_{E_i}, \varphi_2|_{E_i}, \ldots, \varphi_m|_{E_i}$$

are simultaneously diagonalizable. Hence, there exists a basis $\mathcal{B}_i$ of E_i such that each basis element of $\mathcal{B}_i$ is an eigenvector of $\varphi_1, \ldots, \varphi_m$. Since $\mathcal{B}_i \subset E_i$, every element of $\mathcal{B}_i$ is, of course, an eigenvector of φ_{m+1} as well. The set

$$\mathcal{B} := \mathcal{B}_1 \cup \mathcal{B}_2 \cup \cdots \cup \mathcal{B}_k$$

is then a basis of V and, by construction, every element of $\mathcal{B}$ is an eigenvector of φ_i for $i = 1, \ldots, m+1$. Hence, $\varphi_1, \ldots, \varphi_{m+1}$ are simultaneously diagonalizable.

($\Rightarrow$): Suppose that $\varphi_1, \ldots, \varphi_m$ are simultaneously diagonalizable. We now show that they also commute with one another. By definition, there exists a basis $v_1, \ldots, v_n$ of V such that v_i is an eigenvector of φ_j for $j = 1, \ldots, m$. Hence, for $i = 1, \ldots, n$ and $j = 1, \ldots, m$, we have

$$\varphi_j(v_i) = \lambda_{ji} v_i$$

for some $\lambda_{ji} \in \mathbb{F}$. Then

$$\begin{aligned} \varphi_l \varphi_j(v_i) &= \lambda_{ji} \varphi_l(v_i) \\ &= \lambda_{ji} \varphi_l(v_i) \\ &= \lambda_{ji} \lambda_{li} v_i \\ &= \varphi_j \varphi_l(v_i) \end{aligned} \tag{264}$$

for $i = 1, \ldots, n$ and $j, l = 1, \ldots, m$. Since $\{v_1, \ldots, v_n\}$ is a basis, (264) implies that $\varphi_j \varphi_l = \varphi_l \varphi_j$ for all $j, l = 1, \ldots, m$. □

Remark 13.18. *The basic mathematical framework underlying quantum mechanics is linear algebra. In quantum mechanics, a physical system is represented by a complex inner product space $(\mathcal{H}, \langle \cdot, \cdot \rangle)$. In this framework, the observables (i.e. the physical quantities one measures like position or momentum) are represented by self-adjoint operators. Recall from Theorem 9.56 that self-adjoint linear maps are diagonalizable. In quantum mechanics, the eigenvectors of a self-adjoint map correspond to various physical states of the system. The eigenvalues of a self-adjoint linear map φ are the possible values that the observable represented by φ can take on (after a measurement). Two self-adjoint operators which commute are simultaneously diagonalizable by Theorem 13.17. Hence, they share the same eigenvectors (or physical states). Physically, commuting self-adjoint operators represent* *observables which can be measured simultaneously. Self-adjoint operators which do not commute represent observables which cannot be measured simultaneously. This is the mathematical underpinning behind the famous Heisenberg uncertainty principle.*

13.4. Geometric Multiplicity vs Algebraic Multiplicity

In this brief section, V is a vector space over $\mathbb{F}$, where $\mathbb{F} = \mathbb{R}$ or $\mathbb{C}$.

Definition 13.19. *Let $\varphi : V \to V$ be a linear map and let p_φ be the characteristic polynomial of φ. Also, let λ be an eigenvalue of φ and let E_λ be the eigenspace of φ associated to λ.*

*(i) The **geometric multiplicity** of λ is $\dim E_\lambda$.*

*(ii) The **algebraic multiplicity** of λ is the largest integer k such that $(x-\lambda)^k \mid p_\varphi(x)$.*

We will denote the geometric multiplicity of λ by $\mathcal{G}(\lambda)$ and the algebraic multiplicity of λ by $\mathcal{A}(\lambda)$.

Example 13.20. *Consider the vector space $\mathbb{R}^2$ and let $\vec{e}_1$ and $\vec{e}_2$ denote the standard basis on $\mathbb{R}^2$. Let $\varphi : \mathbb{R}^2 \to \mathbb{R}^2$ be the linear map defined by*

$$\varphi(\vec{e}_1) = \vec{e}_1, \qquad \varphi(\vec{e}_2) = \vec{e}_1 + \vec{e}_2.$$

The matrix representation of φ with respect to the standard basis $\mathcal{S} = \{\vec{e}_1, \vec{e}_2\}$ is

$$[\varphi]_{\mathcal{S}} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

From this, we find that the characteristic polynomial of φ is

$$p_\varphi(x) = det(xI_2 - [\varphi]_{\mathcal{S}}) = (x-1)^2.$$

φ has only one eigenvalue: 1. From p_φ, we see that the algebraic multiplicity of 1 is $\mathcal{A}(1) = 2$. On the other hand, the eigenspace of 1 is spanned by $\vec{e}_1$. Hence, the geometric multiplicity of 1 is $\mathcal{G}(1) = 1$.

In the previous example, we have $\mathcal{G}(\lambda) \leq \mathcal{A}(\lambda)$. *Is this always the case*? The answer is given by the following result:

Theorem 13.21. *Let $\varphi : V \to V$ be a linear map and let λ be an eigenvalue of φ. Then $\mathcal{G}(\lambda) \leq \mathcal{A}(\lambda)$.*

Proof. Let E_λ be the eigenspace of φ and let $\{v_1, \dots, v_k\}$ be a basis on E_λ. Extend this to a basis on V:

$$\mathcal{B} := \{v_1, \dots, v_k, v_{k+1}, \dots, v_n\}.$$

Since $\varphi(v_i) = \lambda v_i$ for $i \leq k$, the matrix representation of φ with respect to $\mathcal{B}$ has the form

$$[\varphi]_{\mathcal{B}} = \begin{pmatrix} \lambda I_k & X \\ \mathbf{0}_{n-k,k} & Y \end{pmatrix},$$

where I_k is the $k \times k$ identity matrix, $\mathbf{0}_{n-k,k}$ is the $(n-k) \times k$ zero matrix, X is some $(n-k) \times k$ matrix, and Y is some $(n-k) \times (n-k)$ matrix. Let

$$Q = xI_n - [\varphi]_{\mathcal{B}} = \begin{pmatrix} (x-\lambda) I_k & -X \\ \mathbf{0}_{n-k,k} & xI_{n-k} - Y \end{pmatrix}.$$

The characteristic polynomial of φ is then $p_\varphi(x) = \det(Q)$. Since the diagonal elements of the matrix $xI_{n-k} - Y$ are degree 1 polynomials, it follows that these very same elements can be used as pivots to transform $xI_{n-k} - Y$ into an upper triangular matrix. Hence, we only need the row operation

$$cR_i + R_j \to R_j$$

to transform $xI_{n-k} - Y$ (and hence Q) into an upper triangular matrix. The only difference here is that c is not an element of $\mathbb{F}$. Instead, c is a function of x of the form

$$\frac{a}{f(x)}$$

where $a \in \mathbb{F}$ and $f(x)$ is a degree 1 polynomial. Let A denote the upper triangular matrix obtained from $xI_{n-k} - Y$ after row operations and let

$$Q' = xI_n - [\varphi]_{\mathcal{B}} = \begin{pmatrix} (x-\lambda) I_k & -X \\ \mathbf{0}_{n-k,k} & A \end{pmatrix},$$

From our study of determinants, $\det(Q') = \det(Q)$. In addition, we recall that that the determinant of an upper triangular matrix is just the product of all its diagonal elements. Let $h(x)$ denote the product of the diagonal elements of A. Then h is a polynomial of degree $n-k$. Hence,

$$\begin{aligned} p_\varphi &= \det(Q) \\ &= \det(Q') \\ &= (x-\lambda)^k h(x). \end{aligned}$$

Since $(x-\lambda)^k \mid p_\varphi$ and $k = \dim E_\lambda$, it follows immediately that $\mathcal{G}(\lambda) \leq \mathcal{A}(\lambda)$. □

We conclude this section with another characterization of diagonalizable linear maps.

Theorem 13.22. *Let V be a* ***complex*** *vector space and let $\varphi : V \to V$ be a linear map. Also, let $\lambda_1, \ldots, \lambda_k$ denote all the eigenvalues of φ. Then φ is diagonalizable if and only if $\mathcal{G}(\lambda_i) = \mathcal{A}(\lambda_i)$ for $i = 1, \ldots, k$.*

Proof. Let p_φ be the characteristic polynomial of φ. Since V is a complex vector space, $p_\varphi \in \mathbb{C}[x]$. The Fundamental Theorem of algebra implies that p_φ completely factors:

$$p_\varphi = (x - \lambda_1)^{a_1}(x - \lambda_2)^{a_2} \cdots (x - \lambda_k)^{a_k}. \tag{265}$$

From the definition of algebraic multiplicity, we have $\mathcal{A}(\lambda_i) := a_i$ for $i = 1, \ldots, k$. Let E_i denote the eigenspace of φ associated to λ_i.

Suppose first that φ is diagonalizable. Let $\mathcal{B}_i$ be a basis of E_i for $i = 1, \ldots, k$. Let

$$\mathcal{B} := \mathcal{B}_1 \cup \mathcal{B}_2 \cup \cdots \cup \mathcal{B}_k.$$

Let $g_i := \mathcal{G}(\lambda_i) := \dim E_i$ for $i = 1, \ldots, k$. The matrix representation of φ with respect to $\mathcal{B}$ is then

$$[\varphi]_{\mathbb{B}} = \begin{pmatrix} \lambda_1 I_{g_1} & \mathbf{0} & \mathbf{0} & \cdots & \mathbf{0} \\ \mathbf{0} & \lambda_2 I_{g_2} & \mathbf{0} & \cdots & \mathbf{0} \\ \vdots & \vdots & \ddots & \cdots & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \cdots & \lambda_k I_{g_k} \end{pmatrix}, \tag{266}$$

where "$\mathbf{0}$" here denotes zero matrices of various sizes. From (266), we have

$$p_\varphi = (x - \lambda_1)^{g_1}(x - \lambda_2)^{g_2} \cdots (x - \lambda_k)^{g_k}. \tag{267}$$

Comparing (265) and (267), we have $a_i = g_i$ for $i = 1, \ldots, k$. Hence, $\mathcal{A}(\lambda_i) = \mathcal{G}(\lambda_i)$ for $i = 1, \ldots, k$.

Now suppose that $\mathcal{A}(\lambda_i) = \mathcal{G}(\lambda_i)$ for $i = 1, \ldots, k$. Since the degree of the characteristic polynomial is equal to $\dim V$, we have

$$\begin{aligned} \dim V &= \mathcal{A}(\lambda_1) + \mathcal{A}(\lambda_2) + \cdots + \mathcal{A}(\lambda_k) \\ &= \mathcal{G}(\lambda_1) + \mathcal{G}(\lambda_2) + \cdots + \mathcal{G}(\lambda_k) \\ &= \dim E_1 + \dim E_2 + \cdots + \dim E_k. \end{aligned} \tag{268}$$

This implies

$$V = E_1 \oplus E_2 \oplus \cdots \oplus E_k.$$

Proposition 13.12 now implies that φ is diagonalizable. □

13.5. Block Matrices and Jordan Blocks

In this section, we formally introduce the notion of **block matrices** with particular emphasis on **block diagonal matrices**.

Definition 13.23. *A **block matrix** is a matrix of the form*

$$\begin{pmatrix} A_{11} & A_{12} & \cdots & A_{1n} \\ A_{21} & A_{22} & \cdots & A_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ A_{m1} & A_{m2} & \cdots & A_{mn} \end{pmatrix}$$

*where A_{ij} for $i = 1, \ldots, m$ and $j = 1, \ldots, n$ are matrices of appropriate sizes called the **blocks** of A.*

A special (yet important) case of Definition 13.23 is the following:

Definition 13.24. *A **block diagonal matrix** is a matrix of the form*

$$\begin{pmatrix} A_1 & \mathbf{0} & \cdots & \mathbf{0} \\ \mathbf{0} & A_2 & \cdots & \mathbf{0} \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{0} & \mathbf{0} & \cdots & A_k \end{pmatrix}$$

where the blocks $A_1, A_2, \ldots, A_k$ are square matrices (not necessarily of the same size) and $\mathbf{0}$ denotes zero matrices of appropriate sizes.

Example 13.25. *The matrix*

$$A = \begin{pmatrix} 1 & -1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & -2 & 4 & 1 & 0 & 0 \\ 0 & 0 & 2 & 1 & 5 & 0 & 0 \\ 0 & 0 & -3 & 2 & -4 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 6 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & -2 \end{pmatrix}$$

is block diagonal with blocks

$$A_1 = \begin{pmatrix} 1 & -1 \\ 0 & 2 \end{pmatrix}, \qquad A_2 = \begin{pmatrix} -2 & 4 & 1 \\ 2 & 1 & 5 \\ -3 & 2 & -4 \end{pmatrix}, \qquad A_3 = (6), \qquad A_4 = (-2).$$

Recall from our study of determinants that the determinant of an upper triangular matrix is simply the product of its diagonal elements. The following result is a generalization of this.

Theorem 13.26. *Let A be a block matrix of the form*

$$A = \begin{pmatrix} A_{11} & A_{12} & A_{13} & \cdots & A_{1k} \\ \mathbf{0} & A_{22} & A_{23} & \cdots & A_{2k} \\ \mathbf{0} & \mathbf{0} & A_{33} & \cdots & A_{3k} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \cdots & A_{kk} \end{pmatrix}$$

where the block diagonals A_{ii} for $i = 1, \dots, k$ are square matrices (not necessarily of the same size). Then the determinant of A is just the product of the determinants of its diagonal blocks, that is,

$$\det(A) = \det(A_{11})\det(A_{22})\cdots\det(A_{kk}).$$

Proof. Using row operations, we can transform A into an upper triangular matrix. Given the form of A, this amounts to using row operations to transform each of its diagonal blocks into an upper triangular matrix. Let us recall the effect on the determinant from each type of row operation:

1. $R_i \leftrightarrow R_j$ $(i \neq j)$: changes the sign of the determinant
2. $cR_i \to R_i$: scales the determinant by a factor of c
3. $cR_i + R_j \to R_j$: no change

Using only row operations 1 and 3, A can be transformed into an upper triangular matrix A'. Let s_i denote the number of row swaps used in transforming A_{ii} into an upper triangular matrix A'_{ii}. Let α_i denote the product of the diagonal elements of A'_{ii}. From our study of determinants, the determinant of an upper triangular matrix is simply the product of its diagonal elements. Hence, $\det(A'_{ii}) = \alpha_i$. The determinant of A_{ii} and A'_{ii} are then related by

$$\det(A_{ii}) = (-1)^{s_i}\det(A'_{ii}) = (-1)^{s_i}\alpha_i.$$

The determinant of A' is then the product of its all diagonal elements. Hence,

$$\begin{aligned}\det(A') &= \alpha_1\alpha_2\cdots\alpha_k \\ &= \det(A'_{11})\det(A'_{22})\cdots\det(A'_{kk}).\end{aligned}$$

Let $s = \sum_{i=1}^{k} s_i$ be the total number of row swaps needed in transforming A into A'. The determinant of A is then given by

$$\begin{aligned}\det(A) &= (-1)^s\det(A') \\ &= (-1)^s\det(A'_{11})\det(A'_{22})\cdots\det(A'_{kk}) \\ &= (-1)^{s_1}(-1)^{s_2}\cdots(-1)^{s_k}\det(A'_{11})\det(A'_{22})\cdots\det(A'_{kk}) \\ &= ((-1)^{s_1}\det(A'_{11}))\,((-1)^{s_2}\det(A'_{22}))\cdots((-1)^{s_k}\det(A'_{kk})) \\ &= \det(A_{11})\det(A_{22})\cdots\det(A_{kk}).\end{aligned}$$

□

Example 13.27. *Let*

$$A = \begin{pmatrix} 2 & 1 & -3 & 7 \\ -1 & 5 & 8 & 3 \\ 0 & 0 & 5 & -2 \\ 0 & 0 & 2 & 7 \end{pmatrix}.$$

By Theorem 13.26, the determinant of A is

$$\begin{aligned} \det(A) &= \det\begin{pmatrix} 2 & 1 \\ -1 & 5 \end{pmatrix} \det\begin{pmatrix} 5 & -2 \\ 2 & 7 \end{pmatrix} \\ &= (11)(39) \\ &= 429. \end{aligned}$$

The following is a special case of Theorem 13.26:

Corollary 13.28. *The determinant of a block diagonal matrix*

$$A = \begin{pmatrix} A_1 & \mathbf{0} & \cdots & \mathbf{0} \\ \mathbf{0} & A_2 & \cdots & \mathbf{0} \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{0} & \mathbf{0} & \cdots & A_k \end{pmatrix}$$

is the product of the determinants of its diagonal blocks, that is,

$$\det(A) = \det(A_1)\det(A_2)\cdots\det(A_k).$$

Example 13.29. *Consider the matrix A from Example 13.25. By Theorem 13.26, the determinant of A is*

$$\begin{aligned} \det(A) &= \det(A_1)\det(A_2)\det(A_3)\det(A_4) \\ &= (2)(7)(6)(-2) \\ &= -168. \end{aligned}$$

Definition 13.30. *A* ***Jordan block*** *of size n is an $n \times n$ matrix consisting of a number $\lambda \in \mathbb{F}$ along the main diagonal and the number 1 along the superdiagonal:*

$$J_n(\lambda) := \begin{pmatrix} \lambda & 1 & 0 & 0 & \cdots & 0 \\ 0 & \lambda & 1 & 0 & \cdots & 0 \\ 0 & 0 & \lambda & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \ddots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & 1 \\ 0 & 0 & 0 & 0 & \cdots & \lambda \end{pmatrix}$$

A block diagonal matrix consisting of Jordan blocks is said to be in ***Jordan canonical form****.*

Example 13.31. *The matrix*

$$A = \begin{pmatrix} 3 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 3 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & -4 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -4 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

is in Jordan canonical form with Jordan blocks $J_2(3)$, $J_2(-4)$, and $J_3(0)$.

A matrix in Jordan canonical form is a diagonal matrix if and only if it consists of Jordan blocks of size 1. Intuitively, a matrix which is in Jordan canonical form is "close" to being a diagonal matrix. As we have seen, not every linear endomorphism is diagonalizable. However, for every linear endomorphism φ on a **complex** vector space V, we can settle for the next best thing: one can always find a basis $\mathcal{B}$ of V for which the matrix representation $[\varphi]_{\mathcal{B}}$ is in Jordan canonical form. The rest of this chapter will be devoted to proving this result and exploring a few of its consequences.

13.6. Nilpotent Maps

As we alluded to in the previous section, every linear endomorphism on a complex vector space V has a basis $\mathcal{B}$ for which its matrix representation can be put into the Jordan canonical form. We will see later that the Jordan canonical form implies that a linear map can be uniquely decomposed into a sum of a diagonalizable map and a **nilpotent map**. In order to prove the existence of such a basis, we need to spend a little time studying nilpotent maps. This is the purpose of the present section. In this section, $\mathbb{F} = \mathbb{R}$ or $\mathbb{C}$ and V is a vector space over $\mathbb{F}$. Naturally, we begin with the following definition:

Definition 13.32. *A linear map $\varphi \in End(V)$ is* ***nilpotent*** *if $\varphi^k = \mathbf{0}$ for some integer $k > 0$.*

Example 13.33. *The zero endomorphism $\mathbf{0} \in End(V)$ is trivially nilpotent.*

Here is a less trivial example.

Example 13.34. *Consider the vector space $\mathbb{R}^2$ with standard basis $\vec{e}_1, \vec{e}_2$. Let $\varphi : \mathbb{R}^2 \to \mathbb{R}^2$ be the linear map defined by*

$$\varphi(\vec{e}_1) = \vec{e}_2, \qquad \varphi(\vec{e}_2) = \mathbf{0}.$$

Its easy to see that $\varphi^2 = \mathbf{0}$. Hence, φ is nilpotent.

Theorem 13.35. *Let $\varphi \in End(V)$. Then φ is nilpotent if and only if the minimal polynomial of φ is of the form $m_\varphi(x) = x^k$ for some $k \geq 1$.*

Proof. Suppose φ is nilpotent. By definition, $\varphi^n = \mathbf{0}$ for some $n \geq 1$. Since $p(\varphi) = \varphi^n$ for $p(x) = x^n \in \mathbb{F}[x]$, Theorem 13.2 implies that $m_\varphi \mid x^n$. Since $m_\varphi(\varphi) = \mathbf{0}$ and $m_\varphi(x)$ is monic, it follows that $m_\varphi(x) = x^k$ for some $1 \leq k \leq n$.

Now suppose $m_\varphi(x) = x^k$ for some $k \geq 1$. From the definition of the minimal polynomial, we have $m_\varphi(\varphi) = \varphi^k = \mathbf{0}$. Hence, φ is nilpotent. □

Theorem 13.36. *Let $\varphi \in End(V)$ be a nilpotent map. Then 0 is the only eigenvalue of φ.*

Proof. Let λ be an eigenvalue of φ and let $v \in V$ be an associated eigenvector. By definition, v is nonzero. Hence, for any $k \geq 1$, we have

$$\varphi^k(v) = \lambda^k v.$$

If $\lambda \neq 0$, then $\varphi^k(v) \neq \mathbf{0}$ for all $k \geq 1$. In particular, φ is not nilpotent, which is a contradiction. Hence, we conclude that $\lambda = 0$. □

The converse to Theorem 13.36 is not true in general as the following example demonstrates:

Example 13.37. *Consider the vector space* $\mathbb{R}^3$ *and let* $\vec{e}_1, \vec{e}_2, \vec{e}_3$ *denote its standard basis. Let* $\varphi : \mathbb{R}^3 \to \mathbb{R}^3$ *be the linear map defined by*

$$\varphi(\vec{e}_1) = \mathbf{0}, \quad \varphi(\vec{e}_2) = -\vec{e}_3, \quad \varphi(\vec{e}_3) = \vec{e}_2.$$

The characteristic polynomial of φ *is* $p_\varphi = x(x^2+1) \in \mathbb{R}[x]$, *which has only has* 0 *as its eigenvalue. However,* φ *is not nilpotent since* $\varphi^{2k}(\vec{e}_2) = (-1)^k \vec{e}_2$ *for* $k \geq 1$. *It will follow easily from the Cayley-Hamilton Theorem (which we will prove later) that the converse to Theorem 13.36 does hold if* V *is a complex vector space.*

Our goal now for the remainder of this section is to show that if $\varphi : V \to V$ is nilpotent, then there exists a basis $\mathcal{B}$ of V for which the matrix representation of φ with respect to $\mathcal{B}$ is in the Jordan canonical form where all Jordan blocks are of the form $J_p(0)$ for various $p \geq 1$. Such a basis is called a **Jordan basis** for φ. We are going to arrive at a proof of this result by first proving a number of smaller results. In essence, we are building a bridge towards this main result. Each smaller result can be regarded as a plank in this bridge. We begin with the following result:

Lemma 13.38. *Let* $\varphi \in End(V)$ *be a nonzero nilpotent linear map. Suppose* $\varphi^k = \mathbf{0}$ *and* $\varphi^{k-1} \neq \mathbf{0}$ *for some positive integer* k. *Then for any* $v \in V$ *such that* $\varphi^{k-1}(v) \neq \mathbf{0}$, *the set*

$$\{v, \varphi(v), \ldots, \varphi^{k-1}(v)\}$$

is linearly independent.

Proof. We prove this by induction on k. Since φ is nonzero by hypothesis, k is at least 2. Let us first consider the case where $k = 2$. Let $v \in V$ be any vector such that $\varphi(v) \neq \mathbf{0}$ and suppose that

$$a_0 v + a_1 \varphi(v) = \mathbf{0} \tag{269}$$

for some $a_0, a_1 \in \mathbb{F}$. Applying φ to both sides of (269) and using the fact that $\varphi^2 = \mathbf{0}$ and $\varphi(v) \neq \mathbf{0}$, we obtain $a_0 = 0$. Equation (269) reduces to $a_1 \varphi(v) = \mathbf{0}$. Since $\varphi(v) \neq \mathbf{0}$, we conclude that $a_1 = 0$ as well. Hence, $\{v, \varphi(v)\}$ is linearly independent.

Suppose the result is true for all nilpotent maps satisfying $\varphi^k = \mathbf{0}$ and $\varphi^{k-1} \neq \mathbf{0}$ for some $k \geq 2$. Now let $\psi : V \to V$ be a nilpotent map such that $\psi^{k+1} = \mathbf{0}$ and $\psi^k \neq \mathbf{0}$. Let $V' = \text{im } \psi$. Then

$$\psi(V') \subset \psi(V) = \text{im } \psi = V'.$$

Hence, $\psi|_{V'} \in \text{End}(V')$. Let $\psi' := \psi|_{V'}$. Since ψ is a nonzero map, we have $V' \neq \{\mathbf{0}\}$. Let $v' \in V'$ be arbitrary. Then $v' = \psi(v)$ for some $v \in V$ and

$$(\psi')^k(v') = \psi^k(v') = \psi^{k+1}(v) = \mathbf{0}.$$

Hence, $(\psi')^k = \mathbf{0}$. Also, since $\psi^k \neq \mathbf{0}$, there exists $v \in V$ such that $\psi^k(v) \neq \mathbf{0}$. Let $v' = \psi(v)$. Then

$$(\psi')^{k-1}(v') = \psi^{k-1}(v') = \psi^k(v) \neq \mathbf{0}.$$

Hence, $(\psi')^{k-1} \neq \mathbf{0}$. Now let $v' \in V' \subset V$ be any element such that $(\psi')^{k-1}(v') \neq \mathbf{0}$. By the induction hypothesis applied to $\psi' := \psi|_{V'}$, the set

$$\{v', \psi(v'), \ldots, \psi^{k-1}(v')\}$$

is linearly independent. Since $v' \in V'$, there exists $v \in V$ such that $v' = \psi(v)$. The above linearly independent set can be rewritten as

$$\{\psi(v), \psi^2(v), \ldots, \psi^k(v)\}. \tag{270}$$

Now suppose that

$$a_0 v + a_1 \psi(v) + \cdots + a_k \psi^k(v) = \mathbf{0} \tag{271}$$

for some $a_0, a_1, \ldots, a_k \in \mathbb{F}$. Applying ψ to both sides of (271) gives

$$a_0 \psi(v) + a_1 \psi^2(v) + \cdots + a_{k-1} \psi^k(v) = \mathbf{0}, \tag{272}$$

where we have used the fact that $\psi^{k+1} = \mathbf{0}$. However, the set (270) is linearly independent. Hence, $a_0 = a_1 = \cdots = a_{k-1} = 0$. (271) now reduces to $a_k \psi^k(v) = \mathbf{0}$. Since $\psi^k(v) \neq \mathbf{0}$, we conclude that $a_k = 0$ as well. From this, it follows that

$$\{v, \psi(v), \psi^2(v), \ldots, \psi^k(v)\}$$

is linearly independent. This proves the induction step. □

Lemma 13.39. *Let $\varphi : V \to V$ be a nonzero nilpotent map. Let k be the smallest integer such that $\varphi^k = \mathbf{0}$. Let $v \in V$ be any vector such that $\varphi^{k-1}(v) \neq \mathbf{0}$. Also, let*

$$U := \mathit{span}\{v, \varphi(v), \ldots, \varphi^{k-1}(v)\}.$$

Then

$$U \cap \ker \varphi = \mathit{span}\{\varphi^{k-1}(v)\}$$

Proof. By Lemma 13.38, the set

$$\mathcal{B} := \{\varphi^{k-1}(v), \ldots, \varphi(v), v\}$$

is linearly independent. Let $u \in U \cap \ker \varphi$. Since $U = \operatorname{span} \mathcal{B}$, it follows that

$$u = a_0 v + a_1 \varphi(v) + \cdots + a_{k-1} \varphi^{k-1}(v) \tag{273}$$

for some $a_0, a_1, \ldots, a_{k-1} \in \mathbb{F}$. Applying φ to both sides of (273) and using the fact that $\varphi^k = \mathbf{0}$ and $\varphi(u) = \mathbf{0}$ gives

$$\mathbf{0} = a_0 \varphi(v) + a_1 \varphi^2(v) + \cdots + a_{k-2} \varphi^{k-1}(v). \tag{274}$$

Since $\varphi(v), \varphi^2(v), \ldots, \varphi^{k-1}(v)$ is linearly independent, it follows that

$$a_0 = a_1 = \cdots = a_{k-2} = 0.$$

Hence, $u = a_{k-1}\varphi^{k-1}(v)$. From this, we conclude that $U \cap \ker \varphi$ is spanned by the vector $\varphi^{k-1}(v)$. □

Lemma 13.40. *Let $\varphi : V \to V$ be a nonzero nilpotent map. Let k be the smallest integer such that $\varphi^k = \mathbf{0}$ and let $v \in V$ be any vector such that $\varphi^{k-1}(v) \neq \mathbf{0}$. Also, let*

$$\mathcal{B} := \{\varphi^{k-1}(v), \ldots, \varphi(v), v\}$$

and $U :=$ span $\mathcal{B}$. Then

(i) $\varphi(U) \subset U$

(ii) The matrix representation of $\varphi|_U : U \to U$ with respect to $\mathcal{B}$ is the Jordan block $J_k(0)$, that is,

$$[\varphi|_U]_{\mathcal{B}} = J_k(0)$$

(iii) if $\dim V = 2$, then $U = V$ and $[\varphi]_{\mathcal{B}} = J_2(0)$.

Proof. (i): Since $\varphi^k = \mathbf{0}$, it follows that

$$\varphi(\varphi^i v) = \varphi^{i+1}(v) \in U$$

for $i = 0, 1, \ldots, k-1$ (where we set $\varphi^0 := id_V$). This implies that $\varphi(U) \subset U$.

(ii): By Lemma 13.38, $\mathcal{B}$ is linearly independent. Hence, $\mathcal{B}$ is a basis of U. Since $\varphi(\varphi^i(v)) = \varphi^{i+1}(v)$ (with $\varphi^k(v) = \mathbf{0}$), it follows that the matrix representation of $\varphi|_U$ with respect to $\mathcal{B}$ is

$$\begin{aligned} [\varphi|_U]_{\mathcal{B}} &= \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & 0 & \cdots & 1 \\ 0 & 0 & 0 & \cdots & 0 \end{pmatrix} \\ &= J_k(0). \end{aligned}$$

(Note that $\dim U = k$.)

(iii). Since φ is a nonzero nilpotent map, it follows that $k \geq 2$. By Lemma 13.38, $\{\varphi(v), v\}$ is linearly independent. Since $\dim V = 2$, it follows that $k = 2$ and $\mathcal{B} = \{\varphi(v), v\}$ is a basis of V. Hence, $U = V$ here, $\varphi|_U = \varphi$, and

$$\begin{aligned} [\varphi]_{\mathcal{B}} &= \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \\ &= J_2(0). \end{aligned}$$

□

Remark 13.41. *Let* $\mathbf{0} : V \to V$ *be the zero map and let* $n = \dim V$*. For any basis* $\mathcal{B}$*, the matrix representation of* $\mathbf{0}$ *with respect to* $\mathcal{B}$ *is, of course, the* $n \times n$ *zero matrix. Since* $J_1(0) = 0$*, the* $n \times n$ *zero matrix can also be expressed as a block diagonal matrix with* n *Jordan blocks all equal to* $J_1(0)$*. In other words,*

$$[\mathbf{0}]_{\mathcal{B}} = \begin{pmatrix} J_1(0) & 0 & \cdots & 0 \\ 0 & J_1(0) & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & J_1(0) \end{pmatrix}.$$

Lemma 13.42. *Let* $\varphi : V \to V$ *be a nonzero nilpotent linear map such that* $\varphi^2 = \mathbf{0}$*. Then there exists a Jordan basis* $\mathcal{B}$ *of* V *for* φ *such that all the Jordan blocks in the matrix representation* $[\varphi]_{\mathcal{B}}$ *are either* $J_1(0) = 0$ *or* $J_2(0)$*.*

Proof. Since $\varphi^2 = \mathbf{0}$, it follows that im $\varphi \subset \ker \varphi$. Let

$$\{\widetilde{y}_1, \ldots, \widetilde{y}_t\} \tag{275}$$

be a basis on im φ and let $y_i \in V$ be defined by $\varphi(y_i) = \widetilde{y}_i$ for $i = 1, \ldots, t$. Extend (275) to a basis of $\ker \varphi$:

$$\{\widetilde{y}_1, \widetilde{y}_2 \ldots, \widetilde{y}_t, x_1, x_2 \ldots, x_s\}. \tag{276}$$

Let

$$\mathcal{B} := \{\widetilde{y}_1, y_1, \widetilde{y}_2, y_2 \ldots, \widetilde{y}_t, y_t, x_1, \ldots, x_s\}. \tag{277}$$

We now show that $\mathcal{B}$ is linearly independent. Suppose

$$\sum_{i=1}^{t} a_i \widetilde{y}_i + \sum_{i=1}^{t} b_i y_i + \sum_{i=1}^{s} c_i x_i = \mathbf{0}. \tag{278}$$

Applying φ to both sides of (278) gives

$$\sum_{i=1}^{t} b_i \widetilde{y}_i = \mathbf{0}, \tag{279}$$

where we use the fact that $\widetilde{y}_i, x_j \in \ker \varphi$ and $\varphi(y_i) = \widetilde{y}_i$ for $i = 1, \ldots, t$, $j = 1, \ldots, s$. Since (277) is linearly independent, it follows that $b_1 = \cdots = b_t = 0$. Equation (278) now reduces to

$$\sum_{i=1}^{t} a_i \widetilde{y}_i + \sum_{i=1}^{s} c_i x_i = \mathbf{0}. \tag{280}$$

Since (277) is linearly independent, we conclude that

$$a_1 = \cdots = a_t = c_1 = \cdots = c_s = 0.$$

We have thus proven that $\mathcal{B}$ is linearly independent.

By the Rank Nullity Theorem (Theorem 5.60), we have

$$\begin{aligned}\dim V &= \dim \ker \varphi + \dim \ \text{im}\ \varphi \\ &= (t+s) + t \\ &= 2t + s,\end{aligned}$$

which is the cardinality of $\mathcal{B}$. Since $\mathcal{B}$ is also linearly independent, we conclude that $\mathcal{B}$ is a basis on V.

Since

$$\varphi(\widetilde{y}_i) = \mathbf{0}, \quad \varphi(y_i) = \widetilde{y}_i, \quad \varphi(x_j) = \mathbf{0}$$

for $i = 1, \ldots, t$ and $j = 1, \ldots, s$, we see that the matrix representation of φ with respect to $\mathcal{B}$ is a block diagonal matrix which consists of t blocks of $J_2(0)$ and s blocks of $J_1(0) = 0$:

$$[\varphi]_{\mathcal{B}} = \begin{pmatrix} J_2(0) & \cdots & \mathbf{0} & \mathbf{0} & \cdots & \mathbf{0} \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ \mathbf{0} & \cdots & J_2(0) & \mathbf{0} & \cdots & \mathbf{0} \\ \mathbf{0} & \cdots & \mathbf{0} & J_1(0) & \cdots & \mathbf{0} \\ \vdots & \ddots & \vdots & & \ddots & \vdots \\ \mathbf{0} & \cdots & \mathbf{0} & \cdots & \mathbf{0} & J_1(0) \end{pmatrix}.$$

□

We are now in a position to prove the main result of this section (which holds for $\mathbb{F} = \mathbb{R}$ or $\mathbb{C}$). Note that the proof of this result is a bit technical. Hence, the reader may wish to simply skim the proof for the first reading and then read it again for all the details at a later time.

Theorem 13.43. *Let $\varphi : V \to V$ be any nilpotent map and let $n = \dim V$. Then there exists a Jordan basis $\mathcal{B}$ of V for φ such that all the Jordan blocks in the matrix representation $[\varphi]_{\mathcal{B}}$ are of the form $J_p(0)$ for various $p \geq 1$. More explicitly,*

$$[\varphi]_{\mathcal{B}} = \begin{pmatrix} J_{n_1}(0) & \mathbf{0} & \cdots & \mathbf{0} \\ \mathbf{0} & J_{n_2}(0) & \cdots & \mathbf{0} \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{0} & \mathbf{0} & \cdots & J_{n_q}(0) \end{pmatrix}$$

where $\sum_{i=1}^{q} n_i = n$.

Proof. If φ is the zero map, then the result holds by Remark 13.41. So let us assume that φ is a nonzero nilpotent map. Let k be the smallest integer such that $\varphi^k = \mathbf{0}$. Since $\varphi \neq \mathbf{0}$, it follows that $k \geq 2$. Lemma 13.38 implies that $\{\varphi(v), v\}$ is linearly independent. Hence, $\dim V \geq 2$. If $\dim V = 2$, then by statement (iii) of

Lemma 13.40, there exists a basis $\mathcal{B}$ such that $[\varphi]_{\mathcal{B}} = J_2(0)$. Hence, Theorem 13.43 holds for $\dim V = 2$.

We now prove Theorem 13.43 by induction on $\dim V$. So let us assume that if $\dim V < n$ and $\varphi : V \to V$ is a nonzero nilpotent map, there exists a basis $\mathcal{B}$ of V such that $[\varphi]_{\mathcal{B}}$ is a block diagonal matrix consisting of Jordan blocks of the form $J_p(0)$ for various $p \geq 1$. Also, let us also suppose that if k is the smallest integer such that $\varphi^k = \mathbf{0}$ and $v \in V$ satisfies $\varphi^{k-1}(v) \neq \mathbf{0}$, then there exists a subspace C of V (possibly $C = \{\mathbf{0}\}$) which satisfies the following conditions:

(a) $V = \operatorname{span}\{\varphi^{k-1}(v), \ldots, \varphi(v), v\} \oplus C$

(b) $\varphi(C) \subset C$.

Note that for $\dim V = 2$, Lemma 13.40 shows that $V = \operatorname{span}\{\varphi(v), v\}$. Hence, $C = \{\mathbf{0}\}$ in this case. In particular, the existence of a subspace C satisfying conditions (a) and (b) hold for the case of $\dim V = 2$.

Now let $\dim V = n$ and let $\varphi : V \to V$ be a nonzero nilpotent map. Also, let k be the smallest integer such that $\varphi^k = \mathbf{0}$ and let $v \in V$ be any vector such that $\varphi^{k-1}(v) \neq \mathbf{0}$. Let

$$\mathcal{B}_1 := \{\varphi^{k-1}(v), \ldots, \varphi(v), v\}, \qquad U := \operatorname{span} \mathcal{B}_1. \tag{281}$$

Lemma 13.38 implies that $\mathcal{B}_1$ is a basis of U. Lemma 13.40 shows that $\varphi(U) \subset U$ and

$$[\varphi|_U]_{\mathcal{B}_1} = J_k(0).$$

If $U = V$, then we are done. In this case, the desired basis is $\mathcal{B}_1$ and $[\varphi]_{\mathcal{B}_1}$ is a block diagonal matrix which consists of a single Jordan block: $J_k(0)$. So let us suppose that $U \neq V$. We now construct a subspace $C \subset V$ satisfying conditions (a) and (b) above.

Before we do this, note that the existence of a subspace $C \subset V$ satisfying conditions (a) and (b) above implies the existence of a basis $\mathcal{B}$ of V with the property that the matrix representation $[\varphi]_{\mathcal{B}}$ is in Jordan canonical form with Jordan blocks of the form $J_p(0)$ for various $p \geq 1$. Indeed, if such a subspace C exists, then

$$\dim C < \dim V = n$$

since $\dim U = k \geq 2$ and $V = U \oplus C$. If $\varphi|_C = \mathbf{0}$, then the matrix representation of $\varphi|_C$ with respect to any basis of C is the zero matrix. By Remark 13.41, the zero matrix is a special case of the Jordan canonical form where all Jordan blocks are $J_1(0) = 0$. On the other hand, if $\varphi|_C \neq \mathbf{0}$, then by the induction hypothesis applied to the nilpotent map $\varphi|_C : C \to C$, there exists a basis of C such that the matrix representation of $\varphi|_C$ with respect to this basis is a block diagonal matrix whose diagonal blocks are of the form $J_p(0)$ for various $p \geq 1$. Hence, whether $\varphi|_C$ is zero or not, we can always find a basis $\mathcal{B}_2$ of C such that $[\varphi|_C]_{\mathcal{B}_2}$ is a block diagonal matrix with diagonal blocks of the form $J_p(0)$ for various $p \geq 1$. Letting $\mathcal{B} = \mathcal{B}_1 \cup \mathcal{B}_2$ gives a basis of V such that the matrix representation of φ with respect to $\mathcal{B}$ is

$$[\varphi]_{\mathcal{B}} = \begin{pmatrix} [\varphi|_U]_{\mathcal{B}_1} & \mathbf{0} \\ \mathbf{0} & [\varphi|_C]_{\mathcal{B}_2} \end{pmatrix} = \begin{pmatrix} J_k(0) & \mathbf{0} \\ \mathbf{0} & [\varphi|_C]_{\mathcal{B}_2} \end{pmatrix}.$$

Given the form of $[\varphi|_C]_{\mathcal{B}_2}$, it follows immediately that the above matrix representation is a block diagonal matrix whose diagonal blocks are Jordan blocks of the form $J_p(0)$ for various $p \geq 1$. Hence, to prove Theorem 13.43, it suffices to construct a subspace C of V which satisfies conditions (a) and (b). We now focus our full attention on doing just this.

By Lemma 13.42, Theorem 13.43 holds for all nonzero nilpotent maps satisfying $\varphi^2 = \mathbf{0}$. So let us assume that $k \geq 3$. Since $\varphi^k = \mathbf{0}$ and $\varphi \neq \mathbf{0}$, it follows that

$$\ker\varphi \neq \mathbf{0}, \qquad \ker\varphi \neq V.$$

This in turn implies that

$$0 < \dim\ \text{im}\ \varphi < \dim V = n.$$

Note also that

$$\varphi(\text{im}\ \varphi) \subset \varphi(V) = \text{im}\ \varphi.$$

Since $k \geq 3$ is the smallest integer such that $\varphi^k = \mathbf{0}$, it follows that

$$\left(\varphi|_{\text{im}\ \varphi}\right)^{k-1} = \mathbf{0} \quad \text{and} \quad \left(\varphi|_{\text{im}\ \varphi}\right)^{k-2} \neq \mathbf{0}.$$

Let $v' = \varphi(v) \in \text{im}\ \varphi$. Since $\varphi^{k-1}(v) \neq \mathbf{0}$, we have

$$\varphi^{k-2}v' = \varphi^{k-2}(\varphi(v)) = \varphi^{k-1}(v) \neq \mathbf{0}.$$

Also, let

$$\begin{aligned} \widetilde{U} &:= \text{span}\{\varphi^{k-2}(v'), \ldots, \varphi(v'), v'\} \\ &= \text{span}\{\varphi^{k-1}(v), \ldots, \varphi^2(v), \varphi(v)\}. \end{aligned}$$

Since $\dim \text{im}\ \varphi < \dim V = n$, the induction hypothesis applied to the nonzero nilpotent map

$$\varphi|_{\text{im}\ \varphi} : \text{im}\ \varphi \to \text{im}\ \varphi$$

yields a subspace $\widetilde{C} \subset \text{im}\ \varphi$ such that

(a') $\text{im}\ \varphi = \widetilde{U} \oplus \widetilde{C}$

(b') $\varphi(\widetilde{C}) \subset \widetilde{C}$.

By Lemma 13.39, we have

$$U \cap \ker\varphi = \text{span}\{\varphi^{k-1}(v)\}.$$

Let X be a basis of $\ker\varphi$ which extends $\varphi^{k-1}(v)$:

$$X := \{x_1, \ldots, x_s, \varphi^{k-1}(v)\}.$$

There are two cases to consider: $\widetilde{C} = \{\mathbf{0}\}$ and $\widetilde{C} \neq \{\mathbf{0}\}$.

case 1: $\widetilde{C} = \{\mathbf{0}\}$. In this case, we have

$$\text{im}\ \varphi = \widetilde{U} = \text{span}\{\varphi^{k-1}(v), \ldots, \varphi^2(v), \varphi(v)\}.$$

Let

$$Z := \{v, \varphi(v), \ldots, \varphi^{k-1}(v), x_1, \ldots, x_s\}.$$

We now show that Z is linearly independent. To do this, suppose that

$$\sum_{i=0}^{k-1} a_i \varphi^i(v) + \sum_{i=1}^{s} b_i x_i = \mathbf{0} \tag{282}$$

where $\varphi^0 := id_V$. Applying φ to both sides of (282) gives

$$a_0 \varphi(v) + \cdots + a_{k-2}\varphi^{k-1}(v) = \mathbf{0}. \tag{283}$$

Since $\mathcal{B}_1$ is linearly independent, it follows that

$$a_0 = \cdots = a_{k-2} = 0.$$

Hence, (282) reduces to

$$a_{k-1}\varphi^{k-1}(v) + \sum_{i=1}^{s} b_i x_i = \mathbf{0}. \tag{284}$$

Since X is linearly independent, we have

$$a_{k-1} = b_1 = \cdots = b_s = 0.$$

This proves that Z is linearly independent. By the Rank Nullity Theorem (Theorem 5.60), we have

$$\begin{aligned} \dim V &= \dim \ker \varphi + \dim \mathrm{im}\ \varphi \\ &= (s+1) + (k-1) \\ &= s + k. \end{aligned}$$

However, $s + k$ is the cardinality of Z. Since Z is linearly independent, we conclude that Z is in fact a basis of V. Let

$$C = \mathrm{span}\{x_1, \ldots, x_s\}. \tag{285}$$

Since $C \subset \ker \varphi$, we have $\varphi(C) = \{\mathbf{0}\} \subset C$. Also, since Z is a basis of V, it follows from the definition of U in (281) and the definition of C in (285), that $V = U \oplus C$. We have thus constructed a subspace C of V which satisfies conditions (a) and (b) for the $\widetilde{C} = \{\mathbf{0}\}$ case.

case 2: $\widetilde{C} \neq \{\mathbf{0}\}$. Since $\varphi(\widetilde{C}) \subset \widetilde{C}$, Theorem 11.30 shows that the map

$$\overline{\varphi} : V/\widetilde{C} \to V/\widetilde{C}$$

given by $\overline{\varphi}([v]) := [\varphi(v)]$ is a well defined linear map. Moreover, since φ is nilpotent, it follows immediately that $\overline{\varphi}$ is also nilpotent. Indeed,

$$\overline{\varphi}^k([v]) = [\varphi^k(v)] = [\mathbf{0}].$$

From condition (a') above, $\widetilde{C}$ satisfies

$$\mathrm{im}\ \varphi = \mathrm{span}\{\varphi^{k-1}(v), \ldots, \varphi^2(v), \varphi(v)\} \oplus \widetilde{C}. \tag{286}$$

This implies that

$$\operatorname{im} \overline{\varphi} = \operatorname{span}\{[\varphi^{k-1}(v)], \ldots, [\varphi^2(v)], [\varphi(v)]\}. \tag{287}$$

(286) implies that $\varphi^i(v) \notin \widetilde{C}$ for $i = 1, 2, \ldots, k-1$. Hence, $\operatorname{im} \overline{\varphi}$ is a nonzero subspace of $V/\widetilde{C}$. In particular, $\overline{\varphi}$ is a nonzero nilpotent map. Since $\varphi^k = \mathbf{0}$ and $\varphi^{k-1}(v) \notin \widetilde{C}$, it follows that k is also the smallest integer such that $\overline{\varphi}^k = [\mathbf{0}]$. Let

$$\widehat{U} := \operatorname{span}\{[\varphi^{k-1}(v)], \ldots, [\varphi^2(v)], [\varphi(v)], [v]\}. \tag{288}$$

Note that Lemma 13.38 applied to the nonzero nilpotent map $\overline{\varphi}$ implies that

$$\{[\varphi^{k-1}(v)], \ldots, [\varphi^2(v)], [\varphi(v)], [v]\} \tag{289}$$

is a basis of $\widehat{U}$. From our study of quotient vector spaces, we have

$$\dim V/\widetilde{C} = \dim V - \dim \widetilde{C} < \dim V = n,$$

where we use the fact that $\widetilde{C} \neq \{\mathbf{0}\}$. Applying the induction hypothesis to the nonzero nilpotent map $\overline{\varphi}$ yields a subspace $\widehat{C}$ of $V/\widetilde{C}$ such that

(a") $V/\widetilde{C} = \widehat{U} \oplus \widehat{C}$

(b") $\overline{\varphi}(\widehat{C}) \subset \widehat{C}$.

By Proposition 11.24, there exists a subspace C of V containing $\widetilde{C}$ such that

$$\widehat{C} = C/\widetilde{C}.$$

Condition (b") above implies that $\varphi(C) \subset C$. From the definition of U in (281) and the definition of $\widehat{U}$ in (288), we see that every element of $\widehat{U}$ is of the form $[u]$ for some $u \in U$. Consequently, condition (a") implies that for every element $[v] \in V/\widetilde{C}$, there exists a unique $[u] \in \widehat{U}$ and a unique $[c] \in \widehat{C}$ for some $u \in U$ and $c \in C$ such that

$$[v] = [u] + [c].$$

This in turn implies that $v - u - c \in \widetilde{C}$. Since $\widetilde{C} \subset C$, it follows that

$$V = U + C.$$

We now show that this is actually a direct sum. To do this, it suffices to show that

$$\dim V = \dim U + \dim C. \tag{290}$$

Using (a"), we have

$$\dim V/\widetilde{C} = \dim \widehat{U} + \dim \widehat{C}. \tag{291}$$

Since

$$\dim V/\widetilde{C} = \dim V - \dim \widetilde{C}, \qquad \dim \widehat{U} = k = \dim U, \qquad \dim \widehat{C} = \dim C - \dim \widetilde{C},$$

we see that (291) yields (290). Hence, $V = U \oplus C$, which proves that C is the desired subspace satisfying conditions (a) and (b) for case 2. This completes the proof. □

Theorem 13.43 shows that for any nilpotent map $\varphi : V \to V$ (where V is a real or complex vector space), a Jordan basis of V for φ exists. In addition to establishing the existence of a Jordan basis, the proof of Theorem 13.43 also suggests a general strategy for actually finding a Jordan basis. The basic strategy works as follows:

Finding a Jordan basis of a nilpotent map $\varphi : V \to V$.

Set $V_0 := V$ and $\varphi_0 := \varphi$. Carry out the following steps for $i = 0, 1, 2, \ldots$

1. Let k_i be the smallest integer such that $\varphi_i^{k_i} = \mathbf{0}$ and let $v_i \in V_i$ be any vector such that $\varphi_i^{k_i-1}(v_i) \neq \mathbf{0}$. (If $k_i = 1$, i.e. φ_i is the zero map, define $\varphi_i^0 := id_{V_i}$)
2. Let $\mathcal{B}_i := \{\varphi_i^{k_i-1}(v_i), \ldots, \varphi_i(v_i), v_i\}$ and $U_i :=$ span $\mathcal{B}_i$
3. **Construct** a subspace $C_i \subset V_i$ such that
   (a) $V_i = U_i \oplus C_i$
   (b) $\varphi_i(C_i) \subset C_i$
4. If $C_i = \{\mathbf{0}\}$, then **STOP**. $\mathcal{B} := \mathcal{B}_0 \cup \cdots \cup \mathcal{B}_i$ is the Jordan basis of V for φ. If $C_i \neq \{\mathbf{0}\}$, set $V_{i+1} := C_i$ and $\varphi_{i+1} := \varphi|_{V_{i+1}}$ and repeat steps 1 through 4 by replacing i with $i + 1$.

The crucial step in the above strategy is step 3, the construction of the subspace C. From the proof of Theorem 13.43, this subspace C exists. Once again, the proof of Theorem 13.43 provides a strategy for computing the subspace C. The following result will prove useful in finding a Jordan basis.

Theorem 13.44. *Let $\varphi : V \to V$ be a nilpotent map and let E_0 be the eigenspace of φ associated to the eigenvalue 0. Let $\mathcal{B}$ be a Jordan basis of V for φ and let q be the number of Jordan blocks in $[\varphi]_{\mathcal{B}}$.*

(a) Let $J_{k_i}(0)$ be the ith Jordan block of $[\varphi]_{\mathcal{B}}$. Then the basis elements associated to $J_{k_i}(0)$ has the form

$$\mathcal{B}_i = \{\varphi^{k_i-1}(v_i), \ldots, \varphi(v_i), v_i\}$$

for some $v_i \in V$. In particular, $\mathcal{B} = \mathcal{B}_1 \cup \cdots \cup \mathcal{B}_q$.

(b) The set $\{\varphi^{k_1-1}(v_1), \varphi^{k_2-1}(v_2), \ldots, \varphi^{k_q-1}(v_q)\}$ is a basis for E_0. In particular, $\dim E_0 = q$.

Proof. Let q be the number of Jordan blocks in in $[\varphi]_{\mathcal{B}}$. Also, let $J_{k_i}(0)$ be the ith Jordan block in $[\varphi]_{\mathcal{B}}$ and let $\mathcal{B}_i$ denote the basis elements associated to the ith Jordan block $J_{k_i}(0)$ for $i = 1, \ldots, q$. Then

$$\mathcal{B} = \mathcal{B}_1 \cup \mathcal{B}_2 \cup \cdots \cup \mathcal{B}_q.$$

Note that $\mathcal{B}_i$ contains k_i basis vectors. Write

$$\mathcal{B}_i = \{v_1^{(i)}, \ldots, v_{k_i}^{(i)}\}.$$

Let $U_i := \text{span } \mathcal{B}_i$. Then

$$V = U_1 \oplus U_2 \oplus \cdots \oplus U_q$$

and

$$[\varphi|_{U_i}]_{\mathcal{B}_i} = J_{k_i}(0).$$

From the form of $J_{k_i}(0)$, we have

$$\varphi(v_j^{(i)}) = \begin{cases} \mathbf{0} & \text{if } j = 1 \\ v_{j-1}^{(i)} & \text{if } j > 1 \end{cases}$$

Hence, setting $v_i := v_{k_i}^{(i)}$, we have

$$\mathcal{B}_i = \{\varphi^{k_i-1}(v_i), \ldots, \varphi(v_i), v_i\}, \qquad \forall\ i = 1, \ldots, q.$$

This proves (a). We now show that

$$\mathcal{D} := \{\varphi^{k_1-1}(v_1), \varphi^{k_2-1}(v_2), \ldots, \varphi^{k_q-1}(v_q)\}$$

is a basis of E_0 (where $\varphi^0 := id_V$). Let $x \in E_0$ and let us express x as a linear combination of the basis elements of $\mathcal{B} = \mathcal{B}_1 \cup \cdots \cup \mathcal{B}_q$:

$$x = \sum_{i=1}^{q} \sum_{j=1}^{k_i} a_{ij} \varphi^{k_i-j}(v_i) \tag{292}$$

for some $a_{ij} \in \mathbb{F}$. Applying φ to both sides of (292) and using the fact that

$$\varphi(x) = 0x = \mathbf{0}$$

and

$$\varphi^{k_i}(v_i) = \mathbf{0}, \quad \text{for } i = 1, \ldots, q$$

gives

$$\mathbf{0} = \sum_{i=1}^{q} \sum_{j=2}^{k_i} a_{ij} \varphi^{k_i-j+1}(v_i). \tag{293}$$

Since (293) is a linear combination of elements which belong to $\mathcal{B}$, and hence, are linearly independent, we conclude that

$$a_{ij} = 0 \qquad \text{for } j \geq 2,\ i = 1, \ldots, q.$$

Hence, (292) reduces to

$$x = \sum_{i=1}^{q} a_{i1} \varphi^{k_i-1}(v_i) \in \text{span } \mathcal{D}. \tag{294}$$

This shows that $E_0 \subset \text{span } \mathcal{D}$. Also, since $\mathcal{D} \subset E_0$, we have $E_0 = \text{span } \mathcal{D}$. Lastly, since $\mathcal{D} \subset \mathcal{B}$, $\mathcal{D}$ is also linearly independent. Therefore, we conclude that $\mathcal{D}$ is a basis of E_0. This proves (b). $\square$

Example 13.45. *Let $\mathbb{R}[x]_3$ be the vector space of real polynomials of degree 3 or less and let $D : \mathbb{R}[x]_3 \to \mathbb{R}[x]_3$ be the linear map defined by*

$$Dp(x) := \frac{d}{dx}p(x).$$

Clearly, D is nilpotent with $D^4 = \mathbf{0}$ and $D^3 \neq \mathbf{0}$. The eigenspace of D associated to the eigenvalue 0 is simply $E_0 = \mathbb{R}$, which is a one dimensional subspace of $\mathbb{R}[x]_3$. By Theorem 13.44, any Jordan basis of $\mathbb{R}[x]_3$ for D consists of a single Jordan block. Since $D^3x^3 = 6 \neq 0$, it follows from the general strategy outlined above that

$$\mathcal{B} := \{D^3x^3, D^2x^3, Dx^3, x^3\} = \{6, 6x, 3x^2, x^3\}$$

is a Jordan basis of $\mathbb{R}[x]_3$ for D. In this case, $[D]_{\mathcal{B}} = J_4(0)$.

Example 13.46. *Consider the vector space $\mathbb{R}^4$ and let $\vec{e}_1, \vec{e}_2, \vec{e}_3, \vec{e}_4$ denote the standard basis on $\mathbb{R}^4$. Let $\varphi : \mathbb{R}^4 \to \mathbb{R}^4$ be the linear map defined by*

$$\varphi(\vec{e}_1) = \varphi(\vec{e}_4) = \vec{0}, \qquad \varphi(\vec{e}_2) = \vec{e}_1 + 0.5\vec{e}_4, \qquad \varphi(\vec{e}_3) = -1.5\vec{e}_4.$$

Clearly, $\varphi^2 = \mathbf{0}$ and

$$E_0 = \{a\vec{e}_1 + b\vec{e}_4 \mid a, b \in \mathbb{R}\}$$

where E_0 is the eigenspace of φ associated to 0. Since $\dim E_0 = 2$, Theorem 13.44 implies that any Jordan basis of φ consists of 2 Jordan blocks. Using the general strategy for finding a Jordan basis, let

$$\mathcal{B}_1 = \{\varphi(\vec{e}_2), \vec{e}_2\} = \{e_1 + 0.5\vec{e}_4, \vec{e}_2\}$$

and

$$\mathcal{B}_2 = \{\varphi(\vec{e}_3), \vec{e}_3\} = \{-1.5\vec{e}_4, \vec{e}_3\}$$

Then $\mathcal{B} = \mathcal{B}_1 \cup \mathcal{B}_2$ is a Jordan basis of $\mathbb{R}^4$ for φ:

$$[\varphi]_{\mathcal{B}} = \begin{pmatrix} J_2(0) & \mathbf{0} \\ \mathbf{0} & J_2(0) \end{pmatrix}.$$

Example 13.47. *Consider the vector space $\mathbb{R}^5$ and let $\vec{e}_i$ denote its ith standard basis vector. Let $\rho : \mathbb{R}^5 \to \mathbb{R}^5$ be the linear map defined by*

$$\rho(\vec{e}_1) = \vec{0}, \quad \rho(\vec{e}_2) = \vec{e}_1, \quad \rho(\vec{e}_3) = -\vec{e}_1 + \vec{e}_2$$
$$\rho(\vec{e}_4) = 2\vec{e}_1 + \vec{e}_2, \quad \rho(\vec{e}_5) = \vec{e}_1 - \vec{e}_2 + \vec{e}_3 + \vec{e}_4.$$

Then $\rho^4 = \mathbf{0}$ and $\rho^3 \neq \mathbf{0}$. The eigenspace of ρ associated to 0 (which is simply $\ker \rho$) is

$$E_0 = \{a\vec{e}_1 + b(3\vec{e}_2 + \vec{e}_3 - \vec{e}_4) \mid a, b \in \mathbb{R}\}.$$

Since $\dim E_0 = 2$, it follows that any Jordan basis of $\mathbb{R}^5$ for ρ consists of two Jordan blocks. Let

$$\mathcal{B}_1 = \{\rho^3(\vec{e}_5), \rho^2(\vec{e}_5), \rho(\vec{e}_5), \vec{e}_5\} = \{2\vec{e}_1, 2\vec{e}_2, \vec{e}_1 - \vec{e}_2 + \vec{e}_3 + \vec{e}_4, \vec{e}_5\}$$

and

$$\mathcal{B}_2 = \{3\vec{e}_2 + \vec{e}_3 - \vec{e}_4\}$$

Then $\mathcal{B} = \mathcal{B}_1 \cup \mathcal{B}_2$ is a Jordan basis. The matrix representation $[\varphi]_{\mathcal{B}}$ consists of the Jordan blocks $J_4(0)$ and $J_1(0) = 0$:

$$[\varphi]_{\mathcal{B}} = \begin{pmatrix} J_4(0) & \mathbf{0} \\ 0 & 0 \end{pmatrix}.$$

13.7. The Jordan Canonical Form Theorem

In this section, V is a **complex** vector space and $\varphi : V \to V$ is any linear map. Let $m_\varphi \in \mathbb{C}[x]$ denote the minimal polynomial of φ. Since m_φ is a complex polynomial, the Fundamental Theorem of Algebra implies that m_φ factors completely into a product of linear factors:

$$m_\varphi(x) = (x - \lambda_1)^{q_1}(x - \lambda_2)^{q_2} \cdots (x - \lambda_k)^{q_k}$$

where $\lambda_i \neq \lambda_j$ for $i \neq j$. The main result of this section is a generalization of Theorem 13.43 for nilpotent maps. In fact, much of the heavy lifting was already carried out during the proof of Theorem 13.43. In essence, we are going to show that there exists a Jordan basis of V for φ whose Jordan blocks are of the form $J_p(\lambda_i)$ for various $p \geq 1$, $i = 1, \ldots, k$. Here is the precise statement:

Theorem 13.48 (Jordan Canonical Form Theorem)**.** *Let V be a complex vector space and let $\varphi : V \to V$ be a linear map. Also, let*

$$m_\varphi(x) = (x - \lambda_1)^{q_1}(x - \lambda_2)^{q_2} \cdots (x - \lambda_k)^{q_k}$$

be the minimal polynomial of φ. Then there exists a basis $\mathcal{B}$ of V such that the matrix representation $[\varphi]_{\mathcal{B}}$ is a block diagonal matrix of the form

$$[\varphi]_{\mathcal{B}} = \begin{pmatrix} A_1 & \mathbf{0} & \cdots & \mathbf{0} \\ \mathbf{0} & A_2 & \cdots & \mathbf{0} \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{0} & \mathbf{0} & \cdots & A_k \end{pmatrix},$$

where each A_i is itself a block diagonal matrix whose diagonal blocks are Jordan blocks of the form $J_p(\lambda_i)$ for various $p \geq 1$. Moreover, let n_i be the size of the square matrix A_i (i.e. A_i is $n_i \times n_i$). Then $n_i \geq q_i$. The basis $\mathcal{B}$ is called a ***Jordan basis*** *for φ.*

Proof. Let

$$V_i := \ker\,(\varphi - \lambda_i id_V)^{q_i}, \qquad \forall\ i = 1, \ldots, k.$$

Since $m_\varphi(\varphi) = \mathbf{0}$ and the factors $(\varphi - \lambda_i id_V)^{q_i}$ for $i = 1, \ldots, k$ are pairwise coprime, the Primary Decomposition Theorem (Theorem 13.9) implies

$$V = V_1 \oplus \cdots \oplus V_k \tag{295}$$

and

$$\varphi(V_i) \subset V_i, \qquad \forall\ i = 1, \ldots, k. \tag{296}$$

To prove Theorem 13.48, it suffices to consider the restriction of φ to V_i

$$\varphi_i := \varphi|_{V_i} : V_i \to V_i \tag{297}$$

and construct a basis $\mathcal{B}_i$ of V_i such that the matrix representation $[\varphi_i]_{\mathcal{B}_i}$ is a block diagonal matrix whose diagonal blocks are all Jordan blocks of the form $J_p(\lambda_i)$ for various $p \geq 1$.

Let $m_i(x)$ denote the minimal polynomial of φ_i in (297). We first show that

$$m_i(x) = (x - \lambda_i)^{q_i}. \tag{298}$$

From the definition of V_i, we have

$$(\varphi_i - \lambda_i id_{V_i})^{q_i} = \mathbf{0}. \tag{299}$$

This implies that $m_i(x) \mid (x - \lambda_i)^{q_i}$. Hence, $m_i(x) = (x - \lambda_i)^r$ for some $r \leq q_i$. Suppose that $r < q_i$. Let $m'(x)$ be the polynomial obtained from $m_\varphi(x)$ by replacing $(x - \lambda_i)^{q_i}$ with $m_i(x) = (x - \lambda_i)^r$. Since V is given by the direct sum in (295) and $m_i(\varphi)(V_i) = \{0\}$, it follows that $m'(\varphi) = \mathbf{0}$. Since $\deg m'(x) < \deg m_\varphi(x)$, this gives a contradiction. Hence, $r = q_i$ and $m_i(x)$ must be given by (298).

Now let

$$\psi_i := \varphi_i - \lambda_i id_{V_i}.$$

Then

$$\psi_i^{q_i} = m_i(\varphi_i) = \mathbf{0}.$$

Hence, $\psi_i : V_i \to V_i$ is a nilpotent map on V_i and q_i is the smallest integer such that $\psi_i^{q_i} = \mathbf{0}$. Let

$$n_i := \dim V_i.$$

We now show that $n_i \geq q_i$. Let $v_i \in V_i$ be any vector such that $\psi_i^{q_i - 1}(v_i) \neq \mathbf{0}$. (If $q_i = 1$, that is, $\psi_i = \mathbf{0}$, we set $\psi_i^0 := id_{V_i}$.) By Lemma 13.38, the set

$$\{\psi_i^{q_i-1}(v_i), \ldots, \psi_i(v_i), v_i\} \subset V_i$$

is linearly independent. Since this set consists of q_i elements, we conclude that

$$n_i \geq q_i. \tag{300}$$

By Theorem 13.43, there exists a basis $\mathcal{B}_i$ of V_i such that $[\psi_i]_{\mathcal{B}_i}$ consists of Jordan blocks of the form $J_p(0)$ for various $p \geq 1$. Write

$$[\psi_i]_{\mathcal{B}_i} = \begin{pmatrix} J_{p_{1i}}(0) & \mathbf{0} & \cdots & \mathbf{0} \\ \mathbf{0} & J_{p_{2i}}(0) & \cdots & \mathbf{0} \\ \vdots & \mathbf{0} & \ddots & \vdots \\ \mathbf{0} & \mathbf{0} & \cdots & J_{p_{t_i i}(0)} \end{pmatrix}. \tag{301}$$

Since $\psi_i = \varphi_i - \lambda_i id_{V_i}$, we have

$$\begin{aligned} [\psi_i]_{\mathcal{B}_i} &= [\varphi_i]_{\mathcal{B}_i} - [\lambda_i id_{V_i}]_{\mathcal{B}_i} \\ &= [\varphi|_{V_i}]_{\mathcal{B}_i} - \lambda_i I_{n_i}, \end{aligned} \tag{302}$$

where I_{n_i} denote the $n_i \times n_i$ identity matrix. Using (301) and (302), we have

$$\begin{aligned} [\varphi|_{V_i}]_{\mathcal{B}_i} &= [\psi_i]_{\mathcal{B}_i} + \lambda_i I_{n_i} \\ &= \begin{pmatrix} J_{p_{1i}}(\lambda_i) & \mathbf{0} & \cdots & \mathbf{0} \\ \mathbf{0} & J_{p_{2i}}(\lambda_i) & \cdots & \mathbf{0} \\ \vdots & \mathbf{0} & \ddots & \vdots \\ \mathbf{0} & \mathbf{0} & \cdots & J_{p_{t_i i}(\lambda_i)} \end{pmatrix}. \end{aligned} \tag{303}$$

Let

$$A_i := [\varphi|_{V_i}]_{\mathcal{B}_i}. \tag{304}$$

Since $\varphi|_{V_i}$ is an endomorphism of V_i and $n_i := \dim V_i$, we note that A_i is $n_i \times n_i$. Also, since $\mathcal{B}_i$ is a basis of V_i, it follows that

$$\mathcal{B} = \mathcal{B}_1 \cup \cdots \cup \mathcal{B}_k$$

is a basis of V. Equations (295), (296), (303), and (304) imply

$$[\varphi]_{\mathcal{B}} = \begin{pmatrix} A_1 & \mathbf{0} & \cdots & \mathbf{0} \\ \mathbf{0} & A_2 & \cdots & \mathbf{0} \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{0} & \mathbf{0} & \cdots & A_k \end{pmatrix}.$$

Equation (303) shows that A_i has the desired form for $i = 1, \ldots, k$. Moreover, A_i is $n_i \times n_i$ with $n_i \geq q_i$ by (300). This completes the proof. $\square$

Corollary 13.49. *Let V be a complex vector space and let $\varphi : V \to V$ be a linear map. Let*

$$m_\varphi(x) = (x - \lambda_1)^{q_1}(x - \lambda_2)^{q_2} \cdots (x - \lambda_k)^{q_k}$$

be the minimal polynomial of φ with $\lambda_i \neq \lambda_j$ for $i \neq j$. Also, let

$$n_i := \dim \ker(\varphi - \lambda_i id_V)^{q_i}$$

and let p_φ be the characteristic polynomial of φ. Then

(i) $n_i \geq q_i$

(ii) $p_\varphi(x) = (x - \lambda_1)^{n_1}(x - \lambda_2)^{n_2} \cdots (x - \lambda_k)^{n_k}$

In particular, m_φ and p_φ have the same roots (i.e., the eigenvalues of φ) and $m_\varphi \mid p_\varphi$.

Proof. Let $V_i := \ker(\varphi - \lambda_i id_V)^{q_i}$. In the proof of Theorem 13.48, we let $n_i := \dim V_i$ and we showed that $n_i \geq q_i$ for $i = 1, \dots k$. This proves (i).

In the proof of Theorem 13.48, we constructed a basis $\mathcal{B}$ such that the matrix representation of φ with respect to $\mathcal{B}$ is

$$[\varphi]_\mathcal{B} = \begin{pmatrix} A_1 & \mathbf{0} & \cdots & \mathbf{0} \\ \mathbf{0} & A_2 & \cdots & \mathbf{0} \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{0} & \mathbf{0} & \cdots & A_k \end{pmatrix},$$

where, for each i, A_i is an $n_i \times n_i$ block diagonal matrix with Jordan blocks of the form $J_p(\lambda_i)$ for various $p \geq 1$. In particular, A_i is an upper triangular matrix whose diagonal elements are all λ_i. This implies that $[\varphi]_\mathcal{B}$ is an upper triangular matrix as well. From our study of determinants, the determinant of an upper triangular matrix is just the product of its diagonal elements. Hence, the characteristic polynomial of $[\varphi]_\mathcal{B}$ is easily found to be

$$\begin{aligned} p_\varphi(x) &= \det(xI_n - [\varphi]_\mathcal{B}) \\ &= (x - \lambda_1)^{n_1}(x - \lambda_2)^{n_2} \cdots (x - \lambda_k)^{n_k} \end{aligned}$$

where $n = \sum_{i=1}^k n_i$ is the dimension of V. □

Corollary 13.49 shows that the roots of the minimal polynomial of a linear map $\varphi : V \to V$ are precisely the eigenvalues of φ. Strictly speaking, we only proved this for the case of complex vector spaces. However, it turns out to be true for real vector spaces as well. We will verify this later. The proof for the real case hinges on Corollary 13.49. The upshot of Corollary 13.49 and its real version is a result called the **Cayley-Hamilton Theorem**. We will present the Cayley-Hamilton Theorem later in this chapter. For now, here is one simple application of Corollary 13.49:

Corollary 13.50. *Let A be an $n \times n$ strictly upper triangular real or complex matrix. Then $A^n = \mathbf{0}$. In particular, a strictly upper triangular matrix is nilpotent.*

Proof. Let A be an $n \times n$ strictly upper triangular matrix. Let

$$T_A : \mathbb{C}^n \to \mathbb{C}^n$$

be the linear map defined by $T_A(\vec{v}) := A\vec{v}$. Since A is strictly upper triangular, the characteristic polynomial of T_A (and hence A) is $p(x) = x^n$. Let $m(x)$ be the minimal polynomial of T_A. By Corollary 13.49, $m(x) \mid p(x)$. Hence, $m(x) = x^k$ for some $k \leq n$. Hence,

$$m(T_A) = T_A^k = T_{A^k} = \mathbf{0}.$$

This implies that $A^k = \mathbf{0}$. In particular, $A^n = \mathbf{0}$. □

Example 13.51. *As a simple example of Corollary 13.50, consider the matrix*

$$A = \begin{pmatrix} 0 & 2 & 1 \\ 0 & 0 & 3 \\ 0 & 0 & 0 \end{pmatrix}.$$

The characteristic polynomial of A is x^3. Hence, the minimal polynomial must be x, x^2, or x^3. Since A is nonzero, x is ruled out. For x^2, we have

$$A^2 = \begin{pmatrix} 0 & 2 & 1 \\ 0 & 0 & 3 \\ 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 2 & 1 \\ 0 & 0 & 3 \\ 0 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 6 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}.$$

From this, we conclude that x^3 is the minimal polynomial of A.

At this point, we would like to take a closer look at the Jordan basis constructed in the proof of Theorem 13.48. The following definition will prove useful for this discussion:

Definition 13.52. *Let $\varphi : V \to V$ be a linear map and let λ be an eigenvalue of φ. The **generalized eigenspace** of φ associated to λ is the subspace*

$$GE_\lambda := \{v \in V \mid (\varphi - \lambda id_V)^k(v) = \mathbf{0} \text{ for some } k \geq 1\}$$

Note that GE_λ necessarily contains the eigenspace associated to λ. (This is just $k = 1$ in the above definition.) We will hold off on an example until we learn more about generalized eigenspaces.

Proposition 13.53. *Let V be a complex vector space and let $\varphi : V \to V$ be a linear map. Also, let*

$$m_\varphi(x) = (x-\lambda_1)^{q_1}(x-\lambda_2)^{q_2}\cdots(x-\lambda_k)^{q_k}$$
$$p_\varphi(x) = (x-\lambda_1)^{n_1}(x-\lambda_2)^{n_2}\cdots(x-\lambda_k)^{n_k}$$

be the minimal and characteristic polynomials of φ respectively with $\lambda_i \neq \lambda_j$ for $i \neq j$. Then

(a) $GE_{\lambda_i} = \ker(\varphi - \lambda_i id_V)^{q_i}$

(b) $\dim GE_{\lambda_i} = n_i$

Proof. (a): Without loss of generality, we take $i = 1$ and show that

$$GE_{\lambda_1} = \ker(\varphi - \lambda_1 id_V)^{q_1}.$$

From Definition 13.52, we immediately have

$$\ker(\varphi - \lambda_1 id_V)^{q_1} \subset GE_{\lambda_1}.$$

Suppose that $GE_{\lambda_1} \neq \ker(\varphi - \lambda_1 id_V)^{q_1}$. Then there exists $v \in GE_{\lambda_1}$ and an $r > q_i$ such that

$$\ker(\varphi - \lambda_1 id_V)^r(v) = \mathbf{0}$$

and

$$\ker(\varphi - \lambda_1 id_V)^{q_1}(v) \neq \mathbf{0}.$$

Let

$$V_i := \ker(\varphi - \lambda_i id_V)^{q_i},$$

for $i = 1, \dots, k$. Also, let $\widehat{V}_1 := \ker(\varphi - \lambda_1 id_V)^r$. Then $V_1 \subset \widehat{V}_1$. However, since $v \in \widehat{V}_1$ and $v \notin V_1$, we have

$$\dim V_1 < \dim \widehat{V}_1.$$

Let

$$m'(x) = (x-\lambda_1)^r(x-\lambda_2)^{q_2}\cdots(x-\lambda_k)^{q_k}.$$

Since $m_\varphi(x) \mid m'(x)$, we have $m'(\varphi) = \mathbf{0}$. The Primary Decomposition Theorem (Theorem 13.9) applied to the factors of m_φ and m' respectively yield the following direct sum decompositions:

$$V = V_1 \oplus V_2 \oplus \cdots \oplus V_k$$

and

$$V = \widehat{V}_1 \oplus V_2 \oplus \cdots \oplus V_k.$$

The above direct sum decompositions imply

$$\dim V = \dim V_1 + \sum_{i=2}^{k} \dim V_i = \dim \widehat{V}_1 + \sum_{i=2}^{k} \dim V_i,$$

which in turn imply $\dim V_1 = \dim \widehat{V}_1$, a contradiction. Hence, we must have

$$GE_{\lambda_1} = \ker(\varphi - \lambda_1 id_V)^{q_1}.$$

(b): This follows from statement (a) of Proposition 13.53 and statement (ii) of Corollary 13.49. ☐

Corollary 13.54. *Let V be a complex vector space and let $\varphi : V \to V$ be a linear map. Let $\lambda_1, \ldots, \lambda_k$ be the distinct eigenvalues of φ.*

(i) V is a direct sum of the generalized eigenspaces of φ:

$$V = GE_{\lambda_1} \oplus \cdots \oplus GE_{\lambda_k}.$$

(ii) $\varphi(GE_{\lambda_i}) \subset GE_{\lambda_i}$ for $i = 1, \ldots, k$

Proof. By Corollary 13.49, the roots of the minimal polynomial of φ are precisely the eigenvalues of φ. Let

$$m_\varphi(x) = (x - \lambda_1)^{q_1}(x - \lambda_2)^{q_2} \cdots (x - \lambda_k)^{q_k}$$

be the minimal polynomial of φ. Let

$$V_i := \ker(\varphi - \lambda_i id_V)^{q_i}.$$

The proof of Theorem 13.48 shows that $\varphi(V_i) \subset V_i$ for $i = 1, \ldots, k$ and

$$V = V_1 \oplus \cdots \oplus V_k.$$

(i) and (ii) of Corollary 13.54 now follows from Proposition 13.53 which shows that $V_i = GE_{\lambda_i}$. ☐

Let us now revisit the proof of Theorem 13.48 in light of Proposition 13.53 and Corollary 13.54. Let $\varphi : V \to V$ be a linear map on a complex vector space and let $\lambda_1, \ldots, \lambda_k$ denote its distinct eigenvalues.

In the proof of Theorem 13.48, we constructed a Jordan basis of V for φ by constructing a Jordan basis $\mathcal{B}_i$ of GE_{λ_i} for the restriction

$$\varphi|_{GE_{\lambda_i}} : GE_{\lambda_i} \to GE_{\lambda_i}$$

for $i = 1, \ldots, k$. The matrix representation

$$A_i := [\varphi|_{GE_{\lambda_i}}]_{\mathcal{B}_i}$$

consisted of Jordan blocks of the form $J_p(\lambda_i)$. The Jordan basis of V for φ was then the union of these smaller bases:

$$\mathcal{B} = \mathcal{B}_1 \cup \cdots \cup \mathcal{B}_k.$$

The question now is whether all Jordan bases are constructed in this manner. The answer to this question is yes.

Theorem 13.55. *Let V be a complex vector space and let $\varphi : V \to V$ be a linear map. Let $\lambda_1, \ldots, \lambda_k$ be the distinct eigenvalues of φ. Let $\mathcal{B}$ be a Jordan basis of V for φ and let A_i be the block diagonal matrix in $[\varphi]_{\mathcal{B}}$ whose diagonal blocks are Jordan blocks of the form $J_p(\lambda_i)$. Let $\mathcal{B}_i \subset \mathcal{B}$ be the subset of basis elements associated to A_i. Then*

$$GE_{\lambda_i} = \textit{span } \mathcal{B}_i$$

Proof. Let $U_i := \operatorname{span} \mathcal{B}_i$ and let $n_i := \dim U_i$. Then $n = \sum_{i=1}^{k} n_i$ is the dimension of V. Without loss of generality, we take $i = 1$ and we show that $GE_{\lambda_1} = \operatorname{span} \mathcal{B}_1$. Let

$$\psi := \varphi - \lambda_1 id_V$$

and

$$C := [\psi]_{\mathcal{B}}.$$

Let $r \geq 1$ be an integer. Then the matrix representation of

$$\psi^r = (\varphi - \lambda_1 id_V)^r$$

with respect to $\mathcal{B}$ is

$$\begin{aligned} [\psi^r]_{\mathcal{B}} &= C^r \\ &= \begin{pmatrix} (A_1 - \lambda_1 I_{n_1})^r & \mathbf{0} & \cdots & \mathbf{0} \\ \mathbf{0} & (A_2 - \lambda_1 I_{n_2})^r & \cdots & \mathbf{0} \\ \vdots & \vdots & \ddots & \mathbf{0} \\ \mathbf{0} & \cdots & \mathbf{0} & (A_k - \lambda_1 I_{n_k})^r \end{pmatrix}. \end{aligned}$$

For $j > 1$, the matrix $A_j - \lambda_1 I_{n_j}$ is an upper triangular matrix with nonzero diagonal elements since $\lambda_j \neq \lambda_1$. Hence, $\det(A_j - \lambda_1 I_{n_j}) \neq 0$. Using the multiplicative property of determinants, it follows that

$$\det\left((A_j - \lambda_1 I_{n_j})^r\right) = \left(\det(A_j - \lambda_1 I_{n_j})\right)^r \neq 0.$$

Hence, the columns of $(A_j - \lambda_1 I_{n_j})^r$ for $j > 1$ are linearly independent. This in turn implies

$$(A_j - \lambda_1 I_{n_j})^r \vec{u} = \vec{0} \iff \vec{u} = \vec{0} \in \mathbb{C}^{n_j} \qquad \text{for } j > 1.$$

Now let $\vec{u}_j \in \mathbb{C}^{n_j}$ for $j = 1, \ldots, k$ (expressed as column vectors) and let

$$\vec{u} = \begin{pmatrix} \vec{u}_1 \\ \vec{u}_2 \\ \vdots \\ \vec{u}_k \end{pmatrix}.$$

Then

$$C^r\vec{u} = \begin{pmatrix} (A_1 - \lambda_1 I_{n_1})^r \vec{u}_1 \\ (A_2 - \lambda_1 I_{n_2})^r \vec{u}_2 \\ \vdots \\ (A_k - \lambda_1 I_{n_k})^r \vec{u}_k \end{pmatrix}.$$

From this, we see that if $\vec{u}_j \neq \vec{0}$ for any $j > 1$, then $C^r\vec{u} \neq \vec{0}$.

Let $v \in V$. By Theorem 6.19, we have

$$\begin{aligned} [\psi^r(v)]_{\mathcal{B}} &= [\psi^r]_{\mathcal{B}}[v]_{\mathcal{B}} \\ &= C^r[v]_{\mathcal{B}}. \end{aligned}$$

Hence, if $\psi^r(v) = \mathbf{0}$, it follows that $[v]_{\mathcal{B}}$ must be of the form

$$[v]_{\mathcal{B}} = \begin{pmatrix} \vec{u}_1 \\ \vec{0} \\ \vdots \\ \vec{0} \end{pmatrix}.$$

This in turn implies that

$$\psi^r(v) = \mathbf{0} \Rightarrow v \in \text{span } \mathcal{B}_1.$$

Since $r \geq 1$ is arbitrary and $\psi^r = (\varphi - \lambda_1 id_V)^r$, this implies that

$$GE_{\lambda_1} \subset \text{span } \mathcal{B}_1.$$

For the reverse inclusion, note that the matrix $A_1 - \lambda_1 I_{n_1}$ is a block diagonal matrix whose diagonal blocks are Jordan blocks of the form $J_p(0)$. In particular, $A_1 - \lambda_1 I_{n_1}$ is strictly upper triangular. By Corollary 13.50, we have

$$(A_1 - \lambda_1 I_{n_1})^{n_1} = \mathbf{0}.$$

This implies that $C^{n_i}\vec{u} = \vec{0}$ for all $\vec{u}$ of the form

$$\vec{u} = \begin{pmatrix} \vec{u}_1 \\ \vec{0} \\ \vdots \\ \vec{0} \end{pmatrix},$$

where $\vec{u}_1 \in \mathbb{C}^{n_1}$ is arbitrary. By the above discussion, this implies that $\psi^{n_1}(v) = \mathbf{0}$ for all $v \in \text{span } \mathcal{B}_1$. Hence,

$$GE_{\lambda_1} \supset \text{span } \mathcal{B}_1.$$

Putting the two inclusions together yields $GE_{\lambda_1} = \text{span } \mathcal{B}_1$. □

The following result will prove useful for finding a Jordan basis of a linear endomorphism of a complex vector space:

Theorem 13.56. *Let V be a complex vector space and let $\varphi : V \to V$ be a linear map with distinct eigenvalues $\lambda_1, \ldots, \lambda_k$. Let*

$$\mathcal{B} = \mathcal{B}_1 \cup \cdots \cup \mathcal{B}_k$$

be a Jordan basis of V for φ, where $\mathcal{B}_i$ is a basis of GE_{λ_i}.

(a) The number of Jordan blocks of the form $J_p(\lambda_i)$ in the matrix representation $[\varphi]_{\mathcal{B}}$ is equal to $\dim E_{\lambda_i}$, where E_{λ_i} is the eigenspace of φ associated to λ_i.

(b) Let $\mathcal{C} \subset \mathcal{B}_i$ be a subset of basis elements which correspond to some Jordan block $J_p(\lambda_i)$ in $[\varphi]_{\mathcal{B}}$. Let $U :=$ span $\mathcal{C}$ and $\psi := \varphi - \lambda id_V$. Then there exists $u \in U$ such that

$$\mathcal{C} = \{\psi^{p-1}(u), \ldots, \psi(u), u\}.$$

Proof. (a): Without loss of generality, we take $i = 1$. By Corollary 13.54, GE_{λ_1} is invariant under φ, that is,

$$\varphi(GE_{\lambda_1}) \subset GE_{\lambda_1}.$$

Let φ_1 be the restriction of φ to GE_{λ_1}. By Theorem 13.55, all of the Jordan blocks of the form $J_p(\lambda_1)$ in $[\varphi]_{\mathcal{B}}$ are contained in the matrix

$$[\varphi_1]_{\mathcal{B}_1}.$$

Hence, to prove (a), it suffices only to consider the linear map $\varphi_1 : GE_{\lambda_1} \to GE_{\lambda_1}$. Also, let

$$\psi := \varphi - \lambda_1 id_V$$

and note that $\psi(GE_{\lambda_1}) \subset GE_{\lambda_1}$. Let ψ_1 be the restriction of ψ to GE_{λ_1}. Let

$$n_1 := \dim GE_{\lambda_1}.$$

Then

$$[\psi_1]_{\mathcal{B}_1} = [\varphi_1]_{\mathcal{B}_1} - \lambda_1 I_{n_1},$$

which shows that $[\psi_1]_{\mathcal{B}_1}$ is a block diagonal matrix whose diagonal blocks are Jordan blocks of the form $J_p(0)$ for various $p \geq 1$. In particular, $\mathcal{B}_1$ is a Jordan basis for ψ_1. Clearly, $[\varphi_1]_{\mathcal{B}_1}$ and $[\psi_1]_{\mathcal{B}_1}$ have the same number of Jordan blocks.

Since $[\psi_1]_{\mathcal{B}_1}$ is a block diagonal matrix whose diagonal blocks are Jordan blocks of the form $J_p(0)$, $[\psi_1]_{\mathcal{B}_\lambda}$ is, in particular, a strictly upper triangular matrix. Hence, $[\psi_1]_{\mathcal{B}_1}$ is a nilpotent matrix by Corollary 13.50. This in turn implies that

$$\psi_1 : GE_{\lambda_1} \to GE_{\lambda_1}$$

is a nilpotent map. Let $\mathcal{E}_0$ denote the eigenspace of ψ_1 associated to (its only) eigenvalue 0. Statement (b) of Theorem 13.44 shows that the number of Jordan blocks in $[\psi_1]_{\mathcal{B}_1}$ is equal to $\dim \mathcal{E}_0$. However, $\mathcal{E}_0$ consist of all vectors $v \in GE_{\lambda_1}$ satisfying

$$\psi(v) = \varphi(v) - \lambda_1 v = \mathbf{0}.$$

This implies that $\mathcal{E}_0 \subset E_{\lambda_1}$. On the other hand, since $E_{\lambda_1} \subset GE_{\lambda_1}$, we conclude that $\mathcal{E}_0 = E_{\lambda_1}$. Hence, the number of Jordan blocks in both $[\psi_1]_{\mathcal{B}_1}$ and $[\varphi_1]_{\mathcal{B}_1}$ is

$$\dim \mathcal{E}_0 = \dim E_{\lambda_1}.$$

This proves (a).

(b): Once again, we take $i = 1$. Since $\mathcal{C} \subset \mathcal{B}_1$, we have $U \subset GE_{\lambda_1}$. As we noted in (a), the map $\psi_1 := \psi|_{GE_{\lambda_1}}$ is a nilpotent map. Since

$$[\varphi|_U]_{\mathcal{C}} = J_p(\lambda_1),$$

it follows that

$$[\psi|_U]_{\mathcal{C}} = J_p(0),$$

where we note that

$$\psi_1|_U = (\psi|_{GE_{\lambda_1}})|_U = \psi|_{GE_{\lambda_1} \cap U} = \psi|_U.$$

Statement (a) of Theorem 13.44 applied to the nilpotent map ψ_1 shows that there exists an element $u \in U$ such that

$$\mathcal{C} = \{\psi^{p-1}(u), \ldots, \psi(u), u\}.$$

This completes the proof. □

We now outline the general strategy for finding a Jordan basis for a general linear map $\varphi : V \to V$. The strategy is essentially an application of the strategy for finding a Jordan basis of a nilpotent map.

Finding a Jordan basis for a linear map $\varphi : V \to V$.

1. Find all the distinct eigenvalues of φ. Let $\lambda_1, \ldots, \lambda_k$ denote the distinct eigenvalues of φ.
2. Find the generalized eigenspace GE_{λ_i} for $i = 1, \ldots, k$.
3. For $i = 1, \ldots, k$, let
$$\psi_i := (\varphi - \lambda_i id_V)|_{GE_{\lambda_i}}.$$
Note that ψ_i is a nilpotent map.
4. For $i = 1, \ldots, k$, find a Jordan basis $\mathcal{B}_i$ of GE_{λ_i} for the nilpotent map ψ_i.
5. The basis $\mathcal{B} = \mathcal{B}_1 \cup \cdots \cup \mathcal{B}_k$ is the Jordan basis of V for φ.

Example 13.57. *Consider the vector space $\mathbb{C}^3$ and let $\mathcal{S} = \{\vec{e}_1, \vec{e}_2, \vec{e}_3\}$ denote the standard basis on $\mathbb{C}^3$. Let $\varphi : \mathbb{C}^3 \to \mathbb{C}^3$ be the linear map defined by*

$$\begin{aligned}\varphi(\vec{e}_1) &= 3\vec{e}_1 + 3\vec{e}_2 - \vec{e}_3,\\ \varphi(\vec{e}_2) &= -\vec{e}_2\\ \varphi(\vec{e}_3) &= \vec{e}_1 + 3\vec{e}_2 + \vec{e}_3\end{aligned}$$

The characteristic polynomial of φ is found to be

$$p_\varphi(x) = (x-2)^2(x+1).$$

Hence, the eigenvalues of φ are 2 and -1. By Proposition 13.53, we have $\dim GE_2 = 2$ and $\dim GE_{-1} = 1$. Let's calculate their generalized eigenspaces. For the purpose of calculation, its helpful to work with a matrix representation of φ. So lets take the matrix representation of φ with respect to $\mathcal{S}$:

$$[\varphi]_{\mathcal{S}} = \begin{pmatrix} 3 & 0 & 1 \\ 3 & -1 & 3 \\ -1 & 0 & 1 \end{pmatrix}.$$

Let

$$\psi_2 := \varphi - 2id_{\mathbb{C}^3}, \qquad \psi_{-1} := \varphi + id_{\mathbb{C}^3}.$$

The matrix representation of these maps with respect to $\mathcal{S}$ are

$$[\psi_2]_{\mathcal{S}} = \begin{pmatrix} 1 & 0 & 1 \\ 3 & -3 & 3 \\ -1 & 0 & -1 \end{pmatrix}, \quad [\psi_{-1}]_{\mathcal{S}} = \begin{pmatrix} 4 & 0 & 1 \\ 3 & 0 & 3 \\ -1 & 0 & 2 \end{pmatrix}.$$

Let E_2 and E_{-1} denote the eigenspaces of φ associated to 2 and -1 respectively. From the above matrices, it follows that

$$E_2 = span\{\vec{e}_1 - \vec{e}_3\}, \qquad E_{-1} = span\{\vec{e}_2\}.$$

Since $\dim E_2 = \dim E_{-1} = 1$, it follows that there is one Jordan block associated to both 2 and -1. Also, since $\dim \mathbb{C}^3 = 3$, our Jordan basis must give a matrix representation consisting of one Jordan block of size 2 and one of size 1. Since $\dim GE_2 = 2$, it follows that our Jordan basis must give a matrix representation consisting of the blocks $J_2(2)$ and $J_1(-1)$. Let's go ahead and compute GE_2. This amounts to finding the kernel of $(\psi_2)^2$. To do this, we first compute the matrix representation of $(\psi_2)^2$ with respect to $\mathcal{S}$:

$$[(\psi_2)^2]_{\mathcal{S}} = [\psi_2]^2_{\mathcal{S}} = \begin{pmatrix} 0 & 0 & 0 \\ -9 & 9 & -9 \\ 0 & 0 & 0 \end{pmatrix}$$

From this, we see that the kernel of $(\psi_2)^2$ has dimension 2 (as expected). From the above matrix, we see that

$$GE_2 = \text{span}\{\vec{e}_1 - \vec{e}_3, \vec{e}_1 + \vec{e}_2\}.$$

Since $\dim GE_{-1} = 1$, we have $GE_{-1} = E_{-1}$. Moreover, any nonzero vector in GE_{-1} will serve as a Jordan basis of GE_{-1} for $\psi_{-1}|_{GE_{-1}}$. We choose $\mathcal{B}_{-1} = \{\vec{e}_2\}$ for its basis. The associated Jordan block is then $J_1(-1)$.

Let us find a Jordan basis of GE_2 for $\psi_2|_{GE_2}$. Note that

$$(\psi_2)^2|_{GE_2} = \mathbf{0}, \qquad \psi_2|_{GE_2} \neq \mathbf{0}.$$

Since

$$\psi_2(\vec{e}_1 + \vec{e}_2) = \vec{e}_1 - \vec{e}_3 \neq \vec{0},$$

we take the following as a Jordan basis of GE_2 for $\psi_2|_{GE_2}$:

$$\mathcal{B}_2 := \{\psi_2(\vec{e}_1 + \vec{e}_2), \vec{e}_1 + \vec{e}_2\} = \{\vec{e}_1 - \vec{e}_3, \vec{e}_1 + \vec{e}_2\}.$$

A Jordan basis of $\mathbb{C}^3$ for φ is then

$$\mathcal{B} = \mathcal{B}_2 \cup \mathcal{B}_{-1} = \{\vec{e}_1 - \vec{e}_3, \vec{e}_1 + \vec{e}_2, \vec{e}_2\}.$$

The matrix representation of φ with respect to $\mathcal{B}$ is then

$$[\varphi]_{\mathcal{B}} = \begin{pmatrix} 2 & 1 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & -1 \end{pmatrix}.$$

Corollary 13.58. *Let A be an $n \times n$ complex matrix. Then there exists an $n \times n$ invertible matrix P such that $P^{-1}AP$ is in Jordan Canonical Form.*

Proof. Let $T_A : \mathbb{C}^n \to \mathbb{C}^n$ the linear transformation associated to A. Since T_A is a complex endomorphism, Theorem 13.48 shows that there exists a basis

$$\mathcal{B} = \{\vec{p}_1, \vec{p}_2, \ldots, \vec{p}_n\} \subset \mathbb{C}^n$$

such that the matrix representation $[T_A]_{\mathcal{B}}$ is in the Jordan canonical form. Let $\mathcal{S} = \{\vec{e}_1, \vec{e}_2, \ldots, \vec{e}_n\}$ be the standard basis on $\mathbb{C}^n$ and let P be the $n \times n$ matrix whose ith column is $\vec{p}_i$. Also, let $P_{\mathcal{S}\mathcal{B}}$ be the transition matrix from $\mathcal{B}$ to $\mathcal{S}$. Then

$$P_{\mathcal{S}\mathcal{B}} = P, \qquad [T_A]_{\mathcal{S}} = A.$$

From this, we have

$$P^{-1}AP = P_{\mathcal{B}\mathcal{S}}[T_A]_{\mathcal{S}}P_{\mathcal{S}\mathcal{B}} = [T_A]_{\mathcal{B}}.$$

□

Example 13.59. *Let*

$$A = \begin{pmatrix} 2 & 1/2 & 1/2 & 0 \\ 0 & -7/2 & -1/2 & 5 \\ 0 & 11/2 & 5/2 & -5 \\ 0 & -1/2 & -1/2 & 2 \end{pmatrix}.$$

The characteristic polynomial of A *is then*

$$p_A(x) = (x-2)^3(x+3).$$

With a little calculation, we see that the eigenspace associated to 2 *has dimension* 2 *and basis*

$$\{\vec{e}_1, \quad \vec{e}_2 - \vec{e}_3 + \vec{e}_4\}.$$

From $p_A(x)$*, we see that* $\dim GE_2 = 3$.

Hence, if $\mathcal{B}$ *is a Jordan basis of the linear transformation* $T_A : \mathbb{C}^4 \to \mathbb{C}^4$*, then the matrix representation* $[T_A]_{\mathcal{B}}$ *must contain the Jordan blocks* $J_2(2)$ *and* $J_1(2)$.

A basis for the Jordan block associated to $J_1(2)$ *is* $\{\vec{e}_1\}$ *and a basis for the Jordan block* $J_2(2)$ *is*

$$\{(A-2I_2)2\vec{e}_3, 2\vec{e}_3\} = \{\vec{e}_1 - \vec{e}_2 + \vec{e}_3 - \vec{e}_4,\ 2\vec{e}_3\}.$$

Looking at $p_A(x)$ *again, we see that for the eigenvalue* -3*, we have* $\dim GE_{-3} = 1$*. Hence, the Jordan block associated to* -3 *is* $J_1(-3)$*. A basis for this Jordan block is* $\{\vec{e}_2 - \vec{e}_3\}$*. So a Jordan basis for* $T_A : \mathbb{C}^4 \to \mathbb{C}^4$ *is*

$$\{\vec{e}_1,\ \vec{e}_1 - \vec{e}_2 + \vec{e}_3 - \vec{e}_4,\ 2\vec{e}_3,\ \vec{e}_2 - \vec{e}_3\}.$$

From the proof of Corollary 13.58, let

$$P = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & -1 & 0 & 1 \\ 0 & 1 & 2 & -1 \\ 0 & -1 & 0 & 0 \end{pmatrix}.$$

Then

$$P^{-1}AP = \begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 2 & 1 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & -3 \end{pmatrix}.$$

Corollary 13.60. *Let* A *be a complex* $n \times n$ *matrix. Let* $\lambda_1, \lambda_2, \ldots, \lambda_n$ *be the eigenvalues of* A *with* ***multiplicities****. Then* $Tr(A) = \sum_{i=1}^{n} \lambda_i$.

Proof. By Corollary 13.58, there exists a matrix P such that $P^{-1}AP$ is in Jordan Canonical Form. The diagonal elements of $P^{-1}AP$ are precisely the eigenvalues of A with multiplicities. Corollary 13.60 now follows from the fact that

$$\mathrm{Tr}(P^{-1}AP) = \mathrm{Tr}(APP^{-1}) = \mathrm{Tr}(A).$$

□

13.8. Complexification

In general, the Jordan Canonical Form Theorem (Theorem 13.48) does not work for linear endomorphisms on a real vector space. Ultimately, the reason for this is the fact that real polynomials do not always have real roots. The upshot of this is that a linear endomorphism of a real vector space does not always have eigenvalues. Consequently, a Jordan basis does not always exist for real linear maps. The opposite is true for the complex case. In the complex case, polynomials can always be decomposed as a product of linear factors. Hence, a linear endomorphism of a complex vector space has all its eigenvalues. This in turn allows the domain of the endomorphism to be expressed as a direct sum of its generalized eigenspaces thus making a Jordan basis possible.

The existence of a Jordan basis for a linear endomorphism of a complex vector space leads to Corollary 13.49, which shows that the characteristic polynomial and the minimal polynomial of the endomorphism have the same roots (namely the eigenvalues of the endomorphism), but with possibly different multiplicities. Corollary 13.49 also shows that the minimal polynomial of a complex endomorphism must divide its characteristic polynomial. It turns out that these same facts are also true for endomrophisms of a real vector space. One way to show this is through the idea of **complexification**, which will allow us, ultimately, to apply Corollary 13.49 to the real case.

Complexification is a very simple way of turning **real** vector spaces and **real** linear maps into **complex** vector spaces and **complex** linear maps. To a real vector space V, we associate a complex vector space $V^{\mathbb{C}}$ as follows. As a set,

$$V^{\mathbb{C}} := \{v_1 + iv_2 \mid v_1, v_2 \in V\},$$

where $i := \sqrt{-1}$. An element $v_1 + iv_2$ in $V^{\mathbb{C}}$ is to be viewed as a formal sum with real part

$$\mathfrak{R}(v_1 + iv_2) := v_1$$

and imaginary part

$$\mathfrak{I}(v_1 + iv_2) := v_2.$$

Two elements of $V^{\mathbb{C}}$ are then equal if and only if they have the same real parts and the same imaginary parts. The complex vector space structure on $V^{\mathbb{C}}$ is defined as follows:

(1) **vector addition**:

$$(u_1 + iu_2) + (v_1 + iv_2) := (u_1 + v_1) + i(v_1 + v_2)$$

(2) **scalar multiplication**:

$$(a + ib)(v_1 + iv_2) := (av_1 - bv_2) + i(bv_1 + av_2)$$

where $a, b \in \mathbb{R}$, $v_1, v_2 \in V$.

The following is a straightforward exercise which we leave to the reader:

Exercise 13.61. *Verify that $V^{\mathbb{C}}$ satisfies all the conditions a vector space over $\mathbb{C}$ from Definition 5.4.*

Definition 13.62. *Let V be a real vector space. The complex vector space $V^{\mathbb{C}}$ is called the* ***complexification*** *of V.*

The zero vector of $V^{\mathbb{C}}$ is technically

$$\mathbf{0} + i\mathbf{0}.$$

However, for the sake of notational simplicity, one simply denotes the zero vector of $V^{\mathbb{C}}$ as $\mathbf{0}$. Also, the real vector space V (viewed as a set) can be naturally regarded as a subset of $V^{\mathbb{C}}$ by identifying the element $v \in V$ with the element

$$v + i\mathbf{0} \in V^{\mathbb{C}}.$$

In this way, we have

$$V \subset V^{\mathbb{C}}.$$

Example 13.63. *The one dimensional complex vector space $\mathbb{C}$ is just the complexification of the one dimensional real vector space $\mathbb{R}$:*

$$\mathbb{R}^{\mathbb{C}} = \mathbb{C}.$$

Proposition 13.64. *Let V be a real vector space. Let $\mathcal{B}$ be a basis of V. Then $\mathcal{B}$ is also a basis of $V^{\mathbb{C}}$. In particular, $\dim V^{\mathbb{C}} = \dim V$.*

Proof. Let $\mathcal{B} = \{b_1, \ldots, b_n\}$ be a basis of V. Consider the element $v_1 + iv_2 \in V^{\mathbb{C}}$. Express v_1 and v_2 as a linear combination of the basis elements of $\mathcal{B}$:

$$v_1 = \alpha_1 b_1 + \cdots + \alpha_n b_n$$

and

$$v_2 = \beta_1 b_1 + \cdots + \beta_n b_n,$$

for some $\alpha_i, \beta_i \in \mathbb{R}$. Then

$$\begin{aligned} v_1 + iv_2 &= (\alpha_1 b_1 + \cdots + \alpha_n b_n) + i(\beta_1 b_1 + \cdots + \beta_n b_n) \\ &= (\alpha_1 + i\beta_1) b_1 + \cdots + (\alpha_n + i\beta_n) b_n. \end{aligned}$$

This shows that $V^{\mathbb{C}} = \operatorname{span}\{b_1, \ldots, b_n\}$.

We now show that $\mathcal{B}$ is linearly independent in $V^{\mathbb{C}}$. To do this, suppose that

$$z_1 b_1 + \cdots + z_n b_n = \mathbf{0} = \mathbf{0} + i\mathbf{0}.$$

Since $z_j = \Re(z_j) + i\Im(z_j)$ for $j = 1, \ldots, n$, the above sum can be rewritten as

$$(\Re(z_1) b_1 + \cdots + \Re(z_n) b_n) + i(\Im(z_1) b_1 + \cdots + \Im(z_n) b_n) = \mathbf{0} + i\mathbf{0}.$$

The left and right hand sides agree if and only if

$$\Re(z_1) b_1 + \cdots + \Re(z_n) b_n = \mathbf{0}$$

and

$$\Im(z_1) b_1 + \cdots + \Im(z_n) b_n = \mathbf{0}.$$

Since $\mathcal{B}$ is a basis on V and hence linearly independent over $\mathbb{R}$, it follows that

$$\Re(z_j) = \Im(z_j) = 0, \qquad \text{for } j = 1, \ldots, n,$$

which in turn implies that $z_j = 0$ for $j = 1, \ldots, n$. □

A linear map $\varphi : V \to W$ between two real vector spaces can also naturally be turned into a linear map

$$\varphi^{\mathbb{C}} : V^{\mathbb{C}} \to W^{\mathbb{C}},$$

by setting

$$\varphi^{\mathbb{C}}(v_1 + iv_2) := \varphi(v_1) + i\varphi(v_2),$$

for $v_1, v_2 \in V$. The following is another very simple exercise which we leave to the reader:

Exercise 13.65. *Verify that $\varphi^{\mathbb{C}} : V^{\mathbb{C}} \to W^{\mathbb{C}}$ is a linear map between complex vector spaces.*

Definition 13.66. *Let V and W be real vector spaces and let $\varphi : V \to W$ be a linear map. The linear map $\varphi^{\mathbb{C}} : V^{\mathbb{C}} \to W^{\mathbb{C}}$ is called the **complexification** of φ.*

Lemma 13.67. *Let V be a real vector space and let $\varphi : V \to V$ be a linear map. Let $q(x) \in \mathbb{R}[x] \subset \mathbb{C}[x]$. Then*

$$q(\varphi^{\mathbb{C}}) = (q(\varphi))^{\mathbb{C}}.$$

Proof. We first show

$$(\varphi^{\mathbb{C}})^k = (\varphi^k)^{\mathbb{C}}$$

by induction on k. For $k = 1$, the above equality clearly holds. So let us suppose that the above equality holds for some $k \geq 1$. Let $v_1, v_2 \in V$. Then

$$\begin{aligned}(\varphi^{\mathbb{C}})^{k+1}(v_1 + iv_2) &= (\varphi^{\mathbb{C}})^k \varphi^{\mathbb{C}}(v_1 + iv_2) \\ &= (\varphi^{\mathbb{C}})^k (\varphi(v_1) + i\varphi(v_2)) \\ &= (\varphi^k)^{\mathbb{C}} (\varphi(v_1) + i\varphi(v_2)) \\ &= \varphi^k \varphi(v_1) + i\varphi^k \varphi(v_2) \\ &= \varphi^{k+1}(v_1) + i\varphi^{k+1}(v_2) \\ &= (\varphi^{k+1})^{\mathbb{C}}(v_1 + iv_2),\end{aligned}$$

where we use the induction hypothesis in third equality. This completes the induction step.

Now let

$$q(x) = a_k x^k + a_{k-1}x^{k-1} \cdots + a_1 x + a_0 \in \mathbb{R}[x] \subset \mathbb{C}[x].$$

Then

$$\begin{aligned}q(\varphi^{\mathbb{C}}) &= a_k(\varphi^{\mathbb{C}})^k + a_{k-1}(\varphi^{\mathbb{C}})^{k-1} \cdots + a_1\varphi^{\mathbb{C}} + a_0 id_{V^{\mathbb{C}}} \\ &= a_k(\varphi^k)^{\mathbb{C}} + a_{k-1}(\varphi^{k-1})^{\mathbb{C}} \cdots + a_1\varphi^{\mathbb{C}} + a_0(id_V)^{\mathbb{C}} \\ &= \left(a_k(\varphi^k) + a_{k-1}(\varphi^{k-1}) \cdots + a_1\varphi^{\mathbb{C}} + a_0(id_V)\right)^{\mathbb{C}} \\ &= (q(\varphi))^{\mathbb{C}}.\end{aligned}$$

□

Theorem 13.68. *Let V be a real vector space and let $\varphi : V \to V$ be a linear map.*

(i) The characteristic polynomial of φ and $\varphi^{\mathbb{C}}$ are equal.
(ii) The minimal polynomial of φ and $\varphi^{\mathbb{C}}$ are equal.

Proof. (i): Fix a basis $\mathcal{B} = \{b_1, \ldots, b_n\}$ on V. Then

$$\varphi(b_k) = \sum_{j=1}^{n} \alpha_{jk} b_j$$

for some $\alpha_{jk} \in \mathbb{R}$. The matrix representation $[\varphi]_{\mathcal{B}}$ is then the $n \times n$ matrix whose (j, k)-element is a_{jk}.

By Proposition 13.64, $\mathcal{B} \subset V$ is also a basis of $V^{\mathbb{C}}$. From the definition of $\varphi^{\mathbb{C}}$, we have $\varphi^{\mathbb{C}}(b_k) = \varphi(b_k) \in V$. This implies that the matrix representation of $\varphi^{\mathcal{C}}$

with respect to $\mathcal{B}$ is

$$[\varphi^{\mathbb{C}}]_{\mathcal{B}} = [\varphi]_{\mathcal{B}} = \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{nn} \end{pmatrix}.$$

Hence, the characteristic polynomial of $\varphi^{\mathbb{C}}$ and φ must be equal:

$$p_{\varphi^{\mathbb{C}}} = \det(xI_n - [\varphi^{\mathbb{C}}]_{\mathcal{B}}) = \det(xI_n - [\varphi]_{\mathcal{B}}) = p_{\varphi}$$

(ii): Let $m_{\varphi^{\mathbb{C}}}(x)$ be the minimal polynomial of $\varphi^{\mathbb{C}}$. Let

$$k := \deg m_{\varphi^{\mathbb{C}}}(x)$$

Since $\varphi^{\mathbb{C}}$ is a complex linear map, we have $m_{\varphi^{\mathbb{C}}} \in \mathbb{C}[x]$. Hence,

$$m_{\varphi^{\mathbb{C}}}(x) = x^k + z_{k-1}x^{k-1} + \cdots z_1 x + z_0$$

for some $z_0, z_1, \ldots, z_{k-1} \in \mathbb{C}$. Write $z_j = \alpha_j + i\beta_j$ and decompose $m_{\varphi^{\mathbb{C}}}$ into its real and imaginary parts:

$$m_{\varphi^{\mathbb{C}}}(x) = p_1(x) + ip_2(x),$$

where

$$p_1 := x^k + \alpha_{k-1}x^{k-1} + \cdots \alpha_1 x + \alpha_0 \in \mathbb{R}[x] \subset \mathbb{C}[x]$$

and

$$p_2 := \beta_{k-1}x^{k-1} + \cdots \beta_1 x + \beta_0 \in \mathbb{R}[x] \subset \mathbb{C}[x].$$

Let $v \in V$ be arbitrary. By Lemma 13.67, we have

$$\begin{aligned} m_{\varphi^{\mathbb{C}}}(\varphi^{\mathbb{C}})(v) &= p_1(\varphi^{\mathbb{C}})(v) + ip_2(\varphi^{\mathbb{C}})(v) \\ \mathbf{0} &= (p_1(\varphi))^{\mathbb{C}}(v) + i(p_2(\varphi))^{\mathbb{C}}(v) \\ \mathbf{0} &= p_1(\varphi)(v) + ip_2(\varphi)(v) \end{aligned}$$

The last equality implies that $p_1(\varphi)(v) = p_2(\varphi)(v) = \mathbf{0}$. Since $v \in V$ is arbitrary, we conclude that

$$p_1(\varphi) = p_2(\varphi) = \mathbf{0}$$

This fact along with Lemma 13.67 implies that for a general element $v_1 + iv_2 \in V^{\mathbb{C}}$, we have

$$\begin{aligned} p_1(\varphi^{\mathbb{C}})(v_1 + iv_2) &= p_1(\varphi)^{\mathbb{C}}(v_1 + iv_2) \\ &= p_1(\varphi)(v_1) + ip_1(\varphi)(v_2) \\ &= \mathbf{0} + i\mathbf{0} \\ &= \mathbf{0}. \end{aligned}$$

Hence, $p_1(\varphi^{\mathbb{C}}) = \mathbf{0}$. Since $p_1(x)$ has degree k, like $m_{\varphi^{\mathbb{C}}}(x)$, the uniqueness of the minimal polynomial (see Theorem 13.2) implies that

$$m_{\varphi^{\mathbb{C}}}(x) = p_1(x).$$

In particular, $p_2(x) = 0$. We have thus shown that $m_{\varphi^{\mathbb{C}}}(x)$ is a real polynomial which

$$m_{\varphi^{\mathbb{C}}}(\varphi) = \mathbf{0}.$$

Now let $m_\varphi(x) \in \mathbb{R}[x] \subset \mathbb{C}[x]$ be the minimal polynomial of φ. Since $m_\varphi(\varphi) = \mathbf{0}$, the same argument used above for $p_1(x)$ shows that

$$m_\varphi(\varphi^{\mathbb{C}}) = \mathbf{0}.$$

This implies that

$$\deg m_{\varphi^{\mathbb{C}}}(x) \leq \deg m_\varphi(x).$$

On the other hand, since $m_{\varphi^{\mathbb{C}}}(\varphi) = \mathbf{0}$, we also have

$$\deg m_{\varphi^{\mathbb{C}}}(x) \geq \deg m_\varphi(x).$$

From this, we conclude that $m_\varphi(x)$ and $m_{\varphi^{\mathbb{C}}}(x)$ have the same degree. The uniqueness of the minimal polynomial now implies

$$m_\varphi(x) = m_{\varphi^{\mathbb{C}}}(x).$$

□

13.9. The Cayley-Hamilton Theorem

We begin this section by proving the real version of Corollary 13.49:

Proposition 13.69. *Let V be a real vector space and let $\varphi : V \to V$ be a linear map. Let $p_\varphi(x)$ and $m_\varphi(x)$ be the characteristic and minimal polynomials of φ respectively.*

(i) $p_\varphi(x)$ and $m_\varphi(x)$ have the same roots (namely the eigenvalues of φ).

(ii) $m_\varphi(x) \mid p_\varphi(x)$

Proof. Let $p_\varphi(x)$ and $m_\varphi(x)$ be the characteristic and minimal polynomials of φ respectively. Consider the complexification

$$\varphi^{\mathbb{C}} : V^{\mathbb{C}} \to V^{\mathbb{C}}.$$

By Theorem 13.68, the characteristic and the minimal polynomials of $\varphi^{\mathbb{C}}$ are $p_\varphi(x)$and $m_\varphi(x)$ respectively. By Corollary 13.49, $p_\varphi(x)$ and $m_\varphi(x)$ have the same roots. This proves (i).

Corollary 13.49 also implies that $m_\varphi(x) \mid p_\varphi(x)$. Here, we have to be a little bit careful. We are applying Corollary 13.49 to the complex linear map $\varphi^{\mathbb{C}}$. Hence, $p_\varphi(x)$ and $m_\varphi(x)$ are regarded as elements of $\mathbb{C}[x]$ (even though they are both real polynomials). The condition $m_\varphi(x) \mid p_\varphi(x)$ in this case means that there exists $q(x) \in \mathbb{C}[x]$ such that

$$p_\varphi(x) = q(x)m_\varphi(x).$$

What we want to do now is show that $q(x)$ is actually a real polynomial. This is easy to do. Since $q(x) \in \mathbb{C}[x]$, we can express $q(x)$ as a sum of its real and imaginary parts:

$$q(x) = q_1(x) + iq_2(x),$$

where $q_1(x), q_2(x) \in \mathbb{R}[x]$. Then

$$\begin{aligned} p_\varphi(x) &= q(x)m_\varphi(x) \\ &= q_1(x)m_\varphi(x) + iq_2(x)m_\varphi(x). \end{aligned}$$

Since $p_\varphi(x)$ is real, the imaginary part on the right side must be zero. Since $m_\varphi(x)$, $q_1(x)$, and $q_2(x)$ are real, it follows that we must have

$$q_2(x)m_\varphi(x) = 0.$$

Since $m_\varphi(x)$ is monic, it follows that $\deg m_\varphi(x) \geq 1$. In particular, $m_\varphi(x) \neq 0$. This implies that $q_2(x) = 0$. Hence, $q(x) = q_1(x)$ is a real polynomial. We therefore conclude that $m_\varphi(x) \mid p_\varphi(x)$ as real polynomials. This proves (ii). □

We now state the Cayley-Hamilton Theorem:

Theorem 13.70 (Cayley-Hamilton Theorem)**.** *Let V be a real or complex vector space and let $\varphi : V \to V$ be a linear map. Let $p_\varphi(x)$ be the characteristic polynomial of φ. Then $p_\varphi(\varphi) = \mathbf{0}$.*

Proof. Let $m_\varphi(x)$ be the minimal polynomial of φ. If V is a complex vector space, Corollary 13.49 shows that $m_\varphi(x) \mid p_\varphi(x)$. Likewise, if V is a real vector space, Proposition 13.69 also shows that $m_\varphi(x) \mid p_\varphi(x)$. Hence, for the real or complex case, there exists a polynomial $q(x) \in \mathbb{F}[x]$ (where $\mathbb{F} = \mathbb{R}$ or $\mathbb{C}$ depending on whether V is a real or complex vector space) such that

$$p_\varphi(x) = q(x)m_\varphi(x).$$

Hence,

$$p_\varphi(\varphi) = q(\varphi)m_\varphi(\varphi) = q(\varphi)\mathbf{0} = \mathbf{0}.$$

□

At the same time, let us also give the more familiar matrix version of the Cayley-Hamilton Theorem (which is really just a corollary of Theorem 13.70):

Theorem 13.71. *Let A be a real or complex square matrix and let $p_A(x)$ be the characteristic polynomial of A. Then $p_A(A) = \mathbf{0}$.*

Proof. Let A be a square matrix of size $n$and let $\mathbb{F} = \mathbb{R}$ or $\mathbb{C}$ depending on whether A is real or complex. Let

$$T_A : \mathbb{F}^n \to \mathbb{F}^n$$

be the natural linear map associated to A, that is, $T_A(\vec{v}) = A\vec{v}$. Now for any polynomial $q(x) \in \mathbb{F}[x]$, we have

$$q(T_A) = T_{q(A)},$$

that is, the linear map $q(T_A)$ is precisely the linear map associated to the matrix $q(A)$. In particular, this means that $q(T_A) = \mathbf{0}$ if and only if $q(A) = \mathbf{0}$.

Let $\mathcal{S} = \{\vec{e}_1, \ldots, \vec{e}_n\}$ denote the standard basis on $\mathbb{F}^n$. Then the matrix representation of T_A with respect to $\mathcal{S}$ is just A. Hence, the characteristic polynomial of T_A is just

$$p_{T_A}(x) = \det(xI_n - A) = p_A(x).$$

Combining this observation with Theorem 13.70 gives

$$p_{T_A}(T_A) = p_A(T_A) = \mathbf{0}.$$

In light of the above remarks, we have $p_A(A) = \mathbf{0}$. □

Remark 13.72. *There is a very quick, but wrong way to prove the Cayley-Hamilton Theorem that may have entered your mind. For concreteness, let's consider the matrix version. Let A be an $n \times n$ matrix. The characteristic polynomial of A is*

$$p_A(x) = \det(xI_n - A).$$

The incorrect way is simply to substitute A in for x which of course gives

$$p_A(A) = \det(AI_n - A) = \det(A - A) = \det(\mathbf{0}) = 0.$$

The reason this "proof" is incorrect has to do with the meaning of x in the definition of the characteristic polynomial. In the definition, x represents a scalar, not a matrix. The roots of p_A are then the eigenvalues of A. Hence, substituting an $n \times n$ matrix in for x makes no sense here.

Another way to get a sense that the above "proof" is wrong is by considering the value of $p_A(A)$ itself. Indeed, under the quick "proof", the value of $p_A(A)$ is a scalar (namely $0 \in \mathbb{R}$). On the other hand, when we substitute A in for x in the ***polynomial*** *$p_A(x)$, the value of $p_A(A)$ is not a scalar. The value of $p_A(A)$ in this case is the $n \times n$ zero matrix $\mathbf{0}$. This should tell you that something is not quite right with the quick "proof".*

Example 13.73. *Consider the real matrix*

$$A = \begin{pmatrix} 2 & -1 \\ -5 & 3 \end{pmatrix}.$$

The characteristic polynomial is then

$$p_A(x) = \det(xI_2 - A) = x^2 - 5x + 1.$$

By the Cayley-Hamilton Theorem, we have

$$\begin{aligned} p_(A) &= A^2 - 5A + I_2 \\ &= \begin{pmatrix} 9 & -5 \\ -25 & 14 \end{pmatrix} - \begin{pmatrix} 10 & -5 \\ -25 & 15 \end{pmatrix} + \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}. \end{aligned}$$

Example 13.74. *Consider the complex matrix*

$$A = \begin{pmatrix} 3+2i & 5 \\ 1-i & 4-7i \end{pmatrix}.$$

The characteristic polynomial is then

$$p_A(x) = \det(xI_2 - A) = x^2 + (-7+5i)x + (21-8i).$$

By the Cayley-Hamilton Theorem, we have

$$\begin{aligned} p_(A) &= A^2 - (-7+5i)A + (21-8i)I_2 \\ &= \begin{pmatrix} 10+7i & 35-25i \\ 2-12i & -28-61i \end{pmatrix} + \begin{pmatrix} -31+i & -35+25i \\ -2+12i & 7+69i \end{pmatrix} \\ &+ \begin{pmatrix} 21-8i & 0 \\ 0 & 21-8i \end{pmatrix} \\ &= \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}. \end{aligned}$$

We conclude this chapter with the following observation:

Theorem 13.75. *Let V be a real or complex vector space of dimension n and let $\varphi : V \to V$ be a linear map. Then φ is nilpotent if and only if its characteristic polynomial is $p_\varphi(x) = x^n$.*

Proof. ($\Rightarrow$) Suppose φ is nilpotent. By Theorem 13.35, the minimal polynomial of φ is of the form $m_\varphi(x) = x^k$ for some integer $k \geq 1$. Let

$$\varphi^{\mathbb{C}} : V^{\mathbb{C}} \to V^{\mathbb{C}}$$

be the complexification of φ. By Theorem 13.68, φ and $\varphi^{\mathbb{C}}$ have the same minimal polynomial and the same characteristic polynomial. Hence, the minimal polynomial of $\varphi^{\mathbb{C}}$ is also x^k. Corollary 13.49 implies that the characteristic polynomial of $\varphi^{\mathbb{C}}$ is x^n. This in turn implies that the characteristic polynomial of φ is x^n.

($\Leftarrow$) If the characteristic polynomial of φ is $p_\varphi(x) = x^n$, then by the Cayley-Hamilton Theorem we have $p_\varphi(\varphi) = \mathbf{0}$. Hence, φ is nilpotent. □

Corollary 13.76. *Let A be a real or complex $n \times n$ matrix. Then A is nilpotent if and only if its characteristic polynomial is $p_A(x) = x^n$.*

Proof. Let $\mathbb{F} = \mathbb{R}$ or $\mathbb{C}$ depending on whether A is real or complex. Let $T_A : \mathbb{F}^n \to \mathbb{F}^n$ be the natural linear map defined by $T_A(\vec{v}) = A\vec{v}$. Then A is a nilpotent matrix if and only if T_A is a nilpotent map.

By Theorem 13.75, T_A is a nilpotent map if and only if its characteristic polynomial is $p_{T_A}(x) = x^n$. The proof of Theorem 13.71 shows that one always has

$$p_{T_A}(x) = p_A(x).$$

Putting the above statements together proves Corollary 13.76. □

Chapter 13 Exercises

1. Show that the Jordan block $J_k(0)^n = \mathbf{0}$ if and only if $n \geq k$.

2. Find the minimal polynomial of

$$A = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 2 \end{pmatrix}$$

3. Let A be an $n \times n$ matrix and let $p_A(x)$ and $m_A(x)$ be the characteristic polynomial and the minimal polynomial of A respectively. Show that

$$p_A(x) \mid (m_A(x))^n$$

4. Let A be an $n \times n$ complex matrix and let $\lambda \in \mathbb{C}$. Let $GE_\lambda(A)$ denote the generalized eigenspace of A. Let $c \in \mathbb{C}$ be nonzero.
   (a) Show that $c\lambda$ is an eigenvalue of cA.
   (b) Show that $GE_\lambda(A) = GE_{c\lambda}(cA)$.
   (c) Suppose $J_k(\lambda)$ is a Jordan block appearing in the Jordan Canonical Form of A. Show that $J_k(c\lambda)$ is a Jordan block appearing in the Jordan Canonical form of cA.

5. Let
$$A = \begin{pmatrix} 7 & -5 & -2 \\ 1 & 5 & -2 \\ -2 & 6 & 12 \end{pmatrix}.$$
   (a) Compute the characteristic polynomial of A and its eigenvalues.
   (b) For each eigenvalue λ of A, compute GE_λ.
   (c) Find an invertible matrix P such that $P^{-1}AP$ is in Jordan Canonical Form.
   (d) Determine the minimal polynomial of A.

6. Let
$$A = \begin{pmatrix} -27 & -42 & -29 \\ 18 & 30 & 22 \\ 15 & 30 & 9 \end{pmatrix}.$$
   (a) Compute the characteristic polynomial of A and its eigenvalues.
   (b) For each eigenvalue λ of A, compute GE_λ.
   (c) Find an invertible matrix P such that $P^{-1}AP$ is in Jordan Canonical Form.
   (d) Determine the minimal polynomial of A.

7. Let
$$A = \begin{pmatrix} 17 & -2 & 11 \\ -4 & 10 & -4 \\ 3 & 6 & 9 \end{pmatrix}.$$
   (a) Compute the characteristic polynomial of A and its eigenvalues.
   (b) For each eigenvalue λ of A, compute GE_λ.
   (c) Find an invertible matrix P such that $P^{-1}AP$ is in Jordan Canonical Form.
   (d) Determine the minimal polynomial of A.

8. Determine if the following matrices are nilpotent by calculating their characteristic polynomials:
   (a)
$$A = \begin{pmatrix} 15 & 18 & 1 \\ -6 & -6 & -2 \\ -3 & -6 & 3 \end{pmatrix}.$$
   (b)
$$B = \begin{pmatrix} -2 & 1 & 0 \\ -2 & 2 & 2 \\ 2 & -1 & 0 \end{pmatrix}.$$

9. Let $\varphi : V \to V$ be a linear map, and $\varphi^2 = I$, where I is identical map.

(a) Show that the eigenvalues of φ can only be ± 1.
(b) Let E_1 and E_{-1} denote the eigenspace of φ associated to 1 and -1 respectively. Show that

$$V = E_1 \oplus E_{-1}$$

and thus φ is diagonalizable.

10. Are the two matrices

$$\begin{pmatrix} -1 & 3 \\ 3 & 0 \end{pmatrix} \quad \begin{pmatrix} 0 & 3 \\ 3 & -1 \end{pmatrix}$$

simultaneously diagonalizable?

11. Find all symmetric matrices that are simultaneously diagonalizable with

$$\begin{pmatrix} 3 & -1 \\ -1 & 0 \end{pmatrix}.$$

12. Given two matrices

$$A = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \quad \text{and} \quad B = \begin{pmatrix} 1 & 2 \\ 2 & 3 \end{pmatrix}$$

are A and B simultaneously diagonalizable? If yes, please find an orthogonal matrix Q such that both $Q^T AQ$ and $Q^T BQ$ are both diagonal matrices.

13. Let $\varphi \in End(\mathbb{R}^2)$ be the linear maps defined by

$$\varphi(\vec{e}_1) = \vec{e}_1 + \vec{e}_2, \quad \text{and} \quad \varphi(\vec{e}_2) = \vec{e}_2$$

(a) Calculate all eigenvalues of φ.
(b) Calculate the geometric multiplicity and algebraic multiplicity of each eigenvalue.
(c) Determine whether A is diagonalizable.

14. Let $\varphi \in End(\mathbb{R}^3)$ be the linear maps defined by

$$\varphi(\vec{e}_1) = 2\vec{e}_2 + 3\vec{e}_3, \quad \varphi(\vec{e}_2) = \vec{e}_3, \quad \text{and} \quad \varphi(\vec{e}_3) = 0$$

(a) Show that φ is a nilpotent map.
(b) Calculate E_0, the eigenspace of φ associated to 0.
(c) Finding a Jordan basis of φ.
(d) Find the minimal polynomial of φ.

15. Denote by

$$A = \begin{pmatrix} 1+i & 2 & 2+3i \\ 1-i & 2i & 3-3i \\ 2 & -i & 1-i \end{pmatrix}$$

Calculate the characteristic polynomial of A, $p_A(x)$, and then evaluate $p_A(A)$ to verify the Cayley-Hamilton Theorem.

Chapter 14

Applications

14.1. Fibonacci numbers

Probably you are familiar with the sequence of numbers

$$0, 1, 1, 2, 3, 5, 8, 13, 21, \dots .$$

Its called the sequence of Fibonacci numbers after someone who supposedly brought Arabic numbers to Europe in the 14th century. It has something to do with botany and the numbers of petals or seeds on a plant such as a sunflower plant. Of course, you can guess the next number in the sequence: its $13 + 21 = 34$. Obviously each number in the sequence equals the sum of the previous two. If F_n denotes the n^{th} number in the sequence, so that $F_0 = 0$, $F_1 = 1$, $F_9 = 34$, and so on, then

$$F_{n+1} = F_n + F_{n-1} .$$

Consider the sequence of ratios F_{n+1}/F_n, starting with F_2/F_1:

$$1, 2, \frac{3}{2} = 1.5, \frac{5}{3} = 1.\overline{6}, \frac{8}{5} = 1.6, \frac{13}{8} = 1.625, \frac{21}{13} = 1.615,$$

and so on. It appears to be converging, and in fact it is to the value

$$\lambda_1 = \frac{1+\sqrt{5}}{2} = 1.618\dots .$$

For some reason someone thought that this value λ_1 was particularly pleasing so they named it the golden ratio. For example, a room whose floor dimensions are in this ratio is the most attractive. More importantly, λ_1 is an eigenvalue of the matrix

$$\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} . \tag{305}$$

Indeed, the characteristic polynomial of the matrix is $(1-t)(-t) - 1 = t^2 - t - 1$, which has roots λ_1 and its conjugate $\lambda_2 = \frac{1-\sqrt{5}}{2}$. This matrix describes the relation that recursively generates the Fibonacci numbers because

$$\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} F_n \\ F_{n-1} \end{pmatrix} = \begin{pmatrix} F_{n+1} \\ F_n \end{pmatrix} . \tag{306}$$

But why should F_{n+1}/F_n converge to λ_1? In order to explain this let us first determine a formula for F_n. We shall organize things by introducting a vector notation:

$$\vec{v}_n = \begin{pmatrix} F_n \\ F_{n-1} \end{pmatrix} \ ; \ 1 \le n \ ,$$

so that equation (306) reads

$$\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \vec{v}_n = \vec{v}_{n+1} \ . \tag{307}$$

Therefore,

$$\vec{v}_{n+1} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^n \vec{v}_1 = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^n \begin{pmatrix} 1 \\ 0 \end{pmatrix} . \tag{308}$$

It is clear what we must do now: diagonalize the matrix (305) so that we may calculate its n^{th} power, and thereby find a formula for F_n for this is the second coordinate of $\vec{v}_{n+1}$. If λ is an eigenvalue (either one), then $\lambda^2 = \lambda + 1$, so that

$$\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} \lambda \\ 1 \end{pmatrix} = \begin{pmatrix} \lambda + 1 \\ \lambda \end{pmatrix} = \lambda \begin{pmatrix} \lambda \\ 1 \end{pmatrix} .$$

Thus, $(\lambda, 1)$ is an eigenvector for the eigenvalue λ. We have

$$\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} \lambda_1 & \lambda_2 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} \lambda_1 & \lambda_2 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix} .$$

Whence, by (307) we have

$$\begin{aligned}
\vec{v}_{n+1} &= \begin{pmatrix} \lambda_1 & \lambda_2 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} \lambda_1^n & 0 \\ 0 & \lambda_2^n \end{pmatrix} \begin{pmatrix} \lambda_1 & \lambda_2 \\ 1 & 1 \end{pmatrix}^{-1} \begin{pmatrix} 1 \\ 0 \end{pmatrix} \\
&= \frac{1}{\lambda_1 - \lambda_2} \begin{pmatrix} \lambda_1 & \lambda_2 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} \lambda_1^n & 0 \\ 0 & \lambda_2^n \end{pmatrix} \begin{pmatrix} 1 & -\lambda_2 \\ -1 & \lambda_1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} \\
&= \frac{1}{\lambda_1 - \lambda_2} \begin{pmatrix} \lambda_1 & \lambda_2 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} \lambda_1^n & 0 \\ 0 & \lambda_2^n \end{pmatrix} \begin{pmatrix} 1 \\ -1 \end{pmatrix} \\
&= \frac{1}{\lambda_1 - \lambda_2} \begin{pmatrix} \lambda_1 & \lambda_2 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} \lambda_1^n \\ -\lambda_2^n \end{pmatrix} \\
&= \frac{1}{\lambda_1 - \lambda_2} \begin{pmatrix} \lambda_1^{n+1} - \lambda_2^{n+1} \\ \lambda_1^n - \lambda_2^n \end{pmatrix} .
\end{aligned}$$

Therefore, noting $\lambda_1 - \lambda_2 = \sqrt{5}$, we have

$$F_n = \frac{\lambda_1^n - \lambda_2^n}{\sqrt{5}} .$$

This formula might not look like an integer, but it is. On closer inspection we see that because $\lambda_2 \approx -.618$ is less than 1 in absolute value the power λ_2^n approaches

0 as n increases. In fact, for $n > 0$ the n^{th} Fibonacci number F_n is therefore the nearest integer to

$$\frac{\lambda_1^n}{\sqrt{5}} .$$

For example,

$$\frac{\lambda_1^9}{\sqrt{5}} = \frac{(1+\sqrt{5})^9}{2^9\sqrt{5}} \approx 33.99 ,$$

so that $F_9 = 34$. Furthermore, the ratio

$$\frac{F_{n+1}}{F_n} = \frac{\lambda_1^{n+1} - \lambda_2^{n+1}}{\lambda_1^n - \lambda_2^n} \approx \frac{\lambda_1^{n+1}}{\lambda_1^n} = \lambda_1 ,$$

answering our initial question.

This little excursion into Fibonacci numbers introduces us to a concept called a difference equation, or recurrence relation: equation (307) is an instance of a difference equation. The concept is like a differential equation except that for a difference equation change occurs in discrete steps rather than continuously. Generally speaking, a difference equation is a matrix equation

$$\vec{v}_{n+1} = A\vec{v}_n \tag{309}$$

together with an initial value $\vec{v}_1$. It can be thought of as describing an evolving system. The matrix A encodes how the next generation of the state vector $\vec{v}$ is obtained. For example, a linear difference equation, generalizing the Fibonacci numbers, is one

$$F_{n+1} = aF_n + bF_{n-1} .$$

To solve the difference equation means finding an expression for F_n as we did above for $a = b = 1$. We may proceed just as before starting with the difference equation

$$\begin{pmatrix} a & b \\ 1 & 0 \end{pmatrix} \begin{pmatrix} F_n \\ F_{n-1} \end{pmatrix} = \begin{pmatrix} F_{n+1} \\ F_n \end{pmatrix} . \tag{310}$$

We shall leave to the reader further analysis of generalized Fibonacci numbers (310) as it is just the same as before.

Exercise 14.1. *Complete the analysis of generalized Fibonacci numbers* (310). *Solve* (310)*, meaning find a formula for* F_n. *Does* F_{n+1}/F_n *always converge to an eigenvalue? How does it depend on* a *and* b*?*

14.2. Markov processes

Another interesting and important example of a recurrence relation (309) is when:

- ☞ the entries of A are all non-negative, and
- ☞ every column of A sums to 1.

Such a system is called *a Markov process*. The (n^{th} generation of the) state vector $\vec{v}$ may consist of probabilities, as numbers between 0 and 1 , assigned to the states of the system, which also sum to 1 . It is not strictly necessary that the coordinates of a state vector sum to 1 , as this is for probabilities, but rather they may sum to any positive number, which is a constant of the system. Our illustrating example to follow has this feature. It follows directly that if $\vec{v}_n$ is such a state vector, then so is $\vec{v}_{n+1}$.

Let us explain a typical example of a Markov process. Suppose that we wish to model population migration within the New York City. In particular, we wish to examine how people move in and out of Manhattan, but staying in New York City. Let us make the simplifying (but unrealistic) assumption that, although people are moving around within the city, no one is migrating to and from it so that the total population of New York City remains constant. Of course, an individual is either in Manhattan or not. Let x_0 denote the number of people in Manhattan in an initial year 0 , and y_0 the number of those in the other four burroughs: this is the initial state of the system. We are assuming that the sum

$$C = x_0 + y_0$$

remains constant. Suppose that every year 3/10 of the people outside Manhattan move to Manhattan, and 1/10 of the people inside Manhattan leave for the other burroughs. Thus, the next year we have $x_1 = .9x_0 + .3y_0$ and $y_1 = .1x_0 + .7y_0$. The matrix

$$A = \begin{pmatrix} .9 & .3 \\ .1 & .7 \end{pmatrix}$$

therefore describes the situation in the sense that if

$$\vec{v}_n = \begin{pmatrix} x_n \\ y_n \end{pmatrix}$$

is the state of the population after n years, then

$$\vec{v}_{n+1} = A\vec{v_n}$$

describes the population one year later. The matrix A is a Markov process in the sense that we have defined. Our main question is what is the ultimate behaviour of the system? In order to answer this we need to calculate the power A^n because we have

$$\vec{v}_n = A^n \vec{v}_0 \ .$$

Of course, we are going to do this by diagonalizing A . The characteristic polynomial of A is

$$t^2 - 1.6t + .6 = (t-1)(t-.6) \ .$$

The eigenvalues of A are therefore 1 and .6 . We are in luck: the matrix A may be diagonalized over $\mathbb{R}$ as it has two distinct real eigenvalues.

Exercise 14.2. *Prove that* 1 *is always an eigenvalue of a Markov process, and that the other eigenvalue is always a positive number less than* 1 *, provided that the entries of* A *are positive. Thus, a (two-dimensional) Markov process always has two distinct (positive) eigenvalues. Therefore, a Markov process can always be diagonalized.*

The eigenspace of 1 is the null space of

$$\begin{pmatrix} -.1 & .3 \\ .1 & -.3 \end{pmatrix}$$

which is the line $t(3,1)$, and the eigenspace of .6 is the null space of

$$\begin{pmatrix} .3 & .3 \\ .1 & .1 \end{pmatrix}$$

which is the line $t(1,-1)$. Thus,

$$A\begin{pmatrix} 3 & 1 \\ 1 & -1 \end{pmatrix} = \begin{pmatrix} 3 & 1 \\ 1 & -1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & .6 \end{pmatrix}$$

so that

$$\begin{aligned} A^n &= \begin{pmatrix} 3 & 1 \\ 1 & -1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & .6^n \end{pmatrix}\begin{pmatrix} 3 & 1 \\ 1 & -1 \end{pmatrix}^{-1} \\ &= \frac{1}{4}\begin{pmatrix} 3 & 1 \\ 1 & -1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & .6^n \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 1 & -3 \end{pmatrix} \end{aligned}$$

At this point let us pause and think that since we are interested in the ultimate behaviour of the system we may as well assume that n is large, so that $.6^n$ is almost 0 . Certainly this will make the calculation easier for if we replace $.6^n$ by 0 , then for large n we have

$$A^n \approx \frac{1}{4}\begin{pmatrix} 3 & 1 \\ 1 & -1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} = \frac{1}{4}\begin{pmatrix} 3 & 3 \\ 1 & 1 \end{pmatrix} .$$

Thus, after n years, we have

$$\begin{pmatrix} x_n \\ y_n \end{pmatrix} \approx \frac{1}{4}\begin{pmatrix} 3 & 3 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} x_0 \\ y_0 \end{pmatrix} = \begin{pmatrix} \frac{3}{4}(x_0+y_0) \\ \frac{1}{4}(x_0+y_0) \end{pmatrix}$$

and therefore

$$x_n \approx \frac{3}{4}C \; ; \; y_n \approx \frac{1}{4}C .$$

This is the proportion of people inside and outside Manhattan that the system tends toward. Notice that as far as the ultimate proportion x_n/y_n goes, which in this case is 3 , it does not matter what the initial populations x_0 and y_0 are as the ultimate proportion depends only on A .

Thus, the idea of a Markov process is exceedingly basic and natural, and it lends itself to an insightful analysis. The reader may rightfully guess that there are countless examples of Markov processes found in subjects ranging from economics to operations research, and that the idea has been studied in great detail. We shall leave it there, but the interested reader may wish to consult Gilbert Strang's book "Linear Algebra and its Applications" to get a start on the subject. A. T. Bharucha-Reid presents an expert exposition in his book "Elements of the Theory of Markov Processes and Their Applications."

Exercise 14.3. *Create or find another example of a Markov process.*

14.3. Conic sections

Imagine a cone. It is a surface with a pointed end called the vertex of the cone, created by revolving a line through the vertex around another 'axis of symmetry.' Imagine the curve formed by the intersection of the cone with a plane not containing the vertex of the cone. If the plane is perpendicular to the axis of symmetry, then this curve of intersection is a circle. If the plane is tilted slightly, then this curve of intersection is elongated forming what is called an ellipse. Continue tilting the plane until it is parallel with a line on the cone through the vertex: the curve of intersection now forms a parabola. Tilt the plane even more until now it is parallel with the axis of symmetry: now the plane intersects the cone in a hyperbola as its called. These three types of curve, ellipse, parabola, and hyperbola, are known as the conic sections, naturally enough.

The conic sections are planar curves that have x, y-equations. These equations can be derived from their geometric definition just given although this is not trivial. We shall define the conic sections strictly in terms that can be put without leaving the plane. Let us start with the ellipse. Define an ellipse as the set of points P such that the combined distance from P to two other fixed points F_1 and F_2, called the foci of the ellipse, equals a fixed given positive constant $2a$. Thus, for every such point P we have

$$2a = |PF_1| + |PF_2| \; . \tag{311}$$

Imagine a string of length $2a$ whose ends are fixed at F_1 and F_2. When the string is pulled taught through another point P, then P lies on the ellipse. If the perpendicular from a point P on the ellipse to the line on the foci bisects the line segment F_1F_2, then P has distance a to each foci. If this same point P has distance b to the line on the foci, then

$$a^2 = b^2 + c^2 \; , \tag{312}$$

where the length $|F_1F_2| = 2c$, for $c < a$. We now introduce x, y-coordinates placing the x-axis on the line containing the foci, and the origin $(0, 0)$ at the midpoint between F_1 and F_2, so that F_1 has coordinates $(-c, 0)$ and F_2 is $(c, 0)$. The points $(-a, 0)$, $(a, 0)$, $(0, b)$, and $(0, -b)$ all lie on the ellipse, which we call the vertices of the ellipse. Notice from (312) that we must have $b \le a$. A straightforward analysis of the distance equation (311) brings us to the equation

$$\frac{x^2}{a^2} + \frac{y^2}{b^2} = 1 \,, \tag{313}$$

for any point $P(x, y)$ lying on the ellipse. If $a = b$, then the ellipse is a circle of radius a, so that $c = 0$ and the two foci coincide with the origin.

Example 14.4. *The quantity* $e = \frac{c}{a} = \cos(\theta)$ *is called the eccentricity of the ellipse, where* θ *is the angle at a focal point formed by the line on it and the vertex* $(0, b)$ *with the* x*-axis. We have* $0 \le e < 1$. *The eccentricity of a circle is* 0. *At the other extreme when* b *is small, so that the foci are near the vertices* $(\pm a, 0)$, *then* e *is closer to* 1.

Example 14.5. *The ellipse (see Figure 1)*

$$\frac{x^2}{9} + \frac{y^2}{4} = 1 \,,$$

has vertices at $(\pm 3, 0)$ *and* $(0, \pm 2)$. *We have* $c = \sqrt{9-4} = \sqrt{5}$, *so that the foci lie at* $(\pm\sqrt{5}, 0)$. *Its eccentricity is* $e = \frac{\sqrt{5}}{9}$.

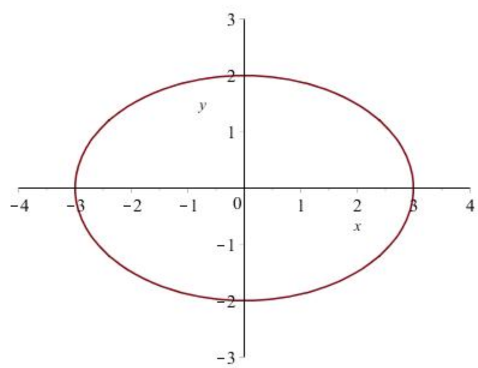


Figure 1. The ellipse $\frac{x^2}{9} + \frac{y^2}{4} = 1$

Of course, any equation

$$Ax^2 + By^2 = C \,;\; 0 < A, B, C \,, \tag{314}$$

also describes an ellipse because it can be put in the form (313), with $a^2 = C/A$ for instance. We recognize that (314) is a level set of a quadratic form. Thus, linear algebra enters the picture: we may put (314) as a matrix equation.

$$\begin{pmatrix} x & y \end{pmatrix} \begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = C\ . \tag{315}$$

Exercise 14.6. *Write the ellipse equation*

$$x^2 + 4y^2 = 16 \tag{316}$$

as a matrix equation (315). *Put the equation into its standard form* (313). *Sketch the ellipse indicating the foci and vertices. What is its eccentricity?*

Suppose the ellipse (316) is rotated about the origin in the plane. Of course, the rotated ellipse is still an ellipse, but how has its equation changed in terms of the same coordinates? Suppose that the rotation is 45° counterclockwise: let $R = R(45^{\mathrm{o}})$ denote this rotation, so that its transpose

$$R^T = R^{-1} = \begin{pmatrix} \frac{\sqrt{2}}{2} & \frac{\sqrt{2}}{2} \\ -\frac{\sqrt{2}}{2} & \frac{\sqrt{2}}{2} \end{pmatrix}$$

rotates the plane 45° clockwise. Then (x, y) lies on the rotated ellipse if and only if the vector

$$R^T \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} \frac{\sqrt{2}}{2} & \frac{\sqrt{2}}{2} \\ -\frac{\sqrt{2}}{2} & \frac{\sqrt{2}}{2} \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}$$

lies on (316). Thus, (x, y) lies on the rotated ellipse if and only if

$$\begin{pmatrix} x & y \end{pmatrix} R \begin{pmatrix} 1 & 0 \\ 0 & 4 \end{pmatrix} R^T \begin{pmatrix} x \\ y \end{pmatrix} = 16\ . \tag{317}$$

This simplifies to

$$\begin{pmatrix} x & y \end{pmatrix} \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 4 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = 32\ , \tag{318}$$

whence

$$\begin{pmatrix} x & y \end{pmatrix} \begin{pmatrix} 5 & -3 \\ -3 & 5 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = 32\ , \tag{319}$$

which comes to

$$5x^2 - 6xy + 5y^2 = 32\ .$$

This is the equation of the ellipse (316) rotated 45° counterclockwise. Notice that rotating the ellipse not only changes the coefficients A, B, C, but also introduces an xy-term in the quadratic form.

What interests us now is the reverse problem. How do we recognize what kind of curve a given equation such as

$$6x^2 - 4xy + 9y^2 = 10 \tag{320}$$

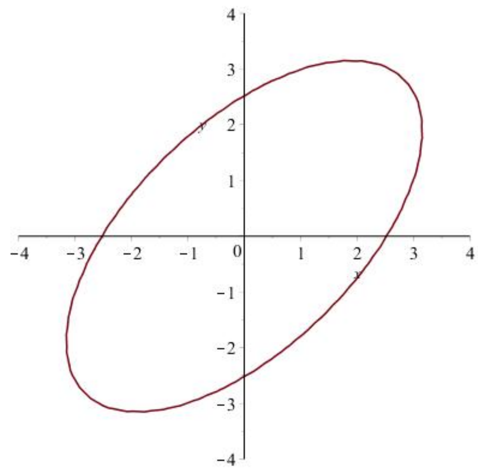


Figure 2. The ellipse $5x^2 - 6xy + 5y^2 = 32$

describes? Let us write it as a matrix equation.

$$\begin{pmatrix} x & y \end{pmatrix} \begin{pmatrix} 6 & -2 \\ -2 & 9 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = 10 \,. \tag{321}$$

Of course, we would like to diagonalize this matrix, which we know can do because it is symmetric, finding a rotation matrix R such that

$$\begin{pmatrix} 6 & -2 \\ -2 & 9 \end{pmatrix} R = R \begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix} ,$$

where λ_1, λ_2 are the eigenvalues of the matrix above, and the columns of R are their normalized eigenvectors. Then the equation (320) we started with is the equation of the ellipse

$$\lambda_1 x^2 + \lambda_2 y^2 = 10$$

rotated counterclockwise by R. Let us complete the problem for the given quadratic equation (320). The characteristic equation of its matrix (321) is

$$t^2 - 15t + 50 = 0 \,,$$

so that the eigenvalues are 5 and 10. The equation of the unrotated ellipse we seek is therefore

$$5x^2 + 10y^2 = 10 \,.$$

Notice that this equation does indeed describe an ellipse because both eigenvalues are positive. In standard form this equation reads

$$\frac{x^2}{2} + y^2 = 1 \,. \tag{322}$$

The vertices of this ellipse are $(\pm\sqrt{2}, 0)$ and $(0, \pm 1)$. From $2 = 1 + c^2$, we see that the foci lie at $(\pm 1, 0)$.

It remains to determine the angle θ of rotation that recovers the original ellipse (320). We shall do this by explicitly determining $R(\theta) = R$ as the matrix whose columns are normalized eigenvectors. The eigenspace of 5 is the null space of

$$\begin{pmatrix} 1 & -2 \\ -2 & 4 \end{pmatrix}$$

which is $t(2,1)$. The other eigenspace must be orthogonal to this so we have

$$R = \frac{\sqrt{5}}{5}\begin{pmatrix} 2 & -1 \\ 1 & 2 \end{pmatrix} = \begin{pmatrix} \cos(\theta) & -\sin(\theta) \\ \sin\theta & \cos(\theta) \end{pmatrix} ,$$

where θ is the angle of counterclockwise rotation. Thus, $\cos(\theta) = \frac{2\sqrt{5}}{5}$, which gives $\theta \approx 27^o$. Summing up, the ellipse (320) is the ellipse (322) rotated approximately 27^o degrees counterclockwise.

Exercise 14.7. *Determine the coordinates of the vertices and foci of the ellipse* (320) *by applying the rotation R to the vertices and foci of* (322)*. Determine the eccentricity of the ellipse.*

Remark 14.8. *The conic sections can be analyzed in an elementary way not using linear algebra. However, the power of the linear algebra approach is that it applies equally well in higher dimensions. For example, in three dimensions the equation of an ellipsoid, which is a football shaped surface, has the form*

$$\frac{x^2}{a^2} + \frac{y^2}{b^2} + \frac{z^2}{c^2} = 1 .$$

Of course, the kinds of rotations in space that can be applied to such a surface are more plentiful than in the plane, but nevertheless it can be handled by the matrix and eigenvalue approach that we have demonstrated in two dimensions.

We turn our attention to the hyperbola. Similar to the ellipse, we may define a hyperbola strictly in planar terms: it is the set of points P such that the difference in the distance from P to two other given and fixed points F_1 and F_2, also called the foci of the hyperbola, equals a fixed given positive constant $2a$. Thus, a point P lies on the hyperbola (defined by its foci and the positive number a) just when

$$2a = |PF_1| - |PF_2| . \tag{323}$$

The point P must be closer to F_2 than to F_1 for this difference to be positive, so that really equation (323) defines just one piece of the whole hyperbola: remember a hyperbola has two pieces. The other piece is described by

$$2a = |PF_2| - |PF_1| .$$

If you live at F_2 and your friend lives at F_1 , then (323) describes all the locations P that are distance $2a$ farther from him than from you.

Let P be the point at distance a from the midpoint of the line segment on F_1 and F_2 (closer to F_2). Then P satisfies (323), so that P lies on the hyperbola: this is one of the vertices of the hyperbola. Let $2c = |F_1F_2|$. We must have $a < c$, so that there is $b > 0$ such that

$$c^2 = a^2 + b^2 \ . \tag{324}$$

As with the ellipse we introduce x, y-coordinates placing the x-axis on the line containing the foci, and the origin $(0, 0)$ at the midpoint between F_1 and F_2 , so that the foci have coordinates $F_1(-c, 0)$ and $F_2(c, 0)$. The vertex defined above has coordinates $(a, 0)$. The other vertex lying on the other piece of the hyperbola has coordinates $(-a, 0)$. Similar to the ellipse an analysis of the distance equation (323) brings us to the equation

$$\frac{x^2}{a^2} - \frac{y^2}{b^2} = 1 \ , \tag{325}$$

for any point $P(x, y)$ lying on the hyperbola. Finally, notice that for points (x, y) on the hyperbola we have

$$\lim_{x\to\infty} \frac{y^2}{x^2} = \frac{b^2}{a^2}$$

so that

$$\lim_{x\to\infty} \frac{y}{x} = \frac{b}{a} \ .$$

The two lines $y = \pm\frac{b}{a}x$ are called (slant) asymptotes of the hyperbola.

Example 14.9. *Choose foci F_1 and F_2 such that $2c = |F_1F_2| = 2\sqrt{2}$, so that $c = \sqrt{2}$. Let $a = 1$ so that from* (324) *we have $b = 1$. Therefore, the equation of the hyperbola is*

$$x^2 - y^2 = 1 \ . \tag{326}$$

The lines $y = \pm x$ are the asymptotes of the hyperbola. (See Figure 3.)

Let us determine the equation of the hyperbola (326) rotated 45° counterclockwise, as we did with the ellipse. As before $R = R(45^\circ)$ denotes this rotation, whose inverse is $R^{-1} = R^T$. Then (x, y) lies on the rotated hyperbola if and only if the vector

$$R^T \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} \frac{\sqrt{2}}{2} & \frac{\sqrt{2}}{2} \\ -\frac{\sqrt{2}}{2} & \frac{\sqrt{2}}{2} \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}$$

lies on (326). Thus, (x, y) lies on the rotated hyperbola if and only if

$$\begin{pmatrix} x & y \end{pmatrix} R \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} R^T \begin{pmatrix} x \\ y \end{pmatrix} = 1 \ . \tag{327}$$

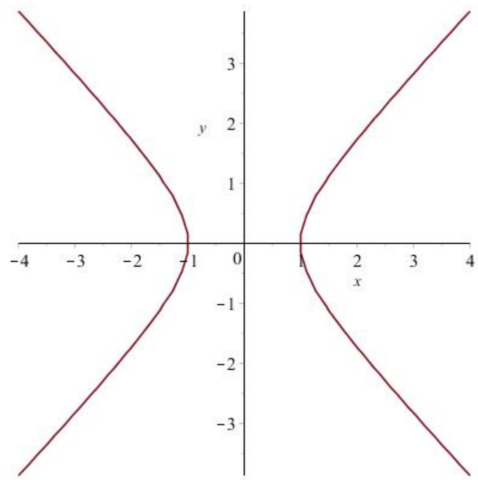


Figure 3. The hyperbola $x^2 - y^2 = 1$

This simplifies to

$$\begin{pmatrix} x & y \end{pmatrix} \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = 2 , \qquad (328)$$

whence

$$\begin{pmatrix} x & y \end{pmatrix} \begin{pmatrix} 0 & 2 \\ 2 & 0 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = 2 , \qquad (329)$$

which comes to

$$2xy = 1 .$$

This is the equation of the hyperbola (326) rotated 45° counterclockwise. Perhaps it is more familiar to you in the form $y = \frac{1}{2x}$, which is a function you may have encountered in calculus. (See Figure 4.)

> **Exercise 14.10.** *Determine the coordinates of the vertices and foci of the hyperbola $2xy = 1$ by applying the rotation R to the vertices and foci of (326).*

Let us consider the reverse problem for hyperbolas. The solution is just the same as for the ellipse: by diagonalization. Suppose we wish to identify the conic section

$$-5x^2 + 6\sqrt{6}xy - 2y^2 = 22 . \qquad (330)$$

As always we begin by writing it as a matrix equation.

$$\begin{pmatrix} x & y \end{pmatrix} \begin{pmatrix} -5 & 3\sqrt{6} \\ 3\sqrt{6} & -2 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = 22 . \qquad (331)$$

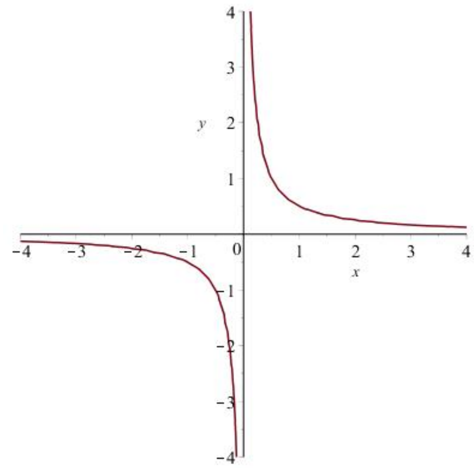


Figure 4. The hyperbola $2xy = 1$

We seek a rotation matrix R such that

$$\begin{pmatrix} -5 & 3\sqrt{6} \\ 3\sqrt{6} & -2 \end{pmatrix} R = R \begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix} ,$$

where λ_1, λ_2 are the eigenvalues of the matrix above, and the columns of R are their normalized eigenvectors. Then the equation (330) we started with is the equation of

$$\lambda_1 x^2 + \lambda_2 y^2 = 22$$

rotated counterclockwise by R. Let us complete the problem for the given quadratic equation (330). The characteristic equation of its matrix (331) is

$$t^2 - 7t - 44 = 0 ,$$

so that the eigenvalues are 4 and -11. The equation of the unrotated conic section we seek is therefore

$$4x^2 - 11y^2 = 22 .$$

This is the equation of a hyperbola because the eigenvalues are opposite in sign. In standard form this equation reads

$$\frac{x^2}{\frac{11}{2}} - \frac{y^2}{2} = 1 . \tag{332}$$

The vertices of this hyperbola are $(\pm\sqrt{\frac{11}{2}}, 0)$. From $c^2 = \frac{11}{2} + 2 = \frac{15}{2}$, we see that the foci lie at $(\pm\sqrt{7.5}, 0)$. The asymptotes are $y = \pm\frac{2}{\sqrt{11}}x$. (See Figure 5.)

Finally, we determine the angle θ of rotation that recovers the original hyperbola (330). The eigenspace of 4 is the null space of

$$\begin{pmatrix} -9 & 3\sqrt{6} \\ 3\sqrt{6} & -6 \end{pmatrix} \sim \begin{pmatrix} -3 & \sqrt{6} \\ \sqrt{6} & -2 \end{pmatrix} \sim \begin{pmatrix} -3 & \sqrt{6} \\ 0 & 0 \end{pmatrix}$$

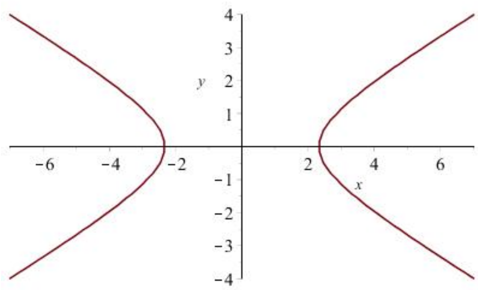


Figure 5. The hyperbola $4x^2 - 11y^2 = 22$

which is $t(\sqrt{6}, 3)$. The other eigenspace must be orthogonal to this so we have

$$R = \frac{\sqrt{15}}{15}\begin{pmatrix} \sqrt{6} & -3 \\ 3 & \sqrt{6} \end{pmatrix} = \begin{pmatrix} \cos(\theta) & -\sin(\theta) \\ \sin\theta & \cos(\theta) \end{pmatrix},$$

where θ is the angle of counterclockwise rotation. Thus, $\cos(\theta) = \frac{\sqrt{10}}{5}$, which gives $\theta \approx 51^o$. Summing up, the hyperbola (330) is the hyperbola (332) rotated approximately 51^o degrees counterclockwise.

Exercise 14.11. *Determine the coordinates of the vertices and foci of the hyperbola* (330) *by applying the rotation to the vertices and foci of* (332)*. Determine the asymptotes of* (330)*.*

Naturally, our third and last conic section the parabola also has a planar description. For it we require a line D, called the directrix of the parabola, and a single focus F. Then the set of all points P such that

$$|PF| = |PD| \tag{333}$$

forms a parabola, where by $|PD|$ we mean the shortest distance from P to D. For instance, if you live at F and D is Main Street, then the parabola consists of all locations in town whose distance from Main Street equals its distance to you.

The midpoint V between F and D satisfies (333), so that it lies on the parabola: we call V the vertex of the parabola. We next impose coordinates, making the x-axis parallel to the directrix and placing the origin at the vertex V, so that the directrix is the line $y = -p$. Therefore, the focus F must have coordinates $(0, p)$.

Then a point $P(x, y)$ satisfies (333) if and only if (x, y) satisfies

$$4py = x^2 \,. \tag{334}$$

Like the ellipse and hyperbola (334) is a quadratic equation, but its different because of course in this case there is a linear term; however we may treat it in just the same way using matrices.

Exercise 14.12. *Derive* (334) *from* (333).

Exercise 14.13. *In calculus you may seen a parabola defined by an equation such as $y = 4x^2$. Use* (334) *to determine the directrix and focus of this parabola.*

Let us put (334) in matrix form.

$$\begin{pmatrix} x & y \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 0 & 4p \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} . \tag{335}$$

We may rotate the parabola just as we did with the other conic sections. If again R denotes a rotation of 45° counterclockwise, then (x, y) lies on the rotated parabola if and only if (x, y) satisfies

$$\begin{pmatrix} x & y \end{pmatrix} R \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} R^T \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 0 & 4p \end{pmatrix} R^T \begin{pmatrix} x \\ y \end{pmatrix} . \tag{336}$$

This simplifies to

$$\begin{pmatrix} x & y \end{pmatrix} \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}$$

$$= \begin{pmatrix} 0 & 4\sqrt{2}p \end{pmatrix} \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}$$

whence

$$\begin{pmatrix} x & y \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = 4\sqrt{2}p \begin{pmatrix} -1 & 1 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \tag{337}$$

which comes to

$$x^2 + 2xy + y^2 + 4\sqrt{2}px - 4\sqrt{2}py = 0 \,.$$

This is the equation of (334) rotated 45° counterclockwise.

Example 14.14. *Let* $p = \sqrt{2}$. *Then the equation of the parabola* $4\sqrt{2}y = x^2$ *rotated* 45^{o} *counterclockwise is*

$$x^2 + 2xy + y^2 + 8x - 8y = 0 \,.$$

What is the equation of the rotated directrix? We may determine this by observing that (x, y) *lies on the rotated directrix if and only if*

$$R^T \begin{pmatrix} x \\ y \end{pmatrix}$$

satisfies $y = -\sqrt{2}$. *This gives* $\frac{\sqrt{2}}{2}(-x + y) = -\sqrt{2}$, *which gives* $y = x - 2$. *Likewise, the focus of the rotated parabola lies at* $(-1, 1)$. *(See Figure 6.)*

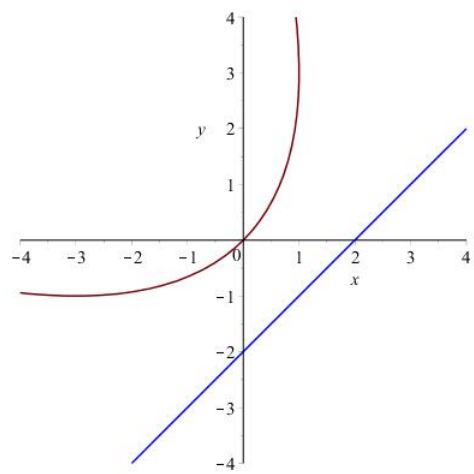


Figure 6. The parabola $x^2 + 2xy + y^2 + 8x - 8y = 0$

Conic sections introduce us to a subject called analytic geometry: the term analytic emphasizes how coordinates mediate the connection between geometry and algebra. In particular, we hope the reader is convinced that the general quadratic equation

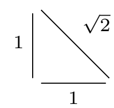
$$Ax^2 + Bxy + Cy^2 + Dx + Ey = F$$

describes a conic section, possibly rotated out of standard position, but also possibly shifted vertically or horizontally.

Exercise 14.15. *How shall we treat vertical and horizontal shifts of a conic section?*

14.4. Algebraic numbers and other things

This section depends on some basic ring theory covered in Chapter 12. We have seen that ring theory serves the purpose of providing a more conceptual foundation for linear algebra, but this section illustrates how linear algebra may be used in the service of algebra. Indeed, let us motivate the discussion by asking a basic question of algebra: what exactly is the number $\sqrt{2}$? For instance, this quantity occurs naturally as the length of the hypotenuse on a right isosceles triangle whose shorter side has length 1.



Or perhaps someone in your mathematical past has said that $\sqrt{2}$ is the quantity which when squared gives 2 and that is that. In a way this might even be the best answer one can offer, but the details matter. For instance, what is a 'quantity' in the first place, and even if we knew how do we identify $\sqrt{2}$? For example, a calculator gives $\sqrt{2} = 1.41421\ldots$, which expresses $\sqrt{2}$ as a limit of rational numbers. This says that you can calculate $\sqrt{2}$ only up to a given error, but it can always be done and to within any given error no matter how small. If you're not familiar with this idea, then perhaps it is not easy to understand or express in a precise manner. Once a clever someone proposed that $\sqrt{2}$ is the collection of rational numbers whose square is less than 2. At first this proposal might sound prepostorous because that's not even a number, its a set of numbers; however, let us not rush to judgement for it turns out that the proposal makes perfect sense. Here is another proposal using matrices:

$$\sqrt{2} = \begin{pmatrix} 0 & 2 \\ 1 & 0 \end{pmatrix} .$$

The square of this matrix

$$\begin{pmatrix} 0 & 2 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 2 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix} .$$

is indeed 2 provided of course that we identify 2 with the constant matrix above (right). What could be simpler? We have identified $\sqrt{2}$ as a matrix. It is therefore no problem to find $\sqrt{2}$ after all, but we have to look to matrices to find it. Thus, linear algebra enters the picture in a natural way.

We are going to explore our matrix solution to the question more thoroughly and try to make sense of it. Our exploration brings into play the Cayley-Hamilton theorem and also several other ideas from algebra. Incidentally, these other ideas from algebra are more basic than even linear algebra, so every aspiring student of linear algebra should learn them. In other words, our understanding of linear algebra improves, and ultimately it depends, on a broader perspective. In fact, we have already encountered these ideas, such as rings, fields, ideasl, and homomorphisms, in one way or another previously in this book.

We would like to produce roots of integral polynomials, or what are called algebraic numbers. For example, the number $\sqrt{2}$ is algebraic because it is a root of the polynomial $t^2 - 2$. We would like to do this in an algebraically consistent manner in the sense that we would like to also create a system of numbers in which the root lives (formally called a ring in Chapter 12). In other words, the basic problem we address is how to invent a root α of an integral polynomial and another field $\mathbb{Q} \subseteq \mathbb{Q}(\alpha)$ in which α lives. We shall find that such a field can be identified as a subring of matrices over $\mathbb{Q}$. In the process we encounter the minimal polynomial of a matrix.

Probably the most basic connection between polynomials and matrices, which we have already encountered in this book, is the fact that it makes sense to evaluate a polynomial at a (square) matrix A. Indeed, if A has dimension n, then the function

$$\mathrm{ev}_A : \mathbb{Q}[t] \to M_n \; ; \; f(t) \mapsto f(A) \; , \tag{338}$$

is a ring homomorphism, where M_n denotes the ring of all $n \times n$ rational matrices. To say that ev_A is a ring homomorphism means that it respects addition and multiplication. For instance, we have

$$\mathrm{ev}_A(f(t)g(t)) = f(A)g(A) = \mathrm{ev}_A(f(t))\mathrm{ev}_A(g(t)) \; ,$$

and likewise for addition.

Definition 14.16. *Let $\mathbb{Q}[A]$ denote the image of ev_A. It consists of all matrices that equal $f(A)$ for some rational polynomial $f(t)$.*

Exercise 14.17. *Show that $\mathbb{Q}[A]$ is subring of M_n. Show that it is commutative with respect to matrix multiplication.*

The kernel of ev_A is by definition the subset of polynomials

$$\mathrm{Ker}(\mathrm{ev}_A) = \{ f(t) \mid \mathrm{ev}_A(f(t)) = f(A) = 0 \} \; .$$

Recall from our study of rings that the kernel of a ring homomorphism is an ideal. Hence, $\ker \mathrm{ev}_A$ is an ideal $\mathbb{Q}[t]$.

Exercise 14.18. *Prove that the subring $\mathbb{Q}[A]$ is isomorphic to the quotient ring $\mathbb{Q}[t]/\mathrm{Ker}(\mathrm{ev}_A)$. Hint: this is an instance of a general fact about ring homomorphisms. Which fact is this?*

An important fact from our study of rings is that every ideal of a polynomial ring over a field is principle, that is, it is generated by a single polynomial. Hence,

$$\mathrm{Ker}(\mathrm{ev}_A) = (\, m(t) \,) \; .$$

In other words, $f(A) = 0$ if and only if $f(t)$ is a multiple of $m(t)$, or as they say $m(t)$ divides $f(t)$ (Recall that we denote the latter by $m(t) \mid f(t)$).

Of course, we may always take $m(t)$ to be monic in the sense that its leading coefficient is 1. In fact, the polynomial $m(t)$ is the unique monic polynomial of least degree such that $m(A) = 0$. We already know this polynomial $m(t)$ by its name: the minimal polynomial of A over $\mathbb{Q}$ (Here, we can regard A as a linear endomorphism of $\mathbb{Q}^n$ in the usual way, where n is the size of the square matrix A.) .

Exercise 14.19. *Show that similar matrices have the same minimal polynomial.*

Exercise 14.20. *Find the minimal polynomial of the matrix*

$$\begin{pmatrix} 3 & -1 & 0 \\ 0 & 2 & 0 \\ 1 & -1 & 2 \end{pmatrix} .$$

By the Cayley-Hamilton theorem the characteristic polynomial of a matrix A is a member of $\mathrm{Ker}(\mathrm{ev}_A)$. Thus, we deduce that the minimal polynomial $m(t)$ of a matrix divides the characteristic polynomial of the matrix.

Exercise 14.21. *Prove that the image subring $\mathbb{Q}[A]$ is isomorphic to the quotient ring $\mathbb{Q}[t]/(m(t))$. Hint: Exercise 14.18.*

Recall from our study of rings that a polynomial $f(t) \in \mathbb{Q}[t]$ of positive degree is irreducible if it does not factor over $\mathbb{Q}$, that is, there does not exist polynomials $g(t)$ and $h(t)$ of positive degree such that $f(t) = g(t)h(t)$.

Proposition 14.22. *A polynomial $p(t)$ over $\mathbb{Q}$ is irreducible over $\mathbb{Q}$ if and only if the quotient ring $\mathbb{Q}[t]/(p(t))$ is a field.*

Proof. This is a special case of Theorem 12.54. □

Corollary 14.23. *$\mathbb{Q}[A]$ is a field if and only if the minimal polynomial of A is irreducible over $\mathbb{Q}$.*

Proof. Let $m(t)$ denote the minimal polynomial of A. Then $\mathbb{Q}[A]$ is field if and only if $\mathbb{Q}[t]/(m(t))$ is a field (Exercise 14.21) if and only if $m(t)$ is irreducible over $\mathbb{Q}$ (Proposition 14.22). □

When $\mathbb{Q}[A]$ is a field we use the notation $\mathbb{Q}(A)$.

Example 14.24. *The minimal polynomial of a matrix need not be irreducible. For instance, the minimal polynomial of*

$$A = \begin{pmatrix} 0 & 4 \\ 1 & 0 \end{pmatrix}$$

equals its characteristic polynomial $t^2 - 4 = (t+2)(t-2)$. *Thus,* $\mathbb{Q}[A]$ *is not a field. For instance, the matrix* $\mathrm{ev}_A(t+2) = A + 2I$ *is a member of* $\mathbb{Q}[A]$, *but it is not invertible.*

We have assembled the tools and concepts sufficient to explain our initial example $\sqrt{2}$. Let $\mathbb{Q}(\sqrt{2})$ denote the image subring $\mathbb{Q}[A]$ for

$$\sqrt{2} = A = \begin{pmatrix} 0 & 2 \\ 1 & 0 \end{pmatrix} .$$

The characteristic polynomial of A is $t^2 - 2$. By Cayley-Hamilton, we have $A^2 - 2I = 0$, but of course we have already verified $A^2 = 2I$ directly by hand. In any case, the minimal polynomial of A must therefore divide $t^2 - 2$.

Exercise 14.25. *Show that* $t^2 - 2$ *is irreducible over* $\mathbb{Q}$. *Show that the minimal polynomial of* A *equals* $t^2 - 2$.

Exercise 14.26. *Show that* $\mathbb{Q}(\sqrt{2})$ *equals the collection of matrices*

$$aI + bA = \begin{pmatrix} a & 2b \\ b & a \end{pmatrix} . \tag{339}$$

As a matter of fact, we may define $\mathbb{Q}(\sqrt{2})$ as the collection of the matrices (339); however, defining $\mathbb{Q}(\sqrt{2})$ as the image of the evaluation homomorphism ev_A adds some perspective to the discussion; for instance Proposition 14.23 tells us when $\mathbb{Q}[A]$ is a field.

Exercise 14.27. *Show that* $\mathbb{Q}(\sqrt{2})$ *is indeed a field, which contains* $\mathbb{Q}$. *Of course, we may appeal to Proposition 14.23, but it can be also be done directly by finding an inverse for every non-*0 *element of* $\mathbb{Q}(\sqrt{2})$. *For instance, if* $\sqrt{2}$ *denotes the above matrix* A, *then what matrix is* $1/\sqrt{2}$ *?*

Exercise 14.28. *Show that the field* $\mathbb{Q}(\sqrt{2})$ *is isomorphic to the subfield of* $\mathbb{R}$ *consisting of all real numbers* $a + b\sqrt{2}$, $a, b \in \mathbb{Q}$, *where now we consider* $\sqrt{2}$ *as a real number.*

Example 14.29. *In this example, let us change base fields to the real numbers* $\mathbb{R}$ *. This takes us out of the realm of algebraic numbers, but the ideas are the same. The characteristic polynomial of the matrix*

$$A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

is $t^2 + 1$ *. We have* $m(t) \mid t^2 + 1$ *. Because* $t^2 + 1$ *is irreducible over* $\mathbb{R}$ *we have* $m(t) = t^2 + 1$ *, and moreover the image subring of* ev_A *(for* $\mathbb{R}$*), which we denote* $\mathbb{R}(i)$ *, is therefore a field. In any case, this can be proved directly. This field is the complex numbers:* $\mathbb{R}(i) = \mathbb{C}$ *. We have used matrices to invent* $i = \sqrt{-1}$ *, identifying* i *as the matrix* A *. Show that the field* $\mathbb{R}(i)$ *equals the collection of all matrices*

$$aI + bA = \begin{pmatrix} a & -b \\ b & a \end{pmatrix} ,$$

where $a, b \in \mathbb{R}$ *. Thus, we identify the complex number* $a + bi$ *with the matrix* $aI + bA$ *.*

Example 14.30. *We continue with base field* $\mathbb{R}$ *, but we start with the polynomial*

$$t^3 - 1 = (t-1)(t^2 + t + 1) .$$

The roots of this polynomial are called cube roots of unity. Of course, 1 is such a root. The other two complex roots are the roots of $t^2 + t + 1$ *. It is not too difficult to find a* 2×2 *matrix whose characteristic polynomial is* $t^2 + t + 1$ *. Indeed, we seek a matrix whose trace equals* -1 *and determinant equals* 1 *. For instance,*

$$B = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}$$

is such a matrix. By the Cayley-Hamilton theorem we have $B^2 + B + I = 0$ *, and because* $t^2 + t + 1$ *is irreducible over* $\mathbb{R}$ *, it is the minimal polynomial of* B *. The image of the evaluation homomorphism for* B

$$\mathrm{ev}_B : \mathbb{R}[t] \to M_2$$

into the ring M_2 *of real matrices equals the collection of matrices*

$$aI + cB = \begin{pmatrix} a & -c \\ c & a - c \end{pmatrix} .$$

In fact, to see this argue by induction on the degree of a polynomial, using $B^2 = -B - I$ *for the inductive step. Moreover, this ring is a field because the minimal polynomial is irreducible over* $\mathbb{R}$ *. Indeed, this field is again the complex numbers. For instance,* i *is the matrix*

$$\frac{1}{\sqrt{3}}I + \frac{2}{\sqrt{3}}B = \frac{1}{\sqrt{3}}\begin{pmatrix} 1 & -2 \\ 2 & -1 \end{pmatrix}.$$

Indeed, by direct calculation, the square of this matrix equals the constant matrix -1. Thus, there is more than one way to present i as a real matrix. Notice that

$$B^2 = \begin{pmatrix} -1 & 1 \\ -1 & 0 \end{pmatrix}$$

is the third cube root of unity.

Perhaps it is appropriate to end by mentioning a fascinating subject called group theory because the three matrices I, B, B^2 collectively form what is called a (cyclic) multiplicative group. In fact, the origins of group theory go back to the problem of finding roots of a polynomial (and someone named Galois), which is precisely the problem we have been discussing in this section. We encourage the reader to begin his own investigations of the subject. Almost any introduction to group theory will do: just google "introduction to group theory"!

Chapter 14 Exercises

1. Solve the Fibonacci sequence

$$3, 3, 6, 9, 15 \ldots$$

2. Solve the difference equation

$$F_{n+1} = F_n - F_{n-1},$$

where $F_1 = 0, F_2 = 1$.

3. The matrix of a Markov process is also called a stochastic matrix. Prove that the product of two stochastic matrices is again one.

4. How can we interpret a steady population growth in the population movement Markov process? For instance, suppose that the population of New York City increases by 2% each year. How do we change the model in order to account for this?

5. Find the equation of the ellipse

$$2x^2 + y^2 = 16$$

rotated 60° counterclockwise. Sketch both ellipses, indicating the vertices and foci.

6. Find the equation of the hyperbola

$$x^2 - y^2 = 1$$

rotated 60^o counterclockwise. Sketch both hyperbolas, indicating the vertices, foci, and asymptotes.

7. Identify (ellipse or hyperbola) and sketch the graph of the following quadratic equation.

$$x^2 - 6xy + y^2 = 8$$

   Identify the vertices, foci, and asymptotes (hyperbola). What is the angle of rotation out of standard position?

8. Find the general equation of the parabola

$$4py = x^2$$

   rotated 60^o counterclockwise. Also find the focus and the directrix of the rotated parabola.

9. Build as a subring of 2×2 rational matrices a field $\mathbb{Q}(\sqrt{5})$ that includes $\mathbb{Q}$ as a subfield. How are the two fields $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{5})$ related?

10. Modular arithmetic is an interesting and important idea of number theory. The ideas we have considered in § 14.4 apply to modular arithmetic. Consider the finite field $\mathbb{Z}_3 = \{0, 1, 2\}$ of numbers modulo 3. Notice that 2 is not a square in this field because $0^2 = 0, 1^2 = 1, 2^2 = 1$. Using the same approach we used to build $\mathbb{Q}(\sqrt{2})$ build a finite field $\mathbb{Z}_3(\sqrt{2})$ of 2×2 matrices over $\mathbb{Z}_3$ in which 2 has a square root. List the elements of this field.

Bibliography

[1] D. S. Dummit, R. M. Foote, *Abstract Algebra*, 2nd Ed., John Wiley & Sons, Inc., 1999.

[2] K. Erdmann, M. Wildon, *Introduction to Lie Algebras*, Springer-Verlag London (2006).

Index