Part III

The Vector Space $\mathbb{R}^n$

Section 12

The Structure of $\mathbb{R}^n$

Focus Questions

By the end of this section, you should be able to give precise and thorough answers to the questions listed below. You may want to keep these questions in mind to focus your thoughts as you complete the section.

- What properties make $\mathbb{R}^n$ a vector space?
- What is a subspace of $\mathbb{R}^n$?
- What properties do we need to verify to show that a set of vectors is a subspace of $\mathbb{R}^n$? Why?
- What important structure does the span of a set of vectors in $\mathbb{R}^n$ have?

Application: Connecting GDP and Consumption in Romania

It is common practice in the sciences to run experiments and collect data. Once data is collected it is necessary to find some way to analyze the data and predict future behavior from the data. One method is to find a curve that best "fits" the data, and one widely used method for curve fitting is called the *least squares* method.

For example, economists are often interested in *consumption*, which is the purchase of goods and services for use by households. In "A Statistical Analysis of GDP and Final Consumption Using Simple Linear Regression, the Case of Romania 1990-2010",[1] the authors collect data and then use simple linear regression to compare GDP (gross domestic product) to consumption in Romania. The data they used is seen in Table 12.1, with a corresponding scatterplot of the data (with consumption as independent variable and GDP as dependent variable). The units for GDP

[1] Bălăcescu, Aniela & Zaharia, Marian. (2012). A STATISTICAL ANALYSIS OF GDP AND FINAL CONSUMPTION USING SIMPLE LINEAR REGRESSION. THE CASE OF ROMANIA 1990?2010. Annals - Economy Series. 4. 26-31. Available from: https://www.researchgate.net/publication/227382939_A_STATISTICAL_ANALYSIS_OF_GDP_AND_FINAL_CONSUMPTION_USING_SIMPLE_LINEAR_REGRESSION_THE_CASE_OF_ROMANIA_1990-2010.

and consumption are milliions of leu (the currency of Romania is the leu – on December 21, 2018, one leu was worth approximately $0.25 U.S.) The authors conclude their paper with the following statement:

> "However, we can appreciate that linear regression model describes the correlation between the value of gross domestic product and the value of final consumption and may be transcribed following form:
>
> PIB = -3127.51+ 1.22 CF.
>
> Analysis of correlation between GDP and final consumption (private consumption and public consumption) will result in an increase of 1.22 units of monetary value of gross domestic product.
>
> We can conclude that the Gross Domestic Product of our country is strongly influenced by the private and public consumption."

Year	GDP	Consumption
1990	85.8	68.0
1991	220.4	167.3
1992	602.9	464.3
1993	2003.9	1523.6
1994	4977.3	3845.2
1995	7648.9	6257.7
1996	11384.2	9713.8
1997	25529.8	21972.2
1998	37055.1	33311.2
1999	55191.4	49311.9
2000	80984.6	69587.4
2001	117945.8	100731.7
2002	152017.0	127118.8
2003	197427.6	168818.7
2004	247368.0	211054.6
2005	288954.6	251038.1
2006	344650.6	294867.6
2007	416006.8	344937.0
2008	514700.0	420917.5
2009	498007.5	402246.0
2010	513640.8	405422.4

Table 12.1: GDP and consumption in Romania.

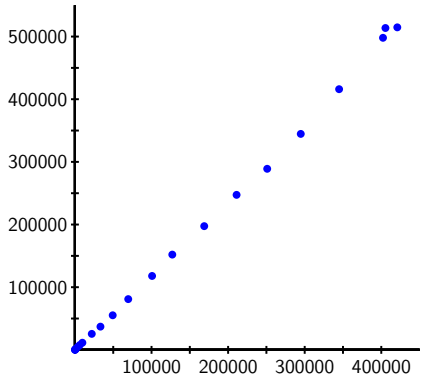


Figure 12.1: GDP and consumption data plot.

As we can see from the scatterplot, the relationship between the GDP and consumption is not exactly linear, but looks to be very close. To make correlations between GDP and consumption as the authors did, we need to understand how they determined their approximate linear relationship

between the variables. With a good approximation function we can then compare the variables, extrapolate from the data, and make predictions or interpolate and estimate between data points. For example, we could use our approximation function to predict, as the authors did, how changes in consumption affect GDP (or vice versa). Later in this section we will see how to find the least squares line to fit this data – the best linear approximation to the data. This involves finding a vector in a certain subspace of $\mathbb{R}^2$ that is closest to a given vector. Linear least squares approximation is a special case of a more general process that we will encounter in later sections where we learn how to project sets onto subspaces.

Introduction

The set $\mathbb{R}^n$ with vector addition and scalar multiplication has a nice algebraic structure. These operations satisfy a number of properties, such as associativity and commutativity of vector addition, the existence of an additive identity and additive inverse, distribution of scalar multiplication over vector addition, and others. These properties make it easier to work with the whole space since we can express the vectors as linear combinations of basis vectors in a unique way. This algebraic structure makes $\mathbb{R}^n$ a *vector space*.

There are many subsets of $\mathbb{R}^n$ that have this same structure. These subsets are called *subspaces* of $\mathbb{R}^n$. These are the sets of vectors for which the addition of any two vectors is defined within the set, the scalar multiple of any vector by any scalar is defined within the set and the set contains the zero vector. One type of subset with this structure is the span of a set of vectors.

Recall that the span of a set of vectors $\{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_k\}$ in $\mathbb{R}^n$ is the set of all linear combinations of the vectors. For example, if $\mathbf{v}_1 = \begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix}$ and $\mathbf{v}_2 = \begin{bmatrix} 1 \\ 0 \\ 1 \end{bmatrix}$, then a linear combination of these two vectors is of the form

$$c_1\mathbf{v}_1 + c_2\mathbf{v}_2 = c_1 \begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix} + c_2 \begin{bmatrix} 1 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} c_1 + c_2 \\ c_1 \\ c_2 \end{bmatrix}.$$

One linear combination can be obtained by letting $c_1 = 2, c_2 = -3$, which gives the vector $2\mathbf{v}_1 - 3\mathbf{v}_2 = \begin{bmatrix} -1 \\ -3 \\ 2 \end{bmatrix}$. All such linear combinations form the span of the vectors $\mathbf{v}_!$ and $\mathbf{v}_2$. In this case, these vectors will form a plane through the origin in $\mathbb{R}^3$.

Now we will investigate if the span of two vectors form a subspace, i.e. if it has the same structure as a vector space.

Preview Activity 12.1. Let $\mathbf{w}_1$ and $\mathbf{w}_2$ be two vectors in $\mathbb{R}^n$. Let $W = \text{Span}\{\mathbf{w}_1, \mathbf{w}_2\}$.

(1) For W to be a subspace of $\mathbb{R}^n$, the sum of any two vectors in W must also be in W.

   (a) Pick two specific examples of vectors $\mathbf{u}, \mathbf{y}$ in W (keeping $\mathbf{w}_1, \mathbf{w}_2$ unknown/general vectors). For example, one specific $\mathbf{u}$ would be $2\mathbf{w}_1 - 3\mathbf{w}_2$ as we used in the above example. Find the sum of $\mathbf{u}, \mathbf{y}$. Is the sum also in W? Explain. (Hint: What does it mean for a vector to be in W?)

(b) Now let $\mathbf{u}$ and $\mathbf{y}$ be arbitrary vectors in W. Explain why $\mathbf{u}+\mathbf{y}$ is in W.

(2) For W to be a subspace of $\mathbb{R}^n$, any scalar multiple of any vector in W must also be in W.

(a) Pick a specific example $\mathbf{u}$ in W. Explain why $2\mathbf{u}, -3\mathbf{u}, \pi\mathbf{u}$ are all also in W.

(b) Now let a be an arbitrary scalar and let $\mathbf{u}$ be an arbitrary vector in W. Explain why the vector $a\mathbf{u}$ is in W.

(3) For W to be a subspace of $\mathbb{R}^n$, the zero vector must also be in W. Explain why the zero vector is in W.

(4) Does vector addition being commutative for vectors in $\mathbb{R}^n$ imply that vector addition is also commutative for vectors in W? Explain your reasoning.

(5) Suppose we have an arbitrary $\mathbf{u}$ in W. There is an additive inverse of $\mathbf{u}$ in $\mathbb{R}^n$. In other words, there is a $\mathbf{u}'$ such that $\mathbf{u}+\mathbf{u}'=\mathbf{0}$. Should this $\mathbf{u}'$ be also in W? If so, explain why. If not, give a counterexample.

(6) Look at the other properties of vector addition and scalar multiplication of vectors in $\mathbb{R}^n$ listed in Theorem 4.3 in Section 4. Which of these properties should also hold for vectors in W?

Vector Spaces

The set of n-dimensional vectors with the vector addition and scalar multiplication satisfy many properties, such as addition being commutative and associative, existence of an additive identity, and others. The set $\mathbb{R}^n$ with these properties is an example of a *vector space*, a general structure examples of which include many other algebraic structures as we will see later.

Definition 12.1. A set V on which an operation of addition and a multiplication by scalars is defined is a **vector space** if for all $\mathbf{u}$, $\mathbf{v}$, and $\mathbf{w}$ in V and all scalars a and b:

(1) $\mathbf{u}+\mathbf{v}$ is an element of V (we say that V is *closed* under the addition in V),

(2) $\mathbf{u}+\mathbf{v}=\mathbf{v}+\mathbf{u}$ (we say that the addition in V is *commutative*),

(3) $(\mathbf{u}+\mathbf{v})+\mathbf{w}=\mathbf{u}+(\mathbf{v}+\mathbf{w})$ (we say that the addition in V is *associative*),

(4) there is a vector $\mathbf{0}$ in V so that $\mathbf{u}+\mathbf{0}=\mathbf{u}$ (we say that V contains an *additive identity* or *zero vector* $\mathbf{0}$),

(5) for each $\mathbf{x}$ in V there is an element $\mathbf{y}$ in V so that $\mathbf{x}+\mathbf{y}=\mathbf{0}$ (we say that V contains an *additive inverse* $\mathbf{y}$ for each element $\mathbf{x}$ in V),

(6) $a\mathbf{u}$ is an element of V (we say that V is *closed* under multiplication by scalars),

(7) $(a+b)\mathbf{u}=a\mathbf{u}+b\mathbf{u}$ (we say that *multiplication by scalars distributes over scalar addition*),

(8) $a(\mathbf{u}+\mathbf{v})=a\mathbf{u}+a\mathbf{v}$ (we say that *multiplication by scalars distributes over addition in* V),

(9) $(ab)\mathbf{u} = a(b\mathbf{u})$,

(10) $1\mathbf{u} = \mathbf{u}$.

Theorem 4.3 in Section 4 shows that $\mathbb{R}^n$ is itself a vector space. As we will see, there are many other sets that have the same algebraic structure. By focusing on this structure and the properties of these operations, we can extend the theory of vectors we developed so far to a broad range of objects, making it easier to work with them. For example, we can consider linear combinations of functions or matrices, or define a basis for different types of sets of objects. Such algebraic tools provide us with new ways of looking at these sets of objects, including a geometric intuition when working with these sets. In this section, we will analyze subsets of $\mathbb{R}^n$ which behave similar to $\mathbb{R}^n$ algebraically. We will call such sets *subspaces*. In a later chapter we will encounter different kinds of sets that are also vector spaces.

Definition 12.2. A subset W of $\mathbb{R}^n$ is a **subspace** of $\mathbb{R}^n$ if W itself is a vector space using the same operations as in $\mathbb{R}^n$.

The following example illustrates the process for demonstrating that a subset of $\mathbb{R}^n$ is a subspace of $\mathbb{R}^n$.

Example 12.3. There are many subsets of $\mathbb{R}^n$ that are themselves vector spaces. Consider as an example the set W of vectors in $\mathbb{R}^2$ defined by

$$W = \left\{ \begin{bmatrix} x \\ 0 \end{bmatrix} \middle| x \text{ is a real number} \right\}.$$

In other words, W is the set of vectors in $\mathbb{R}^2$ whose second component is 0. To see that W is itself a vector space, we need to demonstrate that W satisfies all of the properties listed in Definition 12.1.

To prove the first property, we need to show that the sum of any two vectors in W is again in W. So we need to choose two arbitrary vectors in W. Let $\mathbf{u} = \begin{bmatrix} x \\ 0 \end{bmatrix}$ and $\mathbf{v} = \begin{bmatrix} y \\ 0 \end{bmatrix}$ be vectors in W. Note that

$$\mathbf{u} + \mathbf{v} = \begin{bmatrix} x \\ 0 \end{bmatrix} + \begin{bmatrix} y \\ 0 \end{bmatrix} = \begin{bmatrix} x+y \\ 0 \end{bmatrix}.$$

Since the second component of $\mathbf{u} + \mathbf{v}$ is 0, it follows that $\mathbf{u} + \mathbf{v}$ is in W. Thus, the set W is closed under addition.

For the second property, that addition is commutative in W, we can just use the fact that if $\mathbf{u}$ and $\mathbf{v}$ are in W, they are also vectors in $\mathbb{R}^2$ and $\mathbf{u} + \mathbf{v} = \mathbf{v} + \mathbf{u}$ is satisfied in $\mathbb{R}^2$. So the property also holds in W.

A similar argument can be made for property (3).

Property (4) states the existence of the additive identity in W. Note that $\mathbf{0}$ is an additive identity in $\mathbb{R}^2$ and if it is also an element in W, then it will automatically be the additive identity of W. Since the zero vector can be written as $\mathbf{0} = \begin{bmatrix} x \\ 0 \end{bmatrix}$ with $x = 0$, $\mathbf{0}$ is in W. Thus, W satisfies property 4.

We will postpone property (5) for a bit since we can show that other properties imply property (5).

Property (6) is a closure property, just like property (1). We need to verify that any scalar multiple of any vector in W is again in W. Consider an arbitrary vector $\mathbf{u}$ and an arbitrary scalar a. Now

$$a\mathbf{u} = a\begin{bmatrix} x \\ 0 \end{bmatrix} = \begin{bmatrix} ax \\ 0 \end{bmatrix}.$$

Since the vector $a\mathbf{u}$ has a 0 as its second component, we see that $a\mathbf{u}$ is in W. Thus, W is closed under scalar multiplication.

Properties (7), (8), (9) and (10) only depend on the operations of addition and multiplication by scalars in $\mathbb{R}^2$. Since these properties depend on the operations and not the vectors, these properties will transfer to W.

We still have to justify property (5) though. Note that since $1 - 1 = 0$ in real numbers, by applying property (7) with $a = 1$, $b = -1$, we find that

$$\mathbf{0} = 0\mathbf{u} = (a + b)\mathbf{u} = a\mathbf{u} + b\mathbf{u} = \mathbf{u} + (-1)\mathbf{u}\,.$$

Therefore, $(-1)\mathbf{u}$ is an additive inverse for $\mathbf{u}$. Therefore, to show that the additive inverse of any $\mathbf{u}$ in W is also in W, we simply note that any multiple of $\mathbf{u}$ is also in W and hence $(-1)\mathbf{u}$ must also be in W.

Since W satisfies all of the properties of a vector space, W is a vector space. Any subset of $\mathbb{R}^n$ that is itself a vector space using the same operations as in $\mathbb{R}^n$ is called a *subspace* of $\mathbb{R}^n$.

Example 12.3 and our work Preview Activity 12.1 bring out some important ideas. When checking that a subset W of a vector space $\mathbb{R}^n$ is also a vector space, we can use the fact that all of the properties of the operations in $\mathbb{R}^n$ are transferred to any closed subset W. This implies that properties (2), (3), (7)-(10) are all automatically satisfied for W as well. Property (5) follows from the others. So we only need to check properties (1), (4) and (6). In fact, as we argued in the above example, property (4) also needs to be checked by simply checking that $\mathbf{0}$ of $\mathbb{R}^n$ is in W. We summarize this result in the following theorem.

Theorem 12.4. *A subset W of $\mathbb{R}^n$ is a subspace of $\mathbb{R}^n$ if*

*(1) whenever $\mathbf{u}$ and $\mathbf{v}$ are in W it is also true that $\mathbf{u} + \mathbf{v}$ is in W (that is, W is **closed** under addition),*

*(2) whenever $\mathbf{u}$ is in W and a is a scalar it is also true that $a\mathbf{u}$ is in W (that is, W is **closed** under scalar multiplication),*

(3) $\mathbf{0}$ is in W.

The next activity provides some practice using Theorem 12.4.

Activity 12.1. Use Theorem 12.4 to answer the following questions. Justify your responses. For sets which lie inside $\mathbb{R}^2$, sketch a pictorial representation of the set and explain why your picture confirms your answer.

(a) Is the set $W = \left\{ \begin{bmatrix} x \\ y \end{bmatrix} \middle| y = 2x \right\}$ a subspace of $\mathbb{R}^2$?

(b) Is the set $W = \left\{ \begin{bmatrix} x \\ 0 \\ 1 \end{bmatrix} \middle| x \text{ is a scalar} \right\}$ a subspace of $\mathbb{R}^3$?

(c) Is the set $W = \left\{ \begin{bmatrix} x \\ x+y \end{bmatrix} \middle| x, y \text{ are scalars} \right\}$ a subspace of $\mathbb{R}^2$?

(d) Is the set $W = \left\{ \begin{bmatrix} x \\ y \end{bmatrix} \middle| y = 2x + 1 \right\}$ a subspace of $\mathbb{R}^2$?

(e) Is the set $W = \left\{ \begin{bmatrix} x \\ y \end{bmatrix} \middle| y = x^2 \right\}$ a subspace of $\mathbb{R}^2$?

(f) Is the set $W = \left\{ \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \end{bmatrix} \right\}$ a subspace of $\mathbb{R}^4$?

(g) Is the set $W = \left\{ \begin{bmatrix} x \\ y \\ z \end{bmatrix} \middle| x^2 + y^2 + z^2 \leq 1 \right\}$ a subspace of $\mathbb{R}^3$? Note that W is the unit sphere (a.k.a. unit ball) in $\mathbb{R}^3$.

(h) Is the set $W = \mathbb{R}^2$ a subspace of $\mathbb{R}^3$?

There are several important points that we can glean from Activity 12.1.

- A subspace is a vector space within a larger vector space, similar to a subset being a set within a larger set.
- The set containing the zero vector in $\mathbb{R}^n$ is a subspace of $\mathbb{R}^n$, and it is the only finite subspace of $\mathbb{R}^n$.
- Every subspace of $\mathbb{R}^n$ must contain the zero vector.
- No nonzero subspace is bounded – since a subspace must include all scalar multiples of its vectors, a subspace cannot be contained in a finite sphere or box.
- Since vectors in $\mathbb{R}^k$ have k components, vectors in $\mathbb{R}^k$ are not contained in $\mathbb{R}^n$ when $n \neq k$. However, if $n > k$, then we can think of $\mathbb{R}^n$ as containing a *copy* (what we call an isomorphic image) of $\mathbb{R}^k$ as the set of vectors with zeros as the last $n - k$ components.

The Subspace Spanned by a Set of Vectors

One of the most convenient ways to represent a subspace of $\mathbb{R}^n$ is as the span of a set of vectors. In Preview Activity 12.1 we saw that the span of two vectors is a subspace of $\mathbb{R}^n$. In the next theorem we verify this result for the span of an arbitrary number of vectors, extending the ideas you used in Preview Activity 12.1. Expressing a set of vectors as the span of some number of vectors is a quick

way of justifying that this set is a subspace and it also provides us a geometric intuition for the set of vectors.

Theorem 12.5. *Let $\mathbf{v}_1$, $\mathbf{v}_2$, ..., $\mathbf{v}_k$ be vectors in $\mathbb{R}^n$. Then Span$\{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_k\}$ is a subspace of $\mathbb{R}^n$.*

Proof. Let $\mathbf{v}_1$, $\mathbf{v}_2$, ..., $\mathbf{v}_k$ be vectors in $\mathbb{R}^n$. Let $W = \text{Span}\{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_k\}$. To show that W is a subspace of $\mathbb{R}^n$ we need to show that W is closed under addition and multiplication by scalars and that $\mathbf{0}$ is in W.

First we show that W is closed under addition. Let $\mathbf{u}$ and $\mathbf{w}$ be vectors in W. This means that $\mathbf{u}$ and $\mathbf{w}$ are linear combinations of $\mathbf{v}_1$, $\mathbf{v}_2$, ..., $\mathbf{v}_k$. So there are scalars a_1, a_2, ..., a_k and b_1, b_2, ..., b_k so that

$$\mathbf{u} = a_1\mathbf{v}_1 + a_2\mathbf{v}_2 + \cdots + a_k\mathbf{v}_k \qquad \text{and} \qquad \mathbf{w} = b_1\mathbf{v}_1 + b_2\mathbf{v}_2 + \cdots + b_k\mathbf{v}_k.$$

To demonstrate that $\mathbf{u} + \mathbf{w}$ is in W, we need to show that $\mathbf{u} + \mathbf{w}$ is a linear combination of $\mathbf{v}_1$, $\mathbf{v}_2$, ..., $\mathbf{v}_k$. Using the properties of vector addition and scalar multiplication, we find

$$\begin{aligned}\mathbf{u} + \mathbf{w} &= (a_1\mathbf{v}_1 + a_2\mathbf{v}_2 + \cdots + a_k\mathbf{v}_k) + (b_1\mathbf{v}_1 + b_2\mathbf{v}_2 + \cdots + b_k\mathbf{v}_k) \\ &= (a_1 + b_1)\mathbf{v}_1 + (a_2 + b_2)\mathbf{v}_2 + \cdots + (a_k + b_k)\mathbf{v}_k.\end{aligned}$$

Thus $\mathbf{u} + \mathbf{w}$ is a linear combination of $\mathbf{v}_1$, $\mathbf{v}_2$, ..., $\mathbf{v}_k$ and W is closed under vector addition.

Next we show that W is closed under scalar multiplication. Let $\mathbf{u}$ be in W and c be a scalar. Then

$$c\mathbf{u} = c(a_1\mathbf{v}_1 + a_2\mathbf{v}_2 + \cdots + a_k\mathbf{v}_k) = (ca_1)\mathbf{v}_1 + (ca_2)\mathbf{v}_2 + \cdots + (ca_k)\mathbf{v}_k$$

and $c\mathbf{u}$ is a linear combination of $\mathbf{v}_1$, $\mathbf{v}_2$, ..., $\mathbf{v}_k$ and W is closed under multiplication by scalars.

Finally, we show that $\mathbf{0}$ is in W. Since

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

$\mathbf{0}$ is in W.

Since W satisfies all of the properties of a subspace as given in definition of a subspace, we conclude that W is a subspace of $\mathbb{R}^n$. ■

The subspace $W = \text{Span}\{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_k\}$ is called the *subspace of $\mathbb{R}^n$ spanned by* $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_k$. We also use the phrase "subspace generated by $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_k$" since the vectors $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_k$ are the building blocks of all vectors in W.

Activity 12.2.

(a) Describe geometrically as best as you can the subspaces of $\mathbb{R}^3$ spanned by the following sets of vectors.

$$\left\{ \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix} \right\}$$

$$\left\{ \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix} \right\}$$

(b) Express the following set of vectors as the span of some vectors to show that this set is a subspace. Can you give a geometric description of the set?

$$W = \left\{ \begin{bmatrix} 2x+y-z \\ y \\ z \\ -x+3z \end{bmatrix} : x, y, z \text{ real numbers} \right\}$$

One additional conclusion we can draw from Activities 12.1 and 12.2 is that subspaces of $\mathbb{R}^n$ are made up of "flat" subsets. The span of a single nonzero vector is a line (which is flat), and the span of a set of two distinct nonzero vectors is a plane (which is also flat). So subspaces of $\mathbb{R}^n$ are linear (or "flat") subsets of $\mathbb{R}^n$. That is why we can recognize that the non-flat parabola in Activity 12.1 is not a subspace of $\mathbb{R}^2$.

Examples

What follows are worked examples that use the concepts from this section.

Example 12.6. Let $W = \left\{ \begin{bmatrix} 2r+s+t \\ r+t \\ r+s \end{bmatrix} : r, s, t \in \mathbb{R} \right\}$.

(a) Show that W is a subspace of $\mathbb{R}^3$.

(b) Describe in detail the geometry of the subspace W (e.g., is it a line, a union of lines, a plane, a union of planes, etc.)

Example Solution.

(a) Every vector in W has the form

$$\begin{bmatrix} 2r+s+t \\ r+t \\ r+s \end{bmatrix} = r \begin{bmatrix} 2 \\ 1 \\ 1 \end{bmatrix} + s \begin{bmatrix} 1 \\ 0 \\ 1 \end{bmatrix} + t \begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix}$$

for some real numbers r, s, and t. Thus,

$$W = \text{Span} \left\{ \begin{bmatrix} 2 \\ 1 \\ 1 \end{bmatrix}, \begin{bmatrix} 1 \\ 0 \\ 1 \end{bmatrix}, \begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix} \right\}.$$

As a span of a set of vectors, we know that W is a subspace of $\mathbb{R}^4$.

(b) Let $\mathbf{v}_1 = \begin{bmatrix} 2 \\ 1 \\ 1 \end{bmatrix}$, $\mathbf{v}_2 = \begin{bmatrix} 1 \\ 0 \\ 1 \end{bmatrix}$, and $\mathbf{v}_3 = \begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix}$. The reduced row echelon form of $[\mathbf{v}_1\ \mathbf{v}_2\ \mathbf{v}_3]$ is $\begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & -1 \\ 0 & 0 & 0 \end{bmatrix}$. The pivot columns of $[\mathbf{v}_1\ \mathbf{v}_2\ \mathbf{v}_3]$ form a linearly independent

set with the same span as $\{\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3\}$, So $W = \text{Span}\{\mathbf{v}_1, \mathbf{v}_2\}$ and W forms the plane in $\mathbb{R}^3$ through the origin and the points $(2, 1, 1)$ and $(1, 0, 1)$.

Example 12.7.

(a) Let $X = \text{Span}\left\{\begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}\right\}$ and let $Y = \text{Span}\left\{\begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix}\right\}$. That is, X is the x-axis and Y the y-axis in three-space. Let

$$X + Y = \{\mathbf{x} + \mathbf{y} : \mathbf{x} \in X \text{ and } \mathbf{y} \in Y\}.$$

i. Is $\begin{bmatrix} 2 \\ 3 \\ 0 \end{bmatrix}$ in $X + Y$? Justify your answer.

ii. Is $\begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix}$ in $X + Y$? Justify your answer.

iii. Assume that $X + Y$ is a subspace of $\mathbb{R}^3$. Describe in detail the geometry of this subspace.

(b) Now let W_1 and W_2 be arbitrary subspaces of $\mathbb{R}^n$ for some positive integer n. Let

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

Show that $W_1 + W_2$ is a subspace of $\mathbb{R}^n$. The set $W_1 + W_2$ is called the *sum* of the subspaces W_1 and W_2.

Example Solution.

(a) We let $X = \text{Span}\left\{\begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}\right\}$ and $Y = \text{Span}\left\{\begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix}\right\}$. T

i. Let $\mathbf{w} = \begin{bmatrix} 2 \\ 3 \\ 0 \end{bmatrix}$, $\mathbf{x} = 2\begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}$, and $\mathbf{y} = 3\begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix}$. Since $\mathbf{w} = \mathbf{x} + \mathbf{y}$ with $\mathbf{x} \in X$ and $\mathbf{y} \in Y$ we conclude that $\mathbf{w} \in X + Y$.

ii. Every vector in X has the form $a\mathbf{e}_1$ for some scalar a (where $\mathbf{e}_1 = \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}$, and every vector in Y has the form $b\mathbf{e}_2$ for some scalar b (where $\mathbf{e}_2 = \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix}$). So every vector in $X + Y$ is of the form $a\mathbf{e}_1 + b\mathbf{e}_2 = \begin{bmatrix} a \\ b \\ 0 \end{bmatrix}$. Since the vector $\begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix}$ does not have a 0 in the third component, we conclude that in $\begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix}$ is not in $X + Y$.

iii. As we just argued, every vector in $X + Y$ has the form $a\mathbf{e}_1 + b\mathbf{e}_2$. So $X + Y = \text{Span}\{\mathbf{e}_1, \mathbf{e}_2\}$, which is the xy-plane in $\mathbb{R}^3$.

(b) To see why the set $W_1 + W_2$ is a subspace of $\mathbb{R}^3$, suppose that $\mathbf{x}$ and $\mathbf{y}$ are in $W_1 + W_2$. Then $\mathbf{x} = \mathbf{u}_1 + \mathbf{u}_2$ and $\mathbf{y} = \mathbf{z}_1 + \mathbf{z}_2$ for some $\mathbf{u}_1, \mathbf{z}_1$ in W_1 and some $\mathbf{u}_2, \mathbf{z}_2$ in W_2. Then

$$\mathbf{x} + \mathbf{y} = (\mathbf{u}_1 + \mathbf{u}_2) + (\mathbf{z}_1 + \mathbf{z}_2) = (\mathbf{u}_1 + \mathbf{z}_1) + (\mathbf{u}_2 + \mathbf{z}_2).$$

Since W_1 is a subspace of $\mathbb{R}^3$ it follows that $\mathbf{u}_1 + \mathbf{z}_1 \in W_1$. Similarly, $\mathbf{u}_2 + \mathbf{z}_2 \in W_2$. This makes $\mathbf{x} + \mathbf{y}$ an element of $W_1 + W_2$.

Also, suppose that a is a scalar. Then

$$a\mathbf{x} = a(\mathbf{u}_1 + \mathbf{u}_2) = a\mathbf{u}_1 + a\mathbf{u}_2.$$

Since W_1 is a subspace of $\mathbb{R}^3$ it follows that $a\mathbf{u}_1 \in W_1$. Similarly, $a\mathbf{u}_2 \in W_2$. This makes $a\mathbf{x}$ an element of $W_1 + W_2$.

Finally, since $\mathbf{0}$ is in both W_1 and W_2, and $\mathbf{0} = \mathbf{0} + \mathbf{0}$, it follows that $\mathbf{0}$ is an element of $W_1 + W_2$. We conclude that $W_1 + W_2$ is a subspace of $\mathbb{R}^3$.

Summary

- A vector space is a set V with operations of addition and scalar multiplication defined on V such that for all $\mathbf{u}$, $\mathbf{v}$, and $\mathbf{w}$ in V and all scalars a and b:
  (1) $\mathbf{u} + \mathbf{v}$ is an element of V (we say that V is *closed* under the addition in V),
  (2) $\mathbf{u} + \mathbf{v} = \mathbf{v} + \mathbf{u}$ (we say that the addition in V is *commutative*),
  (3) $(\mathbf{u} + \mathbf{v}) + \mathbf{w} = \mathbf{u} + (\mathbf{v} + \mathbf{w})$ (we say that the addition in V is *associative*),
  (4) there is a vector $\mathbf{0}$ in V so that $\mathbf{u} + \mathbf{0} = \mathbf{u}$ (we say that V contains an *additive identity* or *zero vector* $\mathbf{0}$),
  (5) for each $\mathbf{x}$ in V there is an element $\mathbf{y}$ in V so that $\mathbf{x} + \mathbf{y} = \mathbf{0}$ (we say that V contains an *additive inverse* $\mathbf{y}$ for each element $\mathbf{x}$ in V),
  (6) $a\mathbf{u}$ is an element of V (we say that V is *closed* under multiplication by scalars),
  (7) $(a + b)\mathbf{u} = a\mathbf{u} + b\mathbf{u}$ (we say that *multiplication by scalars distributes over scalar addition*),
  (8) $a(\mathbf{u} + \mathbf{v}) = a\mathbf{u} + a\mathbf{v}$ (we say that *multiplication by scalars distributes over addition in* V),
  (9) $(ab)\mathbf{u} = a(b\mathbf{u})$,
  (10) $1\mathbf{u} = \mathbf{u}$.
- For every n, $\mathbb{R}^n$ is a vector space.
- A subset W of $\mathbb{R}^n$ is a subspace of $\mathbb{R}^n$ if W is a vector space using the same operations as in $\mathbb{R}^n$.
- To show that a subset W of $\mathbb{R}^n$ is a subspace of $\mathbb{R}^n$, we need to prove the following:

(1) $\mathbf{u} + \mathbf{v}$ is in W whenever $\mathbf{u}$ and $\mathbf{v}$ are in W (when this property is satisfied we say that W is *closed* under addition),

(2) $a\mathbf{u}$ is in W whenever a is a scalar and $\mathbf{u}$ is in W (when this property is satisfied we say that W is *closed* under multiplication by scalars),

(3) $\mathbf{0}$ is in W.

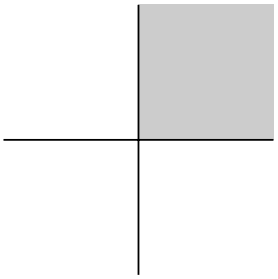
The remaining properties of a vector space are properties of the operation, and as long as we use the same operations as in $\mathbb{R}^n$, the operation properties follow the operations.

- The span of any set of vectors in $\mathbb{R}^n$ is a subspace of $\mathbb{R}^n$.

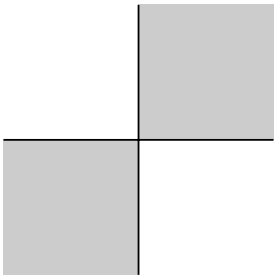
Exercises

(1) Each of the following regions or graphs determines a subset W of $\mathbb{R}^2$. For each region, discuss each of the subspace properties of Theorem 12.4 and explain with justification if the set W satisfies each property or not.

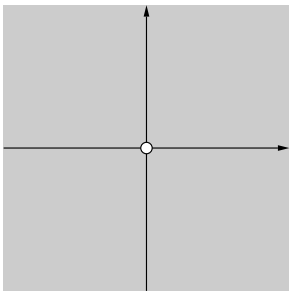
(a)



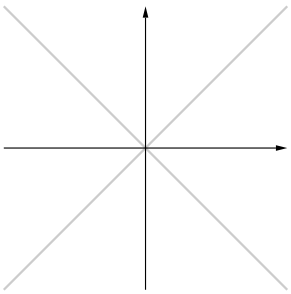
(b)



(c)



(d)



(2) Determine which of the following sets W is a subspace of $\mathbb{R}^n$ for the indicated value of n. Justify your answer.

(a) $W = \{[x\ 0]^\mathsf{T} : x \text{ is a scalar}\}$

(b) $W = \{[2x + y\ x - y\ x + y]^\mathsf{T} : x, y \text{ are scalars}\}$

(c) $W = \{[x + 1\ x - 1]^\mathsf{T} : x \text{ is a scalar}\}$

(d) $W = \{[xy\ xz\ yz]^\mathsf{T} : x, y, z \text{ are scalars}\}$

(3) Find a subset of $\mathbb{R}^2$ that is closed under addition and scalar multiplication, but that does not contain the zero vector, or explain why no such subset exists.

(4) Let $\mathbf{v}$ be a vector in $\mathbb{R}^2$. What is the smallest subspace of $\mathbb{R}^2$ that contains $\mathbf{v}$? Explain. Describe this space geometrically.

(5) What is the smallest subspace of $\mathbb{R}^2$ containing the first quadrant? Justify your answer.

(6) Let $\mathbf{u}$, $\mathbf{v}$, and $\mathbf{w}$ be vectors in $\mathbb{R}^3$ with $\mathbf{w} = \mathbf{u} + \mathbf{v}$. Let $W_1 = \text{Span}\{\mathbf{u}, \mathbf{v}\}$ and $W_2 = \text{Span}\{\mathbf{u}, \mathbf{v}, \mathbf{w}\}$.

(a) If $\mathbf{x}$ is in W_1, must $\mathbf{x}$ be in W_2? Explain.

(b) If $\mathbf{y}$ is in W_2, must $\mathbf{y}$ be in W_1? Explain.

(c) What is the relationship between $\text{Span}\{\mathbf{u}, \mathbf{v}\}$ and $\text{Span}\{\mathbf{u}, \mathbf{v}, \mathbf{w}\}$? Be specific.

(7) Let m and n be positive integers, and let $\mathbf{v}$ be in $\mathbb{R}^n$. Let $W = \{A\mathbf{v} : A \in \mathcal{M}_{m\times n}\}$.

(a) As an example, let $\mathbf{v} = [2\ 1]^\mathsf{T}$ in $\mathbb{R}^2$ with $W = \{A\mathbf{v} : A \in \mathcal{M}_{2\times 2}\}$.

i. Show that the vector $[2\ 1]^\mathsf{T}$ is in W by finding a matrix A that places $[2\ 1]^\mathsf{T}$ in W.

ii. Show that the the vector $[4\ 2]^\mathsf{T}$ is in W by finding a matrix A that places $[4\ 2]^\mathsf{T}$ in W.

iii. Show that the vector $[6\ -1]^\mathsf{T}$ is in W by finding a matrix A that places $[6\ -1]^\mathsf{T}$ in W.

iv. Show that $W = \mathbb{R}^2$.

(b) Show that, regardless of the vector $\mathbf{v}$ selected, W is a subspace of $\mathbb{R}^m$.

(c) Characterize all of the possibilities for what the subspace W can be. (Hint: There is more than one possibility.)

(8) Let S_1 and S_2 be subsets of $\mathbb{R}^3$ such that Span S_1 = Span S_2. Must it be the case that S_1 and S_2 contain at least one vector in common? Justify your answer.

(9) Assume W_1 and W_2 are two subspaces of $\mathbb{R}^n$. Is $W_1 \cap W_2$ also a subspace of $\mathbb{R}^n$? Is $W_1 \cup W_2$ also a subspace of $\mathbb{R}^n$? Justify your answer. (Note: The notation $W_1 \cap W_2$ refers to the vectors common to both W_1, W_2, while the notation $W_1 \cup W_2$ refers to the vectors that are in at least one of W_1, W_2.)

(10) Determine whether the plane defined by the equation $5x + 3y - 2z = 0$ is a subspace in $\mathbb{R}^3$.

(11) If W is a subspace of $\mathbb{R}^n$ and $\mathbf{u}$ is a vector in $\mathbb{R}^n$ not in W, determine whether

$$\mathbf{u} + W = \{\mathbf{u} + \mathbf{v} : \mathbf{v} \text{ is a vector in } W\}$$

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

(12) Two students are talking about examples of subspaces.

Student 1: The x-axis in $\mathbb{R}^2$ is a subspace. It is generated by the vector $\begin{bmatrix} 1 \\ 0 \end{bmatrix}$.

Student 2: Similarly $\mathbb{R}^2$ is a subspace of $\mathbb{R}^3$.

Student 1: I'm not sure if that will work. Can we fit $\mathbb{R}^2$ inside $\mathbb{R}^3$? Don't we need W to be a subset of $\mathbb{R}^3$ if it is a subspace of $\mathbb{R}^3$?

Student 2: Of course we can fit $\mathbb{R}^2$ inside $\mathbb{R}^3$. We can think of $\mathbb{R}^2$ as vectors $\begin{bmatrix} a \\ b \\ 0 \end{bmatrix}$. That's the xy-plane.

Student 1: I don't know. The vector $\begin{bmatrix} a \\ b \\ 0 \end{bmatrix}$ is not exactly same as $\begin{bmatrix} a \\ b \end{bmatrix}$.

Student 2: Well, $\mathbb{R}^2$ is a plane and so is the xy-plane. So they must be equal, shouldn't they?

Student 1: But there are infinitely many planes in $\mathbb{R}^3$. They can't all be equal to $\mathbb{R}^2$. They all "look like" $\mathbb{R}^2$ but I don't think we can say they are equal.

Which student is correct? Is $\mathbb{R}^2$ a subspace of $\mathbb{R}^3$, or not? Justify your answer.

(13) Label each of the following statements as True or False. Provide justification for your response.

(a) **True/False** Any line in $\mathbb{R}^n$ is a subspace in $\mathbb{R}^n$.

(b) **True/False** Any line through the origin in $\mathbb{R}^n$ is a subspace in $\mathbb{R}^n$.

(c) **True/False** Any plane through the origin in $\mathbb{R}^n$ is a subspace in $\mathbb{R}^n$.

(d) **True/False** In $\mathbb{R}^4$, the points satisfying $xy = 2t + z$ form a subspace.

(e) **True/False** In $\mathbb{R}^4$, the points satisfying $x + 3y = 2z$ form a subspace.

(f) **True/False** Any two nonzero vectors generate a plane subspace in $\mathbb{R}^3$.

(g) **True/False** The space $\mathbb{R}^2$ is a subspace of $\mathbb{R}^3$.

(h) **True/False** If W is a subspace of $\mathbb{R}^n$ and $\mathbf{u}$ is in W, then the line through the origin and $\mathbf{u}$ is in W.

(i) **True/False** There are four types of subspaces in $\mathbb{R}^3$: 0, line through origin, plane through origin and the whole space $\mathbb{R}^3$.

(j) **True/False** There are four types of subspaces in $\mathbb{R}^4$: 0, line through origin, plane through origin and the whole space $\mathbb{R}^4$.

(k) **True/False** The vectors $\begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix}$, $\begin{bmatrix} 1 \\ 2 \\ 1 \end{bmatrix}$ and $\begin{bmatrix} 2 \\ 3 \\ 2 \end{bmatrix}$ form a subspace in $\mathbb{R}^3$.

(l) **True/False** The vectors $\begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix}$ and $\begin{bmatrix} 1 \\ 2 \\ 1 \end{bmatrix}$ form a basis of a subspace in $\mathbb{R}^3$.

Project: Least Squares Linear Approximation

We return to the problem of finding the least squares line to fit the GDP-consumption data. We will start our work in a more general setting, determining the method for fitting a linear function to fit any data set, like the GDP-consumption data, in the least squares sense. Then we will apply our result to the GDP-consumption data.

Project Activity 12.1. Suppose we want to fit a linear function $p(x) = mx + b$ to our data. For the sake of our argument, let us assume the general case where we have n data points labeled as (x_1, y_1), (x_2, y_2), (x_3, y_3), ..., (x_n, y_n). (In the GDP-consumption data $n = 21$.) In the unlikely event that the graph of $p(x)$ actually passes through these data points, then we would have the system of equations

$$\begin{aligned} y_1 &= b + mx_1 \\ y_2 &= b + mx_2 \\ y_3 &= b + mx_3 \\ &\vdots \qquad \vdots \\ y_n &= b + mx_n \end{aligned} \tag{12.1}$$

in the unknowns b and m.

(a) As a small example to illustrate, write the system (12.1) using the three points $(x_1, y_1) = (1, 2)$, $(x_2, y_2) = (3, 4)$, and $(x_3, y_3) = (5, 6)$. Identify the unknowns and then write this system in the form $M\mathbf{a} = \mathbf{y}$. Explicitly identify the matrix M and the the vectors $\mathbf{a}$ and $\mathbf{y}$.

(b) Identify the specific matrix M and the specific vectors $\mathbf{a}$ and $\mathbf{y}$ using the data in Table 12.1. Explain why the system $M\mathbf{a} = \mathbf{y}$ is inconsistent. (Remember, we are treating consumption as the independent variable and GDP as the dependent variable.) What does the result tell us about the data?

Project Activity 12.1 shows that the GDP-consumption data does not lie on a line. So instead of attempting to find coefficients b and m that give a solution to this system, which may be impossible, we instead look for a vector $\mathbf{a}^*$ that provides us with something that is "close" to a solution.

If we could find b and m that give a solution to the system $M\mathbf{a} = \mathbf{y}$, then $M\mathbf{a} - \mathbf{y}$ would be zero. If we can't make $M\mathbf{a} - \mathbf{y}$ exactly equal to the vector $\mathbf{0}$, we could instead try to minimize $M\mathbf{a} - \mathbf{y}$ in some way. One way is to minimize the length $||M\mathbf{a} - \mathbf{y}||$ of the vector $M\mathbf{a} - \mathbf{y}$.

If we minimize the quantity $||M\mathbf{a} - \mathbf{y}||$, then we will have minimized a function given by a sum of squares. That is, $||M\mathbf{a} - \mathbf{y}||$ is calculated to be

$$\sqrt{(b + mx_1 - y_1)^2 + (b + mx_2 - y_2)^2 + \cdots + (b + mx_n - y_n)^2}. \tag{12.2}$$

This is why the method we will derive is called the method of least squares. This method provides us with a vector "solution" in a subspace that is related to M. We can visualize $||M\mathbf{a} - \mathbf{y}||$ as in Figure 12.2. In this figure the data points are shown along with a linear approximation (not the best for illustrative purposes). The lengths of the vertical line segments are the summands $(b+mx_i-y_i)$ in (12.2). So we are trying to minimize the sum of the squares of these line segments.

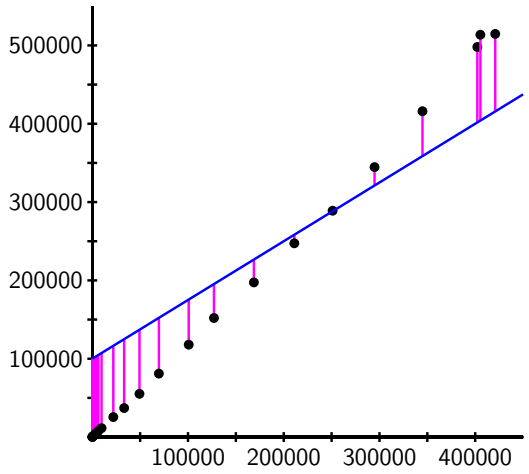


Figure 12.2: Error in the linear approximation.

Suppose that $\mathbf{a}^*$ minimizes $||M\mathbf{a} - \mathbf{y}||$. Then the vector $M\mathbf{a}^*$ is the vector that is closest to $\mathbf{y}$ of all of the vectors of the form $M\mathbf{x}$. The fact that the vectors of the form $M\mathbf{x}$ make a subspace will be useful in what follows. We verify that fact in the next project activity.

Project Activity 12.2. Let A be an arbitrary $m \times k$ matrix. Explain why the set $C = \{A\mathbf{x} : \mathbf{x} \in \mathbb{R}^k\}$ is a subspace of $\mathbb{R}^m$.

Project Activity 12.2 shows us that even though the GDP-consumption system $M\mathbf{a} = \mathbf{y}$ does not have a solution, we can find a vector that is close to a solution in the subspace $\{M\mathbf{x} : \mathbf{x} \in \mathbb{R}^2\}$. That is, find a vector $\mathbf{a}^*$ in $\mathbb{R}^2$ such that $M\mathbf{a}^*$ is as close (in the least squares sense) to $\mathbf{y}$ as we can get. In other words, the error $||M\mathbf{a}^* - \mathbf{y}||$ is as small as possible. In the following activity we see how to find $\mathbf{a}^*$.

Project Activity 12.3. Let

$$S = \sqrt{(b + mx_1 - y_1)^2 + (b + mx_2 - y_2)^2 + \cdots + (b + mx_n - y_n)^2},$$

the quantity we want to minimize. The variables in S are m and b, so we can think of S as a function of the two independent variables m and b. The square root makes calculations more complicated, so it is helpful to notice that S will be a minimum when S^2 is a minimum. Since S^2 is also function of the two variables b and m, the minimum value of S^2 will occur when the partial derivatives of S^2 with respect to b and m are both 0 (if you haven't yet taken a multivariable calculus course, you

can just assume that this is correct). This yields the equations

$$0 = \sum_{i=1}^{n} (mx_i + b - y_i)\, x_i \tag{12.3}$$

$$0 = \sum_{i=1}^{n} (mx_i + b - y_i)\,. \tag{12.4}$$

In this activity we solve equations (12.3) and (12.4) for the unknowns b and m. (Do this in a general setting without using specific values for the x_i and y_i.)

(a) Let $r = \sum_{i=1}^{n} x_i^2$, $s = \sum_{i=1}^{n} x_i$, $t = \sum_{i=1}^{n} y_i$, and $u = \sum_{i=1}^{n} x_i y_i$. Show that the equations (12.3) and (12.4) can be written in the form

$$0 = bs + mr - u$$
$$0 = bn + ms - t.$$

Note that this is a system of two linear equations in the unknowns b and m.

(b) Write the system from part (a) in matrix form $A\mathbf{x} = \mathbf{b}$. Then use techniques from linear algebra to solve the linear system to show that

$$b = \frac{tr - us}{nr - s^2} = \frac{\left(\sum_{i=1}^{n} y_i\right)\left(\sum_{i=1}^{n} x_i^2\right) - \left(\sum_{i=1}^{n} x_i\right)\left(\sum_{i=1}^{n} x_i y_i\right)}{n\left(\sum_{i=1}^{n} x_i^2\right) - \left(\sum_{i=1}^{n} x_i\right)^2} \tag{12.5}$$

and

$$m = \frac{nu - ts}{nr - s^2} = \frac{n\left(\sum_{i=1}^{n} x_i y_i\right) - \left(\sum_{i=1}^{n} x_i\right)\left(\sum_{i=1}^{n} y_i\right)}{n\left(\sum_{i=1}^{n} x_i^2\right) - \left(\sum_{i=1}^{n} x_i\right)^2}. \tag{12.6}$$

Project Activity 12.4. Use the formulas (12.5) and (12.6) to find the values of b and m for the regression line to fit the GDP-consumption data in Table 12.1. You may use the fact that the sum of the GDP data is 3.5164030×10^6, the sum of the consumption data is 2.9233750×10^6, the sum of the squares of the consumption data is $8.806564894 \times 10^{11}$, and the sum of the products of the GDP and consumption data is $1.069946378 \times 10^{12}$. Compare to the results the authors obtained in the paper "A Statistical Analysis of GDP and Final Consumption Using Simple Linear Regression, the Case of Romania 1990-2010".

Section 13

The Null Space and Column Space of a Matrix

Focus Questions

By the end of this section, you should be able to give precise and thorough answers to the questions listed below. You may want to keep these questions in mind to focus your thoughts as you complete the section.

- What is the null space of a matrix?
- What is the column space of a matrix?
- What important structure do the null space and column space of a matrix have?
- What is the kernel of a matrix transformation?
- How is the kernel of a matrix transformation T defined by $T(\mathbf{x}) = A\mathbf{x}$ related to the null space of A?
- What is the range of a matrix transformation?
- How is the range of a matrix transformation T defined by $T(\mathbf{x}) = A\mathbf{x}$ related to the column space of A?
- How do we find a basis for Nul A?
- How do we find a basis for Col A?

Application: The Lights Out Game

Lights Out (LO) is a commercial game released by Tiger Toys in 1995 (later bought out by Hasbro). The game consists of a 5×5 grid in which each square is either lit or unlit. Pressing a square changes the status of the square itself and all the squares to the left, right, up, or down. The player's job

is to turn all the lights out. You can play a sample game at https://www.geogebra.org/m/wcmctahp. There is a method to solve any solvable Lights Out game that can be uncovered through linear algebra that we will uncover later in this section. Column spaces and null spaces play important roles in this method.

Introduction

Recall that a subspace of $\mathbb{R}^n$ is a subset of $\mathbb{R}^n$ which is a vector space in itself. More specifically, a subset W or $\mathbb{R}^n$ is a subspace of $\mathbb{R}^n$ if

(1) whenever $\mathbf{u}$ and $\mathbf{v}$ are in W it is also true that $\mathbf{u} + \mathbf{v}$ is in W (that is, W is **closed** under addition),

(2) whenever $\mathbf{u}$ is in W and a is a scalar it is also true that $a\mathbf{u}$ is in W (that is, W is **closed** under scalar multiplication),

(3) $\mathbf{0}$ is in W.

Given a matrix A, there are several subspaces that are connected to A. Two specific such subspaces are the null space of A and the column space of A. We will see that these subspaces provide answers to the big questions we have been considering since the beginning of the semester, such as "Do columns of A span $\mathbb{R}^m$?" "Are the columns of A linearly independent?" "Is the transformation T defined by matrix multiplication by A one-to-one?" "Is the transformation T onto?"

In this preview activity, we start examining the *null space*.

Preview Activity 13.1.

(1) Let $A = \begin{bmatrix} 2 & 1 & 3 \\ 1 & 1 & 4 \end{bmatrix}$.

(a) Find the general solution to the homogeneous equation $A\mathbf{x} = \mathbf{0}$. Write your solutions in parametric vector form. (Recall that the parametric vector form expresses the solutions to an equation as linear combinations of vectors with free variables as the weights. An example would be $x_3 \begin{bmatrix} 1 \\ 0 \\ -1 \\ 0 \end{bmatrix} + x_4 \begin{bmatrix} -2 \\ 1 \\ 0 \\ 1 \end{bmatrix}$.)

(b) Find two specific solutions $\mathbf{x}_1$ and $\mathbf{x}_2$ to the homogeneous equation $A\mathbf{x} = \mathbf{0}$. Is $\mathbf{x}_1 + \mathbf{x}_2$ a solution to $A\mathbf{x} = \mathbf{0}$? Explain.

(c) Is $3\mathbf{x}_1$ a solution to $A\mathbf{x} = \mathbf{0}$? Explain.

(d) Is $\mathbf{0}$ a solution to $A\mathbf{x} = \mathbf{0}$?

(e) What does the above seem to indicate about the set of solutions to the homogeneous system $A\mathbf{x} = \mathbf{0}$?

(2) Let A be an $m \times n$ matrix. As problem 1 implies, the set of solutions to a homogeneous matrix-vector equation $A\mathbf{x} = \mathbf{0}$ appears to be a subspace. We give a special name to this set.

Definition 13.1. The **null space** of an $m \times n$ matrix A is the set of all solutions to $A\mathbf{x} = \mathbf{0}$.

We denote the null space of a matrix A as Nul A. In set notation we write

$$\text{Nul } A = \{\mathbf{x} : A\mathbf{x} = \mathbf{0}\}.$$

Note that since $A\mathbf{x} = \mathbf{0}$ corresponds to a homogeneous system of linear equations, Nul A also represents the solution set of a homogeneous system.

Let $A = \begin{bmatrix} 2 & 1 & 3 & 0 \\ 1 & 1 & 4 & 1 \end{bmatrix}$. Find all vectors in Nul A.

(3) So far we considered specific examples of null spaces. But what are the properties of a null space in general? Let A be an *arbitrary* $m \times n$ matrix.

(a) The null space of an $m \times n$ matrix is a subset of $\mathbb{R}^k$ for some integer k. What is k?

(b) Now suppose $\mathbf{u}$ and $\mathbf{v}$ are two vectors in Nul A. By definition, that means $A\mathbf{u} = \mathbf{0}$, $A\mathbf{v} = \mathbf{0}$. Use properties of the matrix-vector product to show that $\mathbf{u} + \mathbf{v}$ is also in Nul A.

(c) Now suppose $\mathbf{u}$ is a vector in Nul A and a is a scalar. Explain why $a\mathbf{u}$ is also in Nul A.

(d) Explain why Nul A is a subspace of $\mathbb{R}^n$.

The Null Space of a Matrix and the Kernel of a Matrix Transformation

In this section we explore the *null space* and see how the null space of a matrix is related to the matrix transformation defined by the matrix.

Let A be an $m \times n$ matrix. In Preview Activity 13.1 we defined the null space of a matrix A (see Definition 13.1) as the set of solutions to the matrix equation $A\mathbf{x} = \mathbf{0}$. Note that the null space of an $m \times n$ matrix is a subset of $\mathbb{R}^n$. We saw that the null space of A is closed under addition and scalar multiplication – that is, if $\mathbf{u}$ and $\mathbf{v}$ are in Nul A and a and b are any scalars, then $\mathbf{u} + \mathbf{v}$ and $a\mathbf{u}$ are also in Nul A. Since the zero vector is always in Nul A, we can conclude that the null space of A is a subspace of $\mathbb{R}^n$.

There is a connection between the null space of a matrix and the matrix transformation it defines. Recall that any $m \times n$ matrix A defines a matrix transformation T from $\mathbb{R}^n$ to $\mathbb{R}^m$ by $T(\mathbf{x}) = A\mathbf{x}$. The null space of A is then the collection of vectors $\mathbf{x}$ in $\mathbb{R}^n$ so that $T(\mathbf{x}) = \mathbf{0}$. So if T is a matrix transformation from $\mathbb{R}^n$ to $\mathbb{R}^m$, then the set

$$\{\mathbf{x} \text{ in } \mathbb{R}^n : T(\mathbf{x}) = \mathbf{0}\}$$

is a subspace of $\mathbb{R}^n$ equal to the null space of A. This set is is given a special name.

Definition 13.2. Let $T : \mathbb{R}^n \to \mathbb{R}^n$ be a matrix transformation. The **kernel** of T is the set

$$\text{Ker}(T) = \{\mathbf{x} \in \mathbb{R}^n : T(\mathbf{x}) = \mathbf{0}\}.$$

Activity 13.1. If T is a matrix transformation defined by a matrix A, then there is a convenient way to determine if T is one-to-one.

(a) Let T be the matrix transformation defined by $T(\mathbf{x}) = A\mathbf{x}$, where

$$A = \begin{bmatrix} 1 & 2 & -1 \\ 0 & 1 & 4 \end{bmatrix}.$$

Find all of the vectors in Nul A. If Nul A contains more than one vector, can T be one-to-one? Why?

(b) Let T be the matrix transformation defined by $T(\mathbf{x}) = A\mathbf{x}$, where

$$A = \begin{bmatrix} 1 & 0 \\ 2 & 1 \\ -1 & 4 \end{bmatrix}.$$

Find all of the vectors in Nul A. Is T one-to-one? Why?

(c) To find the vectors in the null space of a matrix A we solve the system $A\mathbf{x} = \mathbf{0}$. Since a homogeneous system is always consistent, there are two possibilities for Nul A: either Nul $A = \{\mathbf{0}\}$ or Nul A contains infinitely many vectors.

i. Under what conditions on A is Nul $A = \{\mathbf{0}\}$? What does that mean about T being one-to-one or not? Explain.

ii. Under what conditions is Nul A infinite? What does that mean about T being one-to-one or not? Explain.

iii. Is is possible for Nul A to be the whole space $\mathbb{R}^n$? If so, give an example. If not, explain why not.

Recall that for a function to be one-to-one, each output must come from exactly one input. Since a matrix transformation T defined by $T(\mathbf{x}) = A\mathbf{x}$ always maps the zero vector to the zero vector, for T to be one-to-one it must be the case that the zero vector is the only vector that T maps to the zero vector. This means that the null space of A must be $\{\mathbf{0}\}$. Activity 13.1 demonstrates that if the matrix A that defines the transformation T has a pivot in every column, then $T(\mathbf{x}) = \mathbf{b}$ will have exactly one solution for each $\mathbf{b}$ in the range of T. So a trivial null space is enough to characterize a one-to-one matrix transformation.

Theorem 13.3. *A matrix transformation T from $\mathbb{R}^n$ to $\mathbb{R}^m$ defined by $T(\mathbf{x}) = A\mathbf{x}$ is one-to-one if and only if*

$$\textit{Nul } A = \textit{Ker}(T) = \{\mathbf{0}\}.$$

The Column Space of a Matrix and the Range of a Matrix Transformation

Given an $m \times n$ matrix A, we have seen that the matrix-vector product $A\mathbf{x}$ is a linear combination of the columns of A with weights from $\mathbf{x}$. It follows that the equation $A\mathbf{x} = \mathbf{b}$ has a solution if and only if $\mathbf{b}$ is a linear combination of the columns of A. So the span of the columns of A tells us for which vectors the equation $A\mathbf{x} = \mathbf{b}$ is consistent. We give the span of the columns of a matrix A a special name.

Definition 13.4. The **column space** of an $m \times n$ matrix A is the span of the columns of A.

We denote the column space of A as Col A. Given that $A\mathbf{x}$ is a linear combination of the columns of A, we can also write the column space of an $m \times n$ matrix A as

$$\text{Col } A = \{A\mathbf{x} : \mathbf{x} \text{ is in } \mathbb{R}^n\}.$$

For the matrix transformation T defined by $T(\mathbf{x}) = A\mathbf{x}$, the set of all vectors of the form $A\mathbf{x}$ is also the range of the transformation T. So for a matrix transformation T with matrix A we have Range$(T) =$ Col A.

Activity 13.2. As a span of a set of vectors, we know that Col A is a subspace of $\mathbb{R}^k$ for an appropriate value of k.

(a) Let $M = \begin{bmatrix} 1 & 1 & 1 & 0 & 2 \\ 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 & -1 \\ 0 & 1 & 0 & 1 & 1 \end{bmatrix}$. The space Col M is a subspace of $\mathbb{R}^k$ for some positive integer k. What is k in this case?

(b) If A is an $m \times n$ matrix, then Col A is a subspace of $\mathbb{R}^k$ for some positive integer k. What is k in this case?

(c) Recall that a matrix transformation T given by $T(\mathbf{x}) = A\mathbf{x}$ where A is an $m \times n$ matrix is onto if for every $\mathbf{b}$ in $\mathbb{R}^m$ there exists a $\mathbf{x}$ in $\mathbb{R}^n$ for which $T(\mathbf{x}) = \mathbf{b}$. How does T being onto relate to the Col A?

As you saw in Activity 13.2, a matrix transformation T defined by $T(\mathbf{x}) = A\mathbf{x}$ is onto if the column space of A, which consists of the image vectors under the transformation T, is equal to $\mathbb{R}^m$. In other words, we want the Range(T) to equal $\mathbb{R}^m$.

Theorem 13.5. *A matrix transformation T from $\mathbb{R}^n$ to $\mathbb{R}^m$ defined by $T(\mathbf{x}) = A\mathbf{x}$ is onto if and only if*

$$\textit{Col } A = \textit{Range}(T) = \mathbb{R}^m.$$

The Row Space of a Matrix

As you might expect, if there is a column space for a matrix then there is also a row space for a matrix. The row space is defined just as the column space as the span of the rows of a matrix.

Definition 13.6. The **row space** of an $m \times n$ matrix A is the span of the row of A.

There is really nothing new here, though. Since the rows of A are the columns of A^T, it follows that Row $A =$ Col A^T. So if we want to learn anything about the row space of A, we can just translate all of our questions to the column space of A^T.

Bases for Nul A and Col A

When confronted with a subspace of $\mathbb{R}^n$, we will usually want to find a minimal spanning set – a smallest spanning set – for the space. Recall that a minimal spanning set is also called a basis for the space. So a basis for a space must span that space, and to be a minimal spanning set we have seen that a basis must also be linearly independent. So to prove that a set is a basis for a subspace of $\mathbb{R}^n$ we need to demonstrate two things: that the set is linearly independent, and that the set spans the subspace.

Activity 13.3. In this activity we see how to find a basis for Col A and Nul A for a specific matrix A. Let

$$A = \begin{bmatrix} 1 & 1 & 1 & 0 & 2 \\ 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 & -1 \\ 0 & 1 & 0 & 1 & 1 \end{bmatrix}.$$

Assume that the reduced row echelon form of A is

$$R = \begin{bmatrix} 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 2 \\ 0 & 0 & 0 & 1 & -1 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}.$$

(a) First we examine Col A. Recall that to find a minimal spanning set of a set of vectors $\{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_k\}$ in $\mathbb{R}^n$ we just select the pivot columns of the matrix $[\mathbf{v}_1\ \mathbf{v}_2\ \cdots\ \mathbf{v}_k]$.

i. Find a basis for Col A.

ii. Does Col A equal Col R? Explain.

(b) Now we look at Nul A.

i. Write the general solution to the homogeneous system $A\mathbf{x} = \mathbf{0}$ in vector form.

ii. Find a spanning set for Nul A.

iii. Find a basis for Nul A. Explain how you know you have a basis.

You should have noticed that Activity 13.3 (a) provides a process for finding a basis for Col A – the pivot columns of A form a basis for Col A. Similarly, Activity 13.3 (b) shows us that we can find a basis for Nul A by writing the general solution to the homogeneous equation $A\mathbf{x} = \mathbf{0}$ as a linear combination of vectors whose weights are the variables corresponding to the non-pivot columns of A – and these vectors form a basis for Nul A. As we will argue next, these process always give us bases for Col A and Nul A.

Let A be an $m \times n$ matrix, and let R be the reduced row echelon form of A. Suppose R has k non-pivot columns and $n - k$ pivot columns. We can rearrange the columns so that the non-pivot columns of R are the last k columns (this just amounts to relabeling the unknowns in the system).

Basis for Nul A. Here we argue that the method described following Activity 13.3 to find a spanning set for the null space always yields a basis for the null space.

First note that Nul R = Nul A, since the system $A\mathbf{x} = \mathbf{0}$ has the same solution set as $R\mathbf{x} = \mathbf{0}$. So it is enough to find a basis for Nul R. If every column of R is a pivot column, then $R\mathbf{x} = \mathbf{0}$ has only the trivial solution and the null space of R is $\{\mathbf{0}\}$. Let us now consider the case where R contains non-pivot columns. If we let $\mathbf{x} = [x_1\ x_2\ \ldots\ x_n]^\mathsf{T}$, and if $R\mathbf{x} = \mathbf{0}$ then we can write x_1, x_2, …, x_{n-k} in terms of x_{n-k+1}, x_{n-k+2}, …, and x_n. From these equations we can write $\mathbf{x}$ as a linear combination of some vectors $\mathbf{v}_1$, $\mathbf{v}_2$, …, $\mathbf{v}_k$ with x_{n-k+1}, x_{n-2+2}, …, x_n as weights. By construction, each of the vectors $\mathbf{v}_1$, $\mathbf{v}_2$, …, $\mathbf{v}_k$ has a component that is 1 with the corresponding component as 0 in all the other $\mathbf{v}_i$. Therefore, the vectors $\mathbf{v}_1$, $\mathbf{v}_2$, …, $\mathbf{v}_k$ are linearly independent and span Nul R (and Nul A). In other words, the method we have developed to find the general solution to $A\mathbf{x} = \mathbf{0}$ always produces a basis for Nul A.

Basis for Col A. Here we explain why the pivot columns of A form a basis for Col A. Recall that the product $A\mathbf{x}$ expresses a linear combination of the columns of A with weights from $\mathbf{x}$, and every such linear combination is matched with a product $R\mathbf{x}$ giving a linear combination of the columns of R *using the same weights*. So if a set of columns of R is linearly independent (or dependent), then the set of corresponding columns in A is linearly independent (or dependent) and vice versa. Since each pivot column of R is a vector with 1 in one entry (a different entry for different pivot columns) and zeros elsewhere, the pivot columns of R are clearly linearly independent. It follows that the pivot columns of A are linearly independent. All that remains is to explain why the pivot columns of A span Col A.

Let $\mathbf{r}_1$, $\mathbf{r}_2$, …, $\mathbf{r}_n$ be the columns of R so that $R = [\mathbf{r}_1\ \ \mathbf{r}_2\ \ \cdots\ \ \mathbf{r}_n]$, and let $\mathbf{a}_1$, $\mathbf{a}_2$, …, $\mathbf{a}_n$ be the columns of A so that $A = [\mathbf{a}_1\ \ \mathbf{a}_2\ \ \cdots\ \ \mathbf{a}_n]$. Suppose $\mathbf{a}_i$ is a non-pivot column for A and $\mathbf{r}_i$ the corresponding non-pivot column in R. Each pivot column is composed of a single 1 with the rest of its entries 0. Also, if a non-pivot column contains a nonzero entry, then there is a corresponding pivot column that contains a 1 in the corresponding position. So $\mathbf{r}_i$ is a linear combination of $\mathbf{r}_1$, $\mathbf{r}_2$, …, $\mathbf{r}_{n-k}$ – the pivot columns of R. Thus,

$$\mathbf{r}_i = c_1\mathbf{r}_1 + c_2\mathbf{r}_2 + \cdots + c_{n-k}\mathbf{r}_{n-k}$$

for some scalars c_1, c_2, …, c_{n-k}. Let $\mathbf{x} = [c_1\ c_2\ \cdots\ c_{n-k}\ 0\ \cdots 0\ -1\ 0\ \cdots\ 0]^\mathsf{T}$, where the -1 is in position i. Then $R\mathbf{x} = \mathbf{0}$ and so $A\mathbf{x} = \mathbf{0}$. Thus,

$$\mathbf{a}_i = c_1\mathbf{a}_1 + c_2\mathbf{a}_2 + \cdots + c_{n-k}\mathbf{a}_{n-k}$$

and $\mathbf{a}_i$ is a linear combination of the pivot columns of A. So every non-pivot column of A is in the span of A and we conclude that the pivot columns of A form a basis for Col A.

IMPORTANT POINT: It is the pivot columns of A that form a basis for Col A, not the pivot columns of the reduced row echelon form R of A. In general, Col $R \neq$ Col A.

We can incorporate the ideas of this section to expand the Invertible Matrix Theorem.

Theorem 13.7 (The Invertible Matrix Theorem)**.** *Let A be an $n \times n$ matrix. The following statements are equivalent.*

(1) The matrix A is an invertible matrix.

(2) The matrix equation $A\mathbf{x} = \mathbf{0}$ has only the trivial solution.

(3) The matrix A has n pivot columns.

(4) Every row of A contains a pivot.

(5) The columns of A span $\mathbb{R}^n$.

(6) The matrix A is row equivalent to the identity matrix I_n.

(7) The columns of A are linearly independent.

(8) The columns of A form a basis for $\mathbb{R}^n$.

(9) The matrix transformation T from $\mathbb{R}^n$ to $\mathbb{R}^n$ defined by $T(\mathbf{x}) = A\mathbf{x}$ is one-to-one.

(10) The matrix equation $A\mathbf{x} = \mathbf{b}$ has exactly one solution for each vector $\mathbf{b}$ in $\mathbb{R}^n$.

(11) The matrix transformation T from $\mathbb{R}^n$ to $\mathbb{R}^n$ defined by $T(\mathbf{x}) = A\mathbf{x}$ is onto.

(12) There is an $n \times n$ matrix C so that $AC = I_n$.

(13) There is an $n \times n$ matrix D so that $DA = I_n$.

(14) The scalar 0 is not an eigenvalue of A.

(15) The matrix A^T is invertible.

(16) Nul $A = \{\mathbf{0}\}$.

(17) Col $A = \mathbb{R}^n$.

Examples

What follows are worked examples that use the concepts from this section.

Example 13.8.

(a) Let $A = \begin{bmatrix} 1 & 0 & -2 & 3 \\ -2 & -4 & 0 & -14 \\ 1 & 3 & 1 & 9 \end{bmatrix}$.

i. Find a basis for Col A.

ii. Describe Col A geometrically (e.g., as a line, a plane, a union of lines, etc.) in the appropriate larger space.

(b) Let $B = \begin{bmatrix} 0 & -2 & 1 \\ -1 & 0 & 1 \\ 6 & -10 & -1 \\ 1 & -4 & 1 \end{bmatrix}$.

i. Find a basis for Nul B.

ii. Describe Nul B geometrically (e.g., as a line, a plane, a union of lines, etc.) in the appropriate larger space.

Example Solution.

(a) We use $A = \begin{bmatrix} 1 & 0 & -2 & 3 \\ -2 & -4 & 0 & -14 \\ 1 & 3 & 1 & 9 \end{bmatrix}$.

i. Technology shows that the reduced row echelon form of A is

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

The first two columns of A are the pivot columns of A. Since the pivot columns of A form a basis for Col A, a basis for Col A is

$$\left\{ \begin{bmatrix} 1 \\ -2 \\ 1 \end{bmatrix}, \begin{bmatrix} 0 \\ -4 \\ 3 \end{bmatrix} \right\}.$$

ii. Let $\mathbf{v}_1 = \begin{bmatrix} 1 \\ -2 \\ 1 \end{bmatrix}$ and $\mathbf{v}_2 = \begin{bmatrix} 0 \\ -4 \\ 3 \end{bmatrix}$. Since neither $\mathbf{v}_1$ nor $\mathbf{v}_2$ is a scalar multiple of the other, we see that Col A is the span of two linearly independent vectors in $\mathbb{R}^3$. Thus, we conclude that Col A is the plane in $\mathbb{R}^3$ through the origin and the points $(1, -2, 1)$ and $(0, -4, 3)$.

(b) We use $B = \begin{bmatrix} 0 & -2 & 1 \\ -1 & 0 & 1 \\ 6 & -10 & -1 \\ 1 & -4 & 1 \end{bmatrix}$.

i. Technology shows that the reduced row echelon form of B is

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

To find a basis for Nul B, we must solve the homogeneous equation $B\mathbf{x} = \mathbf{0}$. If $\mathbf{x} = \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix}$ and $B\mathbf{x} = \mathbf{0}$, the reduced row echelon form of B shows that x_3 is free,

$x_2 = \frac{1}{2}x_3$, and $x_1 = x_3$. So

$$\mathbf{x} = \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = \begin{bmatrix} x_3 \\ \frac{1}{2}x_3 \\ x_3 \end{bmatrix} = x_3 \begin{bmatrix} 1 \\ \frac{1}{2}1 \\ 1 \end{bmatrix}.$$

Thus, a basis for Nul B is

$$\left\{ \begin{bmatrix} 2 \\ 1 \\ 2 \end{bmatrix} \right\}.$$

ii. Since Nul $B = \text{Span}\left\{ \begin{bmatrix} 2 \\ 1 \\ 2 \end{bmatrix} \right\}$ is the span of one nonzero vector in $\mathbb{R}^3$, we conclude that Nul B is the line in $\mathbb{R}^3$ through the origin and the point $(2, 1, 2)$.

Example 13.9. Let $A = \begin{bmatrix} 1 & 3 \\ -1 & 2 \\ 0 & -2 \\ 5 & 6 \end{bmatrix}$, and let T be the matrix transformation defined by $T(\mathbf{x}) = A\mathbf{x}$.

(a) What are the domain and codomain of T? Why?

(b) Find all vectors $\mathbf{x}$ such that $T(\mathbf{x}) = \mathbf{0}$. How is this set of vectors related to Nul A? Explain.

(c) Is T one-to-one? Explain.

(d) Is T onto? If yes, explain why. If no, find a basis for the range of T.

Example Solution.

(a) Recall that $A\mathbf{x}$ is a linear combination of the columns of A with weights from $\mathbf{x}$. So $A\mathbf{x}$ is defined only when the number of components of $\mathbf{x}$ is equal to the number of columns of A. This explains why the domain of T is $\mathbb{R}^2$. Also, since each output of T is a linear combination of the columns of A, the codomain of T is $\mathbb{R}^4$.

(b) The set of vectors $\mathbf{x}$ such that $\mathbf{0} = T(\mathbf{x}) = A\mathbf{x}$ is the same as Nul A. The reduced row echelon form of A is

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \\ 0 & 0 \\ 0 & 0 \end{bmatrix}.$$

Since both columns of A are pivot columns, the columns of A are linearly independent. This implies that $A\mathbf{x} = \mathbf{0}$ has only the trivial solution. Therefore, the only vector $\mathbf{x}$ such that $T(\mathbf{x}) = \mathbf{0}$ is the zero vector in $\mathbb{R}^2$.

(c) The previous part shows that $\text{Ker}(T) = \{\mathbf{0}\}$. This means that T is one-to-one by Theorem 13.3.

(d) Recall that the range of T is the same as Col A. The reduced row echelon form of A has a row of zeros, so $A\mathbf{x} = \mathbf{b}$ is not consistent for every $\mathbf{b}$ in $\mathbb{R}^4$. We conclude that T is not onto. To find a basis for the range of T, we just need to find a basis for Col A. The pivot columns of A form such a basis, so a basis for the range of T is

$$\left\{ \begin{bmatrix} 1 \\ -1 \\ 0 \\ 5 \end{bmatrix}, \begin{bmatrix} 3 \\ 2 \\ -2 \\ 6 \end{bmatrix} \right\}.$$

Summary

- The null space of an $m \times n$ matrix A is the set of vectors $\mathbf{x}$ in $\mathbb{R}^n$ so that $A\mathbf{x} = \mathbf{0}$. In set notation
$$\text{Nul } A = \{\mathbf{x} : A\mathbf{x} = \mathbf{0}\}.$$
- The column space of a matrix A is the span of the columns of A.
- A subset W of $\mathbb{R}^n$ is a subspace of $\mathbb{R}^n$ if
  (1) $\mathbf{u} + \mathbf{v}$ is in W whenever $\mathbf{u}$ and $\mathbf{v}$ are in W (when this property is satisfied we say that W is *closed* under addition),
  (2) $a\mathbf{u}$ is in W whenever a is a scalar and $\mathbf{u}$ is in W (when this property is satisfied we say that W is *closed* under multiplication by scalars),
  (3) $\mathbf{0}$ is in W.
- The null space of an $m \times n$ matrix is a subspace of $\mathbb{R}^n$ while the column space of A is a subspace of $\mathbb{R}^m$.
- The span of any set of vectors in $\mathbb{R}^n$ is a subspace of $\mathbb{R}^n$.
- The kernel of a matrix transformation $T : \mathbb{R}^n \to \mathbb{R}^m$ is the set
$$\text{Ker}(T) = \{\mathbf{x} \in \mathbb{R}^n : T(\mathbf{x}) = \mathbf{0}\}.$$
- The kernel of a matrix transformation T defined by $T(\mathbf{x}) = A\mathbf{x}$ is the same set as Nul A.
- The range of a matrix transformation $T : \mathbb{R}^n \to \mathbb{R}^m$ is the set
$$\text{Range}(T) = \{T(\mathbf{x}) : \mathbf{x} \in \mathbb{R}^n\}.$$
- The range of a matrix transformation T defined by $T(\mathbf{x}) = A\mathbf{x}$ is the same set as Col A.

- A basis for the null space of a matrix A can be found by writing the general solution to the homogeneous equation $A\mathbf{x} = \mathbf{0}$ as a linear combination of vectors whose weights are the variables corresponding to the non-pivot columns of A. The number of vectors in a basis for Nul A is the number of non-pivot columns of A.
- The pivot columns of a matrix A form a basis for the column space of A.

Exercises

(1) Find a basis for the null space and column space of the matrix

$$A = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 0 & 0 & 2 & -2 \\ 1 & 2 & 5 & 2 \end{bmatrix}.$$

Of which spaces are the null and column spaces of A subspaces?

(2) If the column space of $\begin{bmatrix} 1 & 2 & -1 \\ 1 & 1 & 1 \\ 1 & 2 & c \end{bmatrix}$ has basis $\left\{ \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix}, \begin{bmatrix} 2 \\ 1 \\ 2 \end{bmatrix} \right\}$, what must c be?

(3) If the null space of $\begin{bmatrix} 2 & 1 & a \\ 1 & 2 & b \end{bmatrix}$ has basis $\left\{ \begin{bmatrix} 2 \\ -1 \\ 1 \end{bmatrix} \right\}$, what must a and b be?

(4) Find a matrix with at least four non-zero and distinct columns for which the column space has basis $\left\{ \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix}, \begin{bmatrix} 2 \\ 2 \\ 3 \end{bmatrix} \right\}$.

(5) Find a matrix with at least two rows whose null space has basis $\left\{ \begin{bmatrix} 1 \\ 1 \\ -1 \end{bmatrix} \right\}$.

(6) Find a matrix whose column space has basis $\left\{ \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix}, \begin{bmatrix} 2 \\ 2 \\ 3 \end{bmatrix} \right\}$ and whose null space has basis $\left\{ \begin{bmatrix} 2 \\ 1 \\ -1 \end{bmatrix} \right\}$.

(7) If possible, find a 4×4 matrix whose column space does not equal $\mathbb{R}^4$ but whose null space equals $\{\mathbf{0}\}$. Explain your answer. If not possible, explain why not.

(8) Label each of the following statements as True or False. Provide justification for your response.

(a) **True/False** For a 3×4 matrix, the null space contains vectors other than the zero vector.

(b) **True/False** For a 4×3 matrix, the null space contains vectors other than the zero vector.

(c) **True/False** If Nul A is not the zero subspace, then the transformation $\mathbf{x} \mapsto A\mathbf{x}$ is not one-to-one.

(d) **True/False** If the transformation $\mathbf{x} \mapsto A\mathbf{x}$ is onto where A is an $m \times n$ matrix, then Col $A = \mathbb{R}^m$.

(e) **True/False** For a 4×3 matrix A, Col A cannot equal $\mathbb{R}^4$.

(f) **True/False** For a 3×4 matrix A, Col A cannot equal $\mathbb{R}^3$.

(g) **True/False** The null space of the matrix $\begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix}$ consists of the two vectors $[-1\ 0\ 1]^\mathsf{T}$ and $[0\ -1\ 1]^\mathsf{T}$.

(h) **True/False** A basis for the null space of the matrix $\begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix}$ consists of the two vectors $[-1\ 0\ 1]^\mathsf{T}$ and $[0\ -1\ 1]^\mathsf{T}$.

(i) **True/False** There does not exist a matrix whose null space equals its column space.

(j) **True/False** The column space of every 4×4 matrix is $\mathbb{R}^4$ and its null space is $\{\mathbf{0}\}$.

Project: Solving the Lights Out Game

The Lights Out game starts with a 5×5 grid on which some of the squares are lit (on) and some are not lit (off). We will call such a state a *configuration*. Pressing a square that is on turns it off and changes the state of all adjacent (vertically and horizontally) squares, and pressing a square that is off turns it on and changes the state of all adjacent (vertically and horizontally) squares. To model this situation, we consider the number system $\mathbb{Z}_2 = \{0, 1\}$ consisting only of 0 and 1, where 0 represents the off state and 1 the on state. We can also think of 1 as the act of pressing a square and 0 as the act of not pressing – that is,

- $0 + 0 = 0$ (not pressing an off square leaves it off),
- $0 + 1 = 1 = 1 + 0$ (pressing an off square turns it on or not pressing a lit square leaves it lit),
- $1 + 1 = 0$ (pressing a lit square turns it off).

The numbers 0 and 1 in $\mathbb{Z}_2$ will be the only numbers we use when playing the Lights Out game, so all of our matrix entries will be in $\mathbb{Z}_2$ and all of our calculations are done in $\mathbb{Z}_2$.

There are two ways we can view a Lights Out game.

- We can view each configuration as a 5×5 matrix. In this situation, we label the entries in the grid as shown in Figure 13.1. Each entry in the grid will be assigned a 0 or 1 according to whether the light in that entry is off or on.

- For our purposes a better way to visualize a Lights Out configuration is as a 25×1 vector. The components in this vector correspond to the entries in the 5×5 grid with the correspondence given by the numbering demonstrated in Figure 13.1 (for the sake of space, this array is shown in a row instead of a column). Again, each component is assigned a 0 or 1 according to whether the light for that entry is off or on. In this view, each configuration is a vector with 25 components in $\mathbb{Z}_2$.

1	2	3	4	5
6	7	8	9	10
11	12	13	14	15
16	17	18	19	20
21	22	23	24	25

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Figure 13.1: Two representations of the Lights Out game.

We will take the latter perspective and view the Lights Out game as if it is played on a 25×1 board with entries in $\mathbb{Z}_2$. The space of all of these Lights Out configurations is denoted as $\mathbb{Z}_2^{25}$ (similar to $\mathbb{R}^{25}$, but with entries in $\mathbb{Z}_2$ rather than $\mathbb{R}$). Since $\mathbb{Z}_2$ is a field, the space $\mathbb{Z}_2^{25}$ is a vector space just as $\mathbb{R}^{25}$ is. This is the environment in which we will play the Lights Out game.

If we think about the game as played on a 25×1 board, then pressing a square correlates to selecting one of the 25 components of a configuration vector. Each time we press a square, we make a move that changes the status of that square and all the squares vertically or horizontally adjacent to it from the 5×5 board. Recalling that adding 1 to a square has the effect of changing its status (from on to off or off to on), and each move that we make in the game can be represented as a 25×1 vector that is added to a configuration. For example, the move of pressing the first square is given by adding the vector

$$\mathbf{m}_1 = [1\,1\,0\,0\,0\,1\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0]^\mathsf{T}$$

to a configuration vector and the move of pressing the second square is represented by adding the vector

$$\mathbf{m}_2 = [1\,1\,1\,0\,0\,0\,1\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0]^\mathsf{T}.$$

Project Activity 13.1. Let $\mathbf{m}_i$ be the move of pressing the ith square for i from 1 to 25.

(a) Find vector representations for $\mathbf{m}_9$ and $\mathbf{m}_{22}$.

(b) Let $M = [m_{ij}] = [\mathbf{m}_1|\mathbf{m}_2|\cdots|\mathbf{m}_{25}]$. Explain why $m_{ij} = m_{ji}$ for each i and j. In other words, explain why $M^\mathsf{T} = M$. (Such a matrix is called a *symmetric* matrix.)

The goal of the Lights Out game is to begin with an initial configuration $\mathbf{c}$ (a vector in $\mathbb{Z}_2^{25}$) and determine if we can apply a sequence of moves to obtain the configuration in which all the entries are 0 (or all the lights are off). The vector in $\mathbb{Z}_2^{25}$ of all 0s is the zero vector in $\mathbb{Z}_2^{25}$ and we will denote it as $\mathbf{0}$. Some basic algebra of vector addition in $\mathbb{Z}_2$ (or mod 2) will help us understand the strategy.

Start with a configuration $\mathbf{c}$. If we press the ith square, then we obtain the new configuration $\mathbf{c}_1 = \mathbf{m}_i + \mathbf{c}$ (where each move $\mathbf{m}_i$ is also in $\mathbb{Z}_2^{25}$).

Project Activity 13.2.

(a) What happens if we press the ith square twice in a row? Explain in terms of the action and the game and verify using vector addition.

(b) Explain why applying move $\mathbf{m}_i$ then move $\mathbf{m}_j$ is the same as applying move $\mathbf{m}_j$, then $\mathbf{m}_i$.

(c) Explain how the answers to the previous two questions show that to play the game we only need to determine which buttons to press (and only once each) without worrying about the order in which the buttons are pressed.

What we have seen is that to play the game we are really looking for scalars x_1, x_2, ..., x_{25} in $\mathbb{Z}_2$ (in other words, either 0 or 1) so that

$$x_1\mathbf{m}_1 + x_2\mathbf{m}_2 + \cdots + x_{25}\mathbf{m}_{25} + \mathbf{c} = \mathbf{0}. \tag{13.1}$$

Project Activity 13.3. Explain why (13.1) has the equivalent matrix equation

$$M\mathbf{x} = \mathbf{c}, \tag{13.2}$$

where $M = [\mathbf{m}_1|\mathbf{m}_2|\cdots|\mathbf{m}_{25}]$, or

$$M = \begin{bmatrix}
1&1&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
1&1&1&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&1&1&1&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&1&1&1&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&1&1&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
1&0&0&0&0&1&1&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&1&0&0&0&1&1&1&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&1&0&0&0&1&1&1&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&1&0&0&0&1&1&1&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&1&0&0&0&1&1&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&1&0&0&0&0&1&1&0&0&0&1&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&1&0&0&0&1&1&1&0&0&0&1&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&1&0&0&0&1&1&1&0&0&0&1&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&1&0&0&0&1&1&1&0&0&0&1&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&1&0&0&0&1&1&0&0&0&0&1&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&1&1&0&0&0&1&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&1&1&1&0&0&0&1&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&1&1&1&0&0&0&1&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&1&1&1&0&0&0&1&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&1&1&0&0&0&0&1\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&1&1&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&1&1&1&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&1&1&1&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&1&1&1\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&1&1
\end{bmatrix}.$$

Explicitly identify the vector $\mathbf{x}$. Also, explain why $\mathbf{c}$ is on the right side of this equation.

To solve a Lights Out game now, all we need do is determine a solution, if one exists, to the matrix equation (13.2).

Project Activity 13.4. For this activity you may use the fact that the reduced row echelon form of the matrix M (using algebra in $\mathbb{Z}_2$) is as shown below.

(a) Find a basis for the column space of M.

(b) Explain why not every Lights Out puzzle can be solved. That is, explain why there are some initial configurations of lights on and off for which it is not possible to turn out all the lights (without turning off the game). Relate this to the column space of M.

The reduced row echelon form of the matrix M (using algebra in $\mathbb{Z}_2$):

$$\begin{bmatrix}
1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1\\
0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0\\
0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&1\\
0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0\\
0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1\\
0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&1\\
0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&1\\
0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&1&1\\
0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&1&0\\
0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&1&0\\
0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&1&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&1&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&1&1\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&1&1\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&1&1\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&1&0&1\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&1&1&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0
\end{bmatrix}.$$

To find conditions under which a Lights Out game is not solvable, we will demonstrate that if A is an $n \times n$ matrix, then the scalar product of any vector in Nul A^{T} with any column of A is $\mathbf{0}$. Let $A = [a_{ij}]$ be an $n \times n$ matrix with columns $\mathbf{a}_1$, $\mathbf{a}_2$, …, $\mathbf{a}_n$. Represent the entries in the ith column as $\mathbf{a}_i = [a_{1i}\ a_{2i}\ \ldots\ a_{ni}]^{\mathsf{T}}$ for each i between 1 and n. Note that $\mathbf{a}_i$ is also the ith row of A^{T}. Also, let $\mathbf{x} = [x_1\ x_2\ \ldots\ x_n]^{\mathsf{T}}$ be a vector in Nul A^{T}. Then $A^{\mathsf{T}}\mathbf{x} = \mathbf{0}$. Using the row-column method of multiplying a matrix by a vector, when we multiply the ith row of A^{T} with $\mathbf{x}$ we obtain

$$a_{1i}x_1 + a_{2i}x_2 + \cdots + a_{ni}x_n = 0. \tag{13.3}$$

This equation is valid for each i between 1 and n. Recall that the sum in (13.3) is the scalar product of $\mathbf{a}_i$ and $\mathbf{x}$ and is denoted $\mathbf{a}_i \cdot \mathbf{x}$. That is,

$$\mathbf{a}_i \cdot \mathbf{x} = a_{i1}x_1 + a_{i2}x_2 + \cdots + a_{in}x_n.$$

The fact that $\mathbf{x}$ is in Nul A^T means $\mathbf{a}_i \cdot \mathbf{x} = \mathbf{0}$ for every i between 1 and n. In other words, the scalar product of any vector in Nul A^T with any column of A is $\mathbf{0}$. (When the scalar product of two vectors is $\mathbf{0}$, we call the vectors *orthogonal* – a fancy word for "perpendicular".) Since scalar products are linear, we can extend this result to the following.

Theorem 13.10. *Let A be an $n \times n$ matrix. If $\mathbf{x}$ is any vector in Col A and $\mathbf{y}$ is any vector in Nul A^T, then $\mathbf{x} \cdot \mathbf{y} = 0$.*

With Theorem 13.10 in mind we can return to our analysis of the Lights Out game, applying this result to the matrix M.

Project Activity 13.5.

(a) Find a basis for the null space of M^T. (Recall that $M^\mathsf{T} = M$, so you can use the reduced row echelon form of M (using algebra in $\mathbb{Z}_2$) given earlier.)

(b) Use Theorem 13.10 to show that if $\mathbf{c} = [c_1\ c_2\ \ldots\ c_{25}]^\mathsf{T}$ is an initial Lights Out configuration that is solvable, then $\mathbf{c}$ must be orthogonal to each of the vectors in a basis for Nul M^T. Then show that if $\mathbf{c}$ is a solvable initial Lights Out configuration, $\mathbf{c}$ must satisfy

$$c_2 + c_3 + c_4 + c_6 + c_8 + c_{10} + c_{11} + c_{12} + c_{14} + c_{15} + c_{16} + c_{18} + c_{20} + c_{22} + c_{23} + c_{24} = 0$$

and

$$c_1 + c_3 + c_5 + c_6 + c_8 + c_{10} + c_{16} + c_{18} + c_{20} + c_{21} + c_{23} + c_{25} = 0.$$

Be very specific in your explanation.

Project Activity 13.6. Now that we know which Lights Out games can be solved, let $\mathbf{c}$ be an initial configuration to a solvable Lights Out game. Explain how to find a solution to this game. Will the solution be unique? Explain.

Now that we have a strategy for solving the Lights Out game, use it to solve random puzzles at https://www.geogebra.org/m/wcmctahp, or create your own game to solve.

Section 14

Eigenspaces of a Matrix

Focus Questions

By the end of this section, you should be able to give precise and thorough answers to the questions listed below. You may want to keep these questions in mind to focus your thoughts as you complete the section.

- What is an eigenspace of a matrix?
- How do we find a basis for an eigenspace of a matrix?
- What is true about any set of eigenvectors for a matrix that correspond to different eigenvalues?

Application: Population Dynamics

The study of population dynamics – how and why people move from one place to another – is important to economists. The movement of people corresponds to the movement of money, and money makes the economy go. As an example, we might consider a simple model of population migration to and from the state of Michigan.

According to the Michigan Department of Technology, Management, and Budget,[1] from 2011 to 2012, approximately 0.05% of the U.S. population outside of Michigan moved to the state of Michigan, while approximately 2% of Michigan's population moved out of Michigan. A reasonable question to ask about this situation is, if these numbers don't change, what is the long-term distribution of the US population inside and outside of Michigan (under the assumption that the total US population doesn't change.). The answer to this question involves eigenvalues and eigenvectors of a matrix. More details can be found later in this section.

[1] http://michigan.gov/cgi/0,1607,7-158-54534-140915--,00.html

Introduction

Preview Activity 14.1. Consider the matrix transformation T from $\mathbb{R}^2$ to $\mathbb{R}^2$ defined by $T(\mathbf{x}) = A\mathbf{x}$, where

$$A = \begin{bmatrix} 3 & 1 \\ 1 & 3 \end{bmatrix}.$$

We are interested in understanding what this matrix transformation does to vectors in $\mathbb{R}^2$. The matrix A has eigenvalues $\lambda_1 = 2$ and $\lambda_2 = 4$ with corresponding eigenvectors $\mathbf{v}_1 = \begin{bmatrix} -1 \\ 1 \end{bmatrix}$ and $\mathbf{v}_2 = \begin{bmatrix} 1 \\ 1 \end{bmatrix}$.

(1) Explain why $\mathbf{v}_1$ and $\mathbf{v}_2$ are linearly independent.

(2) Explain why any vector $\mathbf{b}$ in $\mathbb{R}^2$ can be written uniquely as a linear combination of $\mathbf{v}_1$ and $\mathbf{v}_2$.

(3) We now consider the action of the matrix transformation T on a linear combination of $\mathbf{v}_1$ and $\mathbf{v}_2$. Explain why

$$T(c_1\mathbf{v}_1 + c_2\mathbf{v}_2) = 2c_1\mathbf{v}_1 + 4c_2\mathbf{v}_2. \tag{14.1}$$

Equation (14.1) illustrates that it would be convenient to view the action of T in the coordinate system where Span$\{\mathbf{v}_1\}$ serves as the x-axis and Span$\{\mathbf{v}_2\}$ as the y-axis. In this case, we can visualize that when we apply the transformation T to a vector $\mathbf{b} = c_1\mathbf{v}_1 + c_2\mathbf{v}_2$ in $\mathbb{R}^2$ the result is an output vector is scaled by a factor of 2 in the $\mathbf{v}_1$ direction and by a factor of 4 in the $\mathbf{v}_2$ direction. For example, consider the box with vertices at $(0, 0)$, $\mathbf{v}_1$, $\mathbf{v}_2$, and $\mathbf{v}_1 + \mathbf{v}_2$ as shown at left in Figure 14.1. The transformation T stretches this box by a fact of 2 in the $\mathbf{v}_1$ direction and a factor of 4 in the $\mathbf{v}_2$ direction as illustrated at right in Figure 14.1. In this situation, the eigenvalues and eigenvectors provide the most convenient perspective through which to visualize the action of the transformation T. Here, Span$\{\mathbf{v}_1\}$ and Span$\{\mathbf{v}_2\}$ are the eigenspaces of the matrix A.

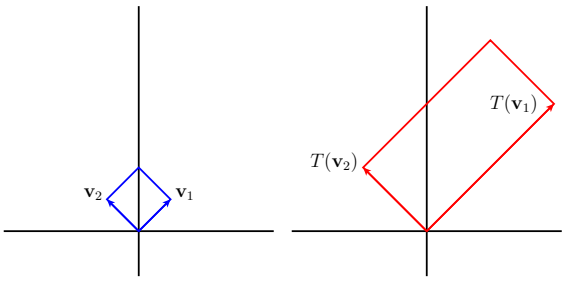


Figure 14.1: A box and a transformed box.

This geometric perspective illustrates how each the span of each eigenvalue of A tells us something important about A. In this section we explore the idea of eigenvalues and spaces defined by eigenvectors in more detail.

Eigenspaces of Matrix

Recall that the eigenvectors of an $n \times n$ matrix A satisfy the equation

$$A\mathbf{x} = \lambda\mathbf{x}$$

for some scalar λ. Equivalently, the eigenvectors of A with eigenvalue λ satisfy the equation

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

In other words, the eigenvectors for A with eigenvalue λ are the non-zero vectors in Nul $A - \lambda I_n$. Recall that the null space of an $n \times n$ matrix is a subspace of $\mathbb{R}^n$. In Preview Activity 14.1 we say how these subspaces provided a convenient coordinate system through which to view a matrix transformation. These special null spaces are called *eigenspaces*.

Definition 14.1. Let A be an $n \times n$ matrix with eigenvalue λ. The **eigenspace** for A corresponding to λ is the null space of $A - \lambda I_n$.

Activity 14.1. The matrix $A = \begin{bmatrix} 2 & 0 & 1 \\ 0 & 2 & -1 \\ 0 & 0 & 1 \end{bmatrix}$ has two distinct eigenvalues.

(a) Find a basis for the eigenspace of A corresponding to the eigenvalue $\lambda_1 = 1$. In other words, find a basis for Nul $A - I_3$.

(b) Find a basis for the eigenspace of A corresponding to the eigenvalue $\lambda_2 = 2$.

(c) Is it true that if $\mathbf{v}_1$ and $\mathbf{v}_2$ are two distinct eigenvectors for A, that $\mathbf{v}_1$ and $\mathbf{v}_2$ are linearly independent? Explain.

(d) Is it possible to have two linearly independent eigenvectors corresponding to the same eigenvalue?

(e) Is it true that if $\mathbf{v}_1$ and $\mathbf{v}_2$ are two distinct eigenvectors corresponding to different eigenvalues for A, that $\mathbf{v}_1$ and $\mathbf{v}_2$ are linearly independent? Explain.

If we know an eigenvalue λ of an $n \times n$ matrix A, Activity 14.1 shows us how to find a basis for the corresponding eigenspace – just row reduce $A - \lambda I_n$ to find a basis for Nul $A - \lambda I_n$. To this point we have always been given eigenvalues for our matrices, and have not seen how to find these eigenvalues. That process will come a bit later. For now, we just want to become more familiar with eigenvalues and eigenvectors. The next activity should help connect eigenvalues to ideas we have discussed earlier.

Activity 14.2. Let A be an $n \times n$ matrix with eigenvalue λ.

(a) How many solutions does the equation $(A - \lambda I_n)\mathbf{x} = \mathbf{0}$ have? Explain.

(b) Can $A - \lambda I_n$ have a pivot in every column? Why or why not?

(c) Can $A - \lambda I_n$ have a pivot in every row? Why or why not?

(d) Can the columns of $A - \lambda I_n$ be linearly independent? Why or why not?

Linearly Independent Eigenvectors

An important question we will want to answer about a matrix is how many linearly independent eigenvectors the matrix has. Activity 14.1 shows that eigenvectors for the same eigenvalue may be linearly dependent or independent, but all of our examples so far seem to indicate that eigenvectors corresponding to different eigenvalues are linearly independent. This turns out to be universally true as our next theorem demonstrates. The next activity should help prepare us for the proof of this theorem

Activity 14.3. Let λ_1 and λ_2 be distinct eigenvalues of a matrix A with corresponding eigenvectors $\mathbf{v}_1$ and $\mathbf{v}_2$. The goal of this activity is to demonstrate that $\mathbf{v}_1$ and $\mathbf{v}_2$ are linearly independent. To prove that $\mathbf{v}_1$ and $\mathbf{v}_2$ are linearly independent, suppose that

$$x_1\mathbf{v}_1 + x_2\mathbf{v}_2 = \mathbf{0}. \tag{14.2}$$

(a) Multiply both sides of equation (14.2) on the left by the matrix A and show that

$$x_1\lambda_1\mathbf{v}_1 + x_2\lambda_2\mathbf{v}_2 = \mathbf{0}. \tag{14.3}$$

(b) Now multiply both sides of equation (14.2) by the scalar λ_1 and show that

$$x_1\lambda_1\mathbf{v}_1 + x_2\lambda_1\mathbf{v}_2 = \mathbf{0}. \tag{14.4}$$

(c) Combine equations (14.3) and (14.4) to obtain the equation

$$x_2(\lambda_2 - \lambda_1)\mathbf{v}_2 = \mathbf{0}. \tag{14.5}$$

(d) Explain how we can conclude that $x_2 = 0$. Why does it follow that $x_1 = 0$? What does this tell us about $\mathbf{v}_1$ and $\mathbf{v}_2$?

Activity 14.3 contains the basic elements of the proof of the next theorem.

Theorem 14.2. *Let λ_1, λ_2, ..., λ_k be k distinct eigenvalues for a matrix A and for each i between 1 and k let $\mathbf{v}_i$ be an eigenvector of A with eigenvalue λ_i. Then the vectors $\mathbf{v}_1$, $\mathbf{v}_2$, ..., $\mathbf{v}_k$ are linearly independent.*

Proof. Let A be a matrix with k distinct eigenvalues λ_1, λ_2, ..., λ_k and corresponding eigenvectors $\mathbf{v}_1$, $\mathbf{v}_2$, ..., $\mathbf{v}_k$. To understand why $\mathbf{v}_1$, $\mathbf{v}_2$, ..., $\mathbf{v}_k$ are linearly independent, we will argue by contradiction and suppose that the vectors $\mathbf{v}_1$, $\mathbf{v}_2$, ..., $\mathbf{v}_k$ are linearly dependent. Note that $\mathbf{v}_1$ cannot be the zero vector (why?), so the set $S_1 = \{\mathbf{v}_1\}$ is linearly independent. If we include $\mathbf{v}_2$ into this set, the set $S_2 = \{\mathbf{v}_1, \mathbf{v}_2\}$ may be linearly independent or dependent. If S_2 is linearly independent, then the set $S_3 = \{\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3\}$ may be linearly independent or dependent. We can continue adding additional vectors until we reach the set $S_k = \{\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3, \ldots, \mathbf{v}_k\}$ which we are assuming is linearly dependent. So there must be a smallest integer $m \geq 2$ such that the set S_m is linearly dependent while S_{m-1} is linearly independent. Since $S_m = \{\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3, \ldots, \mathbf{v}_m\}$ is

linearly dependent, there is a linear combination of $\mathbf{v}_1$, $\mathbf{v}_2$, ..., $\mathbf{v}_m$ with weights not all 0 that is the zero vector. Let c_1, c_2, ..., c_m be such weights, not all zero, so that

$$c_1\mathbf{v}_1 + c_2\mathbf{v}_2 + \cdots + c_{m-1}\mathbf{v}_{m-1} + c_m\mathbf{v}_m = \mathbf{0} \tag{14.6}$$

If we multiply both sides of (14.6) on the left by the matrix A we obtain

$$\begin{aligned} A(c_1\mathbf{v}_1 + c_2\mathbf{v}_2 + \cdots + c_m\mathbf{v}_m) &= A\mathbf{0} \\ c_1A\mathbf{v}_1 + c_2A\mathbf{v}_2 + \cdots + c_mA\mathbf{v}_m &= \mathbf{0} \\ c_1\lambda_1\mathbf{v}_1 + c_2\lambda_2\mathbf{v}_2 + \cdots + c_m\lambda_m\mathbf{v}_m &= \mathbf{0}. \end{aligned} \tag{14.7}$$

If we multiply both sides of (14.6) by λ_m we obtain the equation

$$c_1\lambda_m\mathbf{v}_1 + c_2\lambda_m\mathbf{v}_2 + \cdots + c_m\lambda_m\mathbf{v}_m = \mathbf{0}. \tag{14.8}$$

Subtracting corresponding sides of equation (14.8) from (14.7) gives us

$$c_1(\lambda_1 - \lambda_m)\mathbf{v}_1 + c_2(\lambda_2 - \lambda_m)\mathbf{v}_2 + \cdots + c_{m-1}(\lambda_{m-1} - \lambda_m)\mathbf{v}_{m-1} = \mathbf{0}. \tag{14.9}$$

Recall that S_{m-1} is a linearly independent set, so the only way a linear combination of vectors in S_{m-1} can be $\mathbf{0}$ is if all of the weights are 0. Therefore, we must have

$$c_1(\lambda_1 - \lambda_m) = 0, \quad c_2(\lambda_2 - \lambda_m) = 0, \quad \ldots, \quad c_{m-1}(\lambda_{m-1} - \lambda_m) = 0.$$

Since the eigenvalues are all distinct, this can only happen if

$$c_1 = c_2 = \cdots = c_{m-1} = 0.$$

But equation (14.6) then implies that $c_m = 0$ and so all of the weights c_1, c_2, ..., c_m are 0. However, when we assumed that the eigenvectors $\mathbf{v}_1$, $\mathbf{v}_2$, ..., $\mathbf{v}_k$ were linearly dependent, this led to having at least one of the weights c_1, c_2, ..., c_m be nonzero. This cannot happen, so our assumption that the eigenvectors $\mathbf{v}_1$, $\mathbf{v}_2$, ..., $\mathbf{v}_k$ were linearly dependent must be false and we conclude that the eigenvectors $\mathbf{v}_1$, $\mathbf{v}_2$, ..., $\mathbf{v}_k$ are linearly independent. ■

Examples

What follows are worked examples that use the concepts from this section.

Example 14.3. Let $A = \begin{bmatrix} 4 & -3 & -3 \\ -3 & 4 & 3 \\ 3 & -3 & -2 \end{bmatrix}$ and let T be the matrix transformation defined by $T(\mathbf{x}) = A\mathbf{x}$.

(a) Show that 4 is an eigenvalue for A and find a basis for the corresponding eigenspace of A.

(b) Geometrically describe the eigenspace of A corresponding to the eigenvalue 4. Explain what the transformation T does to this eigenspace.

(c) Show that 1 is an eigenvalue for A and find a basis for the corresponding eigenspace of A.

(d) Geometrically describe the eigenspace of A corresponding to the eigenvalue 1. Explain what the transformation T does to this eigenspace.

Example Solution.

(a) Recall that λ is an eigenvalue of A if $A - \lambda I_3$ is not invertible. To show that 4 is an eigenvalue for A we row reduce the matrix

$$A - (4)I_3 = \begin{bmatrix} 0 & -3 & -3 \\ 3 & 0 & -3 \\ 3 & -3 & -6 \end{bmatrix}$$

to $\begin{bmatrix} 1 & 0 & -1 \\ 0 & 1 & 1 \\ 0 & 0 & 0 \end{bmatrix}$. Since the third column of $A - 4I_3$ is not a pivot column, the matrix $A - 4I_3$ is not invertible. We conclude that 4 is an eigenvalue of A.

The eigenspace of A for the eigenvalue 4 is Nul $(A - 4I_3)$. The reduced row echelon form of $A - 4I_3$ shows that if $\mathbf{x} = \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix}$ and $(A - 4I_3)\mathbf{x} = \mathbf{0}$, then x_3 is free, $x_2 = -x_3$, and $x_1 = x_3$. Thus,

$$\mathbf{x} = \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = \begin{bmatrix} x_3 \\ -x_3 \\ x_3 \end{bmatrix} = x_3 \begin{bmatrix} 1 \\ -1 \\ 1 \end{bmatrix}.$$

Therefore, $\left\{ \begin{bmatrix} 1 \\ -1 \\ 1 \end{bmatrix} \right\}$ is a basis for the eigenspace of A corresponding to the eigenvalue 4.

(b) Since the eigenspace of A corresponding to the eigenvalue 4 is the span of a single nonzero vector $\mathbf{v} = \begin{bmatrix} 1 \\ -1 \\ 1 \end{bmatrix}$, this eigenspace is the line in $\mathbb{R}^3$ through the origin and the point $(1, -1, 1)$. Any vector in this eigenspace has the form $c\mathbf{v}$ for some scalar c. Notice that

$$T(c\mathbf{v}) = Ac\mathbf{v} = cA\mathbf{v} = 4c\mathbf{v},$$

so T expands any vector in this eigenspace by a factor of 4.

(c) To show that 1 is an eigenvalue for A we row reduce the matrix

$$A - (1)I_3 = \begin{bmatrix} 3 & -3 & -3 \\ -3 & 3 & 3 \\ 3 & -3 & -3 \end{bmatrix}$$

to $\begin{bmatrix} 1 & -1 & -1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}$. Since the third column of $A - I_3$ is not a pivot column, the matrix $A - I_3$ is not invertible. We conclude that 1 is an eigenvalue of A.

The eigenspace of A for the eigenvalue 1 is Nul $(A - I_3)$. The reduced row echelon form of $A - I_3$ shows that if $\mathbf{x} = \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix}$ and $(A - I_3)\mathbf{x} = \mathbf{0}$, then x_2 and x_3 are free, and $x_1 = x_2 + x_3$. Thus,

$$\mathbf{x} = \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = \begin{bmatrix} x_2 + x_3 \\ x_2 \\ x_3 \end{bmatrix} = x_2 \begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix} + x_3 \begin{bmatrix} 1 \\ 0 \\ 1 \end{bmatrix}.$$

Therefore, $\left\{ \begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 1 \\ 0 \\ 1 \end{bmatrix} \right\}$ is a basis for the eigenspace of A corresponding to the eigenvalue 1.

(d) Since the eigenspace of A corresponding to the eigenvalue 1 is the span of two linearly independent vectors $\mathbf{v}_1 = \begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix}$ and $\mathbf{v}_2 = \begin{bmatrix} 1 \\ 0 \\ 1 \end{bmatrix}$, this eigenspace is the plane in $\mathbb{R}^3$ through the origin and the points $(1, 1, 0)$ and $(1, 0, 1)$. Any vector in this eigenspace has the form $a\mathbf{v}_1 + b\mathbf{v}_2$ for some scalars a and b. Notice that

$$T(a\mathbf{v}_1 + b\mathbf{v}_2) = A(a\mathbf{v}_1 + b\mathbf{v}_2) = aA\mathbf{v}_1 + bA\mathbf{v}_2 = a\mathbf{v}_1 + b\mathbf{v}_2,$$

so T fixes every vector in this plane.

Example 14.4.

(a) Let $A = \begin{bmatrix} 1 & 2 \\ 2 & 1 \end{bmatrix}$. Note that the vector $\mathbf{v} = \begin{bmatrix} 1 \\ 1 \end{bmatrix}$ satisfies $A\mathbf{v} = 3\mathbf{v}$.

i. Show that $\mathbf{v}$ is an eigenvector of A^2. What is the corresponding eigenvalue?

ii. Show that $\mathbf{v}$ is an eigenvector of A^3. What is the corresponding eigenvalue?

iii. Show that $\mathbf{v}$ is an eigenvector of A^4. What is the corresponding eigenvalue?

iv. If k is a positive integer, do you expect that $\mathbf{v}$ is an eigenvector of A^k? If so, what do you think is the corresponding eigenvalue?

(b) The result of part (a) is true in general. Let M be an $n \times n$ matrix with eigenvalue λ and corresponding eigenvector $\mathbf{x}$.

i. Show that λ^2 is an eigenvalue of M^2 with eigenvector $\mathbf{x}$.

ii. Show that λ^3 is an eigenvalue of M^3 with eigenvector $\mathbf{x}$.

iii. Suppose that λ^k is an eigenvalue of M^k with eigenvector $\mathbf{x}$ for some integer $k \geq 1$. Show then that λ^{k+1} is an eigenvalue of M^{k+1} with eigenvector $\mathbf{x}$. This argument shows that λ^k is an eigenvalue of M^k with eigenvector $\mathbf{x}$ for any positive integer k.

(c) We now investigate the eigenvalues of a special type of matrix.

i. Let $B = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{bmatrix}$. Show that $B^3 = 0$. (A square matrix M is *nilpotent*) if $M^k = 0$ for some positive integer k, so B is an example of a nilpotent matrix.) What are the eigenvalues of B? Explain.

ii. Show that the only eigenvalue of a nilpotent matrix is 0.

Example Solution.

(a) We use the fact that $\mathbf{v}$ is an eigenvector of the matrix A with eigenvalue 3.

i. We have that

$$A^2\mathbf{v} = A(A\mathbf{v}) = A(3\mathbf{v}) = 3(A\mathbf{v}) = 3(3\mathbf{v}) = 9\mathbf{v}.$$

So $\mathbf{v}$ is an eigenvector of A^2 with eigenvalue $9 = 3^2$.

ii. We have that

$$A^3\mathbf{v} = A(A^2\mathbf{v}) = A(9\mathbf{v}) = 9(A\mathbf{v}) = 9(3\mathbf{v}) = 27\mathbf{v}.$$

So $\mathbf{v}$ is an eigenvector of A^3 with eigenvalue $27 = 3^3$.

iii. We have that

$$A^4\mathbf{v} = A(A^3\mathbf{v}) = A(27\mathbf{v}) = 27(A\mathbf{v}) = 27(3\mathbf{v}) = 81\mathbf{v}.$$

So $\mathbf{v}$ is an eigenvector of A^4 with eigenvalue $81 = 3^4$.

iv. The results of the previous parts of this example indicate that $A^k\mathbf{v} = 3^k\mathbf{v}$, or that $\mathbf{v}$ is an eigenvector of A^k with corresponding eigenvalue 3^k.

(b) Let M be an $n \times n$ matrix with eigenvalue λ and corresponding eigenvector $\mathbf{x}$.

i. We have that

$$M^2\mathbf{x} = M(M\mathbf{x}) = M(\lambda\mathbf{x}) = \lambda(M\mathbf{x}) = \lambda(\lambda\mathbf{x}) = \lambda^2\mathbf{x}.$$

So $\mathbf{x}$ is an eigenvector of M^2 with eigenvalue λ^2.

ii. We have that

$$M^3\mathbf{x} = M(M^2\mathbf{x}) = M(\lambda^2\mathbf{x}) = \lambda^2(M\mathbf{x}) = \lambda^2(\lambda\mathbf{x}) = \lambda^3\mathbf{x}.$$

So $\mathbf{x}$ is an eigenvector of M^3 with eigenvalue λ^3.

iii. Assume that $M^k\mathbf{x} = \lambda^k\mathbf{x}$. Then

$$M^{k+1}\mathbf{x} = M(M^k\mathbf{x}) = M(\lambda^k\mathbf{x}) = \lambda^k(M\mathbf{x}) = 2\lambda^k(\lambda\mathbf{x}) = \lambda^{k+1}\mathbf{x}.$$

So $\mathbf{x}$ is an eigenvector of M^{k+1} with eigenvalue λ^{k+1}.

(c) Now we investigate a special type of matrix.

i. Straightforward calculations show that $B^3 = 0$. Since B is an upper triangular matrix, the eigenvalues of B are the entries on the diagonal. That is, the only eigenvalue of B is 0.

ii. Assume that M is a nilpotent matrix. Suppose that λ is an eigenvalue of M with corresponding eigenvector $\mathbf{v}$. Since M is a nilpotent matrix, there is a positive integer k such that $M^k = 0$. But λ^k is an eigenvalue of M^k with eigenvector $\mathbf{v}$. The only eigenvalue of the zero matrix is 0, so $\lambda^k = 0$. This implies that $\lambda = 0$. We conclude that the only eigenvalue of a nilpotent matrix is 0.

Summary

- An eigenspace of an $n \times n$ matrix A corresponding to an eigenvalue λ of A is the null space of $A - \lambda I_n$.
- To find a basis for an eigenspace of a matrix A corresponding to an eigenvalue λ, we row reduce $A - \lambda I_n$ and find a basis for Nul $A - \lambda I_n$.
- Eigenvectors corresponding to different eigenvalues are always linearly independent.

Exercises

(1) For each of the following, find a basis for the eigenspace of the indicated matrix corresponding to the given eigenvalue.

(a) $\begin{bmatrix} 10 & 7 \\ -14 & -11 \end{bmatrix}$ with eigenvalue 3

(b) $\begin{bmatrix} 11 & 18 \\ -3 & -4 \end{bmatrix}$ with eigenvalue 2

(c) $\begin{bmatrix} 2 & 1 \\ -1 & 0 \end{bmatrix}$ with eigenvalue 1

(d) $\begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 2 \\ 1 & 0 & 2 \end{bmatrix}$ with eigenvalue 2

(e) $\begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 2 \\ 1 & 0 & 2 \end{bmatrix}$ with eigenvalue 1

(f) $\begin{bmatrix} 2 & 2 & 4 \\ 1 & 1 & 2 \\ 3 & 3 & 6 \end{bmatrix}$ with eigenvalue 0

(2) Suppose A is an invertible matrix.

(a) Use the definition of an eigenvalue and an eigenvector to algebraically explain why if λ is an eigenvalue of A, then λ^{-1} is an eigenvalue of A^{-1}.

(b) To provide an alternative explanation to the result in the previous part, let $\mathbf{v}$ be an eigenvector of A corresponding to λ. Consider the matrix transformation T_A corresponding to A and $T_{A^{-1}}$ corresponding to A^{-1}. Considering what happens to $\mathbf{v}$ if T_A and then $T_{A^{-1}}$ are applied, describe why this justifies $\mathbf{v}$ is also an eigenvector of A^{-1}.

(3) If $A = \begin{bmatrix} 0 & 1 \\ a & b \end{bmatrix}$ has two eigenvalues 4 and 6, what are the values of a and b?

(4)

(a) What are the eigenvalues of the identity matrix I_2? Describe each eigenspace.

(b) Now let $n > 2$ be a positive integer. What are the eigenvalues of the identity matrix I_n? Describe each eigenspace.

(5)

(a) What are the eigenvalues of the 2×2 zero matrix (the matrix all of whose entries are 0)? Describe each eigenspace.

(b) Now let $n > 2$ be a positive integer. What are the eigenvalues of the $n \times n$ zero matrix? Describe each eigenspace.

(6) Label each of the following statements as True or False. Provide justification for your response.

(a) **True/False** If $A\mathbf{v} = \lambda\mathbf{v}$, then λ is an eigenvalue of A with eigenvector $\mathbf{v}$.

(b) **True/False** The scalar λ is an eigenvalue of a square matrix A if and only if the equation $(A - \lambda I_n)\mathbf{x} = \mathbf{0}$ has a nontrivial solution.

(c) **True/False** If λ is an eigenvalue of a matrix A, then there is only one nonzero vector $\mathbf{v}$ with $A\mathbf{v} = \lambda\mathbf{v}$.

(d) **True/False** The eigenspace of an eigenvalue of an $n \times n$ matrix A is the same as Nul $(A - \lambda I_n)$.

(e) **True/False** If $\mathbf{v}_1$ and $\mathbf{v}_2$ are eigenvectors of a matrix A corresponding to the same eigenvalue λ, then $\mathbf{v}_1 + \mathbf{v}_2$ is also an eigenvector of A.

(f) **True/False** If $\mathbf{v}_1$ and $\mathbf{v}_2$ are eigenvectors of a matrix A, then $\mathbf{v}_1 + \mathbf{v}_2$ is also an eigenvector of A.

(g) **True/False** If $\mathbf{v}$ is an eigenvector of an invertible matrix A, then $\mathbf{v}$ is also an eigenvector of A^{-1}.

Project: Modeling Population Migration

As introduced earlier, data from the Michigan Department of Technology, Management, and Budget shows that from 2011 to 2012, approximately 0.05% of the U.S. population outside of Michigan moved to the state of Michigan, while approximately 2% of Michigan's population moved out of Michigan. We are interested in determining the long-term distribution of population in Michigan.

Let $\mathbf{x}_n = \begin{bmatrix} m_n \\ u_n \end{bmatrix}$ be the 2×1 vector where m_n is the population of Michigan and u_n is the U.S. population outside of Michigan in year n. Assume that we start our analysis at generation 0 and $\mathbf{x}_0 = \begin{bmatrix} m_0 \\ u_0 \end{bmatrix}$.

Project Activity 14.1.

(a) Explain how the data above shows that

$$m_1 = 0.98m_0 + 0.0005u_0$$
$$u_1 = 0.02m_0 + 0.9995u_0$$

(b) Identify the matrix A such that $\mathbf{x}_1 = A\mathbf{x}_0$.

One we have the equation $\mathbf{x}_1 = A\mathbf{x}_0$, we can extend it to subsequent years:

$$\mathbf{x}_2 = A\mathbf{x}_1, \quad \mathbf{x}_3 = A\mathbf{x}_2, \quad ,..., \quad \mathbf{x}_{n+1} = A\mathbf{x}_n$$

for each $n \geq 0$.

This example illustrates the general nature of what is called a *Markov process* (see Definition 9.4). Recall that the matrix A that provides the link from one generation to the next is called the transition matrix.

In situations like these, we are interested in determining if there is a steady-state vector, that is a vector that satisfies

$$\mathbf{x} = A\mathbf{x}. \tag{14.10}$$

Such a vector would show us the long-term population of Michigan provided the population dynamics do not change.

Project Activity 14.2.

(a) Explain why a steady-state solution to (14.10) is an eigenvector of A. What is the corresponding eigenvalue?

(b) Consider again the transition matrix A from Project Activity 14.1. Recall that the solutions to equation (14.10) are all the vectors in Nul $(A - I_2)$. In other words, the eigenvectors of A for this eigenvalue are the nonzero vectors in Nul $(A - I_2)$. Find a basis for the eigenspace of A corresponding to this eigenvalue. Use whatever technology is appropriate.

(c) Once we know a basis for the eigenspace of the transition matrix A, we can use it to estimate the steady-state population of Michigan (assuming the stated migration trends are valid long-term). According to the US Census Bureau[2], the resident US population on December 1, 2019 was 330,073,471. Assuming no population growth in the U.S., what would the long-term population of Michigan be? How realistic do you think this is?

[2] https://www.census.gov/data/tables/time-series/demo/popest/2010s-national-total.html

Section 15

Bases and Dimension

Focus Questions

By the end of this section, you should be able to give precise and thorough answers to the questions listed below. You may want to keep these questions in mind to focus your thoughts as you complete the section.

- What is the dimension of a subspace of $\mathbb{R}^n$? What property of bases makes the dimension a well-defined number?
- If W is a subspace of $\mathbb{R}^n$ with dimension k, what must be true about any linearly independent subset S of W that contains exactly k vectors?
- If W is a subspace of $\mathbb{R}^n$ with dimension k, what must be true about any subset S of W that contains exactly k vectors and spans W?
- What is the rank of a matrix?
- What does the Rank-Nullity Theorem say?

Application: Lattice Based Cryptography

When you use your credit card, you expect that the information that is transmitted is protected so others can't use your card. Similarly, when you create a password for your computer or other devices, you do so with the intention that it will be difficult for others to decipher.

Cryptology is the study of methods to maintain secure communication in the presence of other parties (cryptography), along with the study of breaking codes (cryptanalysis). In essence, cryptology is the art of keeping and breaking secrets. The creation of secure codes (cryptography) can provide confidentiality (ensure that information is available only to the intended recipients), data integrity (prevent data from being altered between the sender and recipient), and authentication (making sure that the information is from the correct source).

Modern cryptology uses mathematical theory that can be implemented with computer hardware and algorithms. The security of public key sytems is largely based on mathematical problems that

are very difficult to solve. For example, the security of the RSA system relies on the fact that it is computationally difficult to find prime factors of very large numbers, and elliptic curve cryptography relies on the difficulty of the discrete logarithm problem for elliptic curves. However, the continual increase in the power of computers threatens the security of these systems, and so cryptographic systems have to keep adapting to the newest technology. For example, Shor's Algorithm (which could run on a quantum computer) can solve the public key cryptographic systems that rely on the integer factorization problem or the discrete logarithm problem. So if a working quantum computer was ever developed, it would threaten the existing cryptographic systems. Lattice-based cryptography is a potential source of systems that may be secure even in such an environment. The security of these systems is dependent on the fact that the average case of the difficulty of certain problems in lattice theory is higher than the worst case problems that underpin current cryptosystems. As we will see later in this section, lattices are built on bases for subspace of $\mathbb{R}^n$.

Introduction

A basis provides a system in which we can uniquely represent every vector in the space we are considering. More specifically, every vector in the space can be expressed as a linear combination of the vectors in the basis in a unique way. In order to be able to cover every point in the space, the basis has to span the space. In order to be able to provide a unique coordinate for each point, there should not be any extra vectors in the basis, which is achieved by linear independence of the vectors. For practical reasons, a basis simplifies many problems because we only need to solve the problem for each of the basis vectors. Solutions of the other cases usually follow because every vector in the space can be expressed as a unique linear combination of the basis vectors.

Recall that a basis for a subspace W of $\mathbb{R}^n$ is a set of vectors which are linearly independent and which span W.

Preview Activity 15.1.

(1) For each of the following sets of vectors, determine whether the vectors form a basis of $\mathbb{R}^3$. Use any appropriate technology for your computations.

(a) $\left\{ \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix} \right\}$

(b) $\left\{ \begin{bmatrix} 1 \\ 0 \\ 1 \end{bmatrix}, \begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 2 \\ 3 \\ 1 \end{bmatrix} \right\}$

(c) $\left\{ \begin{bmatrix} 1 \\ 0 \\ 1 \end{bmatrix}, \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix}, \begin{bmatrix} 0 \\ 3 \\ 3 \end{bmatrix}, \begin{bmatrix} -1 \\ 2 \\ 1 \end{bmatrix} \right\}$

(d) $\left\{ \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix} \right\}$

(2) In problem (1) we should have noticed that a space can have more than one basis, but that any two bases contain the same number of elements. This is a critically important idea that we

investigate in more detail in this problem in one specific case. Assume that W is a subspace of $\mathbb{R}^n$ that has a basis $\mathcal{B} = \{\mathbf{v}_1, \mathbf{v}_2\}$ with two basis vectors. We want to see if any other basis for W can have a different number of elements. Let us now consider a set $U = \{\mathbf{u}_1, \mathbf{u}_2, \mathbf{u}_3\}$ of three vectors in W. Our goal is to determine if U can be a basis for W. Since $\mathcal{B}$ is a basis for W, any vector in W can be written as a linear combination of the vectors in $\mathcal{B}$. So we can write

$$\mathbf{u}_1 = a_{11}\mathbf{v}_1 + a_{21}\mathbf{v}_2 \tag{15.1}$$

$$\mathbf{u}_2 = a_{12}\mathbf{v}_1 + a_{22}\mathbf{v}_2 \tag{15.2}$$

$$\mathbf{u}_3 = a_{13}\mathbf{v}_1 + a_{23}\mathbf{v}_2 \tag{15.3}$$

for some scalars a_{ij}. If U were to be a basis for W, then U would have to be a linearly independent set. To determine the independence or dependence of U we consider the vector equation

$$x_1\mathbf{u}_1 + x_2\mathbf{u}_2 + x_3\mathbf{u}_3 = \mathbf{0} \tag{15.4}$$

for scalars x_1, x_2, and x_3.

(a) Substitute for $\mathbf{u}_1$, $\mathbf{u}_2$, and $\mathbf{u}_3$ from (15.1), (15.2), and (15.3) into (15.4) and perform some vector algebra to show that

$$\mathbf{0} = (a_{11}x_1 + a_{12}x_2 + a_{13}x_3)\,\mathbf{v}_1 + (a_{21}x_1 + a_{22}x_2 + a_{23}x_3)\,\mathbf{v}_2. \tag{15.5}$$

(b) Recall that $\mathcal{B} = \{\mathbf{v}_1, \mathbf{v}_2\}$ is a basis. What does that tell us about the weights in the linear combination (15.5)? Explain why $A\mathbf{x} = \mathbf{0}$, where $A = [a_{ij}]$ and $\mathbf{x} = [x_1\ x_2\ x_3]^\mathsf{T}$.

(c) With A as in part (b), how many solutions does the system $A\mathbf{x} = \mathbf{0}$ have? Explain. (Hint: Consider the number of rows and columns of A.) What does this tell us about the independence or dependence of the set U? Why?

(d) Can U be a basis for W? Explain.

The Dimension of a Subspace of $\mathbb{R}^n$

In Preview Activity 15.1 we saw that a subspace of $\mathbb{R}^n$ can have more than one basis. This prompts the question of how, if at all, are any two bases for a given space related. More specifically, is it possible to have two bases for a given subspace of $\mathbb{R}^n$ that contain different numbers of vectors? As we will see the answer is no, which will lead us to the concept of *dimension*.

Let W be a subspace of $\mathbb{R}^n$ that has a basis $\mathcal{B} = \{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_k\}$ of k vectors. Since we have been calling bases minimal spanning sets, we should expect that any two bases for the same subspace have the same number of elements (otherwise one of the two bases would not be minimal). Our goal in this section is to prove that result – that any other basis of W contains exactly k vectors. The approach will be the same as was used in Preview Activity 15.1. We will let $U = \{\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_m\}$ be a set of vectors in W with $m > k$ and demonstrate that U is a linearly dependent set. To argue linear dependence, let x_1, x_2, …, x_m be scalars so that

$$x_1\mathbf{u}_1 + x_2\mathbf{u}_2 + \cdots + x_m\mathbf{u}_m = \mathbf{0}. \tag{15.6}$$

For each i there exist scalars a_{ij} so that

$$\mathbf{u}_i = a_{1i}\mathbf{v}_1 + a_{2i}\mathbf{v}_2 + \cdots + a_{ki}\mathbf{v}_k.$$

Substituting into (15.6) yields

$$\begin{aligned}\mathbf{0} &= x_1\mathbf{u}_1 + x_2\mathbf{u}_2 + \cdots + x_m\mathbf{u}_m \\ &= x_1(a_{11}\mathbf{v}_1 + a_{21}\mathbf{v}_2 + \cdots + a_{k1}\mathbf{v}_k) + x_2(a_{12}\mathbf{v}_1 + a_{22}\mathbf{v}_2 \\ &\qquad + \cdots + a_{k2}\mathbf{v}_k) + \cdots + x_m(a_{1m}\mathbf{v}_1 + a_{2m}\mathbf{v}_2 + \cdots + a_{km}\mathbf{v}_k) \\ &= (x_1a_{11} + x_2a_{12} + x_3a_{13} + \cdots + x_ma_{1m})\mathbf{v}_1 \\ &\qquad + (x_1a_{21} + x_2a_{22} + x_3a_{23} + \cdots + x_ma_{2m})\mathbf{v}_2 \\ &\qquad + \cdots + (x_1a_{k1} + x_2a_{k2} + x_3a_{k3} + \cdots + x_ma_{km})\mathbf{v}_k. \end{aligned} \tag{15.7}$$

Since $\mathcal{B}$ is a basis, the vectors $\mathbf{v}_1$, $\mathbf{v}_2$, ..., $\mathbf{v}_k$ are linearly independent. So each coefficient in (15.7) is 0 and $\mathbf{x} = [x_1\ x_2\ \cdots\ x_m]^\mathsf{T}$ is a solution to the homogeneous system $A\mathbf{x} = \mathbf{0}$, where $A = [a_{ij}]$. Now A is a $k \times m$ matrix with $m > k$, so not every column of A is a pivot column. This means that $A\mathbf{x} = \mathbf{0}$ has a nontrivial solution. It follows that the vector equation (15.6) has a nontrivial solution and so the m vectors $\mathbf{u}_1$, $\mathbf{u}_2$, ..., $\mathbf{u}_m$ are linearly dependent. We summarize this in the following theorem.

Theorem 15.1. *Let W be a subspace of $\mathbb{R}^n$ containing a basis with k vectors. If $m > k$, then any set of m vectors in W is linearly dependent.*

One consequence of Theorem 15.1 is that, in addition to being a minimal spanning set, a basis is also a maximal linearly independent set.

Activity 15.1. Now let's return to the question of the number of elements in a basis for a subspace of $\mathbb{R}^n$. Recall that we are assuming that W has a basis $\mathcal{B} = \{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_k\}$ of k vectors in $\mathbb{R}^n$. Suppose that $\mathcal{B}'$ is another basis for W containing m vectors.

(a) Given the fact that $\mathcal{B}$ is a basis for W, what does Theorem 15.1 tell us about the relationship between m and k?

(b) Given the fact that $\mathcal{B}'$ is a basis for W, what does Theorem 15.1 tell us about the relationship between m and k?

(c) What do the results of (a) and (b) tell us about the relationship between m and k? What can we conclude about any basis for W?

The result of Activity 15.1 is summarized in the following theorem. Recall that the trivial space is the single element set $\{\mathbf{0}\}$.

Theorem 15.2. *If a nontrivial subspace W of $\mathbb{R}^n$ has a basis of k vectors, then every basis of W contains exactly k vectors.*

This last theorem states that the number of vectors in a basis for a subspace space is a well-defined number. In other words, the number of vectors in a basis is an *invariant* of the subspace. This important number is given a name.

Definition 15.3. The **dimension** of a subspace W of $\mathbb{R}^n$ is the number of vectors in a basis for W. The dimension of the trivial subspace $\{\mathbf{0}\}$ of $\mathbb{R}^n$ is defined to be 0.

We denote the dimension of a subspace W of $\mathbb{R}^n$ by $\dim(W)$. As we will see later, any two vector spaces of the same dimension are basically the same vector space. So the dimension of a vector space is an important number that essentially tells us all we need to know about the structure of the space.

Activity 15.2. Find the dimensions of each of the indicated subspaces of $\mathbb{R}^n$ for the appropriate n. Explain your method.

(a) Span $\left\{ \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 2 \\ 3 \\ 0 \end{bmatrix} \right\}$

(b) xy-plane in $\mathbb{R}^3$

(c) $\mathbb{R}^3$

(d) $\mathbb{R}^n$

Conditions for a Basis of a Subspace of $\mathbb{R}^n$

There are two items we need to confirm before we can state that a subset $\mathcal{B}$ of a subspace W of $\mathbb{R}^n$ is a basis for W: the set $\mathcal{B}$ must be linearly independent and span W. However, if we have the right number (namely, the dimension) of vectors in our set $\mathcal{B}$, then either one of these conditions will imply the other.

Activity 15.3. Let W be a subspace of $\mathbb{R}^n$ with $\dim(W) = k$. We know that every basis of W contains exactly k vectors.

(a) Suppose that S is a subset of W that contains k vectors and is linearly independent. In this part of the activity we will show that S must span W.

i. Suppose that S does not span W. Explain why this implies that W contains a set of $k + 1$ linearly independent vectors.

ii. Explain why the result of part i. tells us that S is a basis for W.

(b) Now suppose that S is a subset of W with k vectors that spans W. In this part of the activity we will show that S must be linearly independent.

i. Suppose that S is not linearly independent. Explain why we can then find a proper subset of S that is linearly independent but has the same span as S.

ii. Explain why the result of part i. tells us that S is a basis for W.

The result of Activity 15.3 is the following important theorem.

Theorem 15.4. *Let W be a subspace of $\mathbb{R}^n$ of dimension k and let S be a subset of W containing exactly k vectors.*

(1) If S is linearly independent, then S is a basis for W.

(2) If S spans W, then S is a basis for W.

Finding a Basis for a Subspace

Since every vector in a subspace of $\mathbb{R}^n$ can be written uniquely as a linear combination of vectors in a basis for the subspace, a basis provides us with the most efficient and convenient way to represent vectors in the subspace. Until now we have been given a set of vectors and have been asked to find a basis from that set, so an important question to address is how we can find a basis for a subspace W of $\mathbb{R}^n$ starting from scratch. Here is one way. If $W = \{\mathbf{0}\}$, then the dimension of W is 0 and W has no basis. So suppose $\dim(W) > 0$. Start by choosing any nonzero vector $\mathbf{w}_1$ in W. Let $\mathcal{B}_1 = \{\mathbf{w}_1\}$. If $\mathcal{B}_1$ spans W, then $\mathcal{B}_1$ is a basis for W. If not, there is a vector $\mathbf{w}_2$ in W that is not in Span$(\mathcal{B}_1)$. Then $\mathcal{B}_2 = \{\mathbf{w}_1, \mathbf{w}_2\}$ is a linearly independent set. If Span$(\mathcal{B}_2) = W$, then $\mathcal{B}_2$ is a basis for W and we are done. If not, repeat the process. Since any basis for W can contain at most $n = \dim(\mathbb{R}^n)$ vectors, we know the process must stop at some point. This process also allows us to construct a basis for a vector space that contains a given nonzero vector.

Activity 15.4. Find a basis for $\mathbb{R}^3$ that contains the vector $\begin{bmatrix} 1 \\ 2 \\ -1 \end{bmatrix}$. When constructing your basis, how do you know when to stop?

Rank of a Matrix

In this section, we define the rank of a matrix and review conditions to add to our Invertible Matrix Theorem.

Activity 15.5. Let $A = \begin{bmatrix} 1 & 2 & -1 & 0 & 0 \\ 0 & 0 & 1 & 0 & -1 \\ 0 & 0 & 0 & 1 & 1 \end{bmatrix}$.

(a) Without performing any calculations, find $\dim(\text{Nul } A)$. Explain.

(b) Without performing any calculations, find $\dim(\text{Col } A)$. Explain.

(c) There is a connection between $\dim(\text{Nul } A)$, $\dim(\text{Col } A)$ and the size of A. Find this connection and explain it.

As Activity 15.5 illustrates, the number of vectors in a basis for Nul A is the number of non-pivot columns in A and the number of vectors in a basis for Col A is the number of pivot columns of A. We define the *rank* of a matrix A (denoted rank(A)) to be the dimension of Col A and the *nullity* of A to be dimension of Nul A. The dimension of the null space of A is also called the *nullity* of A (denoted nullity(A)) Using this terminology we have the Rank-Nullity Theorem.

Theorem 15.5 (The Rank-Nullity Theorem)**.** *Let A be an $m \times n$ matrix. Then*

$$\textit{rank}(A) + \textit{nullity}(A) = n.$$

There is also a row space of a matrix A, which we define to be the span of the rows of A. We can find the row space of A by finding the column space of A^{T}, so the row space is really nothing new. As it turns out, the dimension of the row space of A is always equal to the dimension of the column space of A, and justification for this statement is in the exercises.

The Rank-Nullity Theorem allows us to add extra conditions to the Invertible Matrix Theorem.

Theorem 15.6 (The Invertible Matrix Theorem)**.** *Let A be an $n \times n$ matrix. The following statements are equivalent.*

(a) The matrix A is an invertible matrix.

(b) The matrix equation $A\mathbf{x} = \mathbf{0}$ has only the trivial solution.

(c) The matrix A has n pivot columns.

(d) Every row of A contains a pivot.

(e) The columns of A span $\mathbb{R}^n$.

(f) The matrix A is row equivalent to the identity matrix I_n.

(g) The columns of A are linearly independent.

(h) The columns of A form a basis for $\mathbb{R}^n$.

(i) The matrix transformation T from $\mathbb{R}^n$ to $\mathbb{R}^n$ defined by $T(\mathbf{x}) = A\mathbf{x}$ is one-to-one.

(j) The matrix equation $A\mathbf{x} = \mathbf{b}$ has exactly one solution for each vector $\mathbf{b}$ in $\mathbb{R}^n$.

(k) The matrix transformation T from $\mathbb{R}^n$ to $\mathbb{R}^n$ defined by $T(\mathbf{x}) = A\mathbf{x}$ is onto.

(l) There is an $n \times n$ matrix C so that $AC = I_n$.

(m) There is an $n \times n$ matrix D so that $DA = I_n$.

(n) The scalar 0 is not an eigenvalue of A.

(o) The matrix A^{T} is invertible.

(p) Nul $A = \{\mathbf{0}\}$.

(q) Col $A = \mathbb{R}^n$.

(r) $\dim(\text{Col } A) = n$

(s) $\dim(\text{Nul } A) = 0$

(t) $\text{rank}(A) = n$

Examples

What follows are worked examples that use the concepts from this section.

Example 15.7. Let $W = \left\{ \begin{bmatrix} r+s+u \\ r+3s+2t-u \\ -s-t+u \\ s+t-u \end{bmatrix} : r,s,t,u \in \mathbb{R} \right\}$.

(a) Explain why W is a subspace of $\mathbb{R}^4$.

(b) Find a basis for W and determine the dimension of W.

Example Solution.

(a) We can write any vector in W in the form

$$\begin{bmatrix} r+s+u \\ r+3s+2t-u \\ -s-t+u \\ s+t-u \end{bmatrix} = r\begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \end{bmatrix} + s\begin{bmatrix} 1 \\ 3 \\ -1 \\ 1 \end{bmatrix} + t\begin{bmatrix} 0 \\ 2 \\ -1 \\ 1 \end{bmatrix} + u\begin{bmatrix} 1 \\ -1 \\ 1 \\ -1 \end{bmatrix},$$

so

$$W = \text{Span}\left\{ \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 1 \\ 3 \\ -1 \\ 1 \end{bmatrix}, \begin{bmatrix} 0 \\ 2 \\ -1 \\ 1 \end{bmatrix}, \begin{bmatrix} 1 \\ -1 \\ 1 \\ -1 \end{bmatrix} \right\}.$$

As a span of a set of vectors in $\mathbb{R}^4$, W is a subspace of $\mathbb{R}^4$.

(b) Let $A = \begin{bmatrix} 1 & 1 & 0 & 1 \\ 1 & 3 & 2 & -1 \\ 0 & -1 & -1 & 1 \\ 0 & 1 & 1 & -1 \end{bmatrix}$. To find a basis for W, we note that the reduced row echelon form of A is $\begin{bmatrix} 1 & 0 & -1 & 2 \\ 0 & 1 & 1 & -1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$. Since the pivot columns of A form a basis for Col $A = W$, we conclude that

$$\left\{ \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 1 \\ 3 \\ -1 \\ 1 \end{bmatrix} \right\}$$

is a basis for W. Therefore, $\dim(W) = 2$.

Example 15.8. Find a basis and the dimension of the solution set to the system

$$\begin{aligned} r+ \ \ s- \ \ t+2u &= 0 \\ 3r- \ \ s+2t- \ \ u &= 0 \\ r-3s+4t-5u &= 0 \\ 5r-3s+5t-4u &= 0. \end{aligned}$$

Example Solution.

The coefficient matrix of this system is

$$A = \begin{bmatrix} 1 & 1 & -1 & 2 \\ 3 & -1 & 2 & -1 \\ 1 & -3 & 4 & -5 \\ 5 & -3 & 5 & -4 \end{bmatrix},$$

and the solution set to the system is Nul A. To find a basis for Nul A we row reduce A to

$$\begin{bmatrix} 1 & 0 & \frac{1}{4} & \frac{1}{4} \\ 0 & 1 & -\frac{5}{4} & \frac{7}{4} \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}.$$

The general solution to the system has the form

$$\begin{bmatrix} r \\ s \\ t \\ u \end{bmatrix} = \begin{bmatrix} -\frac{1}{4}t - \frac{1}{4}u \\ \frac{5}{4}t - \frac{7}{4}u \\ t \\ u \end{bmatrix} = t \begin{bmatrix} -\frac{1}{4} \\ \frac{5}{4} \\ 1 \\ 0 \end{bmatrix} + u \begin{bmatrix} -\frac{1}{4} \\ -\frac{7}{4} \\ 0 \\ 1 \end{bmatrix},$$

so $\left\{ \begin{bmatrix} -\frac{1}{4} \\ \frac{5}{4} \\ 1 \\ 0 \end{bmatrix}, \begin{bmatrix} -\frac{1}{4} \\ -\frac{7}{4} \\ 0 \\ 1 \end{bmatrix} \right\}$ is a basis for Nul A and $\dim(\text{Nul } A) = 2$.

Summary

The key idea in this section is the *dimension* of a vector space.

- Any two bases for a vector space *must* contain the same number of vectors. Therefore, we can define the *dimension* of a vector space W to be the number of vectors in any basis for W.
- If W is a subspace of $\mathbb{R}^n$ with dimension k and S is any linearly independent subset of W with k vectors, then S is a basis for W.
- If W is a subspace of $\mathbb{R}^n$ with dimension k and S is any subset of W with k vectors that spans W, then S is a basis for W.
- The rank of a matrix is the dimension of its column space.
- The Rank-Nullity Theorem states that if A is an $m \times n$ matrix, then $\text{rank}(A) + \text{nullity}(A) = n$.

Exercises

(1) Let $A = \begin{bmatrix} 1 & 3 & 1 & 2 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 2 & 6 & 0 & 0 & 1 \\ 1 & 3 & 2 & 4 & 1 \\ 3 & 9 & 1 & 2 & -1 \\ 3 & 9 & 3 & 6 & 1 \end{bmatrix}$.

(a) Find a basis for Col A. What is the dimension of Col A? What, then, is the dimension of Nul A?

(b) Find a basis for Nul A and verify the dimension you found in part (a).

(2) Let $A = \begin{bmatrix} 2 & -1 & 1 \\ 1 & 0 & 1 \\ 1 & -1 & 2 \end{bmatrix}$. The eigenvalues of A are 1 and 2. Find the dimension of each eigenspace of A.

(3) Let $A = \begin{bmatrix} 1 & 2 & -1 & -1 \\ -2 & -4 & 2 & 2 \\ 1 & 2 & -1 & -1 \end{bmatrix}$.

(a) Find a basis for Col A. What is the rank of A?

(b) Find a basis for Nul A. What is the nullity of A.

(c) Verify the Rank-Nullity Theorem for A.

(d) The row space of A is the span of the rows of A. Find a basis for the row space of A and the dimension of the row space of A.

(4) Let A be an $m \times n$ matrix with r pivots, where r is less than or equal to both m, n. Fill in the blanks.

(a) The null space of A is a subspace of _____.

(b) The column space of A is a subspace of _____.

(c) Suppose $r = m$. Then there is a pivot in every _____ and Col $A =$ _____.

(d) Suppose $r = n$. Then there is a pivot in every _____ and Nul $A =$_____.

(e) If A has 3 pivots, then the rank of A is _____.

(f) If A has 3 pivots, then the number of free variables in the system $A\mathbf{x} = \mathbf{0}$ is _____.

(g) The dimension of Col A is equal to the number of _____, i.e. $\dim$ Col $A =$_____.

(h) The dimension of Nul A is equal to the number of _____, i.e. $\dim$ Nul $A =$_____.

(i) $\dim(\text{Nul } A) + \dim(\text{Col } A) =$ _____.

(j) Suppose the columns of A span $\mathbb{R}^m$. Then rank A is _____.

(k) Suppose the columns of A are linearly independent. Then $r =$ _____ and the dimension of Nul A is _____.

(5) Prove the remaining parts of the Invertible Matrix Theorem (Theorem 15.6). Let A be an $n \times n$ matrix.

(a) Prove that A is invertible if and only if $\dim(\text{Nul } A) = 0$.

(b) Prove that A is invertible if and only if $\dim(\text{Col } A) = n$.

(6) We can convert the language of the Rank-Nullity Theorem to matrix transformation language, as we show in this exercise. Let T be the matrix transformation defined by the matrix A.

(a) How is the kernel of T related to A?

(b) How is the range of T related to A?

(c) How is the domain of T related to A?

(d) Explain why the Rank-Nullity Theorem says that $\dim(\text{Ker}(T)) + \dim(\text{Range}(T)) = \dim(\text{Domain}(T))$.

(7) Let W be a subspace of $\mathbb{R}^4$. What are possible values for the dimension of W? Explain. What are the geometric descriptions of W in each case?

(8) Is it possible to find two subspaces W_1 and W_2 in $\mathbb{R}^3$ such that $W_1 \cap W_2 = \{\mathbf{0}\}$ and $\dim W_1 = \dim W_2 = 2$? If possible, give an example and justify that they satisfy the conditions. If not possible, explain why not. (Hint: Dimension two leads to two linearly independent vectors in each of W_i.)

(9) Determine the dimensions of the column space and null space of $\begin{bmatrix} 1 & 2 & 4 & 3 & 2 \\ 1 & 0 & 2 & 1 & 4 \\ 1 & 1 & 3 & 1 & 2 \\ 1 & 0 & 2 & 2 & 5 \end{bmatrix}$.

(10) If possible, find a 3×4 matrix whose column space has dimension 3 and null space has dimension 1. Explain how you found the matrix in addition to explaining why your answer works. If not possible, explain why it is not possible to find such a matrix.

(11)

(a) If possible, find a 5×5 matrix whose column space has the same dimension as its null space. Explain how you found the matrix in addition to explaining why your answer works. If not possible, explain why it is not possible to find such a matrix.

(b) If possible, find a matrix A so that Col $A =$ Nul A. Explain how you found the matrix in addition to explaining why your answer works. If not possible, explain why it is not possible to find such a matrix.

(12) In this exercise we examine why the dimension of a row space of a matrix is the same as the dimension of the column space of the matrix. Let A be an $m \times n$ matrix.

(a) Explain why row operations do not change the row space of a matrix. Then explain why if R is the reduced row echelon form of A, then Row R = Row A, where Row M is the row space of the matrix M.

(b) Explain why the rows of R that contain pivots form a basis for Row R, and also of Row A.

(c) Explain why rank(A) is the number of pivots in the matrix A. Then explain why $\dim(\text{Row } A) = \dim(\text{Col } A)$.

(13) Label each of the following statements as True or False. Provide justification for your response.

(a) **True/False** The dimension of the column space of a 3×2 matrix can be three.

(b) **True/False** There exists a 3×3 matrix whose column space has equal dimension as the null space.

(c) **True/False** If a set of vectors spans a subspace, then that set is a basis of this subspace.

(d) **True/False** If a linearly independent set of vectors spans a subspace, then that set is a basis of this subspace.

(e) **True/False** The dimension of a space is the minimum number of vectors needed to span that space.

(f) **True/False** The dimension of the null space of a 3×2 matrix can at most be 2.

(g) **True/False** Any basis of $\mathbb{R}^4$ contains 4 vectors.

(h) **True/False** If n vectors span $\mathbb{R}^n$, then these vectors form a basis of $\mathbb{R}^n$.

(i) **True/False** Every line in $\mathbb{R}^n$ is a one-dimensional subspace of $\mathbb{R}^n$.

(j) **True/False** Every plane through origin in $\mathbb{R}^n$ is a two-dimensional subspace of $\mathbb{R}^n$.

(k) **True/False** In $\mathbb{R}^n$ any n linearly independent vectors form a basis.

Project: The GGH Cryptosystem

A cryptographic system (or cryptosystem) allows for secure communication between two or more parties. These systems take messages (called *plaintext*) and encrypt them in some way to produce what is called *ciphertext*. This is the scrambled information that is transmitted to the receiver, from which it should not be possible for someone who does not have the proper key to recover the original message. When the message is received by the intended recipient, it must be unscrambled or *decrypted*. Decryption is the process of converting ciphertext back to plaintext.

The Goldreich-Goldwasser-Halevi (GGH) public key cryptosystem[1] uses lattices to encrypt plaintext. The security of the system depends on the fact that the Closest Vector Problem (CVP) is, in general, a very hard problem. To begin to understand these cryptosystems, we begin with lattices.

[1] Published in 1997 by Oded Goldreich, Shafi Goldwasser, and Shai Halevi.

Lattices are closely related to spans of sets of vectors in $\mathbb{R}^n$. If we start with a linearly independent set $S = \{\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_m\}$ in $\mathbb{R}^n$, we can create the span of S – the set of all linear combinations

$$c_1\mathbf{b}_1 + c_2\mathbf{b}_2 + \cdots + c_m\mathbf{b}_m,$$

where c_1, c_2, …, c_m are real numbers. This span creates a subspace of $\mathbb{R}^n$. If we restrict the set from which we choose the coefficients, we can create different types of structures. An important one is a lattice. The *lattice* $\mathcal{L}(S)$ defined by the linearly independent set $S = \{\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_m\}$ is the set of linear combinations

$$c_1\mathbf{b}_1 + c_2\mathbf{b}_2 + \cdots + c_m\mathbf{b}_m,$$

where c_1, c_2, …, c_m are integers. If the vectors in S have integer components, then every point in $\mathcal{L}(S)$ will have integer entries. In these cases, $\mathcal{L}(S)$ is a subset of $\mathbb{Z}^n$, as illustrated in Figure 15.1. Also, if $m = n$ we say that the lattice $\mathcal{L}(S)$ is *full-rank*. We will restrict ourselves to full-rank lattices in this project. A *basis* for a lattice is any set of linearly independent vectors that generates the lattice. There is a little special notation that is often used with lattices. If $\mathcal{B} = \{\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_n\}$ is a basis for $\mathbb{R}^n$, we associate to $\mathcal{B}$ the matrix $B = [\mathbf{b}_1\ \mathbf{b}_2\ \mathbf{b}_3\ \cdots\ \mathbf{b}_n]$. We then use the notation $\mathcal{L}(B)$ to also refer to the lattice defined by $\mathcal{B}$.

Project Activity 15.1. We explore lattices in more detail in this activity.

(a) Let $S_1 = \{[1\ 1]^\mathsf{T}, [-1\ 1]^\mathsf{T}\}$.

i. Find five distinct vectors in $\mathcal{L}(S_1)$.

ii. Is the vector $[1\ 0]^\mathsf{T}$ in $\mathcal{L}(S_1)$? Justify your answer.

iii. We can draw pictures of lattices by plotting the terminal points of the lattice vectors. Draw all of the lattice points in $\mathcal{L}(S_1)$ on the square with vertices $(-4, -4)$, $(4, -4)$, $(4, 4)$, and $(-4, 4)$.

(b) Now let $S_2 = \{[3\ 5]^\mathsf{T}, [1\ 2]^\mathsf{T}\}$. A picture of $\mathcal{L}(S_2)$ is shown in Figure 15.1 with the basis vectors highlighted. As we have seen, $\mathcal{L}(S_1)$ is not the entire space $\mathbb{Z}^2$. Is $\mathcal{L}(S_2) = \mathbb{Z}^2$? Justify your answer.

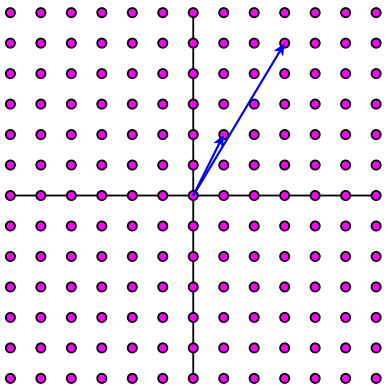


Figure 15.1: The lattice $\mathcal{L}(S_2)$.

Project Activity 15.1 shows that even if $\mathcal{B}$ is a basis for $\mathbb{R}^n$, it does not follow that $\mathcal{L}(\mathcal{B})$ is all of $\mathbb{Z}^n$. So latices can be complicated, and problems in lattice theory can be very difficult.

The GGH cryptosystem relies on the fact that we can convert "good" bases for lattices into "bad" bases. We will not delve into the details of what separates a "good" basis from a "bad" one, but suffice it to say that a good basis is one in which the basis vectors are close to being perpendicular[2] and are all short (that is, they have small norms), while any other basis is a bad basis. An example of a good basis is the basis S_1 for $\mathbb{R}^2$ in Project Activity 15.1, and we will see later that $\{[-2\ 8]^\mathsf{T}, [-1\ 3]^\mathsf{T}\}$ is a bad basis for the same lattice. You should draw a picture of the vectors $[-2\ 8]^\mathsf{T}$ and $[-1\ 3]^\mathsf{T}$ to convince yourself that this is a bad basis for its lattice.

The GGH cryptosystem works with two *keys* – a public key and a private key. The keys are based on lattices. The general process of the GGH cryptosystem is as follows. Begin with a good basis $\mathcal{B} = \{\mathbf{b}_1\ \mathbf{b}_2\ \ldots\ \mathbf{b}_n\}$ of $\mathbb{R}^n$ of vectors with integer components. Let $B = [\mathbf{b}_1\ \mathbf{b}_2\ \cdots\ \mathbf{b}_n]$ be the matrix associated with $\mathcal{B}$. Let $\mathcal{B}' = \{\mathbf{b}'_1, \mathbf{b}'_2, \ldots, \mathbf{b}'_n\}$ be a bad basis for which $\mathcal{L}(\mathcal{B}') = \mathcal{L}(\mathcal{B})$. Let $B' = [\mathbf{b}'_1\ \mathbf{b}'_2\ \cdots\ \mathbf{b}'_n]$ be the matrix associated to the basis $\mathcal{B}'$. The bad basis can be shared with anyone (the public key), but the good basis is kept secret (the private key). Start with a message $\mathbf{m} = [m_1\ m_2\ \cdots\ m_n]^\mathsf{T}$ with integer entries to send.

First we encrypt the message, which can be done by anyone who has the public key $\mathcal{B}'$.

- Create the message vector
$$\mathbf{m}' = m_1\mathbf{b}'_1 + m_2\mathbf{b}'_2 + \cdots + m_n\mathbf{b}'_n = B'\mathbf{m}$$
that is in the lattice using the bad basis $\mathcal{B}'$.
- Choose a small error $\mathbf{e}$ to add to $\mathbf{m}'$ to move $\mathbf{m}'$ off the lattice (small enough so that $\mathbf{m}'$ does not pass by another lattice point). This is an important step that will make the message difficult to decrypt without the key. Let $\mathbf{c} = \mathbf{m}' + \mathbf{e} = B'\mathbf{m} + \mathbf{e}$. The vector $\mathbf{c}$ is the ciphertext that is to be transmitted to the receiver.

Only someone who knows the basis $\mathcal{B}$ can decode the ciphertext. This is done as follows.

- Find the vector $\mathbf{a} = a_1\mathbf{b}_1 + a_2\mathbf{b}_2 + \cdots + a_n\mathbf{b}_n$ in the good basis $\mathcal{B}$ that is closest to $\mathbf{c}$.
- We interpret the vector $[a_1\ a_2\ \ldots\ a_n]^\mathsf{T}$ as being the encoded vector without the error. So to recreate the original message vector we need to undo the encrypting using the bad basis $\mathcal{B}'$. That is, we need to find the weights $y_1, y_2, \ldots, y_n$ such that
$$[a_1\ a_2\ \ldots\ a_n]^\mathsf{T} = y_1\mathbf{b}'_1 + y_2\mathbf{b}'_2 + \cdots + y_n\mathbf{b}'_n = B'[y_1\ y_2\ \cdots\ y_n]^\mathsf{T}.$$
We can do this by as $[y_1\ y_2\ \cdots\ y_n]^\mathsf{T} = B'^{-1}[a_1\ a_2\ \ldots\ a_n]^\mathsf{T}$.

There are several items to address before we can implement this algorithm. One is how we create a bad basis $\mathcal{B}'$ from $\mathcal{B}$ that produces the same lattice. Another is how we find the vector in $\mathcal{B}$ closest to a given vector. The latter problem is called the Closest Vector Problem (CVP) and is, in general, a very difficult problem. This is what makes lattice-based cryptosystems secure. We address the first of these items in the next activity, and the second a bit later.

[2]This is also a good property in vector spaces. We will see in a later section that perpendicular basis vectors make calculations in vector spaces relatively easy. A similar thing is true in lattices, where we are able to solve certain variants of closest vector problem very efficiently.

Project Activity 15.2. Consider again the basis $S_1 = \{[1\ 1]^\mathsf{T}, [-1\ 1]^\mathsf{T}\}$ from Project Activity 15.1, and let $B = \begin{bmatrix} 1 & -1 \\ 1 & 1 \end{bmatrix}$ be the matrix whose columns are the vectors in S_1.

(a) Let T be the triangle with vertices $(0, 0)$, $(1, 1)$, and $(-1, 1)$. Show that this triangle is a right triangle, and conclude that the vectors $\mathbf{v}_1 = [1\ 1]^\mathsf{T}$, and $\mathbf{v}_2 = [-1\ 1]^\mathsf{T}$ are perpendicular.

(b) Let $U = \begin{bmatrix} 3 & 1 \\ 5 & 2 \end{bmatrix}$. Let S_3 be the set whose vectors are the columns of the matrix B_1U. Show that $\mathcal{L}(S_1) = \mathcal{L}(S_3)$.

The two bases $S_1 = \{[1\ 1]^\mathsf{T}, [-1\ 1]^\mathsf{T}\}$ and $S_3 = \{[-2\ 8]^\mathsf{T}, [-1\ 3]^\mathsf{T}\}$ from Project Activity 15.2 are shown in Figure 15.2. This figure illustrates how the matrix U transforms the basis S_1, in which the vectors are perpendicular and short, to one in which the vectors are nearly parallel and significantly longer. So the matrix U converts the "good" basis S_1 into a "bad" basis S_2, keeping the lattice intact. This is a key idea in the GGH cryptosystem. What makes this work is the fact that both U and U^{-1} have integer entries. The reason for this is that, for a 2×2 matrix $U = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$, we know that $U^{-1} = \frac{1}{ad-bc}\begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$. If U has integer entries and $ad - bc = \pm 1$, then U^{-1} will also have integer entries. The number $ad - bc$ is called the *determinant* of U, and matrices with determinant of 1 or -1 are called *unimodular*. That what happened in Project Activity 15.2 happens in the general case is the focus of the next activity.

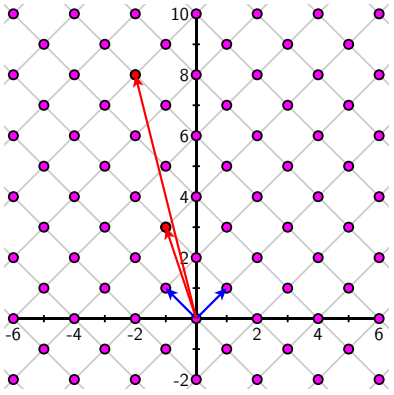


Figure 15.2: The lattices $\mathcal{L}(S_1)$ and $\mathcal{L}(S_3)$.

Project Activity 15.3. We will restrict ourselves to 2×2 matrices in this activity, but the results generalize to $n \times n$ matrices. Let $\mathcal{B} = \{\mathbf{b}_1, \mathbf{b}_2\}$ and $\mathcal{B}' = \{\mathbf{b}'_1, \mathbf{b}'_2\}$ be bases for $\mathbb{R}^2$ with integer entries, and let $B = [\mathbf{b}_1\ \mathbf{b}_2]$ and $B' = [\mathbf{b}'_1\ \mathbf{b}'_2]$ be the matrices associated to these bases. Show that if $B' = BU$ for some unimodular matrix U with integer entries, then $\mathcal{L}(B) = \mathcal{L}(B')$.

Project Activity 15.3 is the part we need for our lattice-based cryptosysystem. Although we won't show it here, the converse of the statement in Project Activity 15.3 is also true. That is, if $\mathcal{B}$ and $\mathcal{B}'$ generate the same lattice, then $B' = BU$ for some unimodular matrix U with integer entries.

There is one more item to address before we implement the GGH cryptosystem. That item is how to solve the Closest Vector Problem. There are some algorithms for approximating the closest vector in a basis. One is Babai's Closest Vector algorithm. This algorithm works in the following way. Consider a lattice with basis $\{\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_n\}$. To approximate the closest vector in the lattice to a vector $\mathbf{w}$, find the weights c_1, c_2, ..., c_n in $\mathbb{R}$ such that $\mathbf{w} = c_1\mathbf{b}_1 + c_2\mathbf{b}_2 + \cdots + c_n\mathbf{b}_n$. Then round the coefficients to the nearest integer. This algorithm works well for a good basis, but is unlikely to return a lattice point that is close to $\mathbf{w}$ if the basis is a bad one.

Now we put this all together to illustrate the GGH algorithm.

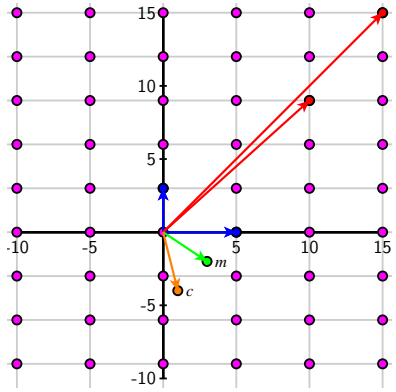


Figure 15.3: Decrypting an encrypted message.

Project Activity 15.4. Let $\mathcal{B} = \{[5\ 0]^\mathsf{T}, [0\ 3]^\mathsf{T}\}$ be the private key, and let $B = \begin{bmatrix} 5 & 0 \\ 0 & 3 \end{bmatrix}$ be the matrix whose columns are the vectors in $\mathcal{B}$. Let U be the unimodular matrix $U = \begin{bmatrix} 2 & 3 \\ 3 & 5 \end{bmatrix}$. Let $\mathbf{m} = [3\ -2]^\mathsf{T}$ be our message and let $\mathbf{e} = [1\ -1]^\mathsf{T}$ be our error vector.

(a) Use the unimodular matrix U to create the bad basis $\mathcal{B}'$.

(b) Determine the ciphertext message $\mathbf{c}$.

(c) A picture of the message vector $\mathbf{m}$ and the ciphertext vector $\mathbf{c}$ are shown in Figure 15.3. Although the closest vector in the lattice to $\mathbf{c}$ can be determined by the figure, actual messages are constructed in high dimensional spaces where a visual approach is not practical. Use Babai's algorithm to find the vector in $\mathcal{L}(\mathcal{B})$ that is closest to $\mathbf{c}$ and compare to Figure 15.3.

(d) The final step in the GGH scheme is to recover the original message. Complete the GGH algorithm to find this message.

(e) The GGH cryptosystem works because the CVP can be reasonable solved using a good basis. That is, Babai's algorithm works if our basis is a good basis. To illustrate that a bad basis will not allow us to reproduce the original message vector, show that Babai's algorithm does not return the closest vector to $\mathbf{c}$ using the bad basis $\mathcal{B}'$.