Department of Mathematics and Applied Mathematics

University of Cape Town

Linear Algebra

(MAM2000W Module 2LA)

Written by John Frith and Anneliese Schauerte
Revised version by Jurie Conradie

2022

Contents

Introduction

The term *linear algebra* may be new to you. The name suggests that it is a form of algebra, and that it may have something to do with lines. This is not so far off the mark. One may well think of linear algebra as the algebra of mathematical objects that in some way resemble the expressions we use to describe straight lines in the plane. You may remember that the vector equation of a line uses vector addition and scalar multiplication. It is exactly these two operations that characterize linear algebra. What is new is that we do not necessarily confine ourselves to lines we can visualise, but also look at objects that can be described in the same way in higher dimensions.

You've already had a taste of linear algebra in your first-year course in Mathematics when you looked at systems of linear equations and matrices. We'll be looking in a more detailed way at the same topics, but will take the subject much further. At the same time the descriptions of lines and planes in terms of vectors you saw in the first year will provide some geometrical motivation for more abstract ideas we want to introduce.

Why do we spend so much time in second-year Mathematics on linear algebra, and make it a compulsory module as well? Here are some reasons:

- It seems to be a tradition all over the world for mathematics students to do a sizeable chunk of linear algebra at some stage in their career.
- Learning about linear algebra prepares the way for more abstract ideas covered in a course in abstract algebra.
- Doing linear algebra forces you to learn how to understand and do mathematical proofs.

While these reasons may satisfy mathematicians and perhaps even prospective mathematicians, many of you who simply want to *use* mathematics in some other field will not be convinced. The reasons above are certainly not sufficient to warrant making linear algebra such a large component of a second year course in mathematics. There is much more to the story. The fact is that linear algebra is an extremely useful subject which crops up (sometimes rather unexpectedly) in all sort of places and subjects. Here is a quote from a text book on linear algebra:

> “Linear algebra is an essential part of the mathematical equipment required in many areas of pure and applied mathematics, computing, the sciences and engineering.”

You can add to that list the areas of statistics, probability, economics, physics, ... So linear algebra is useful, and we’ll try to point out some of its applications as we go along.

On the other hand, this is a mathematics course and you won’t just get a list of applications and recipes for doing mysterious but useful things. To make sense of the subject and to get an understanding of how to use it we will need to get involved in mathematical objects that are more abstract than the ones you may be used to. Another way of saying this is that we are going to give you a somewhat different perspective on some mathematical objects you are already familiar with. You will have a new way of looking at things. Unfortunately this can be unnerving. Changing your point of view is always a bit of a challenge, but it can be well worth the effort. We will try to be explicit about when we are changing gear into a more abstract setting and will try to present examples which will help you to ease this change. But there is no getting away from it that this process will not always be easy, and that you will need some time to get used to driving in a new gear.

One of the problems about this new perspective is that it is going to involve us in some new theory, and getting involved in theory means having (at least sometimes) to *prove* things. In first-year Mathematics courses we were rather informal about proofs, and rightly so, on the whole. Serious proofs of some of the important facts about calculus can be extremely tricky, very lengthy and ultimately rather mystifying; the proofs sometimes don’t seem to illuminate the subject at all. With linear algebra, the situation is rather better. Most facts can be proved quite rigorously and the proofs themselves actually help improve your feel for the subject. We will still reserve the right to omit proofs if they don’t illuminate the subject or would take too long, but this will happen infrequently.

It’s time to look, in very general terms, at what we are we going to do. You may remember that matrices turned out to be extremely useful tools for dealing with systems of linear equations. It will therefore not come as too much of a surprise to hear that we will find ourselves concerned largely with the algebra of matrices. What is perhaps more surprising is that it is this algebra which gives one an insight into all sorts of different situations, as you will see in due course. In your first-year course you would have seen how to add and subtract matrices and multiply them by constants. These operations were quite straight-forward and presented no problems. Multiplying two matrices turned out to be a far more complicated matter, not even possible unless the matrices "matched up" correctly. Our focus will be largely on matrix multiplication. One of the important shifts in perspective you'll have to make is to start thinking of matrices as *functions*, and to think of matrix multiplication as function composition.

But how on earth can we spend an entire module just exploring matrix multiplication? To be quite honest, saying that we'll only look at matrix multiplication would perhaps be over-simplifying the course. But you will eventually notice that being able to factorize a matrix as a product of certain other special matrices ends up being extremely useful and the key to solving all sorts of problems. (Actually, for the more ambitious, this turns out to be a major theme of all mathematics.)

We end this introduction with a very brief description of what we are going to do. Here are the main themes:

Linear Equations and Matrices: In the first chapter we review some of the things you learnt about systems of linear equations, matrices and determinants in your first year, but also go further in each of these topics. We'll revisit matrix multiplication and learn how to factorize matrices using elementary matrices. This is a basic chapter which lays the foundation for things to come.He practiced law for 14 years, but all the time continued his mathematical research and published 250 papers during this time.

Vector Spaces: In this chapter we provide you with a new point of view and bring all sorts of different examples under one roof. Many fundamental concepts are met here which are needed over and over again in later chapters.

Linear Transformations: Here we look at rather special functions between vector spaces, and show how this provides a new way of looking at matrices.

Eigenvectors and Eigenvalues: The aim of this chapter is to show that a large class of square matrices can be factorized in a rather special and satisfactory way. This needs finding eigenvalues of matrices; solving this problem has vast numbers of applications. This is probably the most important chapter from many points of view.

Inner product spaces: In the last chapter we look at vector spaces with more geometrical structure, and show how important and useful a generalized notion of perpendicularity can be.

We conclude with a remark of a more practical nature. The matrices occurring in applications are often very large and doing calculations involving such matrices by hand are tedious, lengthy and prone to error. We'll adopt the following compromise: to illustrate the concepts occurring in this course we'll stick to small matrices and keep the calculations simple. (Such examples are sometimes referred to as "toy examples"!) We will give you information about the computer program **OCTAVE** which allows you to do all the computations you might ever want when it comes to matrices and vectors (and some you might never want!). It will simplify life dramatically and enable you to do real examples instead of somewhat artificially simplified ones. You will find instructions on how to get started in OCTAVE, as well as a list of useful operations you can perform with OCTAVE, in Appendix E. OCTAVE is an open source program, and can be downloaded for free at `https://www.gnu.org/software/octave/`. You can use OCTAVE to check the calculations you do by hand. Knowing how to use a program like OCTAVE is a very useful skill, but we will not be testing your knowledge of it in this course. The program **MATLAB** is quite similar to OCTAVE, but not free.

We'll also refer you to the web-based programme **Linear Algebra Toolkit** which allows you to follow certain basic operation with matrices step by step on the screen. You can find it at `http://www.math.odu.edu/~bogacki/lat/`.

You will need to be comfortable with some basic tools of mathematics in this course. Since you will be proving things, you will need to know something about basic logic. To describe collections of mathematical objects such as numbers, vectors and matrices it will be very useful to use the language of sets. We'll also need to be comfortable with the basic ideas about functions and relations. You'll find the basic facts about these ideas collected together in Appendix A to C, at the end of the notes. (Those of you who have already completed MAM1019H will be familiar with most of these ideas.) When we need them, we'll introduce them to you, illustrate their use with examples in linear algebra and leave you to read more about them in the appendix. You will find there more detail than you need to know about in this module, but all of it is useful material that you will need in other parts of mathematics as well.

Chapter 1

Systems of Equations, Matrices and Vectors

1.1 Some examples

In this introductory section we look at three examples of the way linear algebra can be used in modelling problems. In two of them we try to describe mathematically quantities that change with time. Although the mathematics looks quite different, we show that in all three cases rather similar questions arise, featuring linear equations, matrices and vectors. Although these questions are not difficult to formulate, it will take us a few chapters to develop the machinery that will enable us to answer them.

We will have much more to say about linear equations, vectors and matrices in the rest of this chapter, but for the moment here is a quick reminder of concepts you have already come across in your first year, and that you'll need to understand the examples.

Let m and n be positive integers.

- A *linear equation* in the variables $x_1, x_2, \ldots, x_n$ is an equation of the form

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

  where $a_1, a_2, \ldots, a_n, b$ are constants (the coefficients). A *solution* for such an equation is a set of values for the variables that make the equation true.

- A *matrix* is a rectangular array of numbers. If the array has m rows and n columns, we call it an $m \times n$ matrix.

- An *n-vector* is an $n \times 1$ matrix. (This is, strictly speaking, a column vector. Later we'll use row vectors as well.) Last year you worked mostly with 2-vectors and 3-vectors. In the second example below we'll use 4-vectors as well.

- A number of linear equations in the same variables is called a *system of linear equations*; such a system can be written in matrix form.

Example 1.1.1 In our first example we look at a rather simplified model of transport preferences for UCT students. You may (quite rightly) feel that the model is unrealistic. Try to shelve your criticism for the moment, because even this simplified model illustrates a number of very important ideas. Let's make the following assumptions about UCT students and their transport preferences:

- Ten thousand students have to get to the UCT campus every day; this number stays constant.

- At the start of each month, 20% of students who were using the Jammie Shuttle change to using their own transport and 10% of students using their own transport change to using the Jammie Shuttle.

- At the beginning of the first month of the academic year, 6000 students use the Jammie Shuttle.

We want to explore the way in which the transport preferences will change with time, and what the long term trend (if any) will be. Here are some questions we could ask:

(a) How many students used the Jammie Shuttle, and how many their own transport, at the beginning of the second month?

(b) Is there a specific number of students using the Jammie Shuttle that will result in no change in the number of students using the shuttle occurring from month to month?

(c) What will happen to the number of students using the Jammie Shuttle (given that our assumptions continue to hold) over the next (say) 10 months?

We try to answer these questions by first writing down the assumptions made in the form of equations. To do this, we need to introduce names for the variables. Let

- $x(n)$ be the number of students (in thousands) using the Jammie Shuttle at the beginning of month n.
- $y(n)$ be the number of students (in thousands) using their own transport at the beginning of month n.

This means that

$x(n+1)$ will be the number of students (in thousands) using the Jammie Shuttle at the beginning of month $n+1$.

$y(n+1)$ be the number of students (in thousands) using their own transport at the beginning of month $n+1$.

Of course, x and y are functions of time. We simplify matters somewhat by only looking at the populations once a month, at the beginning of each month, and not at intermediate times. The unit of time is 1 month; the variable n can only take on integer values. (In more technical language we could say that we are setting up a *discrete* model, rather than a *continuous* one.)

Using our assumptions we can write down the following equations:

$$\begin{aligned} x(n+1) &= 0.8x(n) + 0.1y(n) \\ y(n+1) &= 0.9y(n) + 0.2x(n) \end{aligned}$$

and of course

$$x(n) + y(n) = 10.$$

Using matrix notation we could rewrite the first two equations as:

$$\begin{pmatrix} 0.8 & 0.1 \\ 0.2 & 0.9 \end{pmatrix} \begin{pmatrix} x(n) \\ y(n) \end{pmatrix} = \begin{pmatrix} x(n+1) \\ y(n+1) \end{pmatrix}$$

We can now use this set of equations (a mathematical model) to answer the questions.

(a) At the beginning of month 2:

$$\begin{aligned} \begin{pmatrix} 0.8 & 0.1 \\ 0.2 & 0.9 \end{pmatrix} \begin{pmatrix} 6 \\ 4 \end{pmatrix} &= \begin{pmatrix} 4.8 + 0.4 \\ 1.2 + 3.6 \end{pmatrix} \\ &= \begin{pmatrix} 5.2 \\ 4.8 \end{pmatrix} \end{aligned}$$

so there will be 5200 students using the Jammie Shuttle and 4800 using their own transport.

(b) In this case we are looking for values of $x = x(n)$ and $y = y(n)$ such that

$$\begin{pmatrix} 0.8 & 0.1 \\ 0.2 & 0.9 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x \\ y \end{pmatrix}.$$

We can rewrite this as two equations:

$$\begin{aligned} x &= 0.8x + 0.1y \\ y &= 0.9y + 0.2x \end{aligned}$$

which we can rewrite as

$$\begin{aligned} 0 &= -0.2x + 0.1y \\ 0 &= -0.1y + 0.2x \end{aligned}$$

We now effectively have only one equation in x and y since one of the above equations is just a multiple of the other. We thus expect infinitely many different solutions of this one equation in two unknowns. If we now remember that we must also have $x + y = 10$, we can solve for x and y to obtain $x = 3.333$ and $y = 6.667$. You can now check for yourself that these values for x and y really do remain unchanged from year to year. This means that if 3333 students used the Jammie Shuttle at the beginning of a month, the same number will use the Shuttle every month after that.

Let's use the symbol A for the matrix $\begin{pmatrix} 0.8 & 0.1 \\ 0.2 & 0.9 \end{pmatrix}$. At the beginning of month 2 we have, from (a),

$$\begin{pmatrix} x(2) \\ y(2) \end{pmatrix} = A \begin{pmatrix} 6 \\ 4 \end{pmatrix} = \begin{pmatrix} 5.2 \\ 4.8 \end{pmatrix}.$$

At the beginning of month 3, we have

$$\begin{pmatrix} x(3) \\ y(3) \end{pmatrix} = A \begin{pmatrix} 5.2 \\ 4.8 \end{pmatrix} = \begin{pmatrix} 4.64 \\ 5.36 \end{pmatrix}.$$

We can also write this as

$$\begin{pmatrix} x(3) \\ y(3) \end{pmatrix} = A \left(A \begin{pmatrix} 6 \\ 4 \end{pmatrix} \right) = A^2 \begin{pmatrix} 6 \\ 4 \end{pmatrix} = \begin{pmatrix} 4.64 \\ 5.36 \end{pmatrix}.$$

Similarly, at the beginning of month 4, we find

$$\begin{pmatrix} x(4) \\ y(4) \end{pmatrix} = A^3 \left(\begin{pmatrix} 6 \\ 4 \end{pmatrix} \right) = \begin{pmatrix} 4.248 \\ 5.752 \end{pmatrix},$$

and so on. The remarkable thing is that, as you carry on calculating $x(n)$ and $y(n)$ for larger and larger values of n, they tend, fairly quickly, to the values obtained in (b). Why? You'll find out why later in the course.

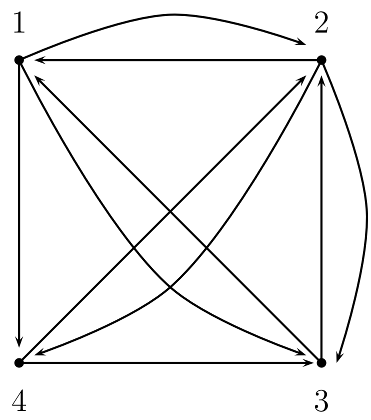
In part (b) above we were given a matrix A and had to find a vector $\mathbf{x}$ such that $A\mathbf{x} = 1\,\mathbf{x}$. Such a vector is an example of an **eigenvector** of the matrix A corresponding to the **eigenvalue** 1. The terms "eigenvalue" and "eigenvalue" will probably not mean much to most of you, but we'll look at this kind of problem in much more detail later in the course. Eigenvalue problems have very wide applications. Notice that the whole example is concerned with working with linear equations and matrices. This means that we can certainly say that it forms part of linear algebra.

In the second example we look at what seems to be a very different kind of problem. But the mathematics turns out to be very similar.

Example 1.1.2 When using a search engine on the Internet, it is possible that the number of "hits" (web sites containing the keywords you've entered) may be very large. You will then have to spend a long time going through the list to decide which sites are useful. It would be very helpful if the search engine could rank the sites it has found in order of importance. To do this, it will need to have a way of deciding on the importance of a site. Suppose it is possible to assign a positive number to each site to indicate its importance (the larger the number, the more important the site). We call this number the *rank* of the site. Then the sites could simply be arranged according to their ranks, with the site with the highest rank at the beginning of the list.

The problem therefore is to find a way of assigning a rank to a site. One way of doing this is to determine the number of other important sites that have links to this site. To do this we add up the ranks of all the sites that have links to the site, and this sum becomes the rank of the site. If you think this through, you will probably soon see a snag: to determine the rank of a site, you have to know the ranks of all the sites linked to it. So where do we start?

Let us consider a very simple case where we have four sites that we want to rank. For convenience we'll number the sites from 1 to 4 (these numbers do not indicate their ranking, we still have to decide on that!). For each of these sites, we know to which of the other sites it is linked. This information is summarised in the diagram below:



In the diagram, the arrow from 1 to 3 indicates that site 1 contains a link to site 3. More generally, an arrow from i to j indicates that site i contains a link to site j. Our problem is to assign a positive number r_i to site i indicating its importance. It turns out to be convenient to require that $0 \leq r_i \leq 1$ for each i and that $r_1 + r_2 + r_3 + r_4 = 1$. We try to assign the rankings r_i in such a way that the ranking of a site is proportional to the sum of the rankings of the sites containing a link to it. This means, for example, that we want

$$r_1 = k(r_2 + r_3),$$

where k is the constant of proportionality. We can write down a similar equation for each of the other sites:

$$\begin{aligned} r_2 &= k(r_1 + r_3 + r_4) \\ r_3 &= k(r_1 + r_2 + r_4) \\ r_4 &= k(r_1 + r_2). \end{aligned}$$

This gives us a system of linear equations in the variables r_1, r_2, r_3 and r_4. In matrix form the system becomes:

$$\begin{pmatrix} r_1 \\ r_2 \\ r_3 \\ r_4 \end{pmatrix} = k \begin{pmatrix} 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 \end{pmatrix} \begin{pmatrix} r_1 \\ r_2 \\ r_3 \\ r_4 \end{pmatrix}.$$

The question is whether there is a constant k such that the system has a solution for which all the r_i are nonnegative. It is possible to show that in this case there is such a k, namely $k = 0.3982$; its value is not important to us, but rather the fact that we get a solution for the variables r_i.

If we write A for the matrix and $\mathbf{r}$ for the vector in this equation, it becomes

$$A\mathbf{r} = k^{-1}\mathbf{r}.$$

The number k^{-1} is an eigenvalue and the vector $\mathbf{r}$ an eigenvector of the matrix A. The problem is therefore similar to the first one, but in this case we want the eigenvalue to be positive, and the eigenvector to have positive entries.

Using this value of k we get the solution

$$r_1 = .2268, r_2 = 0.2847, r_3 = 0.2847, r_4 = .2038.$$

In this case the sites 2 and 3 therefore tie for first place, site 1 comes second and site 4 comes third. This solution, by the way, was obtained using OCTAVE.

Essentially the same method can be used to rank sports teams or individual players in sports like tennis or golf.

The last example looks at an ecological problem which requires solutions of differential equations.

Example 1.1.3 We suppose that on a reasonably large island there are populations of both foxes and rabbits. The idea is that if there are lots of rabbits then the fox population will increase, but if the fox population increases this will tend to thin out the rabbit population. To be more precise, the rate at which the rabbits reproduce will depend on the number of rabbits as well as the number of foxes (although not in the same way, obviously!). A similar statement will apply to the reproduction rate of foxes.

To make things more formal, we let

$x_1 = x_1(t)$ be the number of rabbits on the island at time t and

$x_2 = x_2(t)$ be the number of foxes on the island at time t.

The previous discussion suggests that we might expect x_1 and x_2 to satisfy the following two equations:

$$\begin{aligned} \frac{dx_1}{dt} &= ax_1 + bx_2 \\ \frac{dx_2}{dt} &= cx_1 + dx_2 \end{aligned}$$

Here a, b, c, and d are constants that reflect the interaction of the foxes and the rabbits. One would expect some of the constants to be negative. (Why?) The above two equations constitute a mathematical model for the situation. This is not the only or even the best model; it is just one we might investigate which reflects to some extent our observations of the rabbits and foxes.

The above is a **system** of differential equations. It is systems of this form that we will ultimately be able to solve using our knowledge of linear algebra. At the moment we can only suggest what might be involved. To start with, we could use the notation $\frac{d}{dt}\begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$ to denote the vector $\begin{pmatrix} \frac{dx_1}{dt} \\ \frac{dx_2}{dt} \end{pmatrix}$. Using this notation we can rewrite the system of equations as:

$$\frac{d}{dt}\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$$

and if we let A stand for $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ and $\mathbf{x}$ for $\begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$ it looks even simpler:

$$\frac{d\mathbf{x}}{dt} = A\mathbf{x}. \qquad (*)$$

You may remember that you have solved differential equations of the form

$$\frac{dx}{dt} = ax$$

in your first-year course in Mathematics and that the general solution of such an equation is

$$x = x(t) = Ce^{at}$$

where C is an arbitrary constant. The similarity of our system of differential equations to the above single differential equation leads one to hope that the solution of the system of equations may be of the form

$$x_1 = Ce^{\lambda t} \quad \text{and} \quad x_2 = De^{\lambda t},$$

where C and D are arbitrary constants, and λ is a constant that depends in some way on A. This indeed turns out to be the case, and it remains to see what λ must be. (We'll justify all of this in more detail later in the course.) Let's just try to see what we can say about λ, C and D.

Given that $x_1 = Ce^{\lambda t}$ and $x_2 = De^{\lambda t}$ we have that

$$\frac{dx_1}{dt} = \lambda Ce^{\lambda t} \quad \text{and} \quad \frac{dx_2}{dt} = \lambda De^{\lambda t}.$$

We can now write:

$$\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} Ce^{\lambda t} \\ De^{\lambda t} \end{pmatrix} = e^{\lambda t} \begin{pmatrix} C \\ D \end{pmatrix}$$

and

$$\frac{d}{dt} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} \lambda Ce^{\lambda t} \\ \lambda De^{\lambda t} \end{pmatrix} = \lambda e^{\lambda t} \begin{pmatrix} C \\ D \end{pmatrix}.$$

Substituting these in $(*)$ above we get:

$$\lambda e^{\lambda t} \begin{pmatrix} C \\ D \end{pmatrix} = Ae^{\lambda t} \begin{pmatrix} C \\ D \end{pmatrix} \quad \text{or} \quad \lambda \begin{pmatrix} C \\ D \end{pmatrix} = A \begin{pmatrix} C \\ D \end{pmatrix}.$$

(We can divide by $e^{\lambda t}$; why?) If we write out the last equation, we obtain a system of two linear equations in the two unknowns C and D. The question is: "Is there a value of λ for which this system will have a solution?" This is equivalent to asking for an eigenvalue λ for the matrix A, and a corresponding eigenvector $\begin{pmatrix} C \\ D \end{pmatrix}$ for A. We'll look at these ideas in much more detail later.

The above problem in differential equations has been transformed into a problem of linear algebra. Differential equations are extremely important in all sorts of fields: physics, economics, chemistry, biology to name just a few. Techniques of linear algebra can be of some use in the solving of these differential equations, as we have seen in the above problem. Interestingly enough, even when we can't solve differential equations exactly, linear algebra often comes to the rescue and helps to find approximate solutions.

A final comment: you may feel that linear equations and systems of linear equations are very special and that probably many "real life" situations would be better modelled by using more complicated kinds of equations. In fact you would be right, but the remarkable thing is that one can often, in such situations, make use of linear algebra to obtain useful approximations to the more complicated equations. The moral of the story is that linear algebra is a fundamental tool for understanding many situations; that's why we are doing it.

We have seen in this section that systems of linear equations arise quite naturally in three different examples. This is true in general: many situations in various fields call for the use of systems of linear equations. As soon as systems of linear equations are involved, it is quite natural to introduce matrices and vectors, as we saw in all the above examples. Elementary linear algebra consists in the study of vectors and matrices (roughly speaking).

Exercises

1. An oil refinery produces low-sulfur and high-sulfur fuel. Each ton of low-sulfur fuel requires 5 minutes in the blending plant and 4 minutes in the refining plant; each ton of high-sulfur fuel requires 4 minutes in the blending plant and 2 minutes in the refining plant. If the blending plant is available for 3 hours and the refining plant is available for 2 hours, how many tons of each type of fuel should be manufactured so that the plants are fully utilized?

2. The life cycle of a certain endangered bird species can divided into three stages: *juvenile, subadult* and *adult*. Let the number of juveniles, subadults and adults in year k (where $k = 0, 1, 2, \ldots$) be denoted by j_k, s_k and a_k respectively. From field studies it is known that the number of juveniles in any one year is 33% of the number of adults in the previous year, 18% of juveniles in one year survives to become subadults in the next year and 71% of subadults and 94% of adults in one year will be counted as adults in the next year. Write down a system of equations expressing this information, and then write the system in matrix notation.

1.2 Matrices and the Algebra of Matrices

In the examples in the preceding section we've seen matrices and vectors entering into the picture quite naturally when considering problems that can be phrased in terms of systems of linear equations.. From here on, they are going to play an increasingly important role.

In this section (much of which may be familiar to you) we will set up a standard notation for matrices and examine how matrices relate to one another. We will begin to understand that matrices are "algebraic" objects, which can be added, subtracted, multiplied and sometimes even divided. In the process we'll learn about matrix arithmetic or algebra. You have seen some of these ideas in your first year course, but we are are going to make things somewhat more precise here.

To start with, a note about notation. We'll use upper case letters (like A, B, C) to denote matrices, and lower case letters (like a, b, c) to denote entries of a matrix. We'll also stick to lower case letters for numbers, even when they are not entries of a matrix.

Example 1.2.1 The following are examples of matrices:

$$\text{(a)}\quad A = \begin{pmatrix} 2 & -1 \\ 3 & 0 \\ -1 & \sqrt{2} \end{pmatrix} \quad \text{(b)}\quad B = \begin{pmatrix} a & b & c \\ d & f & g \end{pmatrix} \quad \text{(c)}\quad C = \begin{pmatrix} c_{11} & c_{12} & c_{13} \\ c_{21} & c_{22} & c_{23} \\ c_{31} & c_{32} & c_{33} \end{pmatrix}$$

Example (c) above is important; it introduces you to the so-called double-subscript notation. The first subscript tells you what row the entry is in; the second subscript tells you what column the entry is in. Let's have a definition for completeness:

Definition 1.2.2 *Let m and n be positive integers. An $m \times n$* ***matrix*** *is a rectangular array of numbers in m rows and n columns of the form*

$$\begin{pmatrix} a_{11} & a_{12} & a_{13} & \dots & a_{1n} \\ a_{21} & a_{22} & a_{23} & \dots & a_{2n} \\ . & . & . & & . \\ . & . & . & & . \\ . & . & . & & . \\ a_{m1} & a_{m2} & a_{m3} & \dots & a_{mn} \end{pmatrix}$$

Each a_{ij} is a number called an ***entry*** *or* ***element*** *of the matrix. We will sometimes need to refer to a specific entry in a matrix; we can do so by talking about the entry in the (i, j) position if we want to refer to a_{ij}. (Recall that this is the number in the i-th row and j-th column.) If the entries of a matrix are all real numbers, we call it a* ***real matrix****; if they are complex numbers, we call it a* ***complex matrix****. We think of real numbers as special kinds of complex numbers (those with imaginary part equal to 0); this means that every real matrix is a complex matrix, but not conversely. The numbers m and n are called the* **dimensions** *of the matrix. We will sometimes call $m \times n$ the* **size** *of the matrix.*

*An $n \times 1$ matrix is usually called an n-***vector***; the same applies to a $1 \times n$ matrix. To distinguish between the two we'll call the first one a* **column vector** *and the second a* **row vector***. It will sometimes be useful to think of the rows and columns of matrices as vectors.*

There is some notation that we will often use which may be a bit confusing at first. If we write something like:

$$\text{"\dots the } m \times n \text{ matrix } A = \left(\; a_{ij} \; \right)\text{"},$$

then this just means that we are using double-subscript notation to refer to a matrix whose entries have the general form a_{ij}. The confusing thing is that there is a world of difference between a_{ij}, which is just an entry in the matrix, and $\left(a_{ij} \right)$ which is the whole matrix. Watch out for this!

We'll often denote a vector by a boldface letter such as $\mathbf{x}$; if it is an n-vector, we'll write x_i for its i-th component:

$$\mathbf{x} = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix}.$$

If the dimensions of a matrix A are equal (i.e. if $m = n$), we call it a **square** matrix and the special entries $a_{11}, a_{22}, \ldots, a_{nn}$ form the **(main) diagonal** of A.

Now that we can write matrices and their entries in a general way, we are ready to start talking about the algebra of matrices. The definitions we give below are not new to you, but they are given in a form which is probably more precise than in your first year course. Some of these definitions (such as the definition for addition of matrices) are more or less what one would expect; some (like the definition of multiplication) are surprisingly complicated. We will see why these are the appropriate definitions as we go along. Before we do anything else, we need to know when two matrices are equal.

Definition 1.2.3 *If $A = \left(a_{ij} \right)$ and $B = \left(b_{ij} \right)$ are matrices we say that $A = B$ if they have the same size* and *and their corresponding entries are the same. More precisely, if A is an $m \times n$ matrix and B is a $p \times q$ matrix, then*

$$A = B \text{ if and only if } m = p \text{ and } n = q \text{ and } a_{ij} = b_{ij} \text{ for all } i, j.$$

The phrase "for all i, j" above is a somewhat lazy way of saying "for all integers i such that $1 \leq i \leq m$ and for all integers j such that $1 \leq j \leq n$. Note that if two matrices have different sizes they cannot be equal.

Definition 1.2.4 *If $A = \left(a_{ij} \right)$ and $B = \left(b_{ij} \right)$ are both $m \times n$ matrices, then their* ***sum*** *is defined. It is written $A + B$ and is the $m \times n$ matrix obtained by adding the corresponding entries; more precisely*

$$A + B = \left(a_{ij} \right) + \left(b_{ij} \right) = \left(a_{ij} + b_{ij} \right).$$

Notice that addition of two matrices with different dimensions is not defined. If two matrices $A = \begin{pmatrix} a_{ij} \end{pmatrix}$ and $B = \begin{pmatrix} b_{ij} \end{pmatrix}$ have the same dimension, their sum is the matrix of the same dimension with entry in the i-th row and j-th column equal to $a_{ij} + b_{ij}$.

Example 1.2.5

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

$$\begin{pmatrix} 1+2i & -3 \\ -2i & 2-i \end{pmatrix} + \begin{pmatrix} 3 & -5i \\ 1+i & i \end{pmatrix} = \begin{pmatrix} 4+2i & -3-5i \\ 1-i & 2 \end{pmatrix}$$

Addition of matrices is pretty straightforward. As an algebraic operation it behaves nicely, quite like ordinary addition of numbers. In particular, matrix addition is commutative and associative:

- $A + B = B + A$ (commutative law for addition),
- $(A + B) + C = A + (B + C)$ (associative law for addition),

provided A, B and C are matrices of the same size.

You will be asked to prove these facts in the exercises.

A matrix whose entries are all zero will be called a **zero** matrix; we shall denote any zero matrix by $\mathbf{0}$. If A is any matrix and $\mathbf{0}$ is a zero matrix of the same kind, then

- $A + \mathbf{0} = \mathbf{0} + A = A$.

This means that $\mathbf{0}$ is an *additive identity.*

We denote by $-A$ the matrix $\begin{pmatrix} -a_{ij} \end{pmatrix}$. It's clear that

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

For this reason, we call $-A$ an *additive inverse* of A.

Matrix subtraction can now be defined in the obvious way. If A and B are matrices of the same size, we define the **difference** $A - B$ by

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

This means that the difference of two matrices of the same size can be found by subtracting corresponding entries.

We come now to another important operation with matrices: so-called "scalar multiplication". It is traditional, when working with vectors (and matrices), to use the word **scalar** for a number (real or complex). The terminology is motivated by the fact that, for real vectors and numbers at least, multiplying a vector by a number *scales* its length. Note that the number we are multiplying by should be of the same type as the entries of the matrix. This means that we'll multiply real matrices by real numbers, and complex matrices by complex numbers.

Definition 1.2.6 *If t is a scalar and $B = \left(b_{ij} \right)$ is an $m \times n$ matrix then the **product of** t **and** B is the $m \times n$ matrix tB obtained by multiplying each entry of B by t. More precisely*

$$t \left(b_{ij} \right) = \left(tb_{ij} \right).$$

*We call this operation **scalar multiplication**.*

Example 1.2.7 If $A = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 4 \end{pmatrix}$ then

$$3A = \begin{pmatrix} 3 & 6 & 9 \\ 6 & 9 & 12 \end{pmatrix} \text{ and } (-1)A = \begin{pmatrix} -1 & -2 & -3 \\ -2 & -3 & -4 \end{pmatrix} = -A.$$

If $B = \begin{pmatrix} 2i & 7 & 1-2i \\ -4 & 3i & 0 \end{pmatrix}$, then

$$2iB = \begin{pmatrix} -4 & 14i & 2+i \\ -8i & -6 & 0 \end{pmatrix}.$$

We list some properties of scalar multiplication below. Proofs of these facts are omitted, but you should check a few of them yourselves. The matrices A and B have the same size, and s and t are numbers of the same kind as the entries of A and B.

- $(s+t)A = sA + tA$,
- $s(A+B) = sA + sB$
- $st(A) = s(tA)$,
- $1A = A$,

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

The definition of matrix multiplication (which you have seen in your first year course) looks far from "obvious" when you see it for the first time. It can be motivated by observing that, when we view matrices as **functions** (which we have not done yet in this course), then matrix multiplication corresponds to function composition. We will justify our choice of matrix multiplication at the end of this section. For the moment, just remember that it is the same definition as the one you have seen before and the process is just the so-called "row-column" multiplication.

Definition 1.2.8 *Let* $A = \left(\begin{array}{c} a_{ij} \end{array} \right)$ *be an* $m \times n$ *matrix and* $B = \left(\begin{array}{c} b_{ij} \end{array} \right)$ *be an* $n \times p$ *matrix, then the* product AB of A and B *is an* $m \times p$ *matrix* $C = \left(\begin{array}{c} c_{ij} \end{array} \right)$ *and for each* i *and* j*, with* $1 \leq i \leq m$ *and* $1 \leq j \leq p$*,*

$$c_{ij} = a_{i1}b_{1j} + a_{i2}b_{2j} + \ldots + a_{in}b_{nj}.$$

Note that the definition only allows you to multiply matrices if they have the right dimensions (matrix A must have the same number of columns as the number of rows of matrix B). Secondly, the definition really does just say that to find the entry in the i^{th} row and j^{th} column of AB you must multiply each entry in row i of matrix A by the corresponding entry in column j of matrix B and then add all these products; this is called the *dot product* of row i of A and column j of B. (You may still remember the notion of the dot product of two 2- or 3-vectors from your first year course; the dot product of two n-vectors is defined in the same way.) The definition could be expressed more concisely using Σ notation as follows:

$$\left(\begin{array}{c} a_{ij} \end{array} \right) \left(\begin{array}{c} b_{ij} \end{array} \right) = \left(\begin{array}{c} c_{ij} \end{array} \right), \text{ where } c_{ij} = \sum_{k=1}^{n} a_{ik}b_{kj}.$$

Make sure you understand that this really is no different from what was given in the definition.

Example 1.2.9 Let $A = \left(\begin{array}{ccc} 1 & 2 & 0 \\ -1 & 0 & 2 \end{array} \right)$ and $B = \left(\begin{array}{cc} 2 & 1 \\ 3 & -1 \\ 2 & 0 \end{array} \right)$. Then A is a 2×3 matrix and B is a 3×2 matrix. Since A has the same number of columns as the number of rows of B (namely 3), the product AB is defined, and must be a 2×2 matrix. If we denote this product by $\left(\begin{array}{c} c_{ij} \end{array} \right)$, then

$$\begin{aligned} c_{11} &= 1.2\,+\,2.3\,+\,0.2 = 8 \\ c_{12} &= 1.1\,+\,2.-1\,+\,0.0 = -1 \\ c_{21} &= -1.2\,+\,0.3\,+\,2.2 = 2 \\ c_{22} &= -1.1\,+\,0.-1\,+\,2.0 = -1 \end{aligned}$$

So the product AB is $\begin{pmatrix} 8 & -1 \\ 2 & -1 \end{pmatrix}$.

Example 1.2.10 Let $A = \begin{pmatrix} 2i & -3 \\ 1+i & i \end{pmatrix}$ and $B = \begin{pmatrix} 3 & -i & 0 \\ -2i & 3 & 1-i \end{pmatrix}$.
Then AB is the 2×3 matrix $\begin{pmatrix} 12i & -7 & -3-3i \\ 5+3i & 1+2i & 1+i \end{pmatrix}$.

We'll move on now to some of the properties of matrix multiplication. You have seen some of these before, but it's important to revisit them. The first item is not a property; it's a non-property!

WARNING: In general it need not be the case that $AB = BA$, even if both products are defined. **Thus matrix multiplication is not commutative.**

Example 1.2.11

$$\begin{pmatrix} 1 & 2 \\ 2 & 3 \end{pmatrix} \begin{pmatrix} 1 & 4 \\ -2 & 3 \end{pmatrix} = \begin{pmatrix} -3 & 10 \\ -4 & 17 \end{pmatrix}$$

but

$$\begin{pmatrix} 1 & 4 \\ -2 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 \\ 2 & 3 \end{pmatrix} = \begin{pmatrix} 9 & 14 \\ 4 & 5 \end{pmatrix}.$$

In fact it may even happen that AB is defined whereas BA is not, in which case they could hardly be equal!

Although the non-commutativity of matrix multiplication is mildly irritating, it need not be too much of a problem. You just have to be very careful that you are writing down your matrices in the right order whenever you work with products, and under no circumstances must you submit to the temptation of interchanging the order while simplifying expressions! Fortunately, matrix multiplication does have some of the other properties of ordinary multiplication; in particular we have that

- $A(BC) = (AB)C$ (associative law),
- $A(B + C) = AB + AC$ (left distributive law), and
- $(A + B)C = AC + BC$ (right distributive law)

all hold for all A, B and C (as long as the relevant products are all defined). Note that it is necessary to state two distributive laws, exactly because matrix multiplication is not commutative.

The proofs of these properties are somewhat tedious and tend to get bogged down in keeping track of all the different subscripts. The associative law is particularly important, though. The essential ingredients of the proofs are the facts that the associative and distributive laws hold for ordinary multiplication and addition of real numbers (or complex numbers, for that matter). We will see a somewhat more conceptual proof of the associative law when we consider the fact that matrix multiplication corresponds to composition of functions. We'll leave the distributive laws as exercises.

Next in our string of definitions come identity matrices; these are hopefully old friends.

Definition 1.2.12 *We let I_n denote the $n \times n$ matrix which has 1's on the main diagonal and zeros elsewhere. I_n is called the $n \times n$* **identity matrix***.*

So
$$I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \text{ and } I_3 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix},$$
and so on. It is easy to check that $AI_n = A$ and $I_nB = B$ for any $m \times n$ matrix A and any $n \times p$ matrix B; in particular, $AI_n = A = I_nA$ for an $n \times n$ matrix A. For this reason, I_n is called a *multiplicative identity.*

We have almost all the definitions we need for developing matrix algebra further now. The one thing that is missing from our list of definitions of basic algebraic operations is any mention of division. We'll look at this in the last section when we deal with inverses of matrices (and see that the story is far more involved than it is for division of numbers).

The next two pages are for those of you who have wondered why the definition of matrix multiplication is so complicated. To give some motivation for the definition we are going to show that matrix multiplication is related to function composition.

You may find it useful to look at Appendix C.1, where functions and function composition are discussed, before reading what follows.

The equation $A\mathbf{x} = \mathbf{y}$ can be re-interpreted in a way which reminds one of function notation. When we write $f(x) = y$, where f is some (real-valued) function, we think of f as being applied to an input x to produce an output y. If we think, in our matrix equation, of $\mathbf{x}$ as being a possible input, we can think of the equation as indicating that we are applying the matrix A to this input and producing $\mathbf{y}$ as the output (and the way you get the output is by using row-column multiplication, that is matrix multiplication). This means that we can think of the matrix A as the function f defined by $f(\mathbf{x}) = A\mathbf{x}$.

Taking this a step further, suppose that A and B are matrices and $\mathbf{x}, \mathbf{y}$ and $\mathbf{z}$ are vectors (or matrices with a single column each, if you like), and that $A\mathbf{x} = \mathbf{y}$ and $B\mathbf{y} = \mathbf{z}$ (this implies that all the matrices are of the right size so that all the products are defined). Then it follows that

$$B(A\mathbf{x}) = \mathbf{z}.$$

We can also use associativity of matrix multiplication to deduce that

$$(BA)\mathbf{x} = \mathbf{z}.$$

The upshot of this is that if we apply the matrix A to the vector $\mathbf{x}$ and then apply the matrix B to the result, we get the same result as when we apply the product matrix BA to X. Now let's think of the matrices A and B as functions f and g, so that $f(\mathbf{x}) = A\mathbf{x}$ and $g(\mathbf{y}) = B\mathbf{y}$. The composite function $g \circ f$ is then given by

$$(g \circ f)(\mathbf{x}) = g(f(\mathbf{x})) = g(A\mathbf{x}) = B(A\mathbf{x}) = (BA)\mathbf{x}.$$

This means that if the function f corresponds to multiplication by the matrix A and the function g corresponds to multiplication by the matrix B, then the composition $g \circ f$ of the functions g and f corresponds to the matrix product BA!

$$\begin{tikzcd}
\mathbf{x} \arrow[r, "A", "f"'] \arrow[rr, bend left, "BA", "g \circ f"'] & A\mathbf{x} \arrow[r, "B", "g"'] & \begin{array}{c}(BA)\mathbf{x} \\ = \\ B(A\mathbf{x})\end{array}
\end{tikzcd}$$

This is telling us that if we think of matrices as functions, then composition of these functions corresponds to matrix multiplication. It is this important fact that motivates and justifies the rather complicated definition of matrix multiplication. Note that we needed the fact that matrix multiplication is associative in the equation above.

Let's look at an example to illustrate this idea.

Example 1.2.13 Let

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

Let us define the functions f and g by $f(\mathbf{x}) = A\mathbf{x}$ and $g(\mathbf{y}) = B\mathbf{y}$. If we write $\mathbf{y} = f(\mathbf{x}) = A\mathbf{x}$, $\mathbf{y} = g(\mathbf{y}) = B\mathbf{y}$ and

$$\mathbf{x} = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \qquad \mathbf{y} = \begin{pmatrix} y_1 \\ y_2 \\ y_3 \end{pmatrix} \qquad \mathbf{z} = \begin{pmatrix} z_1 \\ z_2 \end{pmatrix},$$

then

$$\begin{pmatrix} y_1 \\ y_2 \\ y_3 \end{pmatrix} = \mathbf{y} = A\mathbf{x} = \begin{pmatrix} 3x_1 - x_2 \\ 2x_1 + 5x_2 \\ -x_1 + 2x_2 \end{pmatrix}$$

and

$$\begin{pmatrix} z_1 \\ z_2 \end{pmatrix} = Z = B\mathbf{y} = \begin{pmatrix} 2y_1 - 3y_2 + 4y_3 \\ 4y_1 + y_3 \end{pmatrix}$$

Then we can write down z_1 and z_2 in terms of x_1 and x_2; working it out, we get

$$\begin{aligned} z_1 &= 2(3x_1 - x_2) - 3(2x_1 + 5x_2) + 4(-x_1 + 2x_2) = -4x_1 - 9x_2 \\ z_2 &= 4(3x_1x_2t) + (-x_1 + 2x_2) = 11x_1 - 2x_2, \end{aligned}$$

or

$$\begin{pmatrix} z_1 \\ z_2 \end{pmatrix} = \begin{pmatrix} -4x_1 - 9x_2 \\ 11x_1 - 2x_2 \end{pmatrix} = \begin{pmatrix} -4 & -9 \\ 11 & -2 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}.$$

From this we can see that $\mathbf{z} = C\mathbf{x}$, where

$$C = \begin{pmatrix} -4 & -9 \\ 11 & -2 \end{pmatrix}.$$

Since $\mathbf{z} = g(\mathbf{y}) = g(f(\mathbf{x})) = (g \circ f)(\mathbf{x})$, it follows that $(g \circ f)(\mathbf{x}) = C\mathbf{x}$; this means that the composition of g and f is also a function defined by a matrix, namely the matrix C. Now

$$BA = \begin{pmatrix} 2 & -3 & 4 \\ 4 & 0 & 1 \end{pmatrix} \begin{pmatrix} 3 & -1 \\ 2 & 5 \\ -1 & 2 \end{pmatrix} = \begin{pmatrix} -4 & -9 \\ 11 & -2 \end{pmatrix} = C,$$

so that $g \circ f$ is defined by the product of the matrices defining f and g. This shows that the general result we stated before this example holds in this particular case. Note that our proof of the general result depended on the associative rule for matrix multiplication, but that we did not use this rule in this example.

In general then, *we have defined matrix multiplication so that*

$$A(BX) = (AB)X$$

holds whenever both sides make sense. We have not seen a proof of this yet, but we have seen an example that supports this idea. However a general proof would not look very different from the example we looked at above. The only difference would be that instead of having particular entries in the matrices concerned we would have to allow letters to represent arbitrary entries. You are asked to do this in an exercise.

In Chapter 3 we will again see that thinking of a matrix as a function is a very useful idea. In anticipation of some of the things we will be doing there, we write the definition of this function in a slightly different, but very useful way. Suppose $A = \begin{pmatrix} a_{ij} \end{pmatrix}$ is an $m \times n$ matrix and $\mathbf{x} = \begin{pmatrix} x_i \end{pmatrix}$ an n-vector, written as a column vector. If f is the function defined by $f(\mathbf{x}) = A\mathbf{x}$, then $A\mathbf{x}$ is an m-vector, and for $i = 1, 2, \ldots, m$, the i-th entry of this vector is given by

$$a_{i1}x_1 + a_{i2}x_2 + \cdots a_{in}x_n.$$

If we write $\mathbf{a_i}$ for the i-th column of A, we get the vector equation

$$A\mathbf{x} = x_1\mathbf{a_1} + x_2\mathbf{a_2} + \cdots x_n\mathbf{a_n} = \sum_{i=1}^{n} x_i\mathbf{a_i}.$$

This tells us that $A\mathbf{x}$ can be written as a sum of scalar multiples of the columns of the matrix A. (Such a sum is known as a *linear combination*, as we will see in the next chapter.)

Matrix multiplication can be viewed in other ways as well, all of them useful from time to time. One such way is the following:

$$\boxed{\text{The } j^{th} \text{ column of the product } AB \text{ is } A \text{ times the } j^{th} \text{ column of } B.}$$

This follows from the definition of matrix multiplication: the i-th entry in the j-th column of AB is the dot product of the i-th row of A and the j-th column of B. The next example illustrates this statement for two particular matrices.

Example 1.2.14 Let $A = \begin{pmatrix} 2 & -1 & 1 \\ 4 & 0 & 2 \end{pmatrix}$ and let $B = \begin{pmatrix} 1 & 3 \\ 2 & -1 \\ 0 & 2 \end{pmatrix}$. Then

$$AB = \begin{pmatrix} 0 & 9 \\ 4 & 16 \end{pmatrix}.$$

Now if we calculate $A\begin{pmatrix} 1 \\ 2 \\ 0 \end{pmatrix}$, we get $\begin{pmatrix} 0 \\ 4 \end{pmatrix}$. This shows that the first column of AB is the same as A times the first column of B. Similarly, $A\begin{pmatrix} 3 \\ -1 \\ 2 \end{pmatrix} = \begin{pmatrix} 9 \\ 16 \end{pmatrix}$, showing that the second column of AB is A times the second column of B.

Convince yourself that the same reasoning will work for any two matrices for which the product exists.

We finish this section with some facts about *symmetric matrices.* They will crop up again, but much later in the course. Here are some definitions.

Definition 1.2.15 *A matrix $A = (a_{ij})$ is called* **symmetric** *if it is square and $a_{ij} = a_{ji}$ for all i and j.*

Example 1.2.16 The matrix $\begin{pmatrix} 1 & 2 \\ 2 & -1 \end{pmatrix}$ is symmetric; the matrix $\begin{pmatrix} 1 & 2 & 3 \\ 2 & -1 & 3 \\ 3 & 4 & 1 \end{pmatrix}$ is not.

Another less formal way of stating that a matrix is symmetric is to say that if you "flip" it about the main diagonal there is no change. This idea of a matrix "flip" is quite useful, and in the next definition we give a name to a matrix obtained by doing such a "flip".

Definition 1.2.17 *If A is an $m \times n$ matrix, its* ***transpose****, written A^T, is the $n \times m$ matrix obtained from A by making each row of A the corresponding column of A^T. More formally, if $A = \begin{pmatrix} a_{ij} \end{pmatrix}$ is an $m \times n$ matrix, then the transpose A^T is the $n \times m$ matrix $B = \begin{pmatrix} b_{ij} \end{pmatrix}$ such that $b_{ij} = a_{ji}$ for every i and j.*

Example 1.2.18 The transpose of $\begin{pmatrix} 2 & 3 & 5 \\ 1 & 3 & -1 \end{pmatrix}$ is $\begin{pmatrix} 2 & 1 \\ 3 & 3 \\ 5 & -1 \end{pmatrix}$.

The transpose of $\begin{pmatrix} 1 & 2 & 3 \end{pmatrix}$ is $\begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix}$.

Since the entry in row i and column j of A^T is just the entry in row j and column i of A, it is clear that a square matrix A is symmetric if and only if $A^T = A$.

Transposes are an important tool, and we will use them quite a bit later on. For the moment we conclude this section with a few useful facts.

Theorem 1.2.19 *Let A and B be matrices. Then*

(a) $(A^T)^T = A$;

(b) if $A + B$ is defined, $(A + B)^T = A^T + B^T$;

(c) if AB is defined, $(AB)^T = B^T A^T$ (Note the change of order!).

Proof: Parts (a) and (b) are easy. Write out the proof for part (b) as an exercise. For part (c), use the definition of matrix multiplication to find the entry in row i and column j of both $(AB)^T$ and $B^T A^T$, and compare. ■

At the end of this and subsequent sections you will find a short summary. Once you have worked through a section, use the summary as a checklist to make sure that you have mastered the important concepts and skills in the chapter.

Summary:

- We have revisited the basic algebra of matrices and looked at matrix addition, subtraction, multiplication and scalar multiplication.
- Matrix algebra satisfies many of the laws that we know hold in the algebra of real numbers. The one notable exception is that matrix multiplication is **not commutative**.

- If a matrix is interpreted as a function that operates on vectors, then matrix multiplication can be interpreted as function composition.
- We looked at symmetric matrices and some of their properties, and at the notion of the transpose of a matrix.

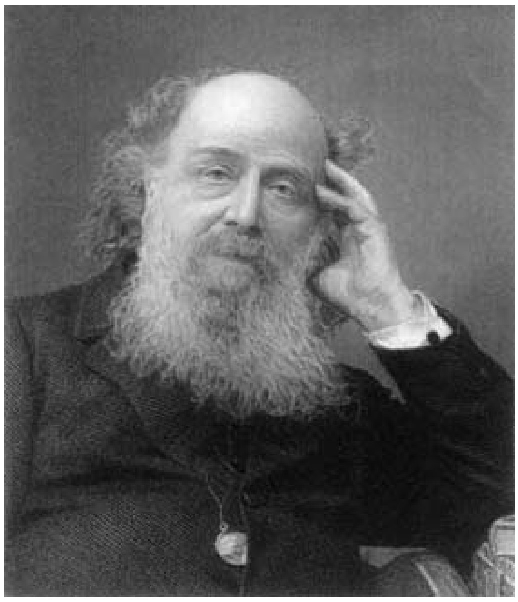
At the end of some sections you will also find notes on the history of some of the concepts discussed in that section, and the mathematicians involved in the development of these ideas.

Historical note.

Although the term "matrix" was not used in mathematics before the nineteenth century, the idea of using rectangular arrays of numbers in the solution of systems of linear equations dates back to China, somewhere between 200 and 100 B C. (There are records, on Babylonian clay tablets, of solutions of linear systems as early as 300 B C.)

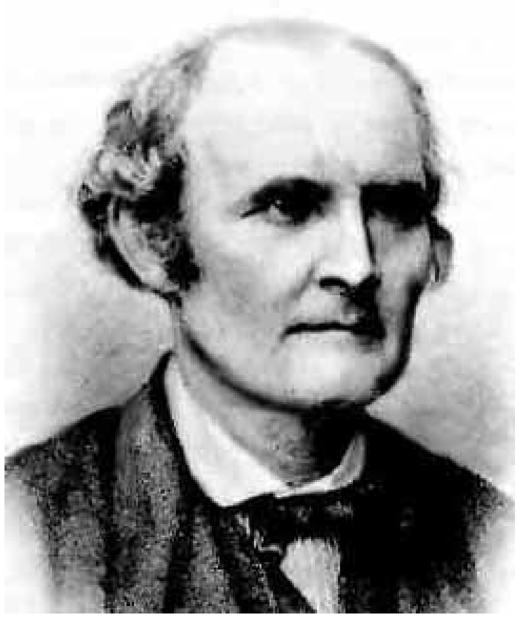
Results in matrix theory started appearing, in disguise (i.e without using the terminology and notation that is now common), in Europe and Japan from the sixteenth century onwards. These results were associated with the names of well-known mathematicians like Leibniz, Gauss, Cauchy, Jacobi, Kronecker and Weierstrass. The results were mostly obtained in specific contexts, and it is unlikely that the full generality of the ideas being used were realised at the time.

The first one to use the term "matrix" was the English mathematician James Joseph Sylvester (1814 – 1897), in 1850. He defined a matrix as "an oblong arrangement of terms". Sylvester studied at Cambridge, but, being Jewish, refused to take the religious oath to the Church of England that was required at the time for graduation. This refusal also made it impossible for him to be awarded a fellowship at Cambridge. He started his lecturing career at the University of London, and after three years took up a chair at the University of Virginia.



His stay in America came to an abrupt end after a few months when he struck a student who had been reading a newspaper in his lectures with a sword stick. The student collapsed and Sylvester, thinking he had killed him, fled to New York and later returned to England. (The student survived!)
Back in London, Sylvester worked as an actuary and a lawyer. At the courts of Lincoln's Inn he met the mathematician Cayley, who also practiced as a lawyer. They had long walks together during which they discussed mathematics, and matrix theory in particular.

Arthur Cayley (1821 – 1895) also graduated from Cambridge. He won a Fellowship and lectured there for four years. On expiry of the fellowship he had to find a (paying) profession and took up law. He practiced law for 14 years, but all the time continued his mathematical research and published 250 papers during this time.



He quickly realised the importance of the matrix concept, and in 1858 published *Memoir on the theory of matrices*. In this he gives the first abstract definition of a matrix. In 1863 Cayley was appointed as Sadlerian professor of mathematics at the University of Cambridge. Although he had to take a substantial drop in salary, he felt that this was more than compensated for by the opportunity to devote himself entirely to mathematics. He was a prolific researcher and published more than 900 papers. One of his major contributions was to the development of the theory of matrices.

Exercises

1. Prove that if A, B and C are matrices of the same size, then
   (a) $A + B = B + A$;
   (b) $(A + B) + C = A + (B + C)$.

2. Let $A = \begin{pmatrix} -2 & 2 & 3 \\ -2 & 3 & 2 \\ -4 & 2 & 5 \end{pmatrix}$. Write as a single matrix:
   (a) $A - 3I_3$;
   (b) $A - \lambda I_3$ (give the answer in terms of λ).

3. In the following, find AB and BA, if possible; otherwise write "undefined".
   (a) $A = \begin{pmatrix} -1 & -2 \\ -3 & -4 \end{pmatrix}$, $\quad B = \begin{pmatrix} 4 & 3 \\ -2 & -2 \end{pmatrix}$.
   (b) $A = \begin{pmatrix} -1 & 0 & 2 \\ 2 & 1 & 3 \\ 3 & 0 & 0 \end{pmatrix}$, $\quad B = \begin{pmatrix} 4 & 0 & -1 \\ 3 & 2 & 0 \\ 0 & 2 & -4 \end{pmatrix}$.
   (c) $A = \begin{pmatrix} 3 & 2 & -3 \\ 0 & 1 & 0 \end{pmatrix}$, $\quad B = \begin{pmatrix} 3 & -4 \\ 0 & 1 \\ 1 & 0 \end{pmatrix}$.
   (d) $A = \begin{pmatrix} 1 & 3 & -3 \end{pmatrix}$, $\quad B = \begin{pmatrix} 0 \\ 4 \\ -2 \end{pmatrix}$.
   (e) $A = \begin{pmatrix} 3 & -1 \\ 0 & 3 \end{pmatrix}$, $\quad B = \begin{pmatrix} 3 & -1 & 0 \\ 2 & 0 & -1 \end{pmatrix}$.

4. Suppose that the product AB is defined.
   (a) Show that if A has a row of zeros, then AB has a row of zeros.
   (b) Show that if B has a column of zeros, then AB has a column of zeros.

5. Let A and B be $n \times n$ matrices, and O be the $n \times n$ matrix all of whose entries are zero. Prove or disprove:
   (a) If k is a real number and $kA = O$, then $k = 0$ or $A = O$.
   (b) If $AB = O$ then $A = O$ or $B = O$.

6. Show that the identity $(A+B)^2 = A^2 + 2AB + B^2$ does **NOT** always hold for matrices (even if both sides are defined). Find a correct expansion of $(A+B)^2$.

7. Prove $A(B+C) = AB + AC$, if A is $m \times n$ and B and C are $n \times p$.
   (You should be able to give a complete proof in three lines.)

8. Prove that if A is an $m \times n$, B a $n \times p$ and C a $p \times q$ matrix, then $A(BC) = (AB)C$.

9. Prove that if A and B are symmetric matrices and $A + B$ is defined, then $A + B$ is symmetric.

10. Prove or disprove: If A is a symmetric matrix for which $A^2 = \mathbf{0}$, then $A = \mathbf{0}$.

11. A matrix A is called **skew symmetric** iff $A^T = -A$. If B is any square matrix, show that:

    (a) $B + B^T$ is symmetric;

    (b) $B - B^T$ is skew symmetric.

12. Let $A = \begin{pmatrix} 1 & -2 & 1 \\ -1 & 1 & 2 \\ 0 & 2 & 1 \end{pmatrix}$.

    (a) Compute $B = A + A^T$ and $C = A - A^T$. Check that B is symmetric and C is skew symmetric.

    (b) What is the relationship between $B + C$ and A?

13. Show that if A is an $n \times n$ matrix, then A can be written uniquely in the form $A = S + K$, where S is symmetric and K is skew symmetric.
    [Hint: Look at questions 11 and 12 again!]

1.3 Systems of Linear Equations and Matrices

In this section we look at linear equations, systems of linear equations and their solutions. Much of this section is revision of material covered in your first-year course, though you may come across some new terminology . We include the details so that you have a complete set of definitions and examples to refer to. You will soon discover that we use the language and notation of set theory to say and write things more concisely. If you are not familiar with concepts such as *sets, subsets* and *elements*, look at Appendix A.1 for an introduction to these ideas.

As you probably guessed, the word "linear" is related to the word "line". You may be most familiar with the equation of a line in the plane in the form $y = mx+c$, but it is easy to see that we can also write this equation in the form

$$a_1x + a_2y = b,$$

where a_1, a_2 and b are constants. Such an equation is called a **linear equation in the variables** x and y. The equation of a plane in three-dimensional space can be written in the form

$$a_1x + a_2y + a_3z = b,$$

where a_1, a_2, a_3 and b are constants. This is an example of a linear equation in the variables x, y and z. We will often need to consider more variables than three, and therefore it becomes easier to use one letter with subscripts for the variables (and for the coefficients), rather than a different letter for every variable. This leads to the following general definition of a linear equation:

Definition 1.3.1 *Let n be a positive integer. A* **linear equation in the variables** *$x_1, x_2, \ldots, x_n$ is one that can be written in the form*

$$a_1x_1 + a_2x_2 + \ldots + a_nx_n = b$$

where $a_1, \ldots, a_n$ and b are constants.

We will generally be working with constants that are real, but at some stage we will need to work with complex constants as well. In fact one even sometimes needs to consider constants of other types, but we will not do it in this course.

Example 1.3.2 The following equations are linear:

(a) $2x - 3y = 0$

(b) $z = 5 - 3x + \sqrt{2}y$

(c) $x_1 + 2x_2 + 3x_3 + \ldots + nx_n = 1$

(d) $(2 - i)z_1 + 3z_2 - (4 + 3i)z_3 = 1 + i$

The following equations are not linear:

(e) $x^2 + y^2 = 1$

(f) $\sin x + 2\sin 2x + 3\sin 3x = 2$

(g) $x_1 + 2x_2 + \dfrac{3}{x_3} = 3$

Definition 1.3.3 *A* **solution** *of the linear equation $a_1x_1+a_2x_2+\ldots+a_nx_n = b$ is a sequence of numbers $t_1, t_2, \ldots, t_n$ such that if we substitute $x_1 = t_1, x_2 = t_2, \ldots, x_n = t_n$ in the equation, we obtain a true statement. If the numbers $t_1, t_2, \ldots, t_n$ are all real, we call it a real solution; if one or more of the numbers are complex, we'll refer to it as a complex solution. To* **solve** *an equation means to find* **all** *its solutions. The set of all solutions we will call the* **solution set***. We usually write such a solution as a vector, i.e. we write the sequence $t_1, t_2, \ldots, t_n$ as the row vector $(t_1, t_2, \ldots, t_n)$; we could also, and frequently will, write a solution as a column vector.*

In the next example we solve some linear equations. Notice that it quite often happens that we find that an equation has *many* solutions; it is important in this case to **write down a general form for all these solutions**.

Example 1.3.4 The examples below illustrate how we go about solving, and writing down the solution, of a linear equation in respectiveness one, two and three variables.

(a) $3x = \sqrt{2}$.
Divide both sides by 3 to obtain a *unique* solution $x = \frac{\sqrt{2}}{3}$.
The solution set is the set $\left\{\frac{\sqrt{2}}{3}\right\}$.

(b)$4x - 3y = 3$.
One approach is to solve for x in terms of y; this yields $x = \frac{1}{4}(3 + 3y)$. Notice now that for every real value of y we get a corresponding real value for x which yields a solution of the equation; there are thus infinitely many solutions. We want a way to indicate all of them clearly. One way to do this is to express x in terms of y as we've done above. Another commonly used way is to let y have an arbitrary value t (say); then $x = \frac{3}{4} + \frac{3}{4}t$. With this method we express both x and y in terms of the variable t, where t can now have any real value. The variable t is sometimes referred to as a **parameter**. We can then say all solutions are of the form

$$x = \frac{3}{4} + \frac{3}{4}t,\ y = t$$

where t is any real number. Because there is one parameter in the solution, this type of solution is sometimes called a *one parameter family of solutions.* The solution set is

$$\{(x, y) : x = \frac{3}{4} + \frac{3}{4}t, y = t, t \in \mathbf{R}\}.$$

Notice that the solution set is a set of row vectors. We can also think of the solution set as a set of *ordered pairs* of real numbers and therefore a subset of the Cartesian plane $\mathbf{R}^2 = \{(x, y) : x, y \in \mathbf{R}\}$. (You can read more about ordered pairs and Cartesian products in Appendix A.1.)
You could also think of the solution set as a set of column vectors:

$$\left\{ \begin{pmatrix} x \\ y \end{pmatrix} : x = \frac{3}{4} + \frac{3}{4}t, y = t, t \in \mathbf{R} \right\}.$$

Note that the equations $x = \frac{3}{4} + \frac{3}{4}t, y = t$ are the parametric equations of the line in $\mathbf{R}^2$ with Cartesian equation $4x - 3y = 3$. The vector equation of the same line is

$$\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 0.75 \\ 0 \end{pmatrix} + t \begin{pmatrix} 0.75 \\ 1 \end{pmatrix}.$$

We won't always use this set notation, and will often just drop the set brackets. If we do this for the equation above we'll say that the solution of the equation is

$$(x, y) = \left(\frac{3}{4}, 0\right) + t\left(\frac{3}{4}, 1\right), t \in \mathbf{R}.$$

Notice that an equally valid approach would have been to solve for y in terms of x. You would then get a similar description of the solution set. Do this yourself.

(c) $2x_1 - 7x_2 + 10x_3 = 1$.
We can find this solution by solving for x_1 in terms of the other variables, or solving for x_2 in terms of the other variables or even solving for x_3 in terms of the other variables; the choice is yours. Let's solve for x_2 in terms of the other variables. We get:

$$7x_2 = 2x_1 + 10x_3 - 1$$

so

$$x_2 = \frac{2}{7}x_1 + \frac{10}{7}x_3 - \frac{1}{7}.$$

Again, for each possible value of x_1 and x_3 we get an associated value for x_2, so we get an infinite number of solutions. We could write them down as follows: let $x_1 = s$ and $x_3 = t$; then

$$x_1 = s, \quad x_2 = \frac{2}{7}s + \frac{10}{7}t - \frac{1}{7} \quad \text{and } x_3 = t$$

where s and t are any (real) numbers. This is an example of a *two parameter family of solutions*, with s and t the parameters. A specific solution is obtained by choosing values for s and t; for example, if we take $s = 0$ and $t = 1$ we get the

solution $x_1 = 0, x_2 = \frac{9}{7}$ and $x_3 = 1$.
We finish this example off by writing the solution set in the same form as we did at the end of part (b). The solution set is:

$$\{(x_1, x_2, x_3) : x_1 = s, x_2 = \frac{2}{7}s + \frac{10}{7}t - \frac{1}{7}, x_3 = t, \text{ where } s, t \in \mathbf{R}\}.$$

Here is yet another way of writing the same solution set, this time as a set of column vectors:

$$\left\{ s \begin{pmatrix} 1 \\ \frac{2}{7} \\ 0 \end{pmatrix} + t \begin{pmatrix} 0 \\ \frac{10}{7} \\ 1 \end{pmatrix} + \begin{pmatrix} 0 \\ -\frac{1}{7} \\ 0 \end{pmatrix} : s, t \in \mathbf{R} \right\}.$$

For a bit of practice, try solving for, say, x_3 in terms of the other variables and writing down the solution you obtain in that way; it will look different to the above solution set, but will be the same collection of solutions.

In the above examples we solved a single equation in various numbers of variables. What we want to do though is to solve several linear equations simultaneously. We write down a definition to make sure we're all using the same terminology:

Definition 1.3.5
(a) A finite collection of linear equations in the variables $x_1, x_2, \ldots, x_n$ is called a **system of linear equations** *or, more simply, a* **linear system**. *A* **solution** *of a linear system is a sequence of numbers $t_1, t_2, \ldots, t_n$ that is a solution of each of the equations in the system at the same time.*
(b) A linear system of equations can have no solution, a unique solution or many solutions. A system with no solutions is called **inconsistent***; a system with many solutions is called* **indeterminate**.

One of the purposes of this chapter is to find a way of finding **all** the solutions of a linear system, if it has any solutions, or to find out when it has no solutions at all. We will use a process called **Gaussian elimination**. It is conceptually simple and, with a few more ideas, easily implemented on a computer, as you will see.

Consider the following system:

$$\begin{aligned} 2x + 3y - 2z &= -7 \\ 3y + 2z &= 3 \\ 5z &= 15. \end{aligned}$$

It is particularly easy to solve, using a method called **backsubstitution**, because it is in a rather special form called **triangular form** (look at the shape of everything to the left of the "equal" signs). You can easily see the value of z from the last equation; using this value in the second equation allows you to calculate a value for y and then using these two values in the first equation allows you to calculate a value for x. We work backwards from the last equation to the first. We give the details in the example below.

Example 1.3.6 We find a solution for the system

$$\begin{aligned} 2x + 3y - 2z &= -7 \\ 3y + 2z &= 3 \\ 5z &= 15. \end{aligned}$$

First solve the last equation:

$$5z = 15 \quad \text{means } z = 3.$$

Now using this in the second equation, we see

$$3y + 2(3) = 3 \quad \text{so} \quad y = -1.$$

Using these values in the first equation, we get

$$2x + 3(-1) - 2(3) = 2x - 9 = -7 \quad \text{so } x = 1.$$

So the (unique) solution is $(x, y, z) = (1, -1, 3)$.

In general the idea is that **triangular systems can all be solved easily** in much the same way as above using backsubstitution. For this idea to be really useful we need a procedure which can manipulate any system of equations *in a way which doesn't change the solutions* but changes the form of the equations so that they appear in triangular form. This procedure exists; it is called **Gaussian elimination**.

Before we get on to that, though, we're going to cut down on all the writing by using matrices. You have already seen how this can be done in your first year course. In fact, the introduction of matrices will improve our understanding of systems of equations and facilitate the use of computers as well. Suppose we have a system of m linear equations in n variables.

The most general way we could write this system is as follows:

$$\begin{array}{rcl} a_{11}x_1 + a_{12}x_2 + \ldots + a_{1n}x_n & = & b_1 \\ a_{21}x_1 + a_{22}x_2 + \ldots + a_{2n}x_n & = & b_2 \\ \vdots \qquad\qquad\qquad \vdots & & \vdots \\ a_{m1}x_1 + a_{m2}x_2 + \ldots + a_{mn}x_n & = & b_m \end{array}$$

With matrix multiplication we can rewrite this, as you have seen before, in a simpler looking form: let

$$A = \begin{pmatrix} a_{11} & a_{12} & a_{13} & \ldots & a_{1n} \\ a_{21} & a_{22} & a_{23} & \ldots & a_{2n} \\ . & . & . & & . \\ . & . & . & & . \\ . & . & . & & . \\ a_{m1} & a_{m2} & a_{m3} & \ldots & a_{mn} \end{pmatrix}, \quad \mathbf{x} = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix}, \text{ and } \mathbf{b} = \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_m \end{pmatrix}.$$

Then using our definition of matrix multiplication we can rewrite the system of linear equations as a so-called “matrix” equation:

$$A\mathbf{x} = \mathbf{b}.$$

Note that since A is $m \times n$ and $\mathbf{x}$ is $n \times 1$, the multiplication is defined, and the product will be an $m \times 1$ matrix as needed. Our definition of equality for matrices then says that $A\mathbf{x} = \mathbf{b}$ as claimed. This equation is often referred to as the **matrix equation associated with the system**. A is called the **coefficient matrix** and $\mathbf{b}$ is called the **vector of constants**. The $m \times (n + 1)$ matrix

$$\begin{pmatrix} a_{11} & a_{12} & a_{13} & \ldots & a_{1n} & b_1 \\ a_{21} & a_{22} & a_{23} & \ldots & a_{2n} & b_2 \\ . & . & . & & . & \\ . & . & . & & . & \\ . & . & . & & . & \\ a_{m1} & a_{m2} & a_{m3} & \ldots & a_{mn} & b_m \end{pmatrix}$$

is called the **augmented matrix** of the system.

Example 1.3.7 Let’s look at the system of equations

$$\begin{array}{rcl} 2x + 3y - 2z & = & -7 \\ 3y + 2z & = & 3 \\ x - y + 5z & = & 15. \end{array}$$

The matrices

$$\begin{pmatrix} 2 & 3 & -2 \\ 0 & 3 & 2 \\ 1 & -1 & 5 \end{pmatrix} \quad \begin{pmatrix} -7 \\ 3 \\ 15 \end{pmatrix} \quad \begin{pmatrix} 2 & 3 & -2 & -7 \\ 0 & 3 & 2 & 3 \\ 1 & -1 & 5 & 15 \end{pmatrix}$$

are respectively the coefficient matrix, the vector of constants and the augmented matrix of the system.

A system of linear equations for which the vector of constants is the zero vector (i.e. a system with matrix form $A\mathbf{x} = \mathbf{0}$) is called a **homogeneous system**. Such a system has at least one solution, namely $\mathbf{x} = \mathbf{0}$, but it could also have other solutions. We'll return to this topic later in this chapter. The solution $\mathbf{x} = \mathbf{0}$ is usually called the **trivial solution**.

We now go back to our procedure. A linear system can be reduced or transformed to a triangular form by applying three types of operations in a systematic way. It is very important to be sure that we transform the system in such a way that the convenient new triangular system has exactly the same solutions as the system we started with. This means we must be sure that no solutions are introduced or lost as the procedure is applied.

Definition 1.3.8 *Two systems of linear equations in the same variables are called **equivalent** if the two systems have the same solution set.*

Since the three operations we'll be using in our procedure are all reversible, it follows that we do not gain or lose any solutions in the process; in other words, the original system and the transformed one are equivalent. This last statement is a bit of a mouthful; try to convince yourself that it is true. To do this, you must be able to show that any solution of a system will still be a solution of the system obtained by applying one of the allowed operations, and that any solution of the system obtained by applying an operation will also be a solution of the original system (the system before the operation was applied). The three allowed operations are:

1.	Add a multiple of one equation to another equation.
2.	Interchange two equations.
3.	Multiply an equation by a non-zero constant.

The above operations are sometimes referred to as **elementary** operations. (Why do we insist that a row can be multiplied only by a *non-zero* constant in the third operation?)

If we now translate the system of equations into its associated augmented matrix, elementary operations on equations will correspond to operations on the corresponding rows of the augmented matrix. In this context we talk about **elementary row operations**. They are:

1.	Add a multiple of one row to another row.
2.	Interchange two rows.
3.	Multiply a row by a non-zero constant.

In the next section we are going to take a detailed look at the Gaussian elimination procedure. We finish this section by doing one example of Gaussian elimination, just so that you get a feel for it. We leave you to read off the solutions once this has been done. Don't worry if you don't understand why we perform the individual steps; we'll get a better feel for this in the next section.

Example 1.3.9 Consider the system of equations:

$$\begin{aligned} 3x_2 + 2x_3 &= 7 \\ x_1 + 4x_2 - 4x_3 &= 3 \\ 3x_1 + 3x_2 + 8x_3 &= 1. \end{aligned}$$

To solve it, we first write down its associated augmented matrix:

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

The next step is to reduce it to triangular form by using elementary row operations:
Interchange the first and second rows:

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

Add -3 times the first row to the third:

$$\begin{pmatrix} 1 & 4 & -4 & 3 \\ 0 & 3 & 2 & 7 \\ 0 & -9 & 20 & -8 \end{pmatrix}$$

Add 3 times the second row to the third:

$$\begin{pmatrix} 1 & 4 & -4 & 3 \\ 0 & 3 & 2 & 7 \\ 0 & 0 & 26 & 13 \end{pmatrix}$$

We now translate this augmented matrix back into a system of equations:

$$\begin{aligned} x_1 + 4x_2 - 4x_3 &= 3 \\ 3x_2 + 2x_3 &= 7 \\ 26x_3 &= 13 \end{aligned}$$

Finally we use backsubstitution to read off the solutions. We leave you to work out that the unique solution in this case is $(x_1, x_2, x_3) = \left(-3, 2, \frac{1}{2}\right)$.

This brings us to the end of this section.

Summary:

- We now know what a *system of linear equations* is, and we know what a *solution* of such a system is.
- We have seen that triangular systems of linear equations are easy to solve using *backsubstitution.*
- We've started looking at *Gaussian elimination.* This is a procedure for transforming systems of equations into triangular systems of equations without affecting the solutions. To do this, we use *elementary operations.*
- We've introduced *matrices* as a means of representing systems of equations, and performed *elementary row operations* on them.

Exercises

1. In each case below, an augmented matrix is given. Find the associated system and solve it by backsubstitution, if possible. If it is not possible, explain why it is not possible.

   (a) $\begin{pmatrix} 4 & 1 & 3 & 2 \\ 0 & -2 & 1 & 3 \\ 0 & 0 & 6 & 0 \end{pmatrix}$

   (b) $\begin{pmatrix} 3 & 1 & 2 & 3 & 9 \\ 0 & -2 & 1 & 2 & 2 \\ 0 & 0 & -3 & 1 & -1 \\ 0 & 0 & 0 & 2 & 4 \end{pmatrix}$

(c) $\begin{pmatrix} 4 & 1 & 2 & 3 & 1 \\ 0 & 2 & 4 & -1 & 0 \\ 0 & 0 & 3 & 1 & 2 \\ 0 & 0 & 0 & 0 & 5 \end{pmatrix}$

2. Show that if an elementary operation is applied to a system of linear equations, the solution set of the original system is the same as that of the new system. [Hint: Look at each of the three elementary operations separately.]

1.4 Gaussian Elimination

In the previous section we saw that a linear system in triangular form can easily be solved using the method of backsubstitution. We also gave an example to show how a process called Gaussian elimination could be used to transform a system which is not in triangular form into this form. Unfortunately not all linear systems can be transformed in this way into triangular form. (Why? Try to give an example.) In this section we are going to show that Gaussian elimination can be used to transform any system of linear equations (or its augmented matrix) into so-called *row echelon* form. Every system in triangular form is also in row-echelon form, but the converse is not true. However, it is still possible to read off the solution to a system in row-echelon form using backsubstitution. In the process we give a precise algorithm (a "recipe") for doing Gaussian elimination. It may differ slightly from the one you used in the first year, but it has the advantage that it can easily be programmed to be done by a computer.

To start the process, we first need to know exactly what "row echelon form" means. Here is the definition:

Definition 1.4.1 *(a) Any element of a matrix which is the first non-zero element in a row is called a* **pivot***.*
(b) A matrix is in **row echelon form** *if it satisfies the following two conditions:*

1.	*All rows (if any) that contain only zeros are grouped at the bottom of the matrix.*
2.	*Each pivot appears to the right of any pivot in a row above it.*

The first part of the definition is easy, but the second may need some unpacking. What it is really saying is that a row echelon matrix has to look a bit like a staircase, but that the steps need not all be the same width. The matrix below gives a good example of what it could look like:

$$\begin{pmatrix} 0 & \bullet & * & * & * & * & * & * \\ 0 & 0 & \bullet & * & * & * & * & * \\ 0 & 0 & 0 & 0 & \bullet & * & * & * \\ 0 & 0 & 0 & 0 & 0 & 0 & \bullet & * \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

The bullets ($\bullet$) stand for the pivots in the first four rows and are therefore non-zero numbers (not necessarily all the same). Notice that each pivot appears to the right of all pivots above it; this is what forces the matrix to take on the "staircase" form. The stars ($*$) stand for arbitrary numbers and could be zero or non-zero; again, they certainly need not all be equal. The last row has only zeros so has to appear at the bottom of the matrix. Note that a matrix in row-echelon form need **not** have a row of zeros at the bottom; the definition only says that if there are any rows consisting entirely of zeros, they must be at the bottom. Notice also that any element in the matrix which appears below or to the left of a pivot is zero; this is a consequence of the definition too. (Can you work out why?)

Example 1.4.2 Of the following matrices:

(a) $\begin{pmatrix} 7 & 2 & -4 & 1 & 7 & 1 \\ 0 & 0 & -2 & 3 & 0 & 1 \\ 0 & 0 & 0 & 0 & 2 & 2 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$ (b) $\begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ (c) $\begin{pmatrix} 8 & 1 & -2 \\ 0 & 0 & 0 \\ 0 & 4 & 3 \end{pmatrix}$

(d) $\begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$ (e) $\begin{pmatrix} 8 & 1 & -2 \\ 0 & 0 & 1 \\ 0 & 0 & 2 \end{pmatrix}$ (f) $\begin{pmatrix} 2 & 0 & -1 & 3 \\ 0 & -3 & 0 & 5 \\ 0 & 0 & 0 & 2 \end{pmatrix}$

only (a), (d) and (f) are in row echelon form. (Which conditions in the definition of row echelon form are not satisfied by (b), (c) and (e)?)

Now let's see why row echelon form is so useful. We'll suppose in the next examples that a system of equations has had its augmented matrix reduced to row echelon form, and work out the solutions in each case using backsubstitution. (Incidentally, this is precisely how some of the more efficient computer programs actually do it.)

Example 1.4.3 Suppose the augmented matrix for a linear system has been reduced to the matrix in row echelon form

$$\left(\begin{array}{cccc|c} \boxed{2} & 3 & -1 & 5 & 2 \\ 0 & \boxed{3} & 2 & -1 & 2 \\ 0 & 0 & \boxed{\text{-2}} & -8 & 4 \end{array}\right).$$

Since the augmented matrix has five columns, and the last column is the column of constants on the right-hand side of the equations, there must be four variables. Suppose these variables are x_1, x_2, x_3 and x_4. The pivots in rows 1, 2 and 3 are respectively 2, 3 and -2. It is helpful to put squares, or circles, around them, as we've done above. We have also separated the column of constants on the right from the others by means of a vertical line. Our aim is want to find the solution set of the system.

The first step is to write out the associated system of equations; this is:

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

We're now going to introduce some new terminology to help clear up the backsubstitution step, which comes next. The variables x_1, x_2 and x_3 correspond to pivots in the above system; they are called **leading** (or **dependent**) variables. The variable x_4 however does not correspond to any pivot; it is called a **free** variable.

To continue with the problem, we move all free variables to the right hand side of the equations, to obtain:

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

We can now see that if we let $x_4 = t$, where t is an arbitrary number, we can then read off first x_3 and then x_2 and finally x_1, but all in terms of t, of course. (Note that the equations are in triangular form now.) Let's do it: From the third equation we get

$$x_3 = -2 - 4t.$$

Using this in the second equation we get

$$3x_2 = 2 + t - 2(-2 - 4t) = 6 + 9t$$

so

$$x_2 = 2 + 3t.$$

Using the first equation we get

$$2x_1 = 2 - 5t - 3(2 + 3t) + (-2 - 4t) = -6 - 18t$$

so

$$x_1 = -3 - 9t.$$

The solution is thus

$$(x_1, x_2, x_3, x_4) = (-3 - 9t,\ 2 + 3t,\ -2 - 4t,\ t), \quad t \in \mathbf{R}.$$

Example 1.4.4 This example is similar to the previous one, but in this case the augmented matrix for the linear system has been reduced to the matrix in row echelon form

$$\left(\begin{array}{ccccc|c} \boxed{3} & -2 & 1 & 3 & 1 & 14 \\ 0 & 0 & \boxed{2} & 5 & -3 & 2 \\ 0 & 0 & 0 & 0 & \boxed{\text{-3}} & -6 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{array}\right).$$

Note the row of zeros at the bottom of the matrix. There are five variables; let's call them x_1, x_2, x_3, x_4 and x_5. The pivots in rows 1, 2 and 3 are respectively 3, 2 and -3. There is no pivot in row 4! Since the pivots occur in columns 1, 3 and 5, x_1, x_3 and x_5 are dependent variables, and x_2 and x_4 are free variables. The equations associated with this matrix are:

$$\begin{aligned} 3x_1 - 2x_2 + x_3 + 3x_4 + x_5 &= 14 \\ 2x_3 + 5x_4 - 3x_5 &= 2 \\ -3x_5 &= -6 \end{aligned}$$

We take the free variables to the right hand side of the equations to get

$$\begin{aligned} 3x_1 + x_3 + x_5 &= 14 + 2x_2 - 3x_4 \\ 2x_3 - 3x_5 &= 2 - 5x_4 \\ -3x_5 &= -6 \end{aligned}$$

We let $x_2 = s$ and $x_4 = t$, where s and t are arbitrary (real) numbers. We can now read off the solutions in terms of s and t using backsubstitution. From the last equation we get $x_5 = 2$; using the second equation we get

$$2x_3 = 3(2) + 2 - 5t = 8 - 5t$$

so

$$x_3 = 4 - \frac{5}{2}t.$$

Using the first equation we get

$$3x_1 = -(4 - \frac{5}{2}t) - 2 + 14 + 2s - 3t = 8 + 2s - \frac{1}{2}t$$

so

$$x_1 = \frac{8}{3} + \frac{2}{3}s - \frac{1}{6}t.$$

The final solution is

$$(x_1, x_2, x_3, x_4, x_5) = \left(\frac{8}{3} + \frac{2}{3}s - \frac{1}{6}t, s, 4 - \frac{5}{2}t, t, 2\right), s, t \in \mathbf{R}.$$

We hope that you are convinced that if a system of equations is in row echelon form, then it is relatively easy (perhaps rather boring?) to solve the system using backsubstitution. Where do we go from here? Clearly we need a procedure to reduce any system of equations to row echelon form; once we have this, we can then use backsubstitution to solve. Solving systems of linear equations then becomes a two step procedure:

1. Reduce the system to row echelon form.

2. Solve using backsubstitution.

Gaussian elimination is a mechanical procedure which we can use to do step 1. We present it as a **four step algorithm**, which we illustrate in the next example.

Example 1.4.5 We want to solve the following system of equations:

$$\begin{aligned} 6x_3 + 2x_4 - 4x_5 - 8x_6 &= 8 \\ 3x_3 + x_4 - 2x_5 - 4x_6 &= 4 \\ 2x_1 - 3x_2 + x_3 + 4x_4 - 7x_5 + x_6 &= 2 \\ 6x_1 - 9x_2 + 11x_4 - 19x_5 + 3x_6 &= 0. \end{aligned}$$

This is rather a large system of equations to be solving by hand, but it illustrates all the points about doing Gaussian elimination. First we write down the associated augmented matrix:

$$\begin{pmatrix} 0 & 0 & 6 & 2 & -4 & -8 & 8 \\ 0 & 0 & 3 & 1 & -2 & -4 & 4 \\ 2 & -3 & 1 & 4 & -7 & 1 & 2 \\ 6 & -9 & 0 & 11 & -19 & 3 & 0 \end{pmatrix}$$

Now we are ready for the four steps. The first one is

STEP 1: Locate the leftmost nonzero column, and the first pivot of that column.

(A **nonzero column** is a column with at least one nonzero entry.) In our example the first nonzero column is the first column (from the left) and the pivot is the entry 2. (We could also have chosen 6 as a pivot.) Now for step 2.

STEP 2: If necessary (i.e. if the pivot is not in the first row), interchange the first row with the row that contains the pivot.

In our case it is necessary, so we get the matrix

$$\begin{pmatrix} 2 & -3 & 1 & 4 & -7 & 1 & 2 \\ 0 & 0 & 3 & 1 & -2 & -4 & 4 \\ 0 & 0 & 6 & 2 & -4 & -8 & 8 \\ 6 & -9 & 0 & 11 & -19 & 3 & 0 \end{pmatrix}$$

Now for step 3.

STEP 3: Make all other entries in the leftmost nonzero column zero using multiples of row 1.

In our example we need to change to zero the entry 6 in the last row. We do this by adding $(-3)\times$ row 1 to row 4 to get:

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

STEP 4: We now repeat steps 1 to 3 **ignoring the top row**.

If we ignore the first row, the leftmost nonzero column is now the third column and the entry 3 is the first pivot. This means that step 2 is unnecessary. Doing step 3 now, we eliminate the entries below the 3 by adding $(-2)\times$ row 2 to row 3 and then adding row 2 to row 4. This gets us to

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

Now we are at step 4 again. Repeat steps 1 to 3 ignoring both the first and second row. This gets us to

$$\left(\begin{array}{cccccc|c} \boxed{2} & -3 & 1 & 4 & -7 & 1 & 2 \\ 0 & 0 & \boxed{3} & 1 & -2 & -4 & 4 \\ 0 & 0 & 0 & 0 & 0 & \boxed{\text{-4}} & -2 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{array}\right)$$

The matrix is now in echelon form, so we stop. The associated system of equations is

$$\begin{aligned} 2x_1 - 3x_2 + x_3 + 4x_4 - 7x_5 + x_6 &= 2 \\ 3x_3 + x_4 - 2x_5 - 4x_6 &= 4 \\ -4x_6 &= -2 \end{aligned}$$

We can now use backsubstitution to solve: the dependent variables are x_1, x_3 and x_6. Moving the free variables to the right hand side of the equations we get

$$\begin{aligned} 2x_1 + x_3 + x_6 &= 2 + 3x_2 - 4x_4 + 7x_5 \\ 3x_3 - 4x_6 &= 4 - x_4 + 2x_5 \\ -4x_6 &= -2 \end{aligned}$$

Finally, let $x_2 = t_1, x_4 = t_2$ and $x_5 = t_3$ and solve the system by backsubstitution. You should get, after some calculation

$$(x_1, x_2, x_3, x_4, x_5, x_6) = \left(-\frac{1}{4} + \frac{3}{2}t_1 - \frac{11}{6}t_2 + \frac{19}{6}t_3, t_1, 2 - \frac{1}{3}t_2 + \frac{2}{3}t_3, t_2, t_3, \frac{1}{2}\right),$$

where $t_1, t_2, t_3 \in \mathbf{R}$.

A closing remark: you can see that the type of solution you get for a consistent system of equations depends on how many free variables there are. If there are no free variables, you get a unique solution. Otherwise (as in the example above) you get infinitely many solutions. (Why?)

A natural question to ask at this stage is whether Gaussian elimination will also help us to spot when a system of linear equation is inconsistent. The following example looks at such a case.

Example 1.4.6 We try to solve the system

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

The augmented matrix corresponding to the system is

$$
\left(\begin{array}{ccc|c}
0 & 1 & 5 & 4 \\
1 & 4 & 3 & 2 \\
2 & 7 & 1 & 4
\end{array}\right)
$$

We leave it to you to show that Gaussian elimination applied to this matrix gives the echelon form

$$
\left(\begin{array}{ccc|c}
1 & 4 & 3 & 2 \\
0 & 1 & 5 & 4 \\
0 & 0 & 0 & 4
\end{array}\right)
$$

If we write out the equation corresponding to the last row of this matrix, we get

$$0x_1 + 0x_2 + 0x_3 = 4.$$

There are clearly no values of x_1, x_2 and x_3 that satisfy this equation. This shows us that there are no solutions to this system; it is inconsistent.

It is not difficult to see that what we have seen in this particular example applies more generally: If the echelon form of the augmented matrix of a system of linear equations contains a row with all the entries equal to 0, except for the last one, which is **nonzero**, then the system is *inconsistent*. Conversely, if we start with an inconsistent system of equations and perform Gaussian elimination on it, we will always end up with a row like this, since if there is no such row, we will always be able to find at least one solution.

We mention in passing that once a matrix is in row echelon form, we can perform further elementary row operations to get it in what is called **reduced row echelon form**. To do this,

1. Divide each row by the pivot element in that row to get a 1 in the pivot position.

2. Now working from right to left, use elementary row operations to make each entry above a pivot element zero too.

The advantage of this form is that once the augmented matrix of a system is in this form, you can read off the solutions (if any) much more quickly (immediately, if there is a unique solution). But in practice it is more efficient to work with the row echelon form, and we will therefore use it most of the time. The one exception will occur when we find the inverse of an invertible square matrix in Section 1.6. The row echelon form of a matrix is not unique, but it can be shown that the reduced row echelon form is unique.

Summary:

- We've learned about the *row echelon form* of a matrix. (*Warning:* Terminology is not standard here; look carefully at the definitions when you start reading any textbook on linear algebra.)
- We've seen the four step algorithm for performing *Gaussian elimination* which reduces a matrix to row echelon form.
- We've learned to distinguish between *dependent and free variables* in a system of linear equations for which the augmented matrix is in row echelon form.
- We've seen that once the augmented matrix of a system of linear equations is in row echelon form, moving the free variables to the right side of the equation shows you how to write down the solutions of the system in terms of the free variables.
- We've seen that if the echelon form of the augmented matrix of a system contain a row of the form

  $$0\ 0\ 0\ \ldots 0\ b,\ \text{ with } b \neq 0,$$

  then the system is inconsistent.
- It follows that if we have reduced the augmented matrix of a system of linear equations to row echelon form, we will be able to say whether the system has no solutions, a unique solution or infinitely many solutions. In the latter two cases we will be able to write down all the solutions of the system.

Historical note:

Gaussian elimination is named after one of the most prolific mathematicians of all times, Johann Carl Friedrich Gauss (1777 – 1855). Soon after going to school, he amazed his teacher by instantly finding the sum of the integers from 1 to 100 (by noticing that there are 50 pairs of integers each with sum 101). By the age of 20 he had discovered a ruler and compass construction for the regular 17-gon, and soon afterwards he obtained his doctorate with a thesis on the fundamental theorem of algebra. He was initially supported by a stipend from the Duke of Brunswick and this allowed him to devote himself to research.

In 1807 Gauss was appointed as the director of the observatory at Göttingen in Germany, a position he was to occupy for much of his life. In the course of work done on the orbit of the astroid Pallas, Gauss described a systematic method for solving systems of linear equations. This was exactly the algorithm we now know as Gaussian elimination. Gauss had a keen interest in geodesy, and was asked to do a geodetic survey of the state of Hanover. He did the observations by day and the calculations by night. Gaussian elimination was a huge help to him in the enormous amount of calculations he had to do at the time.

Although Gauss gave the first systematic description of the algorithm that now bears his name, he was by no means the first one to use it. In fact, in the early Chinese text *Nine Chapters of the Mathematical Art*, written between 200 BC and 100 BC, an example is given in which a system of three linear equations in three unknowns is solved using a method that is essentially Gaussian elimination followed by backsubstitution. In this example the coefficients of each equation are written as the columns of a matrix (rather than rows), but in all other respects the method is identical to the one described in this section.

Exercises

1. In (a) - (f) determine if the given matrix is in row echelon form.

(a) $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ (b) $\begin{pmatrix} 0 & 1 \\ 2 & 0 \end{pmatrix}$ (c) $\begin{pmatrix} 2 & 1 & -3 \\ 0 & 0 & 1 \end{pmatrix}$

(d) $\begin{pmatrix} 3 & 0 & 1 \\ 0 & -3 & 2 \\ 0 & 4 & 1 \end{pmatrix}$ (e) $\begin{pmatrix} 4 & 1 & 2 & 3 & 0 \\ 0 & 2 & 1 & -1 & 7 \\ 0 & 0 & 0 & 3 & 4 \\ 1 & 0 & 0 & 0 & 2 \end{pmatrix}$ (f) $\begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$

2. In (a) - (e) the augmented matrix for a linear system has been reduced to the given matrix in row echelon form and the variables are given. Find the solution of the system.

(a) $\begin{pmatrix} -2 & 1 & 3 & 4 \\ 0 & 0 & 3 & -6 \end{pmatrix}$ x, y, z

(b) $\begin{pmatrix} 4 & 3 & 7 & 2 & 4 \\ 0 & 0 & 3 & 3 & -6 \end{pmatrix}$ x_1, x_2, x_3, x_4

(c) $\begin{pmatrix} -3 & 2 & 1 & 4 & 6 \\ 0 & 2 & 1 & 2 & -4 \\ 0 & 0 & 2 & 1 & 2 \end{pmatrix}$ x, y, z, w

(d) $\begin{pmatrix} 2 & -1 & -3 & 4 & 2 \\ 0 & 0 & 2 & 1 & -1 \\ 0 & 0 & 0 & 3 & 9 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$ x_1, x_2, x_3, x_4

(e) $\begin{pmatrix} 0 & 4 & -1 & 3 & 7 & 1 \\ 0 & 0 & 0 & 3 & 4 & 9 \\ 0 & 0 & 0 & 0 & 5 & 0 \end{pmatrix}$ x, y, z, u, v

3. Solve each of the following systems by Gaussian elimination.

(a)

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

(b)

$$\begin{aligned} 2x_1 + 3x_2 - x_3 + x_4 &= -5 \\ 4x_1 + 5x_2 + 2x_3 - x_4 &= 4 \\ -2x_1 - x_2 - x_3 - x_4 &= 1 \\ 6x_1 + 7x_2 + x_3 - 4x_4 &= 2 \end{aligned}$$

(c)

$$\begin{aligned} 2u - 3v + w - x + y &= 0 \\ 4u - 6v + 2w - 3x - y &= -5 \\ -2u + 3v - 2w + 2x - y &= 3 \end{aligned}$$

(d)

$$\begin{aligned} 3x_1 - x_2 + x_3 - 4x_4 &= 2 \\ 6x_1 - 3x_2 - x_3 - 4x_4 &= 3 \\ 9x_1 + x_2 \qquad - 8x_4 &= 6 \end{aligned}$$

(e)

$$\begin{aligned} -x_1 + 2x_2 - x_3 &= -4 \\ 3x_1 + 4x_2 + 2x_3 &= 15 \\ -4x_1 + 6x_2 + x_3 &= -7 \end{aligned}$$

4. Use Gaussian elimination and backsubstitution to solve the following system of equations. Remember to write your answer in vector form and show your working.

$$\begin{aligned} x_1 + x_2 + 3x_3 + x_4 &= 2 \\ 2x_1 + 2x_2 + 7x_3 + 4x_4 &= 3 \\ x_1 + x_2 + 5x_3 + 5x_4 &= 0 \end{aligned}$$

5. Let $A = \begin{pmatrix} 5 & -7 & 7 \\ 4 & -3 & 4 \\ 4 & -1 & 2 \end{pmatrix}$. Find a non-zero vector $\mathbf{x}$ such that

   (a) $A\mathbf{x} = \mathbf{x}$;

   (b) $A\mathbf{x} = 5\mathbf{x}$.

6. Say whether each of the following statements is true or false. Give reasons for your answers.
   (a) Every linear system with the same number of equations as unknowns has a unique solution.
   (b) Every linear system with the same number of equations as unknowns has at least one solution.
   (c) A linear system with more equations than unknowns may have an infinite number of solutions.
   (d) A linear system with fewer equations than unknowns may have no solution.

1.5 Inverses of Matrices, and some Logic

In the section on matrix algebra we did not say anything about division of one matrix by another. We'll see that the story here is far more complicated than it is for division of real numbers. In the case of real numbers, we know that for every non-zero real number x there is another real number y such that $xy = 1$. There can be only one such number y, and therefore it is justified to have special name (*multiplicative inverse*) and symbol (x^{-1} or $\frac{1}{x}$) for it. We can then define division with the help of the multiplicative inverse: z divided by x, or z/x, is defined to be zx^{-1}.

We could now try to do the same for matrices. The first step would be to say what is meant by an *inverse* of a matrix. This is what is done in the next definition (one that you should have seen in your first-year course as well). Since identity matrices are multiplicative identities for matrix multiplication, it makes sense to replace the 1 in the equation $xy = 1$ above by an identity matrix of the appropriate size. Since matrix multiplication is **not** commutative, however, we have to be more careful than with real numbers.

Definition 1.5.1 *If A is an $n \times n$ matrix, an* **inverse**, *B, of A is any $n \times n$ matrix such that*

$$AB = I_n = BA,$$

where I_n is the $n \times n$ identity matrix. If a matrix A does have an inverse, then A is said to be **invertible**.

Note that at this stage we are not certain whether a matrix will have an inverse at all, and if it does, whether it might not have more than one. What is clear from the definition is that only square matrices can have inverses. You may remember from first year that some square matrices do **not** have inverses. We shall also see later that if a matrix does have an inverse, then it has only one inverse.

Example 1.5.2 The following matrices do not have inverses:

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

That the first matrix does not have an inverse is trivial, since for any 2×2 matrix, B, we have

$$B\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix},$$

which cannot be the identity matrix!

Suppose $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ were an inverse of the matrix in (b). Then we must have

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

Looking at the entry in the second row and second column, we must therefore have $c.0 + d.0 = 1$ which is clearly impossible for any c and d, so an inverse cannot exist.

So far you have not seen any proofs in these notes. We have asked you to prove a few things in the section on matrix algebra; these mostly involved checking certain facts using the definitions of the various matrix operations. In this section and the next one we'll spend much more time on proving theorems and looking at the logical structure of these proofs. We'll use the proofs as examples to illustrate some of the basic and important things about elementary logic and how it is used in proofs. You will find a more detailed discussion of these matters, with more examples, in Appendix B, and we'll refer you to it from time to time. One of our aims in this module is to help you to read and understand proofs, and to write simple proofs of your own.

It is very important to realise that if you want to prove a theorem, you should know and understand the *definitions* of the concepts that appear in the theorem. Our first theorem below is about inverses; you should therefore know and understand Definition 1.5.1 before you tackle it.

Theorem 1.5.3 *The inverse of a square matrix, if it exists, is unique (or: If a square matrix has an inverse, then it has only one inverse).*

Proof: This proof is typical of those where you are trying to prove that only one of a certain object exists: you assume that there are two such objects and show that they are the same. A little more formally, we want to prove that if B is an inverse of the square matrix A and C is an inverse of A, then $B = C$. Since B and C are both inverses of A, we have

$$AB = BA = I_n \qquad \text{and} \qquad AC = CA = I_n.$$

(This is where we use the definition of an inverse.) Now we use a trick and these equations:

$$B = BI_n = B(AC) = (BA)C = I_nC = C \qquad (*)$$

as we hoped. The trick was to introduce I_n and then rewrite it as AC. You should make sure you understand each of the equalities in $(*)$ and which of the laws of matrix multiplication we use. ■

A consequence of this theorem is that, since the inverse of a matrix A (if it exists) is unique, we can give it a symbol in the same way that we did for numbers. The inverse of A is denoted by the symbol A^{-1}.

In your first year course you learned how to find inverses of matrices using Gauss reduction. Some of you may also have seen a simple formula for the inverse (we now know there is only one) of certain 2×2 matrices; this is given in the next result.

Proposition 1.5.4 *If $ad - bc \neq 0$, then the matrix $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ is invertible, and*

$$A^{-1} = \frac{1}{ad - bc}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}.$$

Proof: According to the definition, A will be invertible if there is a 2×2 matrix B such that $AB = I_2 = BA$. We show that $B = \dfrac{1}{ad-bc}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$ will do. To prove this, notice that

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix} = \begin{pmatrix} ad - bc & 0 \\ 0 & ad - bc \end{pmatrix}$$

The factor $\dfrac{1}{ad - bc}$ will then ensure that the entries on the diagonal are 1.
Now check that $\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ gives the same result. This shows that A is

invertible and that B is an inverse of A. But then Theorem 1.5.3 says that B is *the* inverse of A, and so $A^{-1} = B$. ∎

Incidentally, if B is the inverse of A, we have a case where $AB = BA$. So sometimes we are lucky and have a bit of commutativity in a situation. More often than not we don't, though.

There are formulae for inverses of larger square matrices, but they are not computationally very efficient. It is a general fact that although inverses of matrices are important from a theoretical point of view they are practically of little importance; we will see that all the useful algorithms that we need for working with matrices do not use inverses. Here's an example of what we mean: to solve the matrix equation $A\mathbf{x} = \mathbf{b}$ for $\mathbf{x}$ in the case where A is an invertible square matrix, it might occur to you to find the inverse A^{-1} of A. Then multiplying both sides of the equation by A^{-1} we get $(A^{-1}A)\mathbf{x} = A^{-1}(A\mathbf{x}) = A^{-1}\mathbf{b}$. Since $A^{-1}A = I$, we get $\mathbf{x} = I\mathbf{x} = A^{-1}\mathbf{b}$, so we have solved for $\mathbf{x}$: it is $A^{-1}\mathbf{b}$. Well, while this is correct, and can certainly be used, it will always be more trouble to actually find the inverse A^{-1} than to just use Gaussian elimination to solve for $\mathbf{x}$. You'll see more propaganda about this later.

It is time to introduce some basic ideas and terminology from logic, and review what we have done so far in the light of this. We give a very concise outline here; the details are in Appendix B.1.

- A (mathematical) *statement* or *proposition* is a sentence which is either true or false, but not both.
- When we prove something, we show that a *statement* is true.
- Two or more propositions (statements) can be linked by *connectives* to form a *compound proposition* (*compound statement*).
- *Connectives* are indicated by the words or phrases *and, or, not, if ... then, if and only if.*
- We can use symbols as shorthand for the phrases above; the symbols
  $$\wedge, \vee, \neg, \Rightarrow, \Leftrightarrow$$
  are used respectively for the connectives
  "and", "or", "not", "if ... then" and "if and only if".
- The precise meaning of these connectives can be given by making use of truthtables.

Example 1.5.5 (a) The sentence "3 has a multiplicative inverse" is a proposition, since we can decide whether it is true or false (it is true).

(b) Is the sentence "$AB = BA$" a proposition?
You may have a problem with the fact that we are not told what A and B are. Let's avoid this problem for the moment by assuming that A and B are 2×2 matrices. If we know this, can we say that "$AB = BA$" is a statement? This depends on being able to decide whether it is true or false. Someone with a good memory may say: "It is false; just look at Example 1.2.11." But then someone else may say: "It is true; just take $A = B = I_2$." It now becomes clear that "$AB = BA$" is sometimes true, and sometimes false; it all depends on the choice of A and B. As it stands, it does *not* qualify as a statement. We can think of A and B as being *variables*. Whether the sentence is true or false will depend on the "values" these variables have; for some values it will be true, for others false. Here we use "value" for something that could be put in the place of a variable.
(c) The sentence

$$\text{“If } ad - bc \neq 0, \text{ then } \begin{pmatrix} a & b \\ c & d \end{pmatrix} \text{ is invertible”}$$

looks like a compound proposition. The sentences

$$\text{“}ad - bc \neq 0\text{”} \qquad \text{and} \qquad \text{“} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \text{ is invertible”}$$

are linked by the connective "if ... then". But are these sentences statements? Can we decide whether they are true or false? Surely that depends on the values of a, b, c and d. We again have sentences containing variables; this time they can be taken to be real (or even complex) numbers.

The examples in (b) and (c) show that in mathematics we quite naturally come across sentences that contain variables, and that this disqualifies such sentences from being statements. You may quite rightly feel unhappy about not taking such sentences seriously. They seem to be saying something that makes sense. Perhaps we should have a second look at what they seem to be saying. But let's first agree on a name for such problematical sentences: we'll call a sentence containing variables an **open sentence**. Whether such a sentence is true or false depends on the values of the variables. You can read more about them in Appendix B.3.

There is another bit of terminology associated with such open sentences. When we write down an open sentence, we usually have in mind a set of elements that can be substituted in the place of the variable(s) in the open sentence. We call this set the **universe** for the sentence. Ideally we should specify the universe for the open sentences we use; you will find that this is sometimes omitted if it is clear from the context. We have already suggested the set of all pairs of 2×2 matrices as the universe for the open sentence "$AB = BA$". For the open sentence "$ad - bc \neq 0$" the universe could be taken to be the collection of all ordered sets (a, b, c, d) of real numbers a, b, c and d ($\mathbf{R}^4$ for short).

Associated with an open sentence and a universe there is a **truth set**: the set of all the elements of the universe which when substituted in the open sentence makes it a true statement. So, for example, $(1, 2, 3, 4)$ is in the truth set of $ad - bc \neq 0$, but $(1, 1, 1, 1)$ is not.

But what is the use of open sentences if we cannot even decide whether they are true or false? We need something that will change an open sentence into a statement. If we change the open sentence "$AB = BA$" into

" For all 2×2 matrices A and B, $AB = BA$"

we do get a statement, since we can decide whether it is true or false. (It is false, since we have an example of a pair of 2×2 matrices for which it fails.)

We can also change the open sentence "$AB = BA$" into

" There are 2×2 matrices A and B such that $AB = BA$.

If we do this, we again get a statement, since we can decide whether it is true or false. (It is true.)

Phrases such as "For all" and "There is (are)" are called **quantifiers** and they are used to **bind** the variables in an open sentence to change it into a statement. The examples above introduce the two most important kind of quantifiers. Phrases such as *for all, for every, for any* are called **universal quantifiers** and denoted by the symbol $\forall$, while phrases such as *there is, there exists, for some* are called **existential quantifiers** and denoted by the symbol $\exists$. You can read much more about these in Appendix B.3.

The example (c) is a little more difficult to analyse. You will probably agree that when we say

$$\text{"If } ad - bc \neq 0, \text{ then } \begin{pmatrix} a & b \\ c & d \end{pmatrix} \text{ is invertible."}$$

we really mean

"It does not matter what the real numbers a, b, c and d are,

$$\text{as long as } ad - bc \neq 0, \text{ then } \begin{pmatrix} a & b \\ c & d \end{pmatrix} \text{ is invertible."}$$

Another way to say this is:

$$\text{"For all real numbers } a, b, c, d, \text{ if } ad - bc \neq 0, \text{ then } \begin{pmatrix} a & b \\ c & d \end{pmatrix} \text{ is invertible."}$$

Here the quantifier "For all" is used to bind the variables a, b, c, d in the open sentence

$$\text{"if } ad - bc \neq 0, \text{ then } \begin{pmatrix} a & b \\ c & d \end{pmatrix} \text{ is invertible."}$$

Once we have done this, it becomes a statement; we can show it is true (and have in fact done so already).

This example shows that we tend to be somewhat sloppy when we state results, as was the case with Proposition 1.5.4. What is passed off as a statement, is strictly speaking only an open sentence. Such sloppiness is widespread, and you will come across it often in these notes and many mathematics texts you may read. It is assumed in such cases that it is clear what the quantifier is that is necessary to turn the open sentence into a true statement; almost invariably it will be some form of universal quantifier. We illustrate this with some examples.

Example 1.5.6 Let's look at Theorem 1.5.3: The inverse of a square matrix, if it exists, is unique. In the proof of this theorem we wrote this as: "If B is an inverse of A and C is an inverse of A, then $B = C$". But strictly speaking this is an open sentence, since A is a variable. You will probably all agree that what the sentence is trying to say is that for *every* square matrix, it true that if it has an inverse, then it is unique. We can turn the open sentence above into a statement by writing:

"For every square matrix A, if B is an inverse of A and C is an inverse of A, then $B = C$."

The proof we gave for Theorem 1.5.3 does prove this statement, since it works for *any* square matrix. Note how the connectives "and" and "if ... then" were used in writing the statement.

You may feel that the insistence on putting in quantifiers is bordering on splitting hairs. What makes matters worse is that we are not going to adhere to our own strict standards in future. The reason that we are so petty now is that one should always be aware of the intended quantifier, even when it is not there explicitly. This becomes crucial when trying to prove that a statement is false, as we'll see later.

Two of the connectives listed earlier need some further comment. The word "not" is not strictly speaking a connective, since it is not used to link two statements, but rather to change the meaning of a statement by negating it. Thus applying "not" to the statement "$ad - bc = 0$" we get the statement "$ad - bc \neq 0$", and applying "not" to the statement "A is invertible", we get the statement "A is not invertible".

The connective "if and only if" (which is often abbreviated to "iff") is used to indicate that **two** implications are both true. As an example, the sentence

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \text{ is invertible if and only if } ad - bc \neq 0$$

says two things:

- If $ad - bc \neq 0$, then $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ is invertible.

- If $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ is invertible, then $ad - bc \neq 0$.

When you are asked to prove a statement involving the connective "if and only if", keep in mind that there are two things you need to prove.

It is important when you use **definitions** to realise that they are also compound statements, using the connective "if and only if". The confusing part here is that definitions are usually given with only an "if" where there should really have been an "if and only if". We have been guilty of this ourselves. The definition we gave for an invertible matrix was:

> An $n \times n$ matrix A is invertible if there is a matrix B such that $AB = I_n = BA$.

This should really have read:

> An $n \times n$ matrix A is invertible if and only if there is a matrix B such that $AB = I_n = BA$.

When it is made clear that what is given is a definition, the less precise first version is usually given (and we'll do this in these notes as well). Watch out how both implications in the definition of an invertible matrix are used in the proof of the next theorem.

Most of the theorems you'll see in this course (and elsewhere) will be statements of the form "For every x, if $P(x)$, then $Q(x)$", where $P(x)$ and $Q(x)$ are open sentences depending on the variable x. To prove that such a statement is true, we assume that the statement $P(x)$ is true, and show that it follows from this that the statement $Q(x)$ is true, making sure that our argument is valid for every x in the universe for the open sentences $P(x)$ and $Q(x)$. We have already seen examples of this in the proofs of Theorem 1.5.3 and Proposition 1.5.4, and you'll see it again in the proof of the next theorem.

Theorem 1.5.7 *If A and B are invertible $n \times n$ matrices, then AB is invertible. If this is the case, we have*

$$(AB)^{-1} = B^{-1}A^{-1}.$$

(Note the change of order!)

Before we get started on the proof, note that there are quantifiers missing, but assumed, in the formulation of the theorem. What we want to prove is: "For every positive integer n and for all $n \times n$ matrices A and B, if A is invertible and B is invertible, then AB is invertible."

Proof: If A and B are invertible $n \times n$ matrices, there are matrices A^{-1} and B^{-1} such that $AA^{-1} = I_n = A^{-1}A$ and $BB^{-1} = I_n = B^{-1}B$. To show that AB is invertible, we need to show that there is a matrix C such that $(AB)C = I_n = C(AB)$. We try $C = B^{-1}A^{-1}$. Let's just check the first equality:

$$(AB)C = (AB)(B^{-1}A^{-1}) = A(BB^{-1})A^{-1} = AI_nA^{-1} = AA^{-1} = I_n,$$

as we needed. The check that $C(AB) = I_n$ is similar. This is enough to show that AB is invertible and that C is an inverse for AB; by Theorem 1.5.3 it is the only one and so $(AB)^{-1} = B^{-1}A^{-1}$. Since the proof works for all $n \times n$ matrices A and B and for all n, we have proved the statement. ■

In the above proof, you should be sure about each of the steps in the string of equations. Ask yourself: What have we used at each step? You should also know why we could **not** have tried $A^{-1}B^{-1}$ for the inverse of AB. See what happens if you do!

This theorem enables us to write down a formula for $(A_1A_2 \ldots A_k)^{-1}$. Do this, and check that your formula is correct!

When working with implications, the order in which we write down things is very important. Here is an example.

Look at the statements:

(a) For every square matrix A, if $A = \mathbf{0}$, then A is not invertible.

(b) For every square matrix A, if A is not invertible, then $A = \mathbf{0}$.

These two statements clearly do not say the same thing. We have proved the statement (a) in Example 1.5.2 (the proof works for any square zero matrix). We **cannot** assume that because statement (a) is true, statement (b) will also be true (in fact, it is false).

More generally, if P and Q are statements, then $P \Rightarrow Q$ is a statement again. We call the statement $Q \Rightarrow P$ the **converse** of the statement $P \Rightarrow Q$.

WARNING: If a statement of the form $P \Rightarrow Q$ is true, its converse $Q \Rightarrow P$ need **not** be true.

We tend to use the term "converse" rather loosely. Even though "if $A = \mathbf{0}$, then A is not invertible" is an open sentence rather than a statement, we'll refer to the open sentence "if A is not invertible, then $A = \mathbf{0}$" as its converse. We'll also call the statement (b) above the converse of the statement (a).

We have claimed above that the statement

"For every square matrix A, if A is not invertible, then $A = \mathbf{0}$" $(*)$

is *not* true. How do we prove that a statement of this form is false? The statement claims that *for every* square matrix something is true. To show that the claim is false, it is enough to give an example of *one* square matrix for which that something is not true. The "something" in this case is the implication "if A is not invertible, then $A = \mathbf{0}$". To show that this is not true for one particular matrix A, we have to show that this matrix A is not invertible, and not equal to the zero matrix. This means that to disprove the statement $(*)$ (that is, to show that it is false) we have to find one example of a square matrix that is not invertible and not equal to the zero matrix. This is not difficult; $A = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ will do.

An example like this that is used to disprove a statement containing a universal quantifier is called a **counterexample**. For a more detailed discussion of counterexamples and related matters you can read Appendix B.3.

We have seen in Proposition 1.5.4 that the statement

For all $a, b, c, d \in \mathbf{R}$, if $ad - bc \neq 0$, then $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ is invertible

is true. Its converse is

For all $a, b, c, d \in \mathbf{R}$, if $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ is invertible, then $ad - bc \neq 0$ $(**)$

Is this a true statement? If we want to show it is, it is not immediately clear how one could start a proof. There is a bit of logic that comes to the rescue here. First recall that $\neg Q$ is shorthand for "not Q". A statement of the form

$$P \Rightarrow Q$$

is *logically equivalent* to the statement

$$\neg Q \Rightarrow \neg P.$$

This means that if we can prove that one of them is true, the other will be true as well. We call $\neg Q \Rightarrow \neg P$ the **contra-positive** of $P \Rightarrow Q$. You can read more about logical equivalence and contrapositives in Appendix B.2. There are cases where it turns out to be easier to prove the contrapositive than the statement itself.

Let's return to the statement we are trying to prove, and write down its contrapositive. We have not looked at what is meant by the contrapositive of a statement that contains a quantifier. We'll say that the contrapositive of a statement of the form

$$\text{For every } x,\ P(x) \Rightarrow Q(x)$$

is

$$\text{For every } x,\ \neg\, Q(x) \Rightarrow \neg\, P(x) \qquad .$$

The contrapositive of the statement (∗∗) then becomes

$$\text{For all } a, b, c, d \in \mathbf{R}, \text{ if } ad - bc = 0, \text{ then } \begin{pmatrix} a & b \\ c & d \end{pmatrix} \text{ is not invertible.}$$

This statement is in fact true. You should be able to prove this yourself; it will be easier by the end of the next section.

So far we've been talking only about inverses of matrices and haven't looked at division. You may have noticed that while we *think* of the inverse of A in a similar way to, say, the inverse of 2 (which is $\frac{1}{2}$), we **never** use the notation $\frac{1}{A}$ for A^{-1}. One of the reasons for this is that you might be then tempted to use the symbol $\frac{B}{A}$. This could mean either $A^{-1}B$ or BA^{-1}, and since these could be different you wouldn't know which was intended. You can see that trying to define "division" of matrices is going to get us in a terrible mess, so we don't do it!

Summary:

- We defined inverses of square matrices, and proved that they are unique.
- We looked at some useful concepts from logic and showed how they can help us to prove and disprove statements.

Exercises

1. Prove or disprove each of the following statements:
   (a) If A and B are matrices satisfying $AB = BA = I$, then A and B are both square.
   (b) If A and B are square and $AB = BA$, then $A = B^{-1}$.
2. Prove that if $ad - bc = 0$, then $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ is not invertible.
3. Show that the inverse of an invertible symmetric matrix is again symmetric.
4. In Question 5 of the Exercises in Section 1.2 you discovered that if A and B are two $n \times n$ matrices such that $AB = O$, where O is the $n \times n$ zero matrix, then it need not be the case that $A = O$ or $B = O$. Show that if one of A or B is invertible, then $AB = O$ implies $A = O$ or $B = O$.

5. If A, B and C are $n \times n$ matrices such that $AB = AC$, does it always true that $B = C$? If it is not always true, is it sometimes true? Give reasons for your answers.

1.6 Elementary Matrices and Invertibility

In this section we continue our investigation of invertible matrices. We show that any such matrix can be written as a product of rather special invertible matrices, called "elementary" matrices. In a sense they are rather simple things, so the word elementary is a good one. They also correspond in a very nice way with the elementary row operations which we saw earlier, making the term "elementary" doubly suitable. In fact, we use elementary row operations to define the elementary matrices, as you'll see now.

Definition 1.6.1 *Let e stand for an elementary row operation.*
If A is any matrix, we denote by $e(A)$ the matrix obtained by applying the elementary row operation e to A.
For any n, the matrix obtained by applying e to the $n \times n$ identity matrix I_n is called an ***elementary matrix associated with*** *e. More precisely: any matrix of the form*

$$E = e(I_n)$$

is an elementary matrix.

Note that an elementary matrix is obtained by applying **one** elementary row operation to an identity matrix. **A matrix obtained by applying two or more elementary row operations to an identity matrix does not qualify as an elementary matrix.**

Example 1.6.2 Suppose e is the elementary row operation that adds 2 times row 3 to row 2, and $A = \begin{pmatrix} 2 & 0 & 4 & 3 \\ -1 & 3 & 0 & 2 \\ 5 & 1 & -1 & 0 \end{pmatrix}$. Then

$$e(A) = \begin{pmatrix} 2 & 0 & 4 & 3 \\ 9 & 5 & -2 & 2 \\ 5 & 1 & -1 & 0 \end{pmatrix}.$$

Let's look at an example of each of the three different kinds of elementary matrices.

Example 1.6.3

(a) Suppose e multiplies the third row of a matrix by -2. Then

$$e(I_4) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -2 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

(b) Suppose e interchanges (permutes) row 2 and row 3. Then

$$e(I_3) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$$

(c) Suppose e adds 2 times row 3 to row 2. Then

$$e(I_3) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 2 \\ 0 & 0 & 1 \end{pmatrix}.$$

(d) Notice that identity matrices are also elementary matrices. (Why?)

In general, there is no point in developing a notation which completely specifies which elementary matrix you are using. We will tend to just use the upper-case letter E (or $E_1, E_2, \ldots$ if we want to refer to more than one elementary matrix).

Why have we introduced the notion of an elementary matrix? Precisely because they will allow us to reformulate Gaussian elimination in terms of matrix multiplications rather than row operations. This is explained in the next theorem.

Theorem 1.6.4 *Let e be an elementary row operation and let E be its corresponding $n \times n$ elementary matrix $e(I_n)$. Then, for any $n \times p$ matrix A, we have:*

$$e(A) = EA.$$

Note that the left hand side of the equation above is obtained by performing the elementary operation e on the matrix A, and the right hand side by multiplying A on the left by the elementary matrix E corresponding to the operation e. This theorem says exactly what we want: instead of operating on the rows of a matrix we might just as well multiply it by an elementary matrix. The proof of the theorem is omitted. It involves checking the result for each of the three different kinds of elementary row operations and their corresponding elementary matrices and seeing that the equality holds in each case. We are just going to check some of them here and others will be set as exercises.

Example 1.6.5 Suppose e permutes row 2 and 3. Then

$$e(I_3) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} = E.$$

Let's now pick a 3×4 matrix, say $A = \begin{pmatrix} 2 & 3 & 1 & -1 \\ 0 & -1 & 3 & 2 \\ -2 & 1 & 3 & 4 \end{pmatrix}$ and check that the result holds for this matrix and this elementary operation. Then

$$e(A) = \begin{pmatrix} 2 & 3 & 1 & -1 \\ -2 & 1 & 3 & 4 \\ 0 & -1 & 3 & 2 \end{pmatrix} \text{ and}$$

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

So the result holds in this specific case. It's not difficult to see that the same kind of argument will work for permutations in general. We'll ask you to do checks for the other two types of elementary operations in the exercises. You can also check that for the matrix A and operation e in Example 1.6.2 we have $e(I_3)A = e(A)$.

We've already mentioned that all elementary row operations are reversible using similar elementary row operations. Let's look at the three cases:

(a) If you interchange two rows of a matrix, interchanging them again gets you back to the original matrix.

(b) Multiplying a row by a non-zero constant can be reversed by multiplying the same row by the inverse (reciprocal) of that constant.

(c) Adding a multiple k of a certain row to another row can be undone by subtracting the same multiple k of the first row from the changed row.

What does this mean when expressed in terms of elementary matrices? Perhaps exactly what you expect: it means that all the elementary matrices are invertible and their inverses are also elementary matrices of the same type.

Theorem 1.6.6 *Each elementary matrix is invertible and its inverse is an elementary matrix of the same type.*

Proof: Let e be an elementary row operation and let $E = e(I)$ be its corresponding elementary matrix. Then e has an inverse operation of the same type; we might as well call it e^{-1}. The important thing is that if you apply e^{-1} after you've applied e, you get back to the original matrix, that is, if A is a matrix, then $e^{-1}(e(A)) = A$. Let's denote by E' the elementary matrix corresponding to e^{-1}. (So $E' = e^{-1}(I)$.) Now on the one hand

$$e^{-1}(E) = e^{-1}(e(I)) = I$$

since e^{-1} reverses the effect of e, but, on the other hand

$$e^{-1}(E) = E'E$$

by Theorem 1.6.4. This means that $E'E = I$. Similarly we can check that $EE' = I$. The check is an exercise. We have now proved that $E' = E^{-1}$, so E is invertible. Incidentally, we have proved a bit more; we've actually proved that if $E = e(I)$ then $E^{-1} = e^{-1}(I)$. ∎

We are now nearly ready to consider and prove one of the main theorems concerned with solving systems of linear equations and the invertibility of matrices. It relates a whole lot of different looking conditions to each other in a very nice way. The theorem also has some useful computational consequences which we'll explore. Before we state the theorem we need to pin down a useful concept, called **row equivalence**.

Definition 1.6.7 I*f you can obtain a matrix B from a matrix A by performing elementary row operations on A, then A is said to be* **row equivalent** *to B. More precisely, A is row equivalent to B if there are elementary row operations $e_1, e_2, \ldots, e_k$ such that*

$$B = e_k \ldots e_2 e_1(A).$$

Notice that the above situation is symmetric: if you can get B from A using elementary row operations, you can get A from B by using the inverse operations, which are also elementary. Specifically, if $B = e_k \ldots e_2 e_1(A)$, then $A = e_1^{-1} e_2^{-1} \ldots e_k^{-1} B$.

We can restate a theorem that we've already seen in terms of row equivalence:

Theorem 1.6.8 *Every $m \times n$ matrix is row equivalent to an $m \times n$ matrix in row echelon form.*

Proof: We saw that any matrix can be row reduced to row echelon form, using elementary operations, in a four step algorithm. ■

In order to prove our big theorem, we need to know a bit more about row equivalence. We'll call the next two results "lemmas"; the word "lemma" comes from the Greek and means a smaller result that is used to prove a big result more smoothly.

Lemma 1.6.9 *Let U be an $n \times n$ matrix in row echelon form. If $u_{ii} \neq 0$ for $1 \leq i \leq n$ then U is row equivalent to I.*

Proof: U must look something like

$$\begin{pmatrix} u_{11} & u_{12} & \dots & u_{1n} \\ 0 & u_{22} & \dots & u_{2n} \\ 0 & 0 & \dots & \\ \vdots & & \dots & \vdots \\ 0 & 0 & \dots & u_{nn} \end{pmatrix}$$

Doing something rather similar to Gaussian elimination, we could use row operations involving the last row to make all the entries above u_{nn} zero, and then finally divide the last row by u_{nn} to get a 1 in position (n, n) . We could then turn our attention to the second last column and do the same sort of thing to it using row operations involving the second last row, then the third last column, and so on. Eventually we will get to the point where we have row reduced the matrix U to the identity matrix. (A more formal proof would make use of induction; if you know about proof by induction, try it.) ■

Lemma 1.6.10 *If A and B are row equivalent square matrices, then $A\mathbf{x} = \mathbf{0}$ and $B\mathbf{x} = \mathbf{0}$ have exactly the same solutions.*

Proof: We assume A and B are row equivalent. This means that there are elementary row operations $e_1, e_2, \dots, e_k$ such that $B = e_k \dots e_2 e_1 A$. Let's rephrase that in terms of elementary matrices: we can find elementary matrices $E_1, E_2, \dots, E_k$ such that

$$B = E_k \dots E_2 E_1 A.$$

Now suppose $\mathbf{u}$ is a solution of $A\mathbf{x} = \mathbf{0}$. This means that $A\mathbf{u} = \mathbf{0}$. But then

$$B\mathbf{u} = (E_k \dots E_2 E_1 A)\mathbf{u} = (E_k \dots E_2 E_1)(A\mathbf{u}) = E_k \dots E_2 E_1 \mathbf{0} = \mathbf{0}.$$

So $\mathbf{u}$ is also solution of $B\mathbf{x} = \mathbf{0}$. This shows that every solution of $A\mathbf{x} = \mathbf{0}$ is also a solution of $B\mathbf{x} = \mathbf{0}$. By using the inverses of the E_i's we could reverse the argument and show that any solution of $B\mathbf{x} = \mathbf{0}$ is a solution of $A\mathbf{x} = \mathbf{0}$. That is all we wanted to show. ■

In order to state the theorem, we need a bit more terminology. We have seen that we can generally write a system of linear equations as a matrix equation of the form $A\mathbf{x} = \mathbf{b}$, with A the coefficient matrix, $\mathbf{x}$ the vector of variables and $\mathbf{b}$ the vector of constants. In the case where $\mathbf{b} = \mathbf{0}$ (i.e. all the constants are 0), we say that the system is **homogeneous**; if $\mathbf{b} \neq \mathbf{0}$, the system is called **non-homogeneous**.

For the homogeneous system $A\mathbf{x} = \mathbf{0}$, we can immediately spot one solution: $\mathbf{x} = \mathbf{0}$ (i.e. the case where all the variables are 0). This is often called the *trivial solution*, or the *zero solution*. For some coefficient matrices A, one finds that this is the **only** solution of the equation $A\mathbf{x} = \mathbf{0}$. But there are other coefficient matrices for which there are many solutions (including, of course, the trivial solution). We'll see that this distinction is very important, and we therefore give special names to these two kinds of matrices.

Definition 1.6.11 *A matrix A is said to be* ***singular*** *if the equation $A\mathbf{x} = \mathbf{0}$ has more than one solution; otherwise (i.e in the case the equation $A\mathbf{x} = \mathbf{0}$ has only the trivial solution $\mathbf{x} = \mathbf{0}$) A is said to be* ***non-singular****.*

Example 1.6.12 We want to decide whether the following matrices are singular or non-singular:

$$\text{(a) } A = \begin{pmatrix} 1 & 2 \\ 2 & 4 \end{pmatrix} \qquad\qquad \text{(b)} \quad B = \begin{pmatrix} 1 & 2 \\ 2 & 5 \end{pmatrix}.$$

(a) In this case $A\mathbf{x} = \mathbf{0}$ has many solutions. For example, $\mathbf{x} = \begin{pmatrix} 2 \\ -1 \end{pmatrix}$ is one, and since the zero vector is also a solution, we already have more than one solution. Thus A is singular.
(b) On the other hand, a bit of Gaussian elimination shows you that $B\mathbf{x} = \mathbf{0}$ has only the trivial solution, so B is non-singular. Notice also that A is not invertible and that B is; this is not a coincidence as you will see.

At last we are ready to state and prove the major theorem of this section:

Theorem 1.6.13 (*Invertibility Theorem) Let A be an $n \times n$ matrix. Then the following statements are equivalent:*

(a) A is invertible.

(b) $A\mathbf{x} = \mathbf{b}$ has a unique solution for every n-vector $\mathbf{b}$.

(c) A is non-singular.

(d) A is row equivalent to I_n.

(e) A is a product of elementary matrices.

What is meant by "the following statements are equivalent"? It means that if we choose *any* two statements in the list, each one of them will imply the other. As an example, once we've proved the theorem, it will follow that if A is non-singular, then A is a product of elementary matrices **and** if A is a product of elementary matrices, then A is non-singular. Does this mean that in order to prove this theorem we'll have to look at all possible pairs of statements from the list and prove that for every such pair, each statement of the pair implies the other? This would clearly be a very tedious and time-consuming process. So we rather use the following far more economical strategy: We prove that

$$(a) \Rightarrow (b) \Rightarrow (c) \Rightarrow (d) \Rightarrow (e) \Rightarrow (a).$$

If we can do this, it means that if we start with any one of the conditions from (a) to (e), then we can get to any of the other conditions with a string of implications. This is exactly what we need to show that any two, and hence all, of the conditions are equivalent.

We can now start with the proof of the theorem. You will see that we use the same method that we've used before to prove most of the implications (the so-called *direct proof*). But in one case we also make use of *proof by contradiction* to prove an implication.

To prove that the implication $P \Rightarrow Q$ is true using a proof by contradiction, we assume that P is true but that Q is false. We then try to show that this leads to a *contradiction*. If we can do this, we can deduce that our assumption that P is true **and** Q is false cannot be true. Hence if P is true, Q must be true, that is P implies Q.

You have already seen a simple example of this type of proof in Example 1.5.2, when we proved that the 2×2 zero matrix is not invertible. In that example we can take P to be the statement "$A = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$" and Q to be the statement "A is not invertible." We then assume that P is true and Q is false: this means that A the zero matrix and A is invertible. But then there must be a matrix B such that $AB = I_2$, and as we've seen, this clearly leads to a contradiction. Hence our assumption that A is invertible is false, and so A is not invertible.

You can read more about proof methods in Appendix B.4

Proof: (of Theorem 1.6.13)

(a) $\Rightarrow$ (b): We assume A is invertible, so A^{-1} exists. We first show that there is at least one solution to the equation $A\mathbf{x} = \mathbf{b}$, that is that there exists a solution; this is known as an *existence proof.* Then we show that there is at most one solution, that is that the solution is unique; this part is known as a *uniqueness proof.* (The whole proof is called an *existence-uniqueness proof.*)

Existence: We claim that $\mathbf{x} = A^{-1}\mathbf{b}$ is a solution. To check this, we must show that if we substitute $A^{-1}\mathbf{b}$ for $\mathbf{x}$ we get a true statement. Substituting $A^{-1}\mathbf{b}$ for $\mathbf{x}$ we get

$$A(A^{-1}\mathbf{b}) = (AA^{-1})\mathbf{b} = I\mathbf{b} = \mathbf{b}$$

as required. (This means that the existence of a solution is proved.)

Uniqueness: We now claim that this is the only possible solution. Let's suppose that $\mathbf{x}'$ is a solution too (you've seen this kind of thing before, in the proof of Theorem 1.5.3); then

$$A\mathbf{x}' = \mathbf{b} \Rightarrow A^{-1}(A\mathbf{x}') = A^{-1}\mathbf{b} \Rightarrow \mathbf{x}' = A^{-1}\mathbf{b},$$

so in fact the only solution is indeed $A^{-1}\mathbf{b}$. (The uniqueness of the solution is therefore proved.)

(b) $\Rightarrow$ (c): We assume $A\mathbf{x} = \mathbf{b}$ has a unique solution for every n-vector $\mathbf{b}$. But then this must be true for $\mathbf{b} = \mathbf{0}$, so then $A\mathbf{x} = \mathbf{0}$ has a unique solution. But that is just the definition of A being non-singular, so we've proved that (c) holds.

(c) $\Rightarrow$ (d): We'll assume $A\mathbf{x} = \mathbf{0}$ has a unique solution and hope to deduce that we can row reduce A to I_n. We can certainly reduce A to a matrix $U = \begin{pmatrix} u_{ij} \end{pmatrix}$ in row echelon form. Then matrix U must look like this:

$$\begin{pmatrix} u_{11} & u_{12} & \dots & u_{1n} \\ 0 & u_{22} & \dots & u_{2n} \\ 0 & 0 & \dots & \\ \vdots & & \dots & \vdots \\ 0 & 0 & \dots & u_{nn} \end{pmatrix}.$$

If we can show that the u_{ii} are non-zero for $1 \leq i \leq n$ then Lemma 1.6.9 will ensure that we can carry on row reducing until we obtain I_n as we hoped. We now prove, by contradiction, the statement

If $A\mathbf{x} = \mathbf{0}$ has a unique solution, then $u_{ii} \neq 0$ for $1 \leq i \leq n$.

Suppose that one of the u_{ii}'s is zero. Then, because U is a square matrix in row echelon form, u_{nn} must be zero too. But that means that we have at most $n-1$ pivots, so at least one free variable in the equation $U\mathbf{x} = \mathbf{0}$. That means that we can find infinitely many solutions for this equation, and so U is singular. But since U and A are row equivalent, we have by Lemma 1.6.10 that $A\mathbf{x} = \mathbf{0}$ has infinitely many solutions and so A is singular. This is a contradiction of our assumption (c), that A is non-singular and therefore that $A\mathbf{x} = \mathbf{0}$ has a unique solution. so the assumption that there is a u_{ii} equal to 0 is wrong. Hence we have $u_{ii} \neq 0$ for every i, and the result is proved.

(d) $\Rightarrow$ (e): We assume A is row equivalent to I. That means that there is a sequence of elementary matrices $E_1, E_2, \ldots, E_k$ such that

$$E_k \ldots E_2 E_1 A = I.$$

But then we can easily see that

$$A = E_1^{-1} E_2^{-1} \ldots E_k^{-1},$$

so A is a product of elementary matrices (why?) as needed.

(e) $\Rightarrow$ (a): If A is a product of elementary matrices, it is a product of invertible matrices since elementary matrices are invertible. But a product of invertible matrices is invertible (use Theorem 1.5.7), so we are finished, and the whole theorem is now proved. ■

The equivalence of (a) and (e) of the theorem is useful: it says that the building blocks of invertible matrices are the elementary matrices. (In rather a similar way, prime numbers are the building blocks for all non-zero integers.) It also will give us a way of calculating inverses. (You have seen this before, but the approach here is a bit more sophisticated).

Buried in the theorem is a fact that enables us to actually calculate inverses: If A is invertible, then we know now that A is row equivalent to I. This means that $I = E_k \ldots E_2 E_1 A$, and from this it follows that

$$A^{-1} = IA^{-1} = E_k \ldots E_2 E_1 A A^{-1} = E_k \ldots E_2 E_1.$$

So to find A^{-1}, all we need to do is to keep track of all the E_i we use to reduce A to the identity matrix. A simple way of doing this is to write down A and I side by side and reduce A to I, but applying exactly the same operations to I as you go. When you stop, you will have I on the left and A^{-1} on the right. This follows from the fact that on the right you will have $E_k \ldots E_2 E_1 I = E_k \ldots E_2 E_1$, and this is exactly A^{-1}, as we've seen above. The example below shows how this is done; make sure you understand each step.

Example 1.6.14 We find the inverse of the matrix

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

(If A has no inverse, this will become clear as we go along.)

Put a vertical line between the matrix A on the left and I_3 on the right. When you have I_3 on the left of your line after the reduction, you will have the A^{-1} on the right of your line. (In what follows below and later in the text, we use R_3, say, to indicate Row 3.)

$$\left(\begin{array}{ccc|ccc} 1 & 1 & 3 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 \\ 3 & 1 & 2 & 0 & 0 & 1 \end{array}\right) \xrightarrow[R_3 \to R_3 + (-3)R_1]{} \left(\begin{array}{ccc|ccc} 1 & 1 & 3 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & -2 & -7 & -3 & 0 & 1 \end{array}\right)$$

$$\xrightarrow[R_2 \leftrightarrow R_3]{} \left(\begin{array}{ccc|ccc} 1 & 1 & 3 & 1 & 0 & 0 \\ 0 & -2 & -7 & -3 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 \end{array}\right)$$

$$\xrightarrow[R_2 \to R_2 + 7R_3]{} \left(\begin{array}{ccc|ccc} 1 & 1 & 3 & 1 & 0 & 0 \\ 0 & -2 & 0 & -3 & 7 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 \end{array}\right)$$

$$\xrightarrow[R_1 \to R_1 + (-3)R_3]{} \left(\begin{array}{ccc|ccc} 1 & 1 & 0 & 1 & -3 & 0 \\ 0 & -2 & 0 & -3 & 7 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 \end{array}\right)$$

$$\xrightarrow[R_2 \to -\frac{1}{2}R_2]{} \left(\begin{array}{ccc|ccc} 1 & 1 & 0 & 1 & -3 & 0 \\ 0 & 1 & 0 & \frac{3}{2} & -\frac{7}{2} & -\frac{1}{2} \\ 0 & 0 & 1 & 0 & 1 & 0 \end{array}\right)$$

$$\xrightarrow[R_1 \to R_1 + (-1)R_2]{} \left(\begin{array}{ccc|ccc} 1 & 0 & 0 & -\frac{1}{2} & \frac{1}{2} & \frac{1}{2} \\ 0 & 1 & 0 & \frac{3}{2} & -\frac{7}{2} & -\frac{1}{2} \\ 0 & 0 & 1 & 0 & 1 & 0 \end{array}\right)$$

So the inverse of A is $A^{-1} = \begin{pmatrix} -\frac{1}{2} & \frac{1}{2} & \frac{1}{2} \\ \frac{3}{2} & -\frac{7}{2} & -\frac{1}{2} \\ 0 & 1 & 0 \end{pmatrix}$.

This method can be speeded up quite a bit by doing more than one step at a time. As mentioned above, it also reveals whether the given matrix actually has an inverse or not. If you try to apply the method and you find that you are not able to row reduce the matrix to the identity matrix, then the matrix does not have an inverse. (Make sure that you know why this is the case!)

This is the one case where we have to continue with Gaussian elimination to get to the *reduced* row echelon form of the given matrix A. If the reduced row echelon form of A is the identity matrix, A is invertible; if not, it is not invertible.

Summary:

- We defined elementary matrices (which are invertible and whose inverses are themselves elementary). Elementary row operations can be replaced by multiplication by elementary matrices.
- We defined row equivalence of matrices, and singularity and non-singularity.
- We proved an important theorem which gives various equivalent conditions for deciding when a matrix is invertible.
- We saw how to calculate the inverse of a square matrix (if it has one).

Exercises

1. In each of the cases below, find the inverse operation, e^{-1} of the given elementary row operation e.

   (a) Interchange the first and third row of 4×4 matrices.

   (b) Add -2 times the first row to the second row of 3×3 matrices.

   (c) Multiply the third row of a 3×5 matrix by $\frac{2}{3}$.

   (d) Add 7 times the fourth row to the second row of 4×8 matrices.

2. In each of the cases below, determine if the given matrix is an elementary matrix. If it is, find the corresponding elementary operation.

   (a) $\begin{pmatrix} -1 & 0 & 2 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ (b) $\begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$

(c) $\begin{pmatrix} 1 & 0 & 0 \\ 2 & 1 & 0 \\ 0 & 2 & 1 \end{pmatrix}$ (d) $\begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$

3. In this question we write E for the elementary matrix corresponding to the elementary row operation e.

   (a) Let e be the elementary row operation that adds 5 times row 1 to row 2, and let
   $$B = \begin{pmatrix} 1 & 2 \\ 3 & -1 \\ 4 & 0 \end{pmatrix}.$$
   Find: $e(I_3)$, $e(B)$, EB.

   (b) Let e be the elementary row operation that multiplies Row 2 by 6, and let
   $$C = \begin{pmatrix} 1 & 2 \\ 3 & -1 \end{pmatrix}.$$
   Find: $e(I_2), e(C), EC$.

   Compare your answers with Theorem 1.6.4 and Example 1.6.5.

4. Consider the matrix $A = \begin{pmatrix} 1 & 0 \\ 2 & 3 \end{pmatrix}$

   (a) Find elementary matrices E_1 and E_2 such that $E_2E_1A = I$.

   (b) Write A^{-1} as a product of elementary matrices.

   (c) Write A as a product of elementary matrices.

5. In each of the following cases, determine if the given matrix has an inverse, and find the inverse if it exists. Check your answer by calculating $A \cdot A^{-1}$.

   (a) $\begin{pmatrix} -1 & 2 \\ -3 & 5 \end{pmatrix}$ (b) $\begin{pmatrix} 3 & -2 \\ 6 & -4 \end{pmatrix}$ (c) $\begin{pmatrix} 1 & 1 \\ 3 & 2 \end{pmatrix}$ (d) $\begin{pmatrix} 2 & 5 \\ 1 & 2 \end{pmatrix}$

   (e) $\begin{pmatrix} 1 & 2 & 3 & 1 \\ 1 & 3 & 3 & 2 \\ 2 & 4 & 3 & 3 \\ 1 & 1 & 1 & 1 \end{pmatrix}$ (f) $\begin{pmatrix} 0.5 & 0 & 0.5 \\ 0 & 1 & 0 \\ 0.5 & 0 & -0.5 \end{pmatrix}$ (g) $\begin{pmatrix} 1 & 1 & 0 & 0 \\ 3 & 2 & 0 & 0 \\ 0 & 0 & 2 & 5 \\ 0 & 0 & 1 & 2 \end{pmatrix}$

6. Use Theorem 1.6.13 to show that, if A and B are square and $AB = I$ then $BA = I$. [Hint: Use (c) of this theorem.]

7. Use Theorem 1.6.13 (**not** Theorem 1.5.7) to show that, if A and B are square and AB is invertible, then A and B are both invertible too.
[Hint: Prove B invertible first using Theorem 1.6.13(c).]

8. Let A be an $m \times n$ matrix, $\mathbf{b}$ a non-zero n-vector. Suppose the system of linear equations $A\mathbf{x} = \mathbf{b}$ is consistent, and $\mathbf{x} = \mathbf{c}$ is a solution of $A\mathbf{x} = \mathbf{b}$. (There may be many solutions; $\mathbf{c}$ is just one of them.) Show that **any** solution of $A\mathbf{x} = \mathbf{b}$ can be written in the form $\mathbf{x} = \mathbf{z} + \mathbf{c}$, where $\mathbf{z}$ is a solution of the homogeneous equation $A\mathbf{x} = \mathbf{0}$.

9. In this question, $A = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 1 & 1 \\ 0 & 1 & 2 \end{pmatrix}$.

   (a) Find all vectors $\mathbf{b}$ for which the equation $A\mathbf{x} = \mathbf{b}$ has:
   (i) infinitely many solutions
   (ii) no solutions
   (iii) a unique solution.
   Show how you arrived at your answer.

   (b) Is A singular or non-singular? Justify your answer.

10. Prove or disprove:

    (a) If N is an $n \times n$ matrix and $N^3 = O$, then $I_n - N$ is non-singular.

    (b) If A is an $m \times n$ matrix and if $A\mathbf{x} = \mathbf{0}$ has a unique solution, then $A\mathbf{x} = \mathbf{b}$ has a unique solution for every m-vector $\mathbf{b}$.

11. In this question, $A = \begin{pmatrix} 1 & 0 & 0 \\ 4 & 1 & 5 \\ 3 & 0 & 1 \end{pmatrix}$.

    (a) Write A^{-1} as a product of elementary matrices.

    (b) Write A as a product of elementary matrices. (Give each elementary matrix explicitly.)

12. If B is a square matrix and $B = E_k \dots E_2 E_1 U$ for some elementary matrices $E_k, \dots, E_2, E_1$ and U is in row echelon form, is B invertible? Justify your answer.

1.7 Determinants

Some of you may have seen determinants of 2×2 or even 3×3 matrices in earlier courses in Mathematics or Applied Mathematics. In this section we look briefly at more general determinants. But what is a determinant, and why are we interested in it at all? Essentially, a determinant is a **number** that we associate with any *square* matrix. The property of determinants that we will be primarily interested in is the way in which it "measures" whether the matrix is invertible or not. We'll see that the determinant of a square matrix is 0 if and only if it is *not* invertible. From a numerical point of view the determinant is also useful. It turns out that if the absolute value of the determinant is small, then the matrix can be difficult to work with when it comes to solving systems of equations with the matrix as coefficient matrix.

We can think of a 2×2 matrix as a function from the plane $\mathbf{R}^2$ into itself: every point in $\mathbf{R}^2$ has a position vector, and if we multiply this vector by the matrix, we get another 2-vector, which we can think of as the position vector of a point in the plane. It can be shown that determinants can be used to measure the factor by which a 2×2 matrix (considered as such a function) will scale the area of a region in the plane. The same is true for 3×3 matrices and volumes. This lies behind the use of a special determinant, called a Jacobian, used in double and triple integrals, as you will see if you do a course in advanced calculus. Some of you may also have seen determinants in Statistics courses. By and large though, the value of determinants lies more in their theoretical uses, rather than practical applications. From our point of view they will be useful mainly in the study of eigenvalues and eigenvectors, as we'll see in Chapter 4.

There are many different (but equivalent) ways of defining the determinant of a square matrix. We use the notation $\det(A)$ or $|A|$ for the determinant of the matrix A. A warning is probably appropriate here: The notation $|A|$ has **nothing** to do with absolute values. The determinant of a matrix can be a negative number, or even a complex number (in the case where A is a complex matrix).

Most of you have probably seen a definition for 2×2 matrices. Here it is again:

$$\text{If } A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}, \text{ then } |A| = \det(A) = a_{11}a_{22} - a_{12}a_{21}.$$

Example 1.7.1

(a) $\begin{vmatrix} 1 & 2 \\ 2 & 4 \end{vmatrix} = 1.4 - 2.2 = 0$. Notice that $\begin{pmatrix} 1 & 2 \\ 2 & 4 \end{pmatrix}$ is not invertible.

(b) $\begin{vmatrix} 1 & 2 \\ 3 & 4 \end{vmatrix} = 1.4 - 2.3 = -2$. Notice that $\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$ is invertible.

Note that $\begin{vmatrix} a & b \\ c & d \end{vmatrix} = 0$ if and only if one row is a multiple of the other. Try to prove this yourself.

We are going to give a **recursive definition** for the determinant of a square matrix. This means that we'll define the determinant of an $n \times n$ matrix in terms of determinants of $(n-1) \times (n-1)$ matrices. If we start from scratch, we should first define the determinant of a 1×1 matrix! Such a matrix is just a number, and we define its determinant to be equal to that number:

$$\text{If } A = \begin{pmatrix} a \end{pmatrix}, \text{ then } \det(A) = a.$$

A closer look at the definition of the determinant of a 2×2 matrix given above shows that we can interpret it in the following rather complicated way: a_{11} is an entry from the first row of A, and it is multiplied by the determinant of the 1×1 matrix left when the row and column of A containing a_{11} is deleted, i.e. by $\det\begin{pmatrix} a_{22} \end{pmatrix} = a_{22}$, to give $a_{11}a_{22}$. The second term $-a_{12}a_{21}$ can be interpreted in the same way, but it includes a sign change. The general definition for determinants will follow the same pattern. To make it easier to state, we introduce some handy terminology and notation.

Definition 1.7.2 *Let A be a square matrix.*

*(a) If we delete the i^{th} row and j^{th} column of A, the determinant of the resulting matrix is called the $(i,j)^{th}$ **minor** of A (often denoted by M_{ij}). (If A is an $n \times n$ matrix, M_{ij} will be the determinant of an $(n-1) \times (n-1)$ matrix.)*

*(b) The number $(-1)^{i+j}M_{ij}$ is called the $(i,j)^{th}$ **cofactor** of A (often denoted by C_{ij}).*

Example 1.7.3 If $A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$, then $M_{11} = a_{22}$ and $M_{12} = a_{21}$;

$C_{11} = (-1)^{1+1}a_{22} = a_{22}$ and $C_{12} = (-)^{1+2}a_{21} = -a_{21}$.

If $A = \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix}$, then

$$M_{11} = \begin{vmatrix} a_{22} & a_{23} \\ a_{32} & a_{33} \end{vmatrix}, \quad M_{12} = \begin{vmatrix} a_{21} & a_{23} \\ a_{31} & a_{33} \end{vmatrix} \quad M_{13} = \begin{vmatrix} a_{21} & a_{22} \\ a_{31} & a_{32} \end{vmatrix}$$

and

$$C_{11} = (-1)^{1+1}M_{11} = M_{11}, \quad C_{12} = (-1)^{1+2}M_{12} = -M_{12}, \quad C_{13} = (-1)^{1+3} = M_{13}.$$

We can now rewrite the definition of the determinant of a 2×2 matrix in terms of the new notation:

$$\text{If } A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}, \text{ then } |A| = \det(A) = a_{11}C_{11} + a_{12}C_{12}.$$

We use this as motivation for the definition of the determinant of a 3×3 matrix.

Definition 1.7.4 *Let A be a 3×3 matrix. Then the determinant of A is defined by*

$$\det(A) = a_{11}C_{11} + a_{12}C_{12} + a_{13}C_{13};$$

in full:

$$\begin{aligned} \det \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix} &= a_{11} \begin{vmatrix} a_{22} & a_{23} \\ a_{32} & a_{33} \end{vmatrix} - a_{12} \begin{vmatrix} a_{21} & a_{23} \\ a_{31} & a_{33} \end{vmatrix} \\ &\quad + a_{13} \begin{vmatrix} a_{21} & a_{22} \\ a_{31} & a_{32} \end{vmatrix}. \end{aligned}$$

Example 1.7.5 We illustrate the above definition:

$$\begin{aligned} \begin{vmatrix} 2 & 3 & 1 \\ 5 & 3 & 0 \\ 7 & 6 & 4 \end{vmatrix} &= 2 \begin{vmatrix} 3 & 0 \\ 6 & 4 \end{vmatrix} - 3 \begin{vmatrix} 5 & 0 \\ 7 & 4 \end{vmatrix} + 1 \begin{vmatrix} 5 & 3 \\ 7 & 6 \end{vmatrix} \\ &= 2(3 \times 4 - 0 \times 6) - 3(5 \times 4 - 0 \times 7) + 1(5 \times 6 - 3 \times 7) \\ &= 24 - 60 + 9 = -27 \end{aligned}$$

Note that in order to find the determinant of a 3×3 matrix, we have to know how to find the determinant of a 2×2 matrix. We now give the definition for a determinant of a $n \times n$ matrix, using the same idea.

Definition 1.7.6 *Let A be an $n \times n$ matrix. Them the determinant of A is defined by*

$$\begin{aligned} det(A) &= a_{11}C_{11} + a_{12}C_{12} + \ldots + a_{1n}C_{1n} \\ &= \sum_{j=1}^{n} a_{1j}C_{1j}. \end{aligned}$$

We see again that to calculate the determinant of an $n \times n$ matrix we need to know how to calculate the determinant of an $(n-1) \times (n-1)$ matrix. It is in this sense that the definition is recursive.

The formula in the definition above is often referred to as the **expansion of** $\det(A)$ **along the first row**.

It is clear from the definition that even calculating the value of the determinant of a 3×3 matrix involves a fair amount of work, and things get worse the larger the matrices become. We will soon look at some properties of determinants that will help to simplify the calculations. But fortunately we can use OCTAVE or the *Linear Algebra Toolkit* to calculate determinants, and this is definitely the way to go for large matrices. In most of our examples we'll stick to 3×3 matrices.

We now state two important properties of determinants, but without proof. The proofs use induction and are rather long and somewhat messy (since we have to keep track of the subscripts). They require perseverance more than anything else! If you are interested, you'll find proofs in any good textbook on linear algebra with a proper treatment of determinants.

The first property says that a determinant can be expanded along the first column as well:

Proposition 1.7.7 L*et A be an $n \times n$ matrix. Then*

$$\det(A) = a_{11}C_{11} + a_{21}C_{21} + \cdots + a_{n1}C_{n1} = \sum_{i=1}^{n} a_{i1}C_{i1}.$$

Corollary 1.7.8 *If A is a square matrix,* $\det(A^T) = \det(A)$.

(A *corollary* to a proposition or a theorem is a result that can easily be deduced from the proposition or theorem.)

Proof: The expansion of $\det(A^T)$ along the first row equals the expansion of $\det(A)$ along its first column. ■

The second property says that interchanging two rows in a matrix results in a change of sign in the determinant:

Proposition 1.7.9 L*et A be a square matrix and B be the matrix obtained by interchanging any two rows of A. Then*

$$\det(B) = -\det(A).$$

Corollary 1.7.10 *Let A be a square matrix and B be the matrix obtained by interchanging any two columns of A. Then*

$$\det(B) = -\det(A).$$

Proof: Use Corollary 1.7.8 and the fact that interchanging two columns in A has the same result as interchanging the corresponding rows in A^T. ■

We are now in a position to prove that a determinant may be expanded along any row or column.

Theorem 1.7.11 L*et A be an $n \times n$ matrix. Then*

(a) $\det(A) = \sum_{j=1}^{n} a_{ij}C_{ij}$ *for any particular i between* 1 *and n.*

(We refer to this as expanding $\det(A)$ *along the i^{th} row.)*

(b) $\det(A) = \sum_{i=1}^{n} a_{ij}C_{ij}$ *for any particular j between* 1 *and n.*

(This we refer to as expanding det(A) along the j^{th} column.)

Proof: (a) Let $1 < i \leq n$. We can make row i the first row by interchanging adjacent rows $i-1$ times. Let B be the matrix obtained in this way. Repeated application of Proposition 1.7.9 then gives $\det(B) = (-1)^{i-1}\det(A)$. Let us write A_{ij} for the $(n-1) \times (n-1)$ matrix obtained by deleting the i-th row of A and the j-th column of A, and similarly for B. Then it follows that $A_{ij} = B_{1j}$, and also $a_{ij} = b_{1j}$. Hence

$$\begin{aligned}
\det(A) = (-1)^{i-1}\det(B) &= (-1)^{i-1}\sum_{j=1}^{n}(-1)^{1+j}b_{1j}\det(B_{1j}) \\
&= (-1)^{i-1}\sum_{j=1}^{n}(-1)^{1+j}a_{ij}\det(A_{ij}) \\
&= \sum_{j=1}^{n}(-1)^{i+j}a_{ij}\det(A_{ij}) \\
&= \sum_{j=1}^{n}a_{ij}C_{ij}.
\end{aligned}$$

(b) The proof is similar, but uses Proposition 1.7.7. ■

We now give some further useful properties of determinants. For the first one, recall (from the first tutorial) that an *upper triangular matrix* is a square matrix with all the entries below the main diagonal equal to 0; a *lower triangular matrix* has the entries above the diagonal 0.

Theorem 1.7.12 *Let A be an $n \times n$ matrix.*

(a) If A is a triangular matrix (upper or lower) then $\det(A) = a_{11}a_{22}\ldots a_{nn}$.

(b) If a row or column of A has zeros only then $\det(A) = 0$.

(c) If A has two identical rows (or columns), then $\det(A) = 0$.

(d) If a row or column of A is multiplied by a constant k, then the determinant of the resulting matrix is $k\det(A)$. This means that for an $n \times n$ matrix A, $\det(kA) = k^n \det(A)$.

(e) If the matrix B is obtained from A by adding a multiple of one row of A to another row of A, then $\det(B) = \det(A)$.

Proof: (a) If A is lower triangular, we can expand along the first row, in which only the first entry is (possibly) not zero. Thus the expansion will have at most one non-zero term. The minor in this term can again be expanded along its first row, in which the only the first entry is (possibly) non-zero. Repeating the process leads to the result.

(b) Expand along the zero row or column.

(c) Let B be the matrix obtained from A by interchanging the two identical rows. Then we have, on the one hand, $\det(B) = -\det(A)$ (by Proposition 1.7.9), and on the other, $\det(B) = \det(A)$, since clearly $A = B$. Hence $\det(B) = -\det(B)$, from which we get $\det(B) = 0$. The proof for columns is similar.

(d) Expanding along the row or column that has been multiplied by k gives the result.

(e) Suppose we have added k times row j to row i of A to obtain B. Each element of row i of B is of the form $a_{ik} + ka_{jk}$. Expanding $\det(B)$ along this row gives us $\det(B) = \det(A) + k\det(C)$, where C is a matrix obtained from A by replacing row i by row j. Since two rows of C are identical, we have from (c) that $\det(C) = 0$, from which the result follows. ■

Example 1.7.13 We illustrate the proof of (a) with an example:

$$\begin{aligned}\begin{vmatrix} 2 & 0 & 0 \\ 5 & 3 & 0 \\ 7 & 6 & 4 \end{vmatrix} &= 2\begin{vmatrix} 3 & 0 \\ 6 & 4 \end{vmatrix} - 0 + 0 \text{ (expanding along the top row)} \\ &= 2(3 \times 4 - 0 \times 6) = 2.3.4\end{aligned}$$

We now turn to determinants of elementary matrices; these are quite simple.

Theorem 1.7.14 *Let E be an elementary matrix.*

(a) If E is associated with adding a multiple of one row to another row, then $\det(E) = 1$.

(b) If E is associated with a row interchange, then $\det(E) = -1$.

(c) If E is an elementary matrix associated with multiplication of row i by a non-zero Listen to:constant k, then $\det(E) = k$.

(d) For any elementary matrix E and any $n \times n$ matrix A, $\det(EA) = \det(E)\det(A)$.

Proof: (a) This follows from the fact that in this case E is either upper or lower triangular with 1's on the diagonal.

(b) E is obtained by interchanging two rows of I, so $\det(E) = -\det(I) = -1$.

(c) E differs from I by having k in position (i, i), since row i of I has been multiplied by k .

(d) You can see that this is true for the elementary matrices that correspond to row interchange or multiplication of a row by a non-zero constant. We know that in the case of a row interchange, the associated elementary matrix has determinant -1, and that interchanging two rows multiplies the determinant of any matrix by -1. In the case that we are multiplying a row of a matrix by a non-zero constant k, we already know that this multiplies the determinant of the matrix by k, and k is also the determinant of the associated elementary matrix. In the case that the row operation involves adding a multiple of one row to another row, the determinant of the resulting matrix is unchanged, by Theorem 1.7.12(e), and $\det(E) = 1$, from which the result follows. ∎

Example 1.7.15 We illustrate the last statement with an example:

$$\begin{vmatrix} 1 & 2 \\ 3 & 4 \end{vmatrix} = -2.$$

If we now add twice row 1 to row 2, the resulting matrix is $\begin{pmatrix} 1 & 2 \\ 5 & 8 \end{pmatrix}$; its determinant is also -2.

We are now in a position to link up the idea of a determinant to invertibility of a matrix. (We can't really claim to prove the result, since our "proof" depends on results about determinants which we have not all proved here.)

Theorem 1.7.16 *Let A be a square matrix. Then* $\det(A) \neq 0$ *if and only if A is invertible.*

Proof: Assume A is invertible; then $A = E_k E_{k-1} \ldots E_1$ where the E_i's are all elementary. Now apply the last result repeatedly to show that

$$\det(A) = \det(E_k)\det(E_{k-1})\ldots\det(E_1) \neq 0.$$

Conversely, assume that $\det(A) \neq 0$. We know that A is row equivalent to some matrix U in row-echelon form. That means

$$A = E_k E_{k-1} \ldots E_1 U$$

where the E_i's are all elementary. But since $\det(A) \neq 0$ then also $\det(U) \neq 0$ (why?) so none of the entries on the diagonal of U can be zero (why?), so U is row equivalent to the identity matrix. But then we know that A is also row-equivalent to the identity matrix, so is invertible. ∎

We note that we can now add another equivalent condition to the list in the Invertibility Theorem (Theorem 1.6.13, namely:

(f) $\det(A) \neq 0$.

In Section 1.1 we saw that equations of the type $A\mathbf{x} = \lambda\mathbf{x}$, where A is a square matrix and λ a scalar arise quite naturally in modelling certain problems. There is an uninteresting solution to such an equation: taking $\mathbf{x} = \mathbf{0}$ gives a solution, and this solution is valid for every scalar λ. It is far more interesting to know for which values of λ (if any) we can get a non-zero solution $\mathbf{x}$ for the equation. These values of λ are so important that they deserve a name (a name you have seen before!):

Definition 1.7.17 L*et A be a square matrix. A scalar λ is called an* ***eigenvalue*** *of A if there is a vector $\mathbf{x} \neq \mathbf{0}$ such that $A\mathbf{x} = \lambda\mathbf{x}$. The non-zero vector $\mathbf{x}$ is called an* ***eigenvector*** *corresponding to the eigenvalue λ.*

Determinants help us to find eigenvalues:

Theorem 1.7.18 *Let A be a square matrix. Then*

$$\lambda \text{ is an eigenvalue of } A \text{ if and only if } \det(\lambda I - A) = 0.$$

Proof: We first note that $A\mathbf{x} = \lambda\mathbf{x}$ if and only if $(\lambda I - A)\mathbf{x} = \mathbf{0}$.
There is a non-zero $\mathbf{x}$ such that $(\lambda I - A)\mathbf{x} = \mathbf{0}$ if and only if $\lambda I - A$ is singular. But this is the case if and only if $\lambda I - A$ is not invertible, and as we have seen above, this will be the case if and only if $\det(\lambda I - A) = 0$. ■

Example 1.7.19 We use this theorem to find all the eigenvalues of $A = \begin{pmatrix} 2 & 3 \\ 4 & 3 \end{pmatrix}$.
In the light of the theorem it makes sense to find λ such that $\det(\lambda I - A) = 0$. Now

$$\lambda I - A = \begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix} - \begin{pmatrix} 2 & 3 \\ 4 & 3 \end{pmatrix} = \begin{pmatrix} \lambda - 2 & -3 \\ -4 & \lambda - 3 \end{pmatrix},$$

so

$$\det(\lambda I - A) = (\lambda - 2)(\lambda - 3) - 12 = \lambda^2 - 5\lambda - 6 = (\lambda - 6)(\lambda + 1).$$

This means that the only eigenvalues of A are 6 and -1.

We will have much more to say about eigenvalues (and eigenvectors) in Chapter 4.

Using Theorem 1.7.16 we can prove a further important fact about determinants:

Theorem 1.7.20 *Let A and B be $n \times n$ matrices. Then*

$$\det(AB) = \det(A)\det(B).$$

Proof: We consider two mutually exclusive cases:
(1) Assume B is singular. Then so is AB (why?) so

$$\det(A)\det(B) = \det(A) \times 0 = 0 = \det(AB).$$

(2) Assume A is non-singular; then $A = E_k E_{k-1} \dots E_1$ where the E_i's are elementary. Then

$$\begin{aligned} \det(AB) &= \det(E_k E_{k-1} \dots E_1 B) \\ &= \det(E_k) \dots \det(E_1)\det(B) \\ &= \det(A)\det(B) \end{aligned}$$

■

This theorem has a useful consequence:

Corollary 1.7.21 *Let A be a square matrix such that $\det(A) \neq 0$. Then*

$$\det(A^{-1}) = \frac{1}{\det(A)}$$

Proof: $\det(A^{-1})\det(A) = \det(A^{-1}A) = \det(I) = 1$. ■

We illustrate how the computation of determinants can be speeded up by using some of the facts mentioned above.

Example 1.7.22 We compute the determinant of $\begin{pmatrix} 3 & 6 & -9 \\ 0 & 0 & -2 \\ -2 & 1 & 5 \end{pmatrix}$.

$$\begin{aligned}
\begin{vmatrix} 3 & 6 & -9 \\ 0 & 0 & -2 \\ -2 & 1 & 5 \end{vmatrix} &= \begin{vmatrix} 3 & 6 & -9 \\ 0 & 0 & -2 \\ 0 & 5 & -1 \end{vmatrix} \qquad \text{(added } \tfrac{2}{3} \text{ times row 1 to row 3)} \\
&= (-1)\begin{vmatrix} 3 & 6 & -9 \\ 0 & 5 & -1 \\ 0 & 0 & -2 \end{vmatrix} \quad \text{(interchanged 2 rows)} \\
&= (-1)(-30) = 30.
\end{aligned}$$

We could have seen this more easily, perhaps, by expanding along the second row. (Why would this be easy?)

The *Linear Algebra Toolkit* has a facility for evaluating determinants in this way.

Warning: Do not fall into the trap of thinking that row reducing a matrix to its row echelon form and then finding the determinant of the row reduced form will give you the determinant of the original matrix. You can see, for instance, from the above example that each row interchange used will introduce a factor of -1. Similarly, multiplying a row by a constant would also introduce a new factor.

There are many theoretical uses for determinants. You can, for instance, use determinants to compute the inverse of a matrix. (The method is computationally very inefficient, so has little practical value.) You can also use determinants to compute solutions to the equation $A\mathbf{x} = \mathbf{b}$ (as long as A is square). Again, the formula (called "Cramer's rule") is not useful practically, but has important theoretical consequences. To state it, we introduce the following notation: If A is an $n \times n$ matrix and $\mathbf{b}$ an n-vector, we'll write $A_k[\mathbf{b}]$ for the matrix obtained from A by replacing the k-th column by the vector $\mathbf{b}$.

Theorem 1.7.23 (*Cramer's Rule) Let A be an invertible $n \times n$ matrix and $\mathbf{b} \in \mathbf{R}^n$. Then the system $A\mathbf{x} = \mathbf{b}$ has a unique solution given by*

$$x_k = \frac{\det(A_k[\mathbf{b}])}{\det(A)}, \ \textit{for } k = 1, 2, \ldots, n.$$

Proof: We give an outline of the proof and ask you to check the detail. Using the fact that $A\mathbf{x} = \mathbf{b}$ it can be checked that $AI_k[\mathbf{x}] = A_k[\mathbf{b}]$.
This implies that $(\det(A))(\det(I_k[\mathbf{x}])) = \det(AI_k[\mathbf{x}]) = \det(A_k[\mathbf{b}])$. Since $\det(I_k[\mathbf{x}]) = x_k$, the result follows. ■

Summary:

In this section we looked at the definition, properties and some uses of determinants of square matrices.

- The determinant of a square matrix A is a *number* associated with the matrix and is denoted by $\det(A)$ or $|A|$.
- The definition of a determinant is recursive: the determinant of an $n \times n$ matrix is given in terms of determinants of $(n-1) \times (n-1)$ matrices, called minors.
- A square matrix is invertible if and only if its determinant is non-zero.
- The determinant of the product of two square matrices equals the product of their determinants.
- Determinants can be used to find eigenvalues of square matrices.
- Cramer's rule gives a formula in terms of determinants for the solution of the system $A\mathbf{x} = \mathbf{b}$ in the case where A is an invertible square matrix.

Historical note:

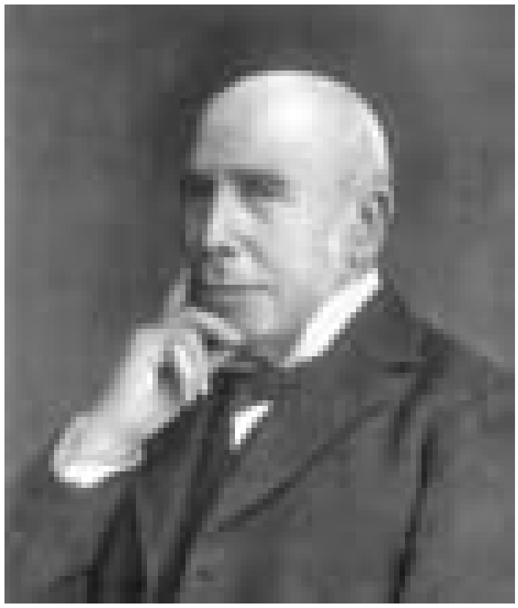
The idea of a determinant of a square matrix first appeared in Europe and Japan at about the same time, but it was the Japanese mathematician Takakuza Seki Kowa who first published his results in 1683. Although not explicitly defining determinants, he showed by means of examples how to calculate determinants of up to 5×5 matrices, and how to use them in solving equations. Seki was a child prodigy; fortunately his talent was recognized at the age of nine by a servant. Seki built up a library of Japanese and Chinese books on mathematics and essentially taught himself. He anticipated many European discoveries in mathematics, such as for example the Newton-Raphson method for solving linear equations and Newton's interpolation method.

In the same year that Seki published his results on determinants the German mathematician Gottfried Leibniz described the use of determinants in the solutions of systems of linear equations in a letter to L'Hospital. He studied the properties of determinants and essentially formulated what is now known as Cramer's rule.

Results on determinants first appeared in print in the book *Treatise of Algebra* written in 1730 by Maclaurin, but only published after his death, in 1748. It contains proofs for the 2×2 and 3×3 case of Cramer's rule. The statement for the general case was published by Cramer in 1750.

The history of determinants has a South African connection. Two of the classic works on the subject, the *Treatise on the theory of determinants* and the five-volume *History of determinants*, were written by Sir Thomas Muir. Muir was born near Lanark, Scotland and studied at the University of Glasgow. His original plan was to study Greek, but he was persuaded by by lord Kelvin to change to mathematics. He later became a popular lecturer at this university. In 1892 Muir was offered the chair of Mathematics at Stanford University in California.

He was persuaded by Cecil John Rhodes to go to the then Cape Colony as Superintendent General of Education, however. When he arrived in Cape Town, he enthusiastically set about reforming the education system. In 1897 he was appointed as vice-chancellor of the University of Cape Town, a position he held for four years. He also became the first recipient of an honourary doctorate from the university. After his retirement in 1915 he continued his work on the *History of determinants*, and he was still writing the sixth volume at the time of his death, at the age of 89, in 1934.



Exercises

The following OCTAVE command may come in useful:

det (A) gives the determinant of the matrix A.

1. Evaluate the following determinants:

(a) $\begin{vmatrix} 4 & 1 \\ 8 & 2 \end{vmatrix}$ (b) $\begin{vmatrix} -5 & 6 \\ -7 & -2 \end{vmatrix}$ (c) $\begin{vmatrix} -2 & 7 & 6 \\ 5 & 1 & -2 \\ 3 & 8 & 4 \end{vmatrix}$ (d) $\begin{vmatrix} 3 & 0 & 0 \\ 2 & -1 & 5 \\ 1 & 9 & -4 \end{vmatrix}$

2. Find the determinants of the following matrices by inspection.

(a) $\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -5 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$ (b) $\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$ (c) $\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & -9 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$

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

3. Evaluate

$$\begin{vmatrix} 0 & 0 & 0 & 0 & -3 \\ 0 & 0 & 0 & -4 & 0 \\ 0 & 0 & -1 & 0 & 0 \\ 0 & 2 & 0 & 0 & 0 \\ 5 & 0 & 0 & 0 & 0 \end{vmatrix}.$$

4. Find the determinant of $A = \begin{pmatrix} 4 & -1 & 1 & 6 \\ 0 & 0 & -3 & 3 \\ 4 & 1 & 0 & 14 \\ 4 & 1 & 3 & 2 \end{pmatrix}$.

5. Let $A = \begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix}$. Assuming that $\det(A) = -7$, find

   (a) $\det(3A)$ (b) $\det(A^{-1})$ (c) $\det(2A^{-1})$ (d) $\det((2A)^{-1})$

   (e) $\det\begin{pmatrix} a & g & d \\ b & h & e \\ c & i & f \end{pmatrix}$.

6. Find the eigenvalues of the matrix $A = \begin{pmatrix} 1 & 2 & 0 \\ -1 & -1 & 1 \\ 0 & 1 & 1 \end{pmatrix}$.

7. Prove that if A and B are square matrices of the same size and A is singular, then AB is also singular.

Chapter 2

Vector Spaces

2.1 What are vector spaces?

This is a chapter where we increase the level of abstraction. We will first present some examples with which you are very familiar, however, and by the time we get to the main idea of this chapter it should be easier to digest.

You've seen in the last chapter that vectors and matrices go very handily together: if you work with matrices you are likely to find yourself working with vectors and vice versa. In this chapter we take a long hard look at vectors and show that we can fit the vectors we are familiar with into a more general context. In the next chapter matrices will get much the same kind of treatment.

Let's first ask ourselves the question "What are vectors?". You've all presumably worked with the idea that a vector is something that has "both magnitude and direction" and that's certainly a very useful idea to have. When you were introduced to vectors in first year mathematics, you spent a lot of time looking at what we called 2-vectors and 3-vectors. These we associated with points in two- and three-dimensional space respectively, and wrote them as ordered pairs and ordered triples of real numbers. Certainly any 2- or 3-vector has both magnitude and direction. You can interpret the 2-vector $(1, 1)$ as an arrow from the origin to the point $(1, 1)$ which then has length $\sqrt{2}$ and direction 45 degrees measured anticlockwise from the positive x-axis. A similar idea works for 3-vectors.

But what did we actually **do** with these vectors? Well, we seemed to spend most of our time doing algebra: we added and subtracted vectors, we multiplied them by scalars to scale their lengths, we worked with dot products and cross products, we found projections of one vector onto another, all of which involved a great deal of algebra. So vectors certainly have a very algebraic side to them. They are also very geometrical, and you have seen already just how useful they are in describing the geometry of two- and three-dimensional space. In this chapter, though, we are going to explore how we can generalize the algebraic aspects of vectors. This does not mean that we are going to ignore the geometrical perspective. Examples drawn from the familiar context of $\mathbf{R}^2$ and $\mathbf{R}^3$ will still be our main motivation and illustration of the more abstract ideas we'll introduce.

Let's now think about the most important features of the algebraic side of vectors. They seem to be that

- any two vectors can be added;
- any vector can be multiplied by a number (usually called a *scalar* in this context);
- you can take dot products of any two vectors.

The list could probably be expanded, but that seems to be the essence of what you actually do with vectors. Note that the dot product has its geometric side as well: we use it to find angles and lengths.

The next idea is the new one: Would it make sense to look for other situations where you have a set of "things" that can be added together and which you can multiply by numbers, in such a way that they behave much like 2-vectors or 3-vectors? To answer this (admittedly rather vague) question, we'll first need to be convinced that such situations do in fact arise. Here are some examples.

Example 2.1.1 We've seen 2-vectors and 3-vectors; how about 4-vectors? They would be ordered 4-tuples i.e things of the form (x_1, x_2, x_3, x_4) where x_1, x_2, x_3 and x_4 are any real numbers. Do they occur in real life? Certainly; you just need to be considering some situation which involves four independent variables and you are forced to work with 4-vectors. We have, in fact, already seen that such vectors arise naturally when looking at systems of linear equations with four unknowns. For those of you doing physics, you have probably already had to use 4-vectors when working with relativity: three variables for space and one for time. How do you add a 4-vector to a 4-vector? Simply add the corresponding entries or components. A similar comment applies to multiplying a 4-vector by a number. One can also define a dot product much as one does for 2- or 3-vectors.

Example 2.1.2 Once we've made the jump to 4-vectors the next step is easy. We could consider 23-vectors or 132-vectors, or for that matter n-vectors, for any positive integer $n \geq 2$. Adding them and multiplying them by numbers can be done in the same way as for 4-vectors. Such vectors arise naturally when you consider systems of linear equations with a large number of independent variables.

Incidentally, it was this jump from 3-vectors to what we now call n-vectors that was the longest in coming. Mathematicians only realized that it made sense and was a worthwhile idea in the nineteenth century. Because our world seems to be (to some extent) 3-dimensional it took courage to assert that 4 or more dimensions were useful or feasible.

So far, all our examples have a bit of a "length and direction" feel, although the idea of a length or direction in 4 or 23 dimensions takes some getting used to. The next example goes even further and leaves the geometric ideas behind.

Example 2.1.3 What about functions? For simplicity, let's agree to work with functions from $\mathbf{R}$ to $\mathbf{R}$. Is it possible to add functions, and multiply them by numbers? This is not such a strange idea; in fact, it is something that you certainly did when you were considering rules for differentiation, for example. (Remember the rules for differentiating sums of functions, and constant multiples of functions?) How does one add the functions f and g? We want to do it in such a way that we create a new function $f+g$; to do this we have to specify the value of $f+g$ for every $x \in \mathbf{R}$. This is done in the most natural way: for $x \in \mathbf{R}$,

$$(f+g)(x) = f(x) + g(x).$$

For example, if $f(x) = x^2$ and $g(x) = 2x$, then $(f+g)(x) = x^2 + 2x$. Multiplying a function by a real number is equally straightforward: if f is a function and r a real number we define the function rf by putting, for $x \in \mathbf{R}$,

$$(rf)(x) = rf(x).$$

What we're getting at is that there are some aspects of working with functions which remind one of working with vectors. This leads to the important idea that we might begin to consider functions as "vectors" of some kind, although obviously very different from 2-vectors or n-vectors. Can we also talk about "dot products" of functions? The answer is that we can, in fact in more than one way, but we will only get to this right at the end of this course.

Now this collection of examples suggests the following idea: there are many sets arising quite naturally in mathematics that seem to have many properties in common with sets of ordinary vectors. In particular, there is some sense in which we can add the elements of these sets, and multiply them by numbers. There is some justification for calling the elements of these sets "vectors" as well, and these sets of elements "spaces of vectors", or " vector spaces". You have to be careful, however, not to mix "vectors" of different kinds. (You can't add 2-vectors to functions or 3-vectors to 23-vectors!) You have to know what kinds of things you are regarding as "vectors" in a particular situation, and work with those things only.

We are now ready to start talking about the idea of a **vector space**. A vector space, very loosely speaking, is a set of objects that can be added and multiplied by numbers, and behave in many respects like the familiar 2- and 3-vectors when you perform these operations.

To identify a vector space we have to know

- what the objects (or *vectors*, as we'll call them) are;
- how to add any two of these vectors; and
- how to multiply a vector by a number (i.e. how to scale it).

Once we start adding vectors and multiplying them by numbers, we will also need to know what rules there are for these operations. For example: Does it matter in what order we add two vectors? Can we add more than two vectors at a time? Without such rules we'll not be able to work with and simplify expressions containing vectors. This means that our idea of such a general, or abstract, vector space should include some basic rules for the algebra of vectors.

What we are going to do now is write down quite carefully what a vector space is. There is general consensus (after a few centuries of haggling) about what sort of things are considered to be vector spaces and the conditions are quite precise. This *definition* of a vector space will be the starting point for everything we are going to say about vector spaces in future. The beauty of this approach is that, instead of proving the same things over and over again for each particular vector space that we need to work in, we actually prove things that hold in *every* vector space. You can then use these facts in any specific vector space you happen to be interested in. This can save you a lot of work. This is an enormous shift of perspective and gives you an overview of things that occur in a similar kind of way in very different situations. You get a great deal of insight from this changed, more general, point of view. There is a price to be paid: it takes some time and thought to get used to this more abstract approach. But in the long run the advantages are huge.

A remark about the notation and terminology we are going to use from now on is appropriate at this stage. Abstract vector spaces will usually be denoted by capital letters like U,V and W. We'll use small boldface letters to denote elements of an abstract vector space (for example $\mathbf{u}, \mathbf{v}$ and $\mathbf{w}$). We'll also call the elements of a vector space "vectors". You do have to keep in mind that these things could be very different from ordinary vectors; they could be functions, for example. When working in a particular kind of vector space, we'll usually use notation for elements of the vector space that is appropriate to that vector space. As an example, when working with a vector space of functions, we'll use letters like f and g for elements of the space; when working with spaces of polynomials, we'll usually denote the "vectors" by letters such as p and q.

The notation may at first be a bit confusing, since you may be used to think of small letters as representing numbers. Since we'll be multiplying the elements of abstract vector spaces (the 'vectors") by numbers, it will be good to distinguish in our notation between "vectors" and "numbers" (or "scalars" as we'll call them from now on). A common way of doing this, and one that we'll also adopt, is to use small Greek letters to denote numbers, and Roman (ordinary) small letters to denote vectors. You may well feel that this makes something that already sounds complicated more so. To help you, we've included the Greek alphabet as an appendix (Appendix D). The good new is that we'll use two reasonably familiar Greek letters (λ and μ) most of the time. You've probably seen them being used in first year maths already, for example in the vector and parametric equations of lines and planes.

There is a problem with the notation suggested so far: it is not possible to *write* in boldface. Since we'll be using Greek letters for scalars, it should not cause confusion if we agree to use ordinary (not boldface) letters for vectors when writing. If you want to make sure that there can be no confusion, you could also underline letters to indicate vectors; for example, you could write $\underline{v}$ for the vector $\mathbf{v}$. We'll continue to use boldface letters in the printed notes to help you to get used to the idea of an abstract "vector".

Before we write down the definition, we need to be very clear about what some of the terminology we are going to use in the definition means. As pointed out above, the essential ingredients of a vector space are a *set* (let's call it V) of things we'll call vectors, and *operations of addition and multiplying by numbers* defined for vectors in V.

- When we say that an addition has been defined on V, we actually mean that for any two vectors $\mathbf{u}$ and $\mathbf{v}$ in V we must have $\mathbf{u} + \mathbf{v}$ **also a member of the set** V. It's no good if on adding $\mathbf{u}$ to $\mathbf{u}$ you get something which is no longer in V. To emphasize this, we say that V must be **closed under the addition defined**.
- Also for any number λ and any vector $\mathbf{u}$ the product $\lambda\mathbf{u}$ must still be a member

of V. We call the process of multiplying a vector by a number **scalar multiplication**, and we say that V must be **closed under scalar multiplication**.

- We have so far talked rather vaguely about multiplying a vector by a *number*, without specifying what our numbers (or **scalars**, as we'll call them from now on) are. Most of the time our scalars will be the set of all real numbers, $\mathbf{R}$. There will be occasions when we need our scalars to be the set of complex numbers, $\mathbf{C}$. It is even possible, and useful, in some contexts to consider other sets of numbers as well, but we'll not do it in this module. (You may see this in the module 2IA.)

Here is the definition of a vector space at last. It's a long one, because all sorts of conditions have to be met for something to be as useful as the collections of 2-vectors and 3-vectors are.

Definition 2.1.4 *Let V be a set on which an addition and scalar multiplication have been defined. (This means, of course, that V must be closed under these two operations.) Then we call V a* ***vector space*** *(or* ***linear space****) if the following conditions are satisfied for* ***every*** *$\mathbf{u}, \mathbf{v}$ and $\mathbf{w}$ in V and* ***every*** *scalar λ and μ:*

1. $\mathbf{u} + \mathbf{v} = \mathbf{v} + \mathbf{u}$.
2. $(\mathbf{u} + \mathbf{v}) + \mathbf{w} = \mathbf{u} + (\mathbf{v} + \mathbf{w})$.
3. *There is an element $\mathbf{z}$ in V, called a* ***zero vector*** *of V, such that $\mathbf{u} + \mathbf{z} = \mathbf{u}$ for every $\mathbf{u} \in V$. (We'll soon show that there is only one zero vector in V, and therefore we are entitled to use a special symbol for it. It makes sense to use the symbol $\mathbf{0}$ for the zero vector.)*
4. *For every $\mathbf{u}$ in V there is an element $\mathbf{v}$ called the* ***negative*** *of $\mathbf{u}$ which satisfies $\mathbf{u} + \mathbf{v} = \mathbf{0}$. (We'll also show that for every $\mathbf{u} \in V$, there is only one such $\mathbf{v}$. We use the special symbol $-\mathbf{u}$ for this $\mathbf{v}$.)*
5. $\lambda(\mathbf{u} + \mathbf{v}) = \lambda\mathbf{u} + \lambda\mathbf{v}$.
6. $(\lambda + \mu)\mathbf{u} = \lambda\mathbf{u} + \mu\mathbf{u}$.
7. $(\lambda\mu)\mathbf{u} = \lambda(\mu\mathbf{u})$.
8. $1\mathbf{u} = \mathbf{u}$.

If there is any need to specify which set of scalars we are using, we will make this quite clear by talking about the vector space V ***over*** $\mathbf{R}$ *(if the scalars are real numbers) or* ***over*** $\mathbf{C}$ *(if the scalars are complex numbers). Such vector spaces are respectively called* ***real*** *and* ***complex vector spaces.***

We'll often refer to the conditions in the definition above as the *axioms* for a vector space.

Now it's time to test our definition with many examples. It's especially important to have some examples of things that are not vector spaces as well, to get a feel for the definition.

Example 2.1.5 For $n \geq 2$, let

$$\mathbf{R}^n = \{(x_1, x_2, \ldots, x_n) : x_1, x_2, \ldots, x_n \in \mathbf{R}\}.$$

Define addition and scalar multiplication by

$$\begin{aligned}(x_1, x_2, \ldots, x_n) + (y_1, y_2, \ldots, y_n) &= (x_1 + y_1, x_2 + y_2, \ldots, x_n + y_n)\\ \lambda(x_1, x_2, \ldots, x_n) &= (\lambda x_1, \lambda x_2, \ldots, \lambda x_n)\end{aligned}$$

for $(x_1, x_2, \ldots, x_n), (y_1, y_2, \ldots, y_n) \in \mathbf{R}^n, \lambda \in \mathbf{R}$. With these operations $\mathbf{R}^n$ is an example of a vector space (over $\mathbf{R}$). The zero element in $\mathbf{R}^n$ is just the vector $(0, 0, \ldots, 0)$, and the negative of a vector $(x_1, x_2, \ldots, x_n)$ in $\mathbf{R}^n$ is the vector $(-x_1, -x_2, \ldots, -x_n)$. This follows from

$$(x_1, x_2, \ldots, x_n) + (0, 0, \ldots, 0) = (x_1 + 0, x_2 + 0, \ldots, x_n + 0) = (x_1, x_2, \ldots, x_n)$$

and

$$(x_1, x_2, \ldots, x_n) + (-x_1, -x_2, \ldots, -x_n) = (x_1 - x_1, x_2 - x_2, \ldots, x_n - x_n) = (0, 0, \ldots, 0).$$

Check some of the other axioms yourself. You will notice that in each case an axiom is satisfied because a similar axiom holds for real numbers. Taking $n = 2$ and $n = 3$ gives us the familiar vector spaces $\mathbf{R}^2$ and $\mathbf{R}^3$. We excluded the case $n = 1$ above, but we could have considered it as well. This means that we can even think of $\mathbf{R}$ as a vector space over $\mathbf{R}$, so that in this example the vectors and the scalars are the same!

You will notice that we have written the elements of $\mathbf{R}^n$ as *row* vectors. We could just as well have written them as *column* vectors, but there are obvious space-saving advantages to using row vectors! When working with matrices and vectors (such as we have already done when we wrote systems of linear equations in matrix form), it is more appropriate to use column vectors.

A useful convention that we'll adopt from now on is that when we write "$\mathbf{x} \in \mathbf{R}^n$" we'll assume that $\mathbf{x} = (x_1, x_2, \ldots, x_n)$.

Example 2.1.6 Similarly, we can consider the set

$$\mathbf{C}^n = \{(z_1, z_2, \ldots, z_n) : z_1, z_2, \ldots, z_n \in \mathbf{C}\},$$

with addition and scalar multiplication defined in the same way as in the previous example, but with the difference that the scalars in this case are complex numbers. This is an example of a vector space over $\mathbf{C}$.

Example 2.1.7 Let's take $\mathbf{R}^2$ with the usual addition defined above, but with scalar multiplication defined by $\lambda(x, y) = (\lambda x, y)$, for $(x, y) \in \mathbf{R}^2, \lambda \in \mathbf{R}$. This is obviously not the usual scalar multiplication, but it might still work. Since addition is defined in the same way as in the first example, we need not check any conditions involving only addition. It is clear from the definition that $\mathbf{R}^2$ is closed under the scalar multiplication defined here (for if $(x, y) \in \mathbf{R}^2$ and $\lambda \in \mathbf{R}$, then $(\lambda x, y) \in \mathbf{R}^2$). But this is not enough; we also have to check that the axioms 5 to 8 above are satisfied. As it turns out, we do **not** get a vector space in this case. To show that this is the case, it suffices to find one axiom which is not satisfied. Consider the following:

$$\begin{aligned} (\lambda + \mu)(x, y) &= ((\lambda + \mu)x, y) = (\lambda x + \mu x, y), \quad \text{but} \\ \lambda(x, y) + \mu(x, y) &= (\lambda x, y) + (\mu x, y) = (\lambda x + \mu x, 2y). \end{aligned}$$

For these to be equal, we need to have $y = 2y$ for all y. But this is certainly not the case if, for example, $y = 1$. This shows that axiom 6 of the definition is not satisfied, and so we do not have a vector space.

We present some examples now which move outside the realm of $\mathbf{R}^n$ and $\mathbf{C}^n$. These are thus somewhat more abstract examples, but are also extremely important.

Example 2.1.8 Let n be a positive integer and let P_n denote the set of all polynomials in x with real coefficients and with degree at most n. We say that two polynomials $p = a_0 + a_1x + a_2x^2 + \ldots + a_nx^n$ and $q = b_0 + b_1x + b_2x^2 + \ldots + b_nx^n$ in P_n are equal if (and only if) corresponding coefficients are equal, i.e. $p = q$ if and only if $a_0 = b_0, a_1 = b_1, \ldots, a_n = b_n$. We can easily define an addition and scalar multiplication for P_n. For $p = a_0 + a_1x + a_2x^2 + \ldots + a_nx^n$ and $q = b_0 + b_1x + b_2x^2 + \ldots + b_nx^n$ in P_n, and λ a real number, put

$$p + q = (a_0 + b_0) + (a_1 + b_1)x + (a_2 + b_2)x^2 + \ldots + (a_n + b_n)x^n$$

and

$$\lambda p = (\lambda a_0) + (\lambda a_1)x + (\lambda a_2)x^2 + \ldots + (\lambda a_n)x^n.$$

P_n is closed under the addition and scalar multiplication we have defined for it, since the expressions on the right hand side above are both polynomials of degree at most n. It is also easy to check that all the axioms hold. The zero vector for P_n is the polynomial $0 + 0x + 0x^2 + \ldots + 0x^n$ and $-p$ is just $(-a_0) + (-a_1)x + \ldots + (-a_n)x^n$. Therefore P_n is a vector space over $\mathbf{R}$. These so-called **polynomial spaces** are very important vector spaces. (Why did we say "degree at most n" and not just "degree n" in this example?) In the same way we can define a vector space over $\mathbf{C}$ consisting of polynomials with complex coefficients, for which the scalars are complex numbers.

It is difficult to be absolutely consistent with notation, and you may with some justification object to the fact that we used $a_0, a_1, \ldots, a_n$ and $b_0, b_1, \ldots, b_n$ for the coefficients of polynomials. After all, they are real *numbers* and should therefore be denoted by Greek letters! This notation for polynomials is used so widely and unlikely to cause confusion, so we've opted to stick with tradition rather than consistency in this case.

Example 2.1.9 Let a and b be real numbers, with $a < b$, and let $F[a, b]$ denote the set of all real-valued functions defined everywhere on the interval $[a, b]$. For example $f(x) = \frac{1}{x}$ is a member of $F[1, 2]$ but not of $F[-1, 2]$. (Why not?) For f, g in $F[a, b]$ and $\lambda \in \mathbf{R}$ we define the functions $f + g$ and λf by

$$(f + g)(x) = f(x) + g(x) \text{ and } (\lambda f)(x) = \lambda f(x) \text{ for } x \in [a, b].$$

With these definitions of addition and scalar multiplication it follows that if we add two functions defined on $[a, b]$, the result is a function defined on $[a, b]$. If we multiply a function defined on $[a, b]$ by a real constant, it is again a function defined on $[a, b]$. This means that $F[a, b]$ is closed under the usual function addition and scalar multiplication. The other axioms for a vector space are also satisfied, as you will see in the exercises. Thus, in this context, $F[a, b]$ is indeed a vector space over $\mathbf{R}$. A vector in this space is just some real-valued function defined on $[a, b]$. The zero "vector" is the function which takes on value 0 everywhere on $[a, b]$. If $f \in F[a, b]$ then the negative of f in the vector space $F[a, b]$ is the function g such that $g(x) = -f(x)$ for every $x \in [a, b]$ (since $(f + g)(x) = f(x) + g(x) = f(x) + (-f(x)) = 0$ for every $x \in \mathbf{R}$). Note that g is continuous if f is. This example is also tremendously important, and is used in the study of differential equations, for example.

If we consider the set of complex-valued functions on $[a, b]$ (rather than the real-valued ones) and take the scalars to be complex numbers, we get a vector space over $\mathbf{C}$ when we define addition and scalar multiplication in the same way.

Example 2.1.10 There is a rather trivial vector space which consists of exactly one element. Take $V = \{0\}$, and define $0 + 0 = 0$ and $\lambda 0 = 0$ for any number λ. This is indeed a vector space, as you can check. It's also a rather small and uninteresting vector space. The vector spaces we shall meet are all rather large (infinite, to say the least.) There are vector spaces that are finite, but for those you need rather special sets of scalars. You may see examples of such vector spaces if you do 2IA.

Example 2.1.11 Let m and n be fixed positive integers, and let $M_{m\times n}(\mathbf{R})$ be the set of all $m \times n$ real matrices. Then $M_{m\times n}(\mathbf{R})$ becomes a real vector space when we use the usual addition of matrices and the usual multiplication by real numbers as operations. There is no need not show from scratch that all the axioms hold; look up whatever you need in section 1.2 of these notes. In the same way the set $M_{m\times n}(\mathbf{C})$ of all complex $m \times n$ matrices is a complex vector space. If, as is often the case, the scalars are clear from the context, or what we are saying is true for both real and complex scalars, we'll abbreviate the notation to $M_{m\times n}$

We have now seen quite a few examples of vector spaces. It's time to start collecting together a few facts about any vector space so that working with them becomes easier. If we work in the abstract setting of vector spaces, all that we are allowed to take for granted are the rules (axioms) listed in the definition of a vector space. There is a great temptation to use other "obvious" rules as well. But this is not allowed until you have *proved* that these obvious rules can be deduced from the axioms. As an example, you may be sorely tempted to assume that $0\mathbf{u} = \mathbf{0}$ in any vector space. But this is *not* one of the axioms, so before we can use it, we'll have to prove that it follows from the axioms in the definition. In the next theorem we prove a number of useful facts about every vector space, using only the axioms we laid down for a vector space in the definition.

Theorem 2.1.12 *Let V be a vector space, let $\mathbf{u}$ be a vector in V, and let λ be a scalar. Then we have:*

(a) The zero vector is unique; so is the negative of a vector. (We have already mentioned this in Definition 2.1.4.)

(b) $0\mathbf{u} = \mathbf{0}$

(c) $\lambda\mathbf{0} = \mathbf{0}$

(d($(-1)\mathbf{u} = -\mathbf{u}$

(e) If $\lambda\mathbf{u} = \mathbf{0}$, then either $\lambda = 0$ or $\mathbf{u} = \mathbf{0}$.

Before we prove (some) of these facts, it's important for you to work out what each of the above statements is really saying. For instance (b) is saying that no matter how scalar multiplication is defined, no matter what vector space, it will always turn out that $0\mathbf{u}$ must give the zero vector. Statement (d) says that, no matter what scalar multiplication you use, to get the negative of $\mathbf{u}$ you simply multiply it by the scalar -1.

Proof: (a) We prove only that the zero vector is unique. We know, by axiom 3, that there is a zero vector $\mathbf{z}$ in V such that $\mathbf{u}+\mathbf{z}=\mathbf{u}$ for every $\mathbf{u} \in V$. Suppose there is another vector $\mathbf{z}'$ in V with the same property: $\mathbf{u}+\mathbf{z}'=\mathbf{u}$ for every $\mathbf{u} \in V$. Then

$$\mathbf{z}' = \mathbf{z}' + \mathbf{z} = \mathbf{z} + \mathbf{z}' = \mathbf{z}.$$

Make sure that you know why each equality in the line above holds! Now that we know there is only one zero vector, we can use the special symbol $\mathbf{0}$ for it, and we'll do so in future.
Write out your own proof to show that for each vector its negative is unique.

(b) This proof is quite slick. Whatever $0\mathbf{u}$ is, we know it is a vector in V and it has a negative, $-(0\mathbf{u})$, by axiom 4. Thus

$$\begin{aligned}
\mathbf{0} &= 0\mathbf{u} + (-(0\mathbf{u})) \quad \text{by axiom 4} \\
&= (0+0)\mathbf{u} + (-(0\mathbf{u})) \qquad \text{(a mean trick)} \\
&= [0\mathbf{u} + 0\mathbf{u}] + (-(0\mathbf{u})) \qquad \text{by axiom 6} \\
&= 0\mathbf{u} + [0\mathbf{u} + (-(0\mathbf{u}))] \qquad \text{by axiom 2} \\
&= 0\mathbf{u} + \mathbf{0} \qquad \text{by axiom 4} \\
&= 0\mathbf{u} \qquad \text{by axiom 3}
\end{aligned}$$

which is just what we wanted to prove. There are other ways of arranging this proof; see if you can find one that appeals to you more. This one may seem artificial, but it has the merit of being absolutely correct!

(c), (d) and (e) These proofs are exercises. ∎

You may have asked yourself whether we are going to consider dot products in this section. Unfortunately not; we will return to them later in the course (in Chapter 5). As it happens, it's not always obvious what a dot or inner product for a given vector space should be. In fact it may not exist at all, in some sense.

Summary:

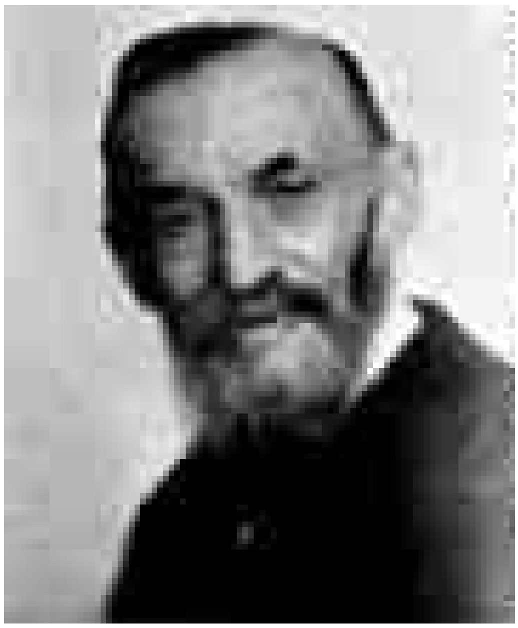
- In this section you were introduced to the definition of a general (abstract) vector space, and looked at many examples of such spaces.

- You also learned a few basic facts about the algebra of a vector space.
- A particularly important concept that was introduced in this section was that of a set of objects being **closed** under a particular operation. Checking this sort of thing is an important skill that you should master. This idea will occur again in the next section.

Historical note:

The idea that one could define operations on geometrical entities like points, lines and planes first appeared in the work of the Czech mathematician Bernard Bolzano, in a book that was published in 1804. The notion of a vectors as a directed line segments that could be added and multiplied by numbers appeared in later work by the German August Möbius and the Italian Giusto Bellavitis, in 1827 and 1832. The work of Hamilton on quaternions, Cayley on matrices and Laguerre on systems of linear equations all prepared the way for a more abstract algebraic approach to the study of vectors.

Such an abstract approach, involving algebraic operation on unspecified abstract quantities, was considered in detail by the German Hermann Grassmann between 1844 and 1862. He considered operations of addition, scalar multiplication and multiplication in his highly original work. Since the structures he considered also allowed multiplication, they were not vector spaces in the modern sense, but his work contains many of the fundamental ideas of abstract linear algebra.



The axiomatic definition of a real linear space as we use it today was first given by the Italian mathematician Guiseppe Peano in a book published in 1888. It is remarkable in that it not only introduces modern set-theoretic notation, but reads almost like a modern linear algebra textbook. Peano was born in Cuneo in Piemonte in Italy in 1858. His parents worked on a farm, but fortunately his mother's brother, a priest and a lawyer, noticed that Guiseppe was very talented and arranged for him to attend a secondary school and later the university in Turin. He graduated from there with a doctorate in mathematics in 1880 and immediately secured a position as an assistant lecturer at the University of Turin.

He worked on differential equations, mathematical logic, set theory and what we now call linear algebra. From 1892 he worked on a very ambitious project, an attempt to produce a textbook that could be used for any mathematics course, written in the notation of mathematical logic. When he started using the first volume of this work, it had a disastrous effect on his teaching!

He is perhaps best known for the Peano axioms for the set of natural numbers, and his example of a space filling curve (a continuous curve that passes through every point inside a unit square). Peano's work on mathematical logic had a profound effect on Bertrand Russell, who described his meeting with Peano in 1900 as the turning point in his intellectual life. Peano died in Turin in 1932.

Exercises

1. In each of the following cases a set of objects is given, together with operations of addition and scalar multiplication. Which of these are vector spaces? Justify your answers.
   (a) The set of all ordered pairs of real numbers (x, y) with the operations: $(x, y) + (a, b) = (x + a, y + b)$ and $\lambda(x, y) = (2\lambda x, 2\lambda y)$.
   (b) The set of all ordered pairs of real numbers of the form (x, y), where $x \geq 0$, with the usual operations of addition and scalar multiplication.
   (c) The set of all functions $f : \mathbf{R} \to \mathbf{R}$ such that $f(2) = 0$ with the usual operations (as defined in Example 2.1.3).
   (d) The set of all positive real numbers with the operations $x + y = xy$ and $\lambda x = x^\lambda$.
   (e) All polynomials of degree 3, with the usual operations (as defined in Example 2.1.8).
2. Fill in the details missing in Example 2.1.9 and Example 2.1.11.
3. Is the set of all invertible 2×2 matrices, with the usual operations, a vector space?
4. The set of all ordered pairs of real numbers (x, y) is equipped with the operations

$$(x, y) + (a, b) = (x + a + 1, y + b + 1) \text{ and } \lambda(x, y) = (\lambda x, \lambda y).$$

   Check each condition in the definition of a vector space, and determine whether it holds or not.

5. Prove that in any vector space, the negative of a vector is unique. (Hint: suppose that there are two vectors with the property of a negative vector, and show them equal. This result is part of Theorem 2.1.12 .

6. Complete the proof of Theorem 2.1.12.
[Hint: For (c), begin with the equation $\lambda(\mathbf{0}+\mathbf{0}) = \lambda\mathbf{0}$.
For (d), use $(-1)\mathbf{u}+\mathbf{u} = (-1)\mathbf{u}+1\mathbf{u}$.]

7. Show that, in any vector space, for any $\mathbf{u} \neq \mathbf{0}$, if $\lambda\mathbf{u} = \mu\mathbf{u}$ then $\lambda = \mu$.

2.2 Subspaces

In this section we look at quite a natural question: Is it possible for a subset S of a vector space V to be a vector space itself, and if so, when will this be the case? Since V is a vector space, we can add any two elements of V. In particular, we can add any two elements in the subset S of V. In the same way we can multiply any element in S by a scalar, since we can do it for any element of V. But will S with this addition and scalar multiplication it inherits from V satisfy all the axioms for a vector space? This looks highly likely: if all the axioms are satisfied in V, surely they will also be satisfied in the subset S of V?

We have to be quite careful, though. We know that the sum of any two elements in V must be in V again (V is closed under addition). If the two elements are in the subset S, their sum will definitely be in V, but will it necessarily be in S? In other words, is S necessarily closed under addition? We could as a similar question about scalar multiplication. Let's first look at some examples to get a feel for the problem.

Example 2.2.1 Let $V = \mathbf{R}^2$, with its usual addition and scalar multiplication, and S be the line in $\mathbf{R}^2$ through the origin in the direction $(1,2)$. From your first year course you will recall that this line is the set of points $\{(0,0)+\lambda(1,2) : \lambda \in \mathbf{R}\}$. This means that any point on this line is of the form $(0,0)+\lambda(1,2) = \lambda(1,2)$ for some $\lambda \in \mathbf{R}$. We check to see whether S is closed under addition. To do this, we must take two arbitrary vectors in the set S, say $\lambda(1,2)$ and $\mu(1,2)$, with λ and μ real numbers, and add them to see if the result is still in S. The sum is

$$\lambda(1,2)+\mu(1,2) = (\lambda+\mu)(1,2),$$

which is still a real multiple of $(1,2)$ and therefore an element of S. Thus S is indeed closed under addition. You can check that it is closed under scalar multiplication in the same way (do this!). Can we now say that S is a vector space itself? The axioms for a vector space are satisfied for elements of V. This means that they will also be satisfied for elements of S, as long as we know that the zero element is in S, and the negative of each element in S is also in S. Since $(0,0) = 0(1,2))$ and $-(\lambda(0,1)) = (-\lambda)(0,1)$, this is indeed the case, and we can conclude that S is a vector space itself.

Example 2.2.2 Let V be $\mathbf{R}^2$, again with its usual addition and scalar multiplication, and S be the line in $\mathbf{R}^2$ with vector equation $(x,y) = (1,1) + \lambda(1,2)$ where $\lambda \in \mathbf{R}$. This is just the line in the last example but shifted to pass through $(1,1)$. In this case S is not closed under addition. To see this, take the point $(1,1)$ which is a member of S and add it to itself: you get the point $(2,2)$ which is **not** a member of S. Therefore S is not closed under addition. There is no need to go further: S cannot be a vector space. (You can in fact check that $\mathbf{0}$ is not a member of S, and that S is not closed under scalar multiplication.)

It is clear from these two examples that a subset of a vector space could be, but need not be a vector space itself. These examples also show that closure under addition and closure under scalar multiplication are essential ideas. Let's make them precise.

Definition 2.2.3 *Let V be a vector space and S a subset of V.*

(a) We say S is ***closed under addition in*** *V if whenever two members of S are added, their sum* is also a member of S. *More concisely:*

$$\mathbf{u}, \mathbf{v} \in S \Rightarrow \mathbf{u} + \mathbf{v} \in S \textit{ for } \textbf{\textit{any}} \ \mathbf{u}, \mathbf{v}.$$

(b) We say S is ***closed under scalar multiplication in*** *V if, whenever $\mathbf{u}$ is a member of S, then for* ***any*** *scalar λ, $\lambda\mathbf{u}$* is also a member of S. *More concisely:*

$$\mathbf{u} \in S \Rightarrow \lambda\mathbf{u} \in S \textit{ for } \textbf{\textit{any}} \textit{ scalar } \lambda \textit{ and vector } \mathbf{u}.$$

Let's illustrate these definitions with a simple example.

Example 2.2.4 Let $V = \mathbf{R}^2$, with its usual addition and scalar multiplication.

(a) Let S be the first quadrant of $\mathbf{R}^2$, axes included, i.e.

$$S = \{(x,y) \in \mathbf{R}^2 : x \geq 0, y \geq 0\}.$$

We check whether S is closed under addition and scalar multiplication. If (a, b) and (c, d) are in S, then $a \geq 0, b \geq 0, c \geq 0$ and $d \geq 0$. The sum of the two vectors is $(a + c, b + d)$ and since $a + c \geq 0, b + d \geq 0$ the sum of the two vectors is in S. Thus S is closed under addition. On the other hand, S is not closed under scalar multiplication: we have $(1, 1) \in S$, but $(-1)(1, 1) = (-1, -1)$ is no longer a member of S.

(b) Let T be the first and third quadrants (axes included again).Then T is not closed under addition; for example we have $(1, 0) \in T$ and $(0, -1) \in T$ but $(1, 0)+(0, -1) = (1, -1)$ is not in the first or third quadrant and therefore not in T. On the other hand, T is closed under scalar multiplication. (Write out a proof yourself.)

We are going to use the term "subspace" for a subset of a vector space that is itself a vector space. Here is the precise definition:

Definition 2.2.5 *A subset S of a vector space V is a **subspace** of V iff*

- *S is non-empty,*
- *S is closed under addition, and*
- *S is closed under scalar multiplication.*

If you do some more mathematics, you will come across other contexts in which the word "subspace" is also used, but in a different sense. For this reason what we have called a subspace here is sometimes referred to as a *vector subspace* or *linear subspace*. Since there is no danger of confusion in this course, we'll stick to "subspace", but when you are reading other books on linear algebra, keep in mind that they may use different terminology.

Example 2.2.6

(a) The sets S and T in Example 2.2.4 above are not subspaces of $\mathbf{R}^2$.

(b) The line in Example 2.2.1 is a subspace of $\mathbf{R}^2$, but the line of Example 2.2.2 is not.

Example 2.2.7 Let $V = \mathbf{R}^3$ with its usual addition and scalar multiplication, and S be the plane with equation $2x + 3y + 4z = 0$ in $\mathbf{R}^3$. We'll check closure under addition first. We must take two arbitrary members of S, add them, and be sure that the result is a member of S. Let $\mathbf{x} = (x_1, x_2, x_3)$ and $\mathbf{y} = (y_1, y_2, y_3)$ be members of S. Then we know that $2x_1 + 3x_2 + 4x_3 = 0$ and $2y_1 + 3y_2 + 4y_3 = 0$. What about the sum $\mathbf{x}+\mathbf{y}$? This is the point $(x_1+y_1, x_2+y_2, x_3+y_3)$. But is it a member of S? We must check that it satisfies the equation of the plane given. So we must consider

$$2(x_1 + y_1) + 3(x_2 + y_2) + 4(x_3 + y_3)$$

and check that it is 0. This is easy, since we get

$$\begin{aligned} 2x_1 + 2y_1 + 3x_2 + 3y_2 + 4x_3 + 4y_3 &= (2x_1 + 3x_2 + 4x_3) + (2y_1 + 3y_2 + 4y_3) \\ &= 0 + 0 = 0, \end{aligned}$$

and so S is closed under addition. You should complete the example by showing that S is closed under scalar multiplication and that S is non-empty. Once you have done this, it will follow that S is a subspace of $\mathbf{R}^3$.

There is just one slightly subtle point to clear up. If a subspace S of V is just a non-empty subset of V closed under the addition and scalar multiplication of V, is S still a vector space in it own right (i.e. do all the axioms 1 to 8 of the definition of a vector space still hold for S)? The answer is given by the next theorem.

Theorem 2.2.8 *A subspace S of a vector space V is a vector space in its own right.*

Proof: The first thing to observe is that since S is already known to be closed under addition and scalar multiplication, the only things left to check are the axioms 1 to 8 of Definition 2.1.4 of the last section. With the exception of axioms 3 and 4 they are satisfied rather trivially: they hold in S because they already hold in V. For axiom 3, take any vector $\mathbf{u}$ in S (we can do this, since S is non-empty). Since S is closed under scalar multiplication, $0\mathbf{u} = \mathbf{0}$ must also be a member of S and so S does indeed have its own zero vector (the same one as V). Lastly, to check axiom 4, note that if $\mathbf{u}$ is a member of S, then so is $(-1)\mathbf{u} = -\mathbf{u}$, since S is closed under scalar multiplication. So for any $\mathbf{u}$ a member of S we find that $-\mathbf{u}$ is also member of S. We have now checked all the required conditions for S to be a vector space. Notice that we used Theorem 2.1.12 from the last section in this proof. (Where do we use it?) ■

Checking that some set S is or is not a subspace of some given vector space, V, is one of the basic things that you must be able to do easily. The strategy is fairly simple:

- If you suspect that S is not a subspace you need to show that *one* of the conditions fails, which will involve you in providing a counterexample. For instance, you could try showing that the zero vector in V is not a member of S, or that two particular members of S added together result in a vector not in S, or that a particular vector in S multiplied by a particular scalar is no longer a member of S.

- If you suspect that S is indeed a subspace, first check that it is non-empty (tip: try checking to see that the zero vector is a member). You must then show that it is closed under addition, so take two *arbitrary* members of S and show that their sum remains a member of S. Then you must show it is closed under scalar multiplication, so take an *arbitrary* member of S, multiply it by an *arbitrary* scalar and show that the result is still in S.

What we've said above may seem terribly obvious to some of you, but we have found from experience that the strategy is not obvious to everyone.

Let's do a few examples.

Example 2.2.9 We give some examples of subsets that *are* also subspaces.

(a) Let S be the x-axis in $\mathbf{R}^2$, $V = \mathbf{R}^2$. Then $S = \{(x, 0) : x \in \mathbf{R}\}$. S is non-empty. (You will find that the observation that the set under consideration is non-empty is often left out, simply because it is so obvious.) Now take two arbitrary members of S, say $(x_1, 0)$ and $(x_2, 0)$. Their sum is $(x_1 + x_2, 0)$ which is also a member of S. Take an arbitrary scalar, λ. Then $\lambda(x_1, 0) = (\lambda x_1, 0)$ which is still a member of S. So S is a subspace.

(b) Let $V = F[a, b]$, the vector space of all real-valued functions defined on the interval $[a, b]$ (see Example 2.1.9), and $C[a, b]$ be the subset of $F[a, b]$ consisting of all continuous functions. In your first-year course you saw that the sum of two continuous functions is a continuous function, and a constant multiple of a continuous function is also continuous. (You may not have seen proofs of these facts; those of you who do Real Analysis in the second semester will see the proofs.) This means that $C[a, b]$ is closed under addition and scalar multiplication. It is easy to see that $C[a, b]$ is non-empty, and hence it is a subspace.

(c) Let $V = C[1, 3]$ and S be the set of functions $\{f \in C[1, 3] : f(2) = 0\}$. We know from (b) that V is a vector space. Is S non-empty? Yes; for instance the function which is 0 everywhere on $[1, 3]$ satisfies the required condition. (For that matter, so does the function $f(x) = x - 2$.) Now take two arbitrary members of S, say f and

g. We know that $f(2) = 0$ and $g(2) = 0$. Is $f + g$ a member of S? To answer this we only need to consider $(f + g)(2) = f(2) + g(2) = 0 + 0 = 0$, so $f + g$ is also a member of S. It's also easy to see that $\lambda f(2) = \lambda.0 = 0$, so λf is also a member of S for any $\lambda \in \mathbf{R}$ and $f \in S$. Again we conclude that S is a subspace.

(d) Let $V = C[-1, 1]$ and S be the set of continuous functions on $[-1, 1]$ that are solutions of the differential equation $\dfrac{dy}{dx} + 3y = 0,$. Take two functions, say f and g, that satisfy the differential equation. Does $f + g$ satisfy the same equation? We check:

$$\begin{aligned} \frac{d}{dx}(f+g) + 3(f+g) &= \frac{df}{dx} + \frac{dg}{dx} + 3f + 3g \\ &= (\frac{df}{dx} + 3f) + (\frac{dg}{dx} + 3g) \\ &= 0 + 0 = 0, \end{aligned}$$

as we hoped. You should now check, in a similar way, that if f is a solution of the equation, then so is λf for any scalar λ. Why is S non-empty? Think of a **very** simple function that satisfies the equation.

(e) Every vector space V has two rather uninteresting subspaces: V itself, and the subspace $\{\mathbf{0}\}$ containing only the zero vector of V. The latter subspace is sometimes called the **trivial** subspace.

Example 2.2.10 Now for some subsets that *are not* subspaces.

(a) Let S be the union of the x-axis and the y-axis in $\mathbf{R}^2$, $V = \mathbf{R}^2$. Both $(1, 0)$ and $(0, 1)$ are members of S, but their sum is $(1, 1)$, which is not a member of S, so S is not closed under addition. (It is closed under scalar multiplication, though.) Therefore S is not a subspace

(b) Let $V = \mathbf{R}^3$, with its usual addition and scalar multiplication, and S be the plane with equation $x_1 - 2x_2 + 3x_3 = 4$ in $\mathbf{R}^3$. The zero vector $(0, 0, 0)$ does not satisfy the equation, so is not a point on the plane. Thus the plane does not contain the zero vector and cannot be a subspace.

(c) Let $V = M_{2\times2}(\mathbf{R})$, the set of all 2×2 real matrices with its usual addition and scalar multiplication, and S be the set of all 2×2 real matrices A such that $\det(A) = 0$. Both $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ and $\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$ are members of S, but their sum is the matrix I_2 which is not a member of S. Therefore S is not a subspace.

We have seen that not all subsets of vector spaces are subspaces. In the next section we look at a very important construction that will allow us to enlarge a subset which is not a subspace until it becomes a subspace.

Summary:

One important new concept was introduced in this section: that of a *subspace* of vector space.

- A subset is a subspace if it is non-empty and closed under addition and scalar multiplication.
- A subset of a vector space is a subspace if it is a vector space itself, with the operations it inherits from the vector space.
- It is very important to master the skill of checking whether a subset is a subspace.

Exercises

1. In each of the questions below, decide whether or not S is a subspace of V. Justify your answers. In each case, the operations are the usual addition and scalar multiplication.

   (a) $V = \mathbf{R}^4$ and $S = \{(x_1, x_2, x_3, x_4) : x_1 \geq x_2\}$.

   (b) $V = \mathbf{R}^4$ and $S = \{(x_1, x_2, x_3, x_4) : x_1 = 0 \text{ and } x_2 = -x_4\}$.

   (c) $V = P_3$ and $S = \{a_0 + a_1 x : a_0, a_1 \in \mathbf{R}\}$.

   (d) $V = P_3$ and $S = \{x^3 + bx^2 + cx + d : b, c, d \in \mathbf{R}\}$.

   (e) V consists of all 2×2 matrices and $S = \{\begin{pmatrix} a & b \\ c & d \end{pmatrix} : a + b + c + d = 0\}$.

   (f) V consists of all 2×2 matrices and $S = \{\begin{pmatrix} a & 1 \\ 1 & b \end{pmatrix} : a, b \in \mathbf{R}\}$.

   (g) $V = M_{n \times n}(\mathbf{R})$ (for fixed n) and S consists of all the symmetric matrices in V.

2. Let $F(\mathbf{R})$ consist of all real-valued functions defined on the whole real line $\mathbf{R}$. If addition and scalar multiplication is defined as in Example 2.1.9, $F(\mathbf{R})$ is a vector space. Decide whether the following subsets of $F(\mathbf{R})$ are subspaces:

   (a) $S = \{f \in F(\mathbf{R}) : f(0) = 2\}$.

   (b) $S = \{f \in F(\mathbf{R}) : f(2) = 0\}$.

(c) S consists of all differentiable functions in $F(\mathbf{R})$.

3. Let S and T be subspaces of a vector space V. Say, with reasons, which of the following will also be subspaces of V:
(a) $S \cap T$ (b) $S \cup T$ (c) the complement (in V), of S.

4. Prove that a subset S of a vector space V which is closed under scalar multiplication and is non-empty must contain the zero vector.

2.3 Linear combinations and spans

With the exception of the trivial vector space (the one containing only the zero vector), real (and complex) vector spaces always contain infinitely many elements. (Why?) Therefore a finite subset of a vector space cannot be a subspace (except when it is the trivial subspace). In this section we discover how we can enlarge a (finite) subset of a vector space in such a way that it "just" becomes a subspace. The basic idea is a simple one: if a nonempty subset S of a vector space V fails to be a subspace, it does so because it is either not closed under scalar multiplication, or not closed under addition, or both. To ensure that it becomes a subspace, we must enlarge S by throwing in all scalar multiples and sums of elements in S. If $\mathbf{v}_1$ and $\mathbf{v}_2$ are in S, the enlarged set must contain all elements of the form $\lambda_1\mathbf{v}_1$ and $\lambda_2\mathbf{v}_2$; it must also contain the sum $\lambda_1\mathbf{v}_1 + \lambda_2\mathbf{v}_2$ of such elements. In fact, it must not only contain the sum of any two scalar multiples of elements in S, but any finite sum of such multiples. This leads to the following important concept:

Definition 2.3.1 *A* ***linear combination*** *of a set of vectors is a sum of scalar multiples of the vectors. More precisely, a vector* $\mathbf{w}$ *is called a linear combination of the vectors* $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_k$ *if there are scalars* $\lambda_1, \lambda_2, \ldots, \lambda_k$ *such that*

$$\mathbf{w} = \lambda_1\mathbf{v}_1 + \lambda_2\mathbf{v}_2 + \ldots + \lambda_k\mathbf{v}_k.$$

Note, in particular, that it follows from this definition that for two vectors $\mathbf{u}$ and $\mathbf{v}$ in a vector space V, $\mathbf{u}$ is a linear combination of $\mathbf{v}$ if and only if there is a scalar λ such that $\mathbf{u} = \lambda\mathbf{v}$. Linear combinations occur all over the place. In fact, you have come across examples yourself before (think of equations of lines and planes, and solutions of systems of linear equations). Let's look at a few examples.

Example 2.3.2 Let $\mathbf{v}_1 = (2, 1)$, $\mathbf{v}_2 = (-4, -2)$ and $\mathbf{v}_3 = (3, -2)$.

(a) $3\mathbf{v}_1 + \frac{1}{2}\mathbf{v}_2 = (4, 2)$ is a linear combination of $\mathbf{v}_1$ and $\mathbf{v}_2$. Note that $(4, 2) = 2\mathbf{v}_1 + 0\mathbf{v}_2$, so $(4, 2)$ can be written as a linear combination of $\mathbf{v}_1$ and $\mathbf{v}_2$ in more than one way.

(b) To see whether $\mathbf{w} = (1, 4)$ is a linear combination of $\mathbf{v}_1$ and $\mathbf{v}_3$, we have to determine whether there are scalars λ_1 and λ_2 such that

$$\lambda_1\mathbf{v}_1 + \lambda_2\mathbf{v}_3 = \begin{pmatrix} 1 \\ 4 \end{pmatrix}.$$

Thus we have to solve

$$\lambda_1 \begin{pmatrix} 2 \\ 1 \end{pmatrix} + \lambda_2 \begin{pmatrix} 3 \\ -2 \end{pmatrix} = \begin{pmatrix} 1 \\ 4 \end{pmatrix}$$

for λ_1 and λ_2. This means we have to solve the vector equation:

$$\begin{pmatrix} 2 & 3 \\ 1 & -2 \end{pmatrix} \begin{pmatrix} \lambda_1 \\ \lambda_2 \end{pmatrix} = \begin{pmatrix} 1 \\ 4 \end{pmatrix}.$$

Its associated augmented matrix is:

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

which reduces to

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

This gives $\lambda_1 = 2, \lambda_2 = -1$, and so $(1, 4)$ is a linear combination of $\mathbf{v}_1$ and $\mathbf{v}_2$. Note that there is only one way of writing $(1, 4)$ as such a linear combination.

(c) Finally we ask whether $(3, 5)$ can be written as a linear combination of $\mathbf{v}_1$ and $\mathbf{v}_2$. The method is similar; we need to solve the vector equations:

$$\begin{pmatrix} 2 & -4 \\ 1 & -2 \end{pmatrix} \begin{pmatrix} \lambda_1 \\ \lambda_2 \end{pmatrix} = \begin{pmatrix} 3 \\ 5 \end{pmatrix}.$$

Its associated augmented matrix is

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

which reduces to

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

There are no solutions to this system of equations, so $(3, 5)$ is not a linear combination of $(2, 1)$ and $(-4, -2)$.

Example 2.3.3 Let $V = \mathbf{R}^3$ and let $\mathbf{v}_1 = (1, -2, 2), \mathbf{v}_2 = (2, 0, 1)$.

(a) $\mathbf{v}_1$ is not a linear combination of $\mathbf{v}_2$. (Why not?)

(b) If the vector $\mathbf{u} \in \mathbf{R}^3$ is a linear combination of $\mathbf{v}_1$, we must have $\mathbf{u} = \lambda \mathbf{v}_1$ for some $\lambda \in \mathbf{R}$. Geometrically speaking, this means that $\mathbf{u}$ must lie on the line through the origin with direction $\mathbf{v}_1$.

(c) If the vector $\mathbf{u} \in \mathbf{R}^3$ is a linear combination of $\mathbf{v}_1$ and $\mathbf{v}_2$, we must have $\mathbf{u} = \lambda \mathbf{v}_1 + \mu \mathbf{v}_2$ for some $\lambda, \mu \in \mathbf{R}$. Geometrically speaking, this means that $\mathbf{u}$ must lie on the plane through the origin which contains $\mathbf{v}_1$ and $\mathbf{v}_2$.

Important note: A vector $\mathbf{w}$ may be a linear combination of vectors $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_k$ in many different ways. There is not necessarily a unique way of expressing a vector as a linear combination of a given set of vectors.

The next observation is surprisingly useful. We'll be using it frequently later on.

Theorem 2.3.4 *Let A be an $m \times n$ matrix and $\mathbf{v}$ an $n \times 1$ matrix (so $\mathbf{v}$ is an n-vector). Then $\mathbf{w} = A\mathbf{v}$ is a linear combination of the columns of A. Conversely, any linear combination of columns of A can be written as $A\mathbf{v}$ for some n-vector $\mathbf{v}$.*

Proof: Since A is an $m \times n$ matrix, we can think of the columns of A as n m-vectors. Let $\mathbf{c}_1, \mathbf{c}_2, \ldots, \mathbf{c}_n$ be the columns of A and let $\mathbf{v} = \begin{pmatrix} \lambda_1 \\ \lambda_2 \\ \vdots \\ \lambda_n \end{pmatrix}$. Then we could write $A\mathbf{v}$ as

$$(\mathbf{c}_1 \ldots\ldots \mathbf{c}_n) \begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_n \end{pmatrix} = \lambda_1 \mathbf{c}_1 + \ldots + \lambda_n \mathbf{c}_n$$

which expresses $A\mathbf{v}$ as a linear combination of the columns of A. If you don't believe or understand the last step in the proof, you should take actual examples of A and $\mathbf{v}$ and see what happens yourself. For the converse, suppose that

$$\mathbf{w} = \lambda_1 \mathbf{c}_1 + \ldots + \lambda_n \mathbf{c}_n$$

If we put $\mathbf{v} = \begin{pmatrix} \lambda_1 \\ \lambda_2 \\ \vdots \\ \lambda_n \end{pmatrix}$, then $\mathbf{w} = A\mathbf{v}$. ■

The next result is also useful; it really says that linear combinations of linear combinations are still linear combinations.

Theorem 2.3.5 *Suppose* $\mathbf{x}$ *is a linear combination of the vectors* $\mathbf{v}_1, \ldots, \mathbf{v}_k$ *and that each* $\mathbf{v}_i$ *is a linear combination of the vectors* $\mathbf{w}_1, \ldots, \mathbf{w}_n$*. Then* $\mathbf{x}$ *is a linear combination of the vectors* $\mathbf{w}_1, \ldots, \mathbf{w}_n$*.*

Proof: This is an exercise. The example below illustrates the theorem. ■

Example 2.3.6 Suppose that $\mathbf{x} = 2\mathbf{v}_1 + 3\mathbf{v}_2$ and that $\mathbf{v}_1 = \mathbf{w}_1 + 5\mathbf{w}_2$ and $\mathbf{v}_2 = -2\mathbf{w}_1 + 3\mathbf{w}_2$. Then

$$\mathbf{x} = 2(\mathbf{w}_1 + 5\mathbf{w}_2) + 3(-2\mathbf{w}_1 + 3\mathbf{w}_2) = -4\mathbf{w}_1 + 19\mathbf{w}_2.$$

Thus we have expressed $\mathbf{x}$ as a linear combination of $\mathbf{w}_1$ and $\mathbf{w}_2$ as Theorem 2.3.5 claims.

It may be helpful to interpret this example geometrically. Suppose all the vectors in this example lie in $\mathbf{R}^3$. Then the equation $\mathbf{x} = 2\mathbf{v}_1 + 3\mathbf{v}_2$ tells us that $\mathbf{x}$ lies in the plane through the origin containing the vectors $\mathbf{v}_1$ and $\mathbf{v}_2$. The equations $\mathbf{v}_1 = \mathbf{w}_1 + 5\mathbf{w}_2$ and $\mathbf{v}_2 = -2\mathbf{w}_1 + 3\mathbf{w}_2$ tell us that both $\mathbf{v}_1$ and $\mathbf{v}_2$ lie in the plane through the origin containing the vectors $\mathbf{w}_1$ and $\mathbf{w}_2$. The equation $\mathbf{x} = -4\mathbf{w}_1 + 19\mathbf{w}_2$ shows that $\mathbf{x}$ also lies in this plane.

We have argued at the beginning of the section that if a set S of vectors in a vector space V is not a subspace of V, and we want to enlarge S so that the larger set is a subspace of V, then we'll have to include all linear combinations of vectors in S. This is what motivates the definition of the **span** of a set of vectors. It is quite a good word in the following sense: a bridge spans a river in the sense that you use it to get from one side to the other. We say that a certain collection of vectors in a vector space will span a subspace if you can use linear combinations of just those vectors to get from the origin to anywhere you want to be in the subspace. The definition below starts to make this more precise.

Definition 2.3.7 *Let* $\mathbf{v}_1, \ldots, \mathbf{v}_n$ *be vectors in a vector space* V*. The set* U *of* all *linear combinations of* $\mathbf{v}_1, \ldots, \mathbf{v}_n$ *is called the* ***span*** *of* $\mathbf{v}_1, \ldots, \mathbf{v}_n$*. (Some books use the more precise terminology* ***linear span****.) We also say that the vectors* $\mathbf{v}_1, \ldots, \mathbf{v}_n$ ***span*** *the set* U*. We write* $U = span\{\mathbf{v}_1, \ldots, \mathbf{v}_n\}$*. Explicitly:*

$$span\{\mathbf{v}_1, \ldots, \mathbf{v}_n\} = \{\lambda_1\mathbf{v}_1 + \lambda_2\mathbf{v}_2 + \cdots + \lambda_n\mathbf{v}_n : \lambda_1, \lambda_2, \ldots, \lambda_n \in \mathbf{R}\};$$

if V *is a complex vector space, we have to replace* $\mathbf{R}$ *by* $\mathbf{C}$*.*

Example 2.3.8 In $\mathbf{R}^3$ let $\mathbf{i} = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$, $\mathbf{j} = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}$ and $\mathbf{k} = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}$. Then

(a) The vector $\mathbf{i}$ spans the x-axis, since a linear combination of just one vector is just a scalar multiple of that vector.

(b) The vectors $\mathbf{i}$ and $\mathbf{j}$ span the xy-plane, since a linear combination of $\mathbf{i}$ and $\mathbf{j}$ has the form $\lambda\mathbf{i} + \mu\mathbf{j}$, and this is just the vector $\begin{pmatrix} \lambda \\ \mu \\ 0 \end{pmatrix}$ which is a member of the xy-plane. Conversely, the position vector of any point in the xy-plane can be written in this form.

(c) The vectors $\mathbf{i}, \mathbf{j}$ and $\mathbf{k}$ span $\mathbf{R}^3$ since any vector in $\mathbf{R}^3$ can be written as a a linear combination of the three vectors given.

(d) Theorem 2.3.4 tells us that if $\mathbf{w} = A\mathbf{v}$ then $\mathbf{w}$ is in the span of the columns of A.

Example 2.3.9 Let $V = C[a, b]$, the vector space of continuous real-valued functions on $[a, b]$, and consider the $k + 1$ functions $f_0, \ldots, f_k$ in V given by:

$$f_0(x) = 1, \quad f_1(x) = x, \quad f_2(x) = x^2, \quad \ldots, \quad f_k(x) = x^k.$$

The span of these functions is the set of all linear combinations of these functions, but that is just the set of all polynomials functions of degree at most k.

To understand part (c) of the following theorem, you will need to know what is meant by the intersection of a collection, or family, of sets. This is the set consisting of all the elements that are in every one of the sets in the collection. You can read more about arbitrary intersections in Appendix A.3.

Theorem 2.3.10 *Let $\mathbf{v}_1, \ldots, \mathbf{v}_n$ be vectors in a vector space V, and let U be the span of all these vectors. Then*

(a) U is indeed a subspace of V.

(b) U is the smallest subspace of V that contains $\mathbf{v}_1, \ldots, \mathbf{v}_n$. (By this we mean that any subspace containing these vectors must contain all of U as well.)

(c) U is the intersection of the family of all subspaces containing $\mathbf{v}_1, \ldots, \mathbf{v}_n$.

Proof: (a) We must check that U is a nonempty subset of V closed under addition and scalar multiplication. It's clearly nonempty; just take, say, $0\mathbf{v}_1$ which is of course in the span. Incidentally, we've just proved that $\mathbf{0}$ is a member of U. For closure under addition, take two arbitrary members of U; these could be $\mathbf{u} = \lambda_1\mathbf{v}_1 + \ldots + \lambda_n\mathbf{v}_n$ and $\mathbf{w} = \mu_1\mathbf{v}_1 + \ldots + \mu_n\mathbf{v}_n$ where $\lambda_1, \ldots, \lambda_n, \mu_1, \ldots, \mu_n$ are scalars. Then

$$\mathbf{u} + \mathbf{w} = \lambda_1\mathbf{v}_1 + \ldots + \lambda_n\mathbf{v}_n \ + \ \mu_1\mathbf{v}_1 + \ldots + \mu_n\mathbf{v}_n;$$

this can be rearranged to give

$$\mathbf{u} + \mathbf{w} = (\lambda_1 + \mu_1)\mathbf{v}_1 + \ldots + (\lambda_n + \mu_n)\mathbf{v}_n.$$

This shows that $\mathbf{u} + \mathbf{w}$ is again a linear combination of the vectors $\mathbf{v}_1, \ldots, \mathbf{v}_n$, so is a member of U, as needed.

It is just as easy to see that if λ is a scalar and $\mathbf{u} \in S$ then we certainly still have $\lambda\mathbf{u}$ a member of U. This is an exercise.

(b) Let W be any subspace that contains the individual vectors $\mathbf{v}_1, \ldots, \mathbf{v}_n$. Our task is to show that any linear combination of the vectors $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n$ (i.e. an arbitrary member of U) is also a member of W. Now, since $\mathbf{v}_1, \ldots, \mathbf{v}_n$ are members of W, so are the vectors $\lambda_1\mathbf{v}_1, \ldots, \lambda_n\mathbf{v}_n$, where $\lambda_1, \ldots, \lambda_n$ are scalars, since W, being a subspace, is closed under scalar multiplication. But W is also closed under addition, so we immediately have that

$$\lambda_1\mathbf{v}_1 + \ldots + \lambda_n\mathbf{v}_n$$

is a member of W. We've just managed to show that an arbitrary linear combination of the vectors $\mathbf{v}_1, \ldots, \mathbf{v}_n$ is a member of W, which is just what we wanted.

(c) This is an exercise; make sure that you understand what is meant by the intersection of the family of subspaces containing $\mathbf{v}_1, \ldots, \mathbf{v}_n$ before you start. ■

We finish off this section with a few more examples of spans.

Example 2.3.11 Let $M_{2\times 2}(\mathbf{R})$ be the vector space that consists of all 2×2 matrices (with real entries). Let

$$E_1 = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \quad \text{and} \quad E_2 = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}.$$

We want to determine what the span of E_1 and E_2 is. This is the set of all combinations of the form

$$\lambda E_1 + \mu E_2 = \lambda \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} + \mu \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} \lambda & 0 \\ 0 & \mu \end{pmatrix}.$$

A square matrix with all its entries except possibly those on the main diagonal equal to 0 is called a **diagonal matrix**. Thus the span of E_1 and E_2 is the collection of all diagonal 2×2 matrices (which is therefore a subspace of $M_{2\times 2}(\mathbf{R})$).

Example 2.3.12 In P_2 let

$$p_1 = 2x^2 + x + 2, \quad p_2 = x^2 - 2x, \quad p_3 = 5x^2 - 5x + 2.$$

We check whether the polynomial $p = x^2 + x + 2$ is a member of $\text{span}\{p_1, p_2, p_3\}$.

We must check whether there are scalars λ_1, λ_2 and λ_3 such that

$$\lambda_1(2x^2 + x + 2) + \lambda_2(x^2 - 2x) + \lambda_3(5x^2 - 5x + 2) = x^2 + x + 2.$$

Since polynomials are equal exactly when their coefficients are equal, we must have:

$$\begin{aligned} 2\lambda_1 + \lambda_2 + 5\lambda_3 &= 1 \qquad \text{(comparing coefficients of } x^2\text{)} \\ \lambda_1 - 2\lambda_2 - 5\lambda_3 &= 1 \qquad \text{(comparing coefficients of } x\text{)} \\ 2\lambda_1 + 0\lambda_2 + 2\lambda_3 &= 2 \qquad \text{(comparing coefficients of } x^0\text{)} \end{aligned}$$

We must therefore solve the above linear system of equations in λ_1, λ_2 and λ_3. The augmented matrix associated with this system is

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

Reducing this to row echelon form gives

$$\begin{pmatrix} 2 & 1 & 5 & 1 \\ 0 & -2.5 & -7.5 & 0.5 \\ 0 & 0 & 0 & 0.8 \end{pmatrix},$$

which indicates that the system is inconsistent; there is no solution for our system of equations, so the polynomial p is not in $\text{span}\{p_1, p_2, p_3\}$.

Notice that, in general, deciding whether a vector is in the span of some collection of vectors will always reduce to a problem involving solving a system of linear equations, or at least deciding whether the system is consistent or not.

Summary: In this section we have looked at two important concepts:

- A **linear combination** of a finite set of vectors is a sum of scalar multiples of the vectors.
- The **span** of a finite set S of vectors contained in a vector space V is the collection of all linear combinations of vectors in S; it is denoted by $\operatorname{span} S$ and is a subspace of V. It is in fact the smallest subspace of V containing S.

Exercises

1. Is $\begin{pmatrix} -3 & 2 \\ -4 & 1 \end{pmatrix}$ a linear combination of $\begin{pmatrix} 1 & 2 \\ -2 & 1 \end{pmatrix}$ and $\begin{pmatrix} 3 & 2 \\ -1 & 1 \end{pmatrix}$?
2. Let V be the vector space of all continuous functions from $\mathbf{R}$ to $\mathbf{R}$ and
$$f(x) = \cos^2(x) \text{ and } g(x) = \sin^2(x).$$
Which of the following functions lie in the subspace spanned by f and g in V?
   (a) $h_1(x) = \cos(2x)$
   (b) $h_2(x) = 3 + x^2$
   (c) $h_3(x) = 1$
   (d) $h_4(x) = \sin x$
   (e) $h_5(x) = 0$.
3. In P_3, is $q = x^2 + 4x + 7$ a linear combination of:
$$\begin{aligned} p_1 &= 2x^3 - x^2 - 2x - 5 \quad \text{and} \\ p_2 &= 3x^3 - x^2 - x - 4 \quad \text{and} \\ p_3 &= -4x^3 + 2x^2 + 4x + 10 \quad ? \end{aligned}$$
4. Is $(0, -2, 2)$ in the span of $\{(1, 3, -1), (4, 16, -8)\}$?
5. Do the polynomials $x + 1$, $x^2 + x$, $x^2 + 2x + 1$ span P_2?
6. Prove Theorem 2.3.10(c).
(Hint: Let W be the intersection of the family of all subspaces containing $\mathbf{v}_1, \ldots, \mathbf{v}_n$, and show that $U = W$.)

2.4 Linear independence

We meet a most important idea in this section: that of *linear independence*. Before we can get to that, though, we need to discuss the idea of *linear dependence*, which is in some ways the opposite of the idea of linear independence.

It makes sense to say that one vector depends on one or more other vectors if we can write the first vector in terms of the others. But what do we mean by "in terms of"? In a vector space we have two operations at our disposal: scalar multiplication and addition. Writing one vector in terms of another in this context means writing the one as a scalar multiple of the other. Writing one vector in terms of two or more other vectors means writing the first as a sum of multiples of the others, that is, as a *linear combination* of the others.

Here is an example to illustrate this idea.

Example 2.4.1 (a) In $\mathbf{R}^2$ the vector $(2, 4)$ depends on the vector $(1, 2)$ since $(2, 4) = 2(1, 2)$.
(b) Also in $\mathbf{R}^2$, the vector $(2, 3)$ is clearly a linear combination of the vectors $(1, 0)$ and $(0, 1)$:

$$(2, 3) = 2(1, 0) + 3(0, 1).$$

Informally, we can say that $(2, 3)$ "depends" on these two vectors. Of course, we might just as well say that the vector $(1, 0)$ depends on the two vectors $(0, 1)$ and $(2, 3)$ since $(1, 0) = \frac{1}{2}(2, 3) - \frac{3}{2}(0, 1)$. In fact, we will often choose our point of view to suit our needs and decide which vectors we want to see as dependent and which as the vectors that the dependent ones depend on.

It's time now to have a formal definition of the notion of linear dependence.

Definition 2.4.2 *Let V be a vector space. A vector $\mathbf{v} \in V$ is said to be **linearly dependent** on the set of vectors $S = \{\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_k\}$ in V if $\mathbf{v}$ is in the span of S, that is, if $\mathbf{v}$ is a linear combination of the vectors in S. (We use the qualification **linearly** dependent because we use only the linear operations of addition and scalar multiplication to form the linear combination.)*

Example 2.4.3 In the vector space $\mathbf{R}^3$ the vector $(2, 1, 0)$ is dependent on the set of vectors $S_1 = \{(1, 0, 0), (0, 1, 0)\}$ since $(2, 1, 0) = 2(1, 0, 0) + 1(0, 1, 0)$. On the other hand, $(2, 1, 0)$ is not dependent on the set $S_2 = \{(1, 0, 0), (0, 0, 1)\}$, since any linear combination of the vectors in S_2 will have 0 as second component.

We have now made precise the idea that one vector is linearly dependent on a set of other vectors. Is it possible to make precise the idea that a set of vectors is linearly dependent? To do this, we need a definition that will not single out one vector in advance. We could do this by saying a set of vectors is linearly dependent if we can write one of the vectors (not specified in advance) as a linear combination of the others. The practical problem with this approach is that given a set of vectors to test for linear dependence, we'll have to test each vector in the set to see whether it is linearly dependent on the others. As soon as we have found one which is, we can stop and say the set is linearly dependent. If none of the vectors is dependent on the others, we can then say the set is not linearly dependent. But the whole process could be very time-consuming if the set is large. Is there a quicker way to do this?

Let's have another hard look at the example above. The vector $(2, 1, 0)$ is dependent on the vectors $(1, 0, 0)$ and $(0, 1, 0)$ since

$$(2, 1, 0) = 2(1, 0, 0) + 1(0, 1, 0).$$

We can rewrite this as

$$2(1, 0, 0) + 1(0, 1, 0) - (2, 1, 0) = (0, 0, 0).$$

In other words we have managed to write down a linear combination of the three vectors $(1, 0, 0), (0, 1, 0), (2, 1, 0)$ which gives us the zero vector. On the other hand, the vector $(2, 1, 0)$ does not depend on the vectors $(1, 0, 0)$ and $(0, 0, 1)$. Now if we try to write down a linear combination of $(1, 0, 0), (0, 0, 1)$ and $(2, 1, 0)$ which gives the zero vector, we are forced to do it in a rather uninteresting way: we are forced to take all the scalars as 0:

$$0(1, 0, 0) + 0(0, 0, 1) + 0(2, 1, 0) = (0, 0, 0).$$

(We call this a *trivial* linear combination.) You can probably see this without having to write down anything. Even if you can't, or you want to make quite sure, you can try to solve the equation

$$\lambda_1(1, 0, 0) + \lambda_2(0, 0, 1) + \lambda_3(2, 1, 0) = (0, 0, 0);$$

you'll soon see that the only solution is $\lambda_1 = \lambda_2 = \lambda_3 = 0$.

We seem to have reached the following conclusions:

- If a vector $\mathbf{v}$ depends on the vectors $\{\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_k\}$, then we can find a *non-trivial* linear combination of the vectors $\{\mathbf{v}, \mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_k\}$ that gives the zero vector. (By "non-trivial" we mean that the scalars we use are not **all** zero.)

- If a vector $\mathbf{v}$ does not depend on the vectors $\{\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_k\}$, it seems to be impossible to find any linear combination of the vectors $\{\mathbf{v}, \mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_k\}$ which gives the zero vector, other than the obvious one where we take all scalars as 0. (This is the "trivial" linear combination.)

We are now ready to define what we mean by the linear independence and linear independence of a set of vectors. These are arguably the most important definitions in this course. Note that in these definitions we do not single out one vector in the set; all are treated equally.

Definition 2.4.4 *(a) The vectors* $\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_n$ *in a vector space* V *are said to be* ***linearly dependent*** *if there exist scalars* $\lambda_1, \lambda_2, \ldots, \lambda_n$ **not all zero** *such that*

$$\lambda_1\mathbf{u}_1 + \lambda_2\mathbf{u}_2 + \ldots + \lambda_n\mathbf{u}_n = \mathbf{0}.$$

(b) The vectors $\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_n$ *are said to be* ***linearly independent*** *if they are not linearly dependent. In other words, if these vectors are linearly independent and there are scalars* $\lambda_1, \lambda_2, \ldots, \lambda_n$ *such that*

$$\lambda_1\mathbf{u}_1 + \lambda_2\mathbf{u}_2 + \ldots + \lambda_n\mathbf{u}_n = \mathbf{0},$$

then it must be the case that $\lambda_1 = \lambda_2 = \ldots = \lambda_n = 0$*. Another way of saying this is that the* only *linear combination of* $\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_n$ *that yields the zero vector is the one in which all the scalars are zero (the trivial linear combination).*

(c) If the vectors $\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_n$ *are* ***distinct*** *and linearly independent (respectively dependent), we say the set* $S = \{\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_n\}$ *is linearly independent (respectively dependent).*

Important note: It is always possible to find a linear combination of any set of vectors that yields the zero vector. The important point of the last definition is that if you can do it with at least one of the scalars non-zero, then the vectors are linearly dependent; if the only way you can do it is by taking all the scalars zero, the vectors are linearly independent.

So, if you are given a set of distinct vectors $S = \{\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_n\}$ whose linear independence or dependence you wish to establish, your strategy has to be as follows:

1. Let $\lambda_1\mathbf{u}_1 + \lambda_2\mathbf{u}_2 + \ldots + \lambda_n\mathbf{u}_n = \mathbf{0}$. Note that we can regard this as a system of equations in the n variables $\lambda_1, \lambda_2, \ldots, \lambda_n$, and that it always has the (trivial) solution where all the λ_i's are 0.

2. See whether this system of equations has a solution other than this (trivial) one. If it has, the vectors are linearly dependent; if it does not have another solution, they are linearly independent.

Let's now see how to use these definitions. We'll first try out the examples that started the section:

Example 2.4.5 We check whether the vectors $(1, 0, 0), (0, 1, 0), (2, 1, 0)$ are linearly dependent. Let $\lambda_1(1, 0, 0) + \lambda_2(0, 1, 0) + \lambda_3(2, 1, 0) = (0, 0, 0)$. This can be rewritten as the system of equations

$$\begin{aligned} \lambda_1 + 0\lambda_2 + 2\lambda_3 &= 0 \\ 0\lambda_1 + \lambda_2 + 1\lambda_3 &= 0 \end{aligned}$$

The trivial solution is $\lambda_1 = 0, \lambda_2 = 0, \lambda_3 = 0$. But there are many other solutions as well. One of them is $\lambda_1 = 2, \lambda_2 = 1, \lambda_3 = -1$, which is a non-trivial solution, so the given vectors are linearly dependent. The point is that we have found at least one solution which is not the trivial (zero) solution.

Example 2.4.6 Next we consider the vectors $(1, 0, 0), (0, 0, 1), (2, 1, 0)$.

Let $\lambda_1(1, 0, 0) + \lambda_2(0, 0, 1) + \lambda_3(2, 1, 0) = (0, 0, 0)$. This can be rewritten as the system of equations

$$\begin{aligned} \lambda_1 + 0\lambda_2 + 2\lambda_3 &= 0 \\ 0\lambda_1 + 0\lambda_2 + \lambda_3 &= 0 \\ 0\lambda_1 + \lambda_2 + 0\lambda_3 &= 0 \end{aligned}$$

This system has only the (trivial) solution $\lambda_1 = \lambda_2 = \lambda_3 = 0$. This being the case, we have shown that the given set of vectors is linearly independent.

Example 2.4.7 Let's check whether the vectors $(1, 0, 0), (0, 1, 0), (0, 0, 1)$ are linearly independent. Let $\lambda_1(1, 0, 0) + \lambda_2(0, 1, 0) + \lambda_3(0, 0, 1) = (0, 0, 0)$. This can be rewritten as the system of equations

$$\begin{aligned} \lambda_1 &= 0 \\ \lambda_2 &= 0 \\ \lambda_3 &= 0. \end{aligned}$$

and this clearly has only the (trivial) solution $\lambda_1 = 0, \lambda_2 = 0, \lambda_3 = 0$. Thus the three vectors are indeed linearly independent.

Example 2.4.8 We show that the polynomials

$$1, x, x^2, x^3$$

form a linearly independent set in P_3. Let $\lambda_1 1 + \lambda_2 x + \lambda_3 x^2 + \lambda_4 x^3 = \mathbf{0}$, where $\mathbf{0}$ is the zero "vector" of P_3, that is the polynomial with all coefficients equal to 0. Then we can rewrite the equation as

$$\lambda_1 1 + \lambda_2 x + \lambda_3 x^2 + \lambda_4 x^3 = 0 + 0x + 0x^2 + 0x^3.$$

Since two polynomials are equal if and only if corresponding coefficients are equal, we conclude that we must have $\lambda_1 = 0, \lambda_2 = 0, \lambda_3 = 0, \lambda_4 = 0$. This means that the given polynomials are linearly independent.

Remarks:

1. It is worth noticing that when you are checking that a set S of vectors is linearly dependent or not, you end up asking whether a *homogeneous system of linear equations* (i.e. a system where the constants on the right hand side are all zero) has a non-trivial solution or not. In the event that this system does have a non-trivial solution, it will have infinitely many solutions, so there will be many different ways of expressing the zero vector as a linear combination of the given set S.

2. It is easy to see that any set of vectors which **includes** the zero vector can never be linearly independent. Let $S = \{\mathbf{0}, \mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_k\}$; then $1\mathbf{0} + 0\mathbf{u}_1 + 0\mathbf{u}_2 + \ldots + 0\mathbf{u}_k$ is a linear combination of vectors of S which equals $\mathbf{0}$ and in which not all the scalars are zero.

When we started looking at the idea of the linear dependence of a set of vectors, we suggested that it makes sense to say that a set of vectors is linearly dependent if we can express one of the vectors as a linear combination of the others. The formal definitions we eventually gave (Definition 2.4.4) looked rather different. The following theorem is reassuring; it shows that these are different ways of looking at the same thing.

Theorem 2.4.9 *Let S be a subset of a vector space V, and let S have two or more vectors. Then S is:*

(a) linearly dependent if and only if at least one of the vectors in S is expressible as a linear combination of the other vectors in S;

(b) linearly independent if and only if no vector in S is expressible as a linear combination of the other vectors in S.

Proof: We'll prove part (a); the proof of (b) is an exercise.
(a) Let $S = \{\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_k\}$ be a set with two or more vectors. If we assume S is linearly dependent, then there are scalars $\lambda_1, \lambda_2, \ldots, \lambda_k$, not all zero, such that

$$\lambda_1\mathbf{u}_1 + \lambda_2\mathbf{u}_2 + \ldots + \lambda_k\mathbf{u}_k = \mathbf{0}.$$

Since at least one of the λ_i is non-zero, we may as well assume it is λ_1. The reason why we can say this depends on the following lazy trick: we can rearrange the vectors in any order we like, so we rearrange them, if necessary, so that the the first vector is associated with a non-zero scalar. Then we can say:

$$\mathbf{u}_1 = \left(-\frac{\lambda_2}{\lambda_1}\mathbf{u}_2 - \frac{\lambda_3}{\lambda_1}\mathbf{u}_3 - \ldots - \frac{\lambda_k}{\lambda_1}\mathbf{u}_k\right)$$

which means we've expressed $\mathbf{u}_1$ as a linear combination of the other vectors in S.

We must also prove the converse: let's assume that one of the vectors in S is expressible as a linear combination of the others. To be lazy again, we may as well suppose that it is $\mathbf{u}_1$ without affecting the validity of the proof. (Why?) Then

$$\mathbf{u}_1 = \lambda_2\mathbf{u}_2 + \lambda_3\mathbf{u}_3 + \ldots + \lambda_k\mathbf{u}_k$$

so

$$\mathbf{u}_1 - \lambda_2\mathbf{u}_2 - \lambda_3\mathbf{u}_3 - \ldots - \lambda_k\mathbf{u}_k = \mathbf{0}.$$

Thus we have managed to express $\mathbf{0}$ as a non-trivial (why?) linear combination of the vectors in S, and so S is linearly dependent. ■

An aside: you may from time to time find the phrase "without loss of generality" in a proof. This is just a more sophisticated way of saying " we may as well assume".

Example 2.4.10 Let $S = \{(2, -1, 0, 3), (1, 2, 5, -1), (7, -1, 5, 8)\}$. We first show that S is linearly dependent. To do this, we must solve the equation

$$\lambda_1(2, -1, 0, 3) + \lambda_2(1, 2, 5, -1) + \lambda_3(7, -1, 5, 8) = (0, 0, 0, 0).$$

This means we must solve the system of equations

$$\begin{aligned} 2\lambda_1 + \lambda_2 + 7\lambda_3 &= 0 \\ -\lambda_1 + 2\lambda_2 - \lambda_3 &= 0 \\ 0\lambda_1 + 5\lambda_2 + 5\lambda_3 &= 0 \\ 3\lambda_1 - \lambda_2 + 8\lambda_3 &= 0 \end{aligned}$$

You can check that $\lambda_1 = 3, \lambda_2 = 1$, and $\lambda_3 = -1$ is a (non-trivial) solution of the above system, which immediately tells us that the set of vectors is linearly dependent. (If you have difficulty in spotting such a solution, you can do Gaussian elimination on the system. You will find that it has infinitely many solutions, of which the one given above is just one.) By the result above we should now be able to express one of the vectors of S as a linear combination of the others. Since we have that

$$3(2,-1,0,3) + (1,2,5,-1) - (7,-1,5,8) = (0,0,0,0)$$

we can write (for example)

$$(7,-1,5,8) = 3(2,-1,0,3) + (1,2,5,-1),$$

so we have expressed one of the vectors as a linear combination of the others.

So far, we have laboriously checked whether a given set of vectors is linearly independent or not. If we are working in the vector space $\mathbf{R}^n$, then there is an easy criterion which *sometimes* helps. The proof uses a fact which we will use in other proofs, so it's worth noting separately. Here is the fact:

Lemma 2.4.11 *A* homogeneous *system of n linear equations in k unknowns with $k > n$ always has non-trivial solutions.*

Proof: Exercise. (Think about the maximum number of pivots that such a system can have, and the number of free variables.) ∎

Here is the useful criterion:

Theorem 2.4.12 *Let S be a set of k vectors in $\mathbf{R}^n$. If $k > n$ then S is linearly dependent.*

Proof: Let $S = \{\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_k\}$ be a set of vectors in $\mathbf{R}^n$. We wish to show that there are constants $\lambda_1, \lambda_2, \ldots, \lambda_k$ **not** all zero such that

$$\lambda_1\mathbf{u}_1 + \lambda_2\mathbf{u}_2 + \ldots + \lambda_k\mathbf{u}_k = \mathbf{0} \qquad (*).$$

Let us assume that

$$\begin{aligned} \mathbf{u}_1 &= (a_{11}, a_{12}, \ldots, a_{1n}) \\ \mathbf{u}_2 &= (a_{21}, a_{22}, \ldots, a_{2n}) \\ &\vdots \\ \mathbf{u}_k &= (a_{k1}, a_{k2}, \ldots, a_{kn}). \end{aligned}$$

Then equation $(*)$ can be written:

$$\begin{aligned}
a_{11}\lambda_1 + a_{21}\lambda_2 + \ldots + a_{k1}\lambda_k &= 0 \\
a_{12}\lambda_1 + a_{22}\lambda_2 + \ldots + a_{k2}\lambda_k &= 0 \\
&\vdots \\
a_{1n}\lambda_1 + a_{2n}\lambda_2 + \ldots + a_{kn}\lambda_k &= 0
\end{aligned}$$

This is a homogeneous system of n equations in k unknowns, with $k > n$. It will therefore have non-trivial solutions, by Lemma 2.4.11, which means the vectors are linearly dependent. ■

Theorem 2.4.12 is actually pointing out something about the largest set of vectors you can find in $\mathbf{R}^n$ which is linearly independent: it is saying that any set of $n+1$ vectors or more cannot be linearly independent.

Linear independence has a very concrete interpretation in $\mathbf{R}^2$ and $\mathbf{R}^3$.

- Two non-zero vectors are linearly dependent in $\mathbf{R}^2$ or $\mathbf{R}^3$ if and only if one is a multiple of the other. (Why?) This means that they both span the same line through the origin. If they are independent then they don't lie in the same line through the origin.
- Three vectors in $\mathbf{R}^2$ must be linearly dependent. (Why?) If three vectors in $\mathbf{R}^3$ are linearly independent, then they cannot all lie in the same plane containing the origin. On the other hand, if three non-zero vectors in $\mathbf{R}^3$ are linearly dependent, then one of them must lie in the plane (or perhaps line) spanned by the other two.

We have seen that more than n vectors in $\mathbf{R}^n$ will always be linearly dependent. What can we say about exactly n vectors in $\mathbf{R}^n$? It is easy enough to find examples of two linearly dependent vectors in $\mathbf{R}^2$, and also of two linearly independent vectors in $\mathbf{R}^2$. We can distinguish between the two cases using determinants.

Theorem 2.4.13 *Let $S = \{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n\}$ be a set of n vectors in $\mathbf{R}^n$, and let A be the $n \times n$ matrix with these vectors as columns. Then S is linearly independent if and only if $\det(A) \neq 0$.*

Proof: Let $\lambda_1, \lambda_2, \ldots, \lambda_n$ be scalars and put $\mathbf{u} = \begin{pmatrix} \lambda_1 \\ \lambda_2 \\ \vdots \\ \lambda_n \end{pmatrix}$. Then

$$\lambda_1\mathbf{v}_1 + \lambda_2\mathbf{v}_2 + \ldots + \lambda_n\mathbf{v}_n = A\mathbf{u}.$$

It follows from this that the set S is linearly independent if and only if the matrix A is non-singular, and this happens if and only if A is invertible. But A is invertible if and only if $\det(A) \neq 0$. ■

Summary:

- In this section we met one of the key concepts of linear algebra: *linear independence*. A set S of vectors is linearly independent if and only if the *only* linear combination of the vectors in S that gives the zero vector is the trivial linear combination. Another way of looking at this (Theorem 2.4.9) is that a set S of two or more vectors is linearly independent if and only if none of the vectors in S is expressible as a linear combination of the others.
- A set of vectors is linearly dependent if it is not linearly independent.
- In $\mathbf{R}^n$ you cannot have a set of more than n vectors that is linearly independent, that is, every set of $n+1$ or more vectors in $\mathbf{R}^n$ is linearly dependent.
- A set of n vectors in $\mathbf{R}^n$ is linearly independent if and only if the determinant of the matrix with the vectors as columns is non-zero.

Exercises

1. (a) Show that $\{(1,1,0,0),(0,0,1,1),(3,4,5,6)\}$ is a linearly independent subset of $\mathbf{R}^4$.

   (b) Show that $\{3,\ 3+x,\ 3+x+x^2\}$ is a linearly independent subset of P_2.

2. Prove or disprove:

   (a) Every non-empty subset of a linearly dependent set is linearly dependent.

   (b) Every non-empty subset of a linearly independent set is linearly independent.

3. Show that the set $S = \{(1,2,3),(1,-3,4),(2,-2,-1),(-1,-5,14)\}$ is linearly dependent in $\mathbf{R}^3$ (there's an easy reason!), but the first vector is not a linear combination of the others.

4. The set
$$S = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} \right\}$$
is a subset of the vector space $M_{2\times 2}(\mathbf{R})$ of 2×2 real matrices. Is it linearly independent? Does it span the whole space? Give reasons for your answers.

5. Prove that the following holds in any vector space:
If $\mathbf{w}_1 = \mathbf{v}_1$, $\mathbf{w}_2 = \mathbf{v}_1 + \mathbf{v}_2$ and $\mathbf{w}_3 = \mathbf{v}_1 + \mathbf{v}_2 + \mathbf{v}_3$, then $\{\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3\}$ is linearly independent if and only if $\{\mathbf{w}_1, \mathbf{w}_2, \mathbf{w}_3\}$ is linearly independent.

6. Prove Theorem 2.4.9(b).

7. This question uses a bit of logic. It is aimed at getting you to use your knowledge of negation to understand the definition of linear independence.

   (a) Write out the definition of linear dependence using quantifiers and connectives.

   (b) Negate your proposition in (a) to obtain the definition of linear independence. If necessary, rewrite it so that it corresponds to the definition given in the notes.

8. In this section we've only defined what it means for a *finite* subset of a vector space to be linearly dependent. Here is how we can extend the definition to infinite sets:
An infinite set S in a vector space V is linearly dependent if there is a finite subset of S which is linearly dependent.

   (a) Write down a definition for linear independence of an infinite set. [Hint: Look at Question 7.]

   (b) Is it true that an infinite set S is linearly dependent if and only if one of its vectors can be expressed as a linear combination of the others?

   (c) For $n = 0, 1, 2, 3, \ldots$, let $p_n(t) = t^n$, and put $S = \{p_n : n = 0, 1, 2, 3, \ldots\}$. Is S a linearly independent subset of $C[0, 1]$?

2.5 Basis and dimension

We are now in a position to talk meaningfully about an idea which is quite intuitive. If we talk about a line, we instinctively think of it as one dimensional. Why? Let's restrict our attention to a line through the origin in (say) $\mathbf{R}^3$: we know that any such line can be spanned by any **single** vector which points along the line, that the position vector of every point on the line is a multiple of this one vector.

Now let's consider a plane through the origin. Any single vector will not be enough to span the plane, but if we take two vectors in the plane that don't point in the same direction, then the span of these two vectors will be the whole plane. We needed these **two** linearly independent vectors (why linearly independent?) to generate the plane. Perhaps that is why we think of any plane as being two dimensional. Note that we **could** have used more vectors to span our plane, but the point is we didn't need to do so; two carefully chosen vectors did the job.

Finally, let's consider the whole of $\mathbf{R}^3$ itself. No single vector spans $\mathbf{R}^3$; no two vectors span $\mathbf{R}^3$; but any **three** vectors that don't lie in the same plane (i.e. are linearly independent) will span $\mathbf{R}^3$. We are beginning to get the feeling that we call things 1-, 2- or 3-dimensional if we need at most 1, 2 or 3 linearly independent vectors to span them. This will form the basis (a rather atrocious pun, as you'll soon see) for our approach to dimension.

We first introduce the notion of a **basis** for a vector space: it should be a "good" collection of vectors that spans the vector space.

Definition 2.5.1 *Let V be a vector space. A set $B = \{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n\}$ of vectors in V is called a* **basis** *for V if*

(a) B is linearly independent, and

(b) B spans V.

The plural of "basis" is "bases" (pronounced "bayseez").

Remarks: (a) There may be many different bases for the same space; we'll give some examples of this happening soon. One of the important tricks of the trade will be to choose bases that are convenient for whatever purpose we have in mind. Often we choose the most obvious basis, but this will not always be the case. You'll see what we mean in the first example.
(b) According to the definition, a basis must be a *finite* set of vectors. The definition leaves open the possibility that there may be *no finite* set of vectors in a vector space that qualifies for a basis. There are in fact such vector spaces, as you will see in one of the following examples. It is possible to talk about an infinite basis for a vector space, but for the time being we'll only look at finite bases. We'll indicate how infinite bases are defined at the end of this section.

Example 2.5.2 In $\mathbf{R}^3$ the vectors $(1, 0, 0), (0, 1, 0)$ and $(0, 0, 1)$ form a basis for (the whole of) $\mathbf{R}^3$. We have already seen that these three vectors are linearly independent (see Example 2.4.7). It's also pretty obvious that they span $\mathbf{R}^3$. To see this, let (x_1, x_2, x_3) be an arbitrary member of $\mathbf{R}^3$; then

$$(x_1, x{+}_2, x_3) = x_1(1, 0, 0) + x_2(0, 1, 0) + x_3(0, 0, 1).$$

This basis is sometimes called the **standard basis** for $\mathbf{R}^3$.

You should have no difficulty in writing down the standard basis for $\mathbf{R}^n$, for any $n \in \mathbf{N}^+$, using the same approach as for $\mathbf{R}^3$. Do this!

We'll now immediately give you another (somewhat arbitrary) basis for $\mathbf{R}^3$.

Example 2.5.3 We show that the vectors $(2,1,0), (-3,-3,1)$ and $(-2,1,-1)$ form a basis for $\mathbf{R}^3$.

We need to show two things:

(a) The three vectors are linearly independent.

(b) The vectors span $\mathbf{R}^3$.

In fact, it is usually more efficient to show (b) first, after which there is usually not much more to be done to show linear independence. So let (x_1, x_2, x_3) be an arbitrary vector; we must find constants λ_1, λ_2 and λ_3 such that

$$\lambda_1(2,1,0) + \lambda_2(-3,-3,1) + \lambda_3(-2,1,-1) = (x_1, x_2, x_3)$$

in order to convince ourselves that the three vectors do span $\mathbf{R}^3$. We must therefore solve the system of equations:

$$\begin{aligned} 2\lambda_1 - 3\lambda_2 - 2\lambda_3 &= x_1 \\ \lambda_1 - 3\lambda_2 + \lambda_3 &= x_2 \\ 0\lambda_1 + \lambda_2 - \lambda_3 &= x_3 \end{aligned}$$

which has augmented matrix

$$\begin{pmatrix} 2 & -3 & -2 & x_1 \\ 1 & -3 & 1 & x_2 \\ 0 & 1 & -1 & x_3 \end{pmatrix}.$$

In fact, we don't really have to solve for λ_1, λ_2 and λ_3; all we must be sure of is that a solution **exists**; we're not interested in what the values of λ_1, λ_2 and λ_3 are. Now, doing Gaussian elimination, we get:

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

There's no need to go any further; from the last line we will be able to read off a value for λ_3. Using backsubstitution, we can then get values for λ_2 and λ_1. (These values will of course depend on the (given) values of x_1, x_2 and x_3.) The fact that

we **can** get values for λ_1, λ_2 and λ_3 is all that we need; we're not interested in the values themselves. We have therefore showed that the vectors span $\mathbf{R}^3$.
We've actually already done most of the work for proving linear independence. To show linear independence, we have to let

$$\lambda_1(2,1,0) + \lambda_2(-3,-3,1) + \lambda_3(-2,1,-1) = (0,0,0)$$

and prove that the only solution is $\lambda_1 = \lambda_2 = \lambda_3 = 0$. Now if we set up the augmented matrix for this system, we will get

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

But if we use Gaussian elimination on this, we will be performing exactly the steps we performed above and will get

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

which clearly means that $\lambda_3 = 0$ and by further computation that $\lambda_2 = 0$ and $\lambda_1 = 0$. This means that the vectors are linearly independent as required.

Example 2.5.4 We check to see whether the polynomials $1, x, x^2$ and x^3 form a basis for P_3.

We saw in the last section that these polynomials are indeed linearly independent. All that remains is to see that they span P_3. But this is almost trivial. Suppose we are given an arbitrary element of P_3, i.e. a polynomial of degree at most three. Then it must be of the form $a_0 + a_1x + a_2x^2 + a_3x^3$, and this is clearly a linear combination of $1, x, x^2$ and x^3. This shows that P_3 is spanned by the polynomials $1, x, x^2$ and x^3.

It's clear from the ideas in the above example that $B = \{1, x, x^2, \ldots, x^n\}$ is a basis for P_n. We call B the *standard basis* for P_n; there are many others as well.

Example 2.5.5 Let P be the vector space of *all* polynomials in x with real coefficients, with addition and scalar multiplication defined as usual for polynomials. Any finite set S of polynomials must have one of largest degree, say n; then any polynomial of degree $n+1$ or larger would not be in the span of S. This means that S will not span P and can therefore not be a basis for P. Therefore no finite subset of P can be a basis for P. This gives us an example of a vector space that does not have a basis consisting of a finite number of elements.

Example 2.5.6 Let $M_{2\times 3}(\mathbf{R})$ be the vector space of all 2×3 real matrices, and let $B = \{M_1, M_2, \ldots, M_6\}$ where:
$M_1 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$, $M_2 = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix}$, $M_3 = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}$ and

$M_4 = \begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \end{pmatrix}$, $M_5 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$, $M_6 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$.
We show that B is a basis for $M_{2\times 3}(\mathbf{R})$.

To show that B spans $M_{2\times 3}(\mathbf{R})$ take an arbitrary matrix

$$A = \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \end{pmatrix}.$$

Then it's easy to see that

$$A = a_{11}M_1 + a_{12}M_2 + a_{13}M_3 + a_{21}M_4 + a_{22}M_5 + a_{23}M_6$$

so B spans $M_{2\times 3}(\mathbf{R})$.
To see that B is linearly independent, let

$$a_1M_1 + a_2M_2 + \ldots + a_6M_6 = \mathbf{0},$$

where $\mathbf{0}$ is the 2×3 zero matrix. Then

$$\begin{pmatrix} a_1 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & a_2 & 0 \\ 0 & 0 & 0 \end{pmatrix} + \ldots + \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & a_6 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}.$$

From this it's clear that $a_1 = a_2 = \ldots = a_6 = 0$ and we are finished.

We've now established the idea of a basis, but why have we done this? We'll see as we go along that knowing about a basis for a particular vector space makes working with that vector space very much simpler. In some sense, you are entitled to view the basis as a set of building blocks for the whole space. After all, every vector in the space can be expressed as a linear combination of basis members, since they span the space. One often just needs to understand how the basis vectors are behaving to understand how the whole space is behaving. You may, quite rightly, wonder why we need to insist that the basis be a linearly independent set as well. The fact that a basis is also linearly independent gives it some very good additional features (we'll see this in Theorem 2.5.9).

We're now going to prove some very important (i.e. useful) facts about bases.

First we have a simple observation.

Theorem 2.5.7 *Let V be a vector space and S a set of vectors in V. Let U be the subspace spanned by S, i.e. $U = \mathrm{span}\, S$. If S is linearly independent, then S is a basis for U.*

Proof: We already know that S spans U. Since it is also linearly independent, it must be a basis and we are finished! ■

Example 2.5.8 (a) Let $S = \{(1,1,2),(2,0,1)\}$. Then S is linearly independent, since neither vector is a multiple of the other, and S spans a plane in $\mathbf{R}^3$. Thus S is a basis for this plane, which is the plane through the points $(1,1,2),(2,0,1)$ and $(0,0,0)$.

(b) Let $T = S \cup \{(-1,1,1)\}$. T also spans the plane in (a) since, in fact, $(-1,1,1)$ is a linear combination of the other two vectors (check this), so any linear combination of all three vectors in T can be obtained as a linear combination of just the first two members of T. However, T is not a basis for the plane because T is not linearly independent. It is worth noting that although T spans the plane, we can find a smaller set, namely S, which also spans the plane. But there is no proper subset of S which spans the plane; we can think of S as a *minimal* spanning set for the plane.

The following group of results begin to show us why bases are so convenient to work with.

Theorem 2.5.9 *Let $S = \{\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_n\}$ be a basis for a vector space V and let $\mathbf{v}$ be a member of V. Then $\mathbf{v}$ can be expressed in one and only one way as a linear combination of members of S.*

Proof: The fact that $\mathbf{v}$ can be expressed as a linear combination of members of S comes from the fact that S spans V, so there is nothing to prove there. Why is there *only one* way in which this can be done? Well, suppose that there are two ways in which it can be done, say

$$\mathbf{v} = \lambda_1\mathbf{u}_1 + \lambda_2\mathbf{u}_2 + \ldots + \lambda_n\mathbf{u}_n = \mu_1\mathbf{u}_1 + \mu_2\mathbf{u}_2 + \ldots + \mu_n\mathbf{u}_n.$$

Our aim is to show that $\lambda_1 = \mu_1, \lambda_2 = \mu_2, \ldots, \lambda_n = \mu_n$. Consider

$$\begin{aligned} \mathbf{0} = \mathbf{v} - \mathbf{v} &= (\lambda_1\mathbf{u}_1 + \lambda_2\mathbf{u}_2 + \ldots + \lambda_n\mathbf{u}_n) - (\mu_1\mathbf{u}_1 + \mu_2\mathbf{u}_2 + \ldots + \mu_n\mathbf{u}_n) \\ &= (\lambda_1 - \mu_1)\mathbf{u}_1 + (\lambda_2 - \mu_2)\mathbf{u}_2 + \ldots + (\lambda_n - \mu_n)\mathbf{u}_n \end{aligned}$$

but since S is a basis, the $\mathbf{u}_i$'s are linearly independent and so

$$\lambda_1 - \mu_1 = \lambda_2 - \mu_2 = \ldots = \lambda_n - \mu_n = 0.$$

Thus we get that $\lambda_1 = \mu_1, \lambda_2 = \mu_2, \ldots, \lambda_n = \mu_n$ as we wanted. ■

The fact that there is a unique way of expressing any vector in a vector space as a linear combination of basis vectors leads to a new idea.

Definition 2.5.10 *Let $B = \{\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_n\}$ be a basis for a vector space V. If*

$$\mathbf{v} = \lambda_1\mathbf{u}_1 + \lambda_2\mathbf{u}_2 + \ldots + \lambda_n\mathbf{u}_n,$$

then we say that the scalars $\lambda_1, \lambda_2, \ldots, \lambda_n$ are the ***coordinates of* $\mathbf{v}$ *relative to the basis*** *B. We also say that $(\lambda_1, \lambda_2, \ldots, \lambda_n)$ is the* ***coordinate vector of* $\mathbf{v}$ *relative to the basis*** *B.*

Remark: Notice that the order in which you write down the vectors of the basis B will influence the appearance of the coordinate vector relative to that basis. Notice also that if there had **not** been a unique way of writing a vector as a linear combination of basis vectors, then the concept of a coordinate vector would be nonsensical.

Example 2.5.11 Let $\mathbf{v} = (2, 5, -10)$. Then

$$\mathbf{v} = 2(1, 0, 0) + 5(0, 1, 0) - 10(0, 0, 1)$$

and so $2, 5$ and -10 are the coordinates of $\mathbf{v}$ relative to the standard basis for $\mathbf{R}^3$. The coordinate vector relative to this basis is just $(2, 5, -10)$. On the other hand, if we are thinking of the basis $S' = \{(0, 0, 1), (0, 1, 0), (1, 0, 0)\}$ *in that order*, then the coordinate vector of $(2, 5, -10)$ would be $(-10, 5, 2)$.

Remark: We sometimes refer to an **ordered** basis for a vector space V if the order in which we write down the basis vectors is significant in what we are discussing.

Example 2.5.12 To find the coordinate vector of $(2, 5, -10)$ relative to the ordered basis $S = \{(2, 1, 0), (-3, -3, 1), (-2, 1, -1)\}$, we need to find numbers λ_1, λ_2 and λ_3 such that

$$(2, 5, -10) = \lambda_1(2, 1, 0) + \lambda_2(-3, -3, 1) + \lambda_3(-2, 1, -1);$$

the coordinate vector will then be the vector $(\lambda_1, \lambda_2, \lambda_3)$. (We leave it to you to check that these three vectors do indeed form a basis for $\mathbf{R}^3$.) A bit of calculation (Gaussian elimination) shows that

$$(2, 5, -10) = -69(2, 1, 0) - 32(-3, -3, 1) - 22(-2, 1, -1).$$

(You could use the Linear Algebra Toolkit to check this.) So the coordinate vector of $(2, 5, -10)$ relative to this rather arbitrary basis is $(-69, -32, -22)$.

You may well say "Who would ever want to know that?" Your scepticism may be justified, but we will, later in this course, need to work with important non-standard bases and coordinate vectors relative to these bases. The gist of the matter is that a careful choice of basis can often simplify calculations greatly, and give important insights into a problem.

We can now return to the idea raised at the beginning of this section, namely, the idea of dimension. It seems clear what we ought to do now that we have the concept of a basis of a space: we should define the dimension of a space to be the number of vectors that you need to make a basis for the space. For instance $\mathbf{R}^3$ then has dimension three since its standard basis has three vectors in it, and a plane through the origin must have dimension two since you need two linearly independent vectors to span such a plane. There is, however, a major problem with this idea: what if two different bases for a vector space V have different numbers of vectors in them? This would make nonsense of our definition of dimension! What we have to do then is to show that this cannot happen. In other words, we must show that any two bases for a given vector space must have the same number of vectors. Fortunately, it's not too difficult to do this.

Theorem 2.5.13 *Let V be a vector space and let $S = \{\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_n\}$ be a basis for V. Then:*
(a) Every set with more than n vectors is linearly dependent.
(b) No set with fewer than n vectors can span V.

Proof: (a) Let $T = \{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_k\}$ be any set of k vectors in V with $k > n$. We want to show that T is linearly dependent. Since we know S is a basis for V we know that each $\mathbf{v}_i$ can be expressed as a linear combination of the vectors in S. This means that for each i such that $1 \leq i \leq k$ we can find scalars $\lambda_{i1}, \lambda_{i2}, \ldots, \lambda_{in}$ such that

$$\begin{aligned}
\mathbf{v}_1 &= \lambda_{11}\mathbf{u}_1 + \lambda_{12}\mathbf{u}_2 + \ldots + \lambda_{1n}\mathbf{u}_n \\
\mathbf{v}_2 &= \lambda_{21}\mathbf{u}_1 + \lambda_{22}\mathbf{u}_2 + \ldots + \lambda_{2n}\mathbf{u}_n \qquad (1) \\
&\vdots
\end{aligned}$$

$$\mathbf{v}_k = \lambda_{k1}\mathbf{u}_1 + \lambda_{k2}\mathbf{u}_2 + \ldots + \lambda_{kn}\mathbf{u}_n$$

To show that T is linearly dependent we must find scalars $\mu_1, \mu_2, \ldots, \mu_k$, not all zero, such that

$$\mu_1\mathbf{v}_1 + \mu_2\mathbf{v}_2 + \ldots + \mu_k\mathbf{v}_k = \mathbf{0}, \qquad (2)$$

or, using the equations in (1), such that

$$\begin{aligned} & (\mu_1\lambda_{11} + \mu_2\lambda_{21} + \ldots + \mu_k\lambda_{k1})\mathbf{u}_1 \\ + \; & (\mu_1\lambda_{12} + \mu_2\lambda_{22} + \ldots + \mu_k\lambda_{k2})\mathbf{u}_2 \qquad (3) \\ \vdots \; & \\ + \; & (\mu_1\lambda_{1n} + \mu_2\lambda_{2n} + \ldots + \mu_k\lambda_{kn})\mathbf{u}_n = \mathbf{0} \end{aligned}$$

(We replaced the $\mathbf{v}_i$'s by using (1).) Since the $\mathbf{u}_i$'s form a basis we know that the coefficients of the $\mathbf{u}_i$'s in (3) must all be zero. Thus all we have to do now to prove that T is linearly dependent is to find $\mu_1, \mu_2, \ldots, \mu_k$ not all zero that satisfy

$$\begin{aligned} \lambda_{11}\mu_1 + \lambda_{21}\mu_2 + \ldots + \lambda_{k1}\mu_k &= 0 \\ \lambda_{12}\mu_1 + \lambda_{22}\mu_2 + \ldots + \lambda_{k2}\mu_k &= 0 \qquad (4) \\ &\vdots \\ \lambda_{1n}\mu_1 + \lambda_{2n}\mu_2 + \ldots + \lambda_{kn}\mu_k &= 0 \end{aligned}$$

If we can do that, then (3) holds, and so finally we have our μ_i's not all zero such that (2) holds. Now (4) is a homogeneous system of n equations in k unknowns where $k > n$. (You can think of the λ_{ij}'s as known, since they are determined by the $\mathbf{v}_i$'s, which are given.) We already know that such a system must have non-trivial solutions (Lemma 2.4.11). Any such non-trivial solution guarantees what we want.

Before we look at the proof of the next part, we want to remind you here that we've already proved the first part in the special case where $V = \mathbf{R}^n$ in Theorem 2.4.12 in the last section. In that proof, we also needed the fact that a homogeneous system of n equations in k unknowns with $k > n$ has non-trivial solutions.

(b) Let $T = \{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_k\}$ be a set of vectors in V with $k < n$. We want to show that T does not span V. The proof is by contradiction, so we will suppose that T does span V and get a contradiction.

Since we have supposed that T does span V, we must have

$$\begin{aligned} \mathbf{u}_1 &= \lambda_{11}\mathbf{v}_1 + \lambda_{12}\mathbf{v}_2 + \ldots + \lambda_{1k}\mathbf{v}_k \\ \mathbf{u}_2 &= \lambda_{21}\mathbf{v}_1 + \lambda_{22}\mathbf{v}_2 + \ldots + \lambda_{2k}\mathbf{v}_k \qquad (5) \\ &\vdots \\ \mathbf{u}_n &= \lambda_{n1}\mathbf{v}_1 + \lambda_{n2}\mathbf{v}_2 + \ldots + \lambda_{nk}\mathbf{v}_k \end{aligned}$$

To get a contradiction, we will show that there are scalars $\mu_1, \mu_2, \ldots, \mu_n$ not all zero such that

$$\sum_{i=1}^{n} \mu_i \mathbf{u}_i = \mu_1 \mathbf{u}_1 + \mu_2 \mathbf{u}_2 + \ldots + \mu_n \mathbf{u}_n = \mathbf{0}. \qquad (6)$$

If we can do this, it will contradict the linear independence of the $\mathbf{u}_i$'s. Using (5), we get

$$\sum_{i=1}^{n} \mu_i \mathbf{u}_i = \sum_{i=1}^{n} \mu_i \left(\sum_{j=1}^{k} \lambda_{ij} \mathbf{v}_j \right) = \sum_{j=1}^{k} \left(\sum_{i=1}^{n} \lambda_{ij} \mu_i \right) \mathbf{v}_j.$$

We can make this expression equal to the zero vector if we can find $\mu_1, \mu_2, \ldots, \mu_n$ such that $\sum_{i=1}^{n} \lambda_{ij} \mu_i = 0$ for $j = 1, 2, \ldots, k$. This requirement gives us a homogeneous system of k equations in the n unknowns $\mu_1, \mu_2, \ldots, \mu_n$, with $k < n$, and so the result follows from Lemma 2.4.11 again. ■

The last theorem tells us everything we want to know: in particular it tells us that if a vector space V has a basis S with n vectors in it, then so does every other basis T. Why? Because if T has more than n vectors it won't be linearly independent and if it has fewer than n vectors it won't span V. We give this fact the status of a theorem; it is important.

Before we do that though, let's just get some terminology out of the way.

Definition 2.5.14 *If a vector space V has a basis consisting of a finite number of vectors, V is said to be **finite dimensional**. If V does not have such a basis it is said to be **infinite dimensional**.*

You may recall that we have already seen at least one infinite-dimensional vector space: the space P of all polynomials (Example 2.5.5). You have of course seen many finite dimensional spaces already!

There is a minor technical problem about the rather uninteresting vector space which just has one element (which is necessarily the zero vector). We saw in the last section that any set of vectors that includes the zero vector is linearly dependent. This leads to the rather odd conclusion that this vector space has no basis at all; any spanning subset of this space would have to include the zero vector! We agree to say that this space is **zero dimensional**.

Here is the promised theorem:

Theorem 2.5.15 *All bases for a finite dimensional vector space have the same number of vectors.*

Because of this theorem, it does now make sense to talk about the dimension of a finite dimensional space: it is the number of vectors in any basis for the space.

Definition 2.5.16 *The* ***dimension*** *of a finite dimensional space V, denoted by* $\dim(V)$*, is defined to be the number of vectors in any basis for V.*

Example 2.5.17 (a) $\mathbf{R}^2$ has dimension 2: a basis is $\{(1,0),(0,1)\}$.

(b) $\dim(\mathbf{R}^n) = n$. (Why?)

(c) P_3 has dimension 4; a basis is $\{1, x, x^2, x^3\}$. Similarly, $\dim(P_n) = n+1$.

(d) Let W be any "straight line through the origin" in $\mathbf{R}^n$, i.e.

$$W = \{\lambda \mathbf{v} : \lambda \in \mathbf{R}\}$$

for some non-zero vector $\mathbf{v} \in \mathbf{R}^n$. Then $\{\mathbf{v}\}$ is a basis for W and so $\dim(W) = 1$.

(e) Recall that $C[a,b]$ is the set of all continuous real-valued functions on the interval $[a,b]$. For $k = 0, 1, 2, 3 \ldots$, let us define the function $f_k : [a,b] \to \mathbf{R}$ by $f_k(x) = x^k$. If we suppose that $\dim(C[a,b]) = n$ for some $n \in \mathbf{N}$ we obtain a contradiction, since $\{f_0, f_1, f_2, \ldots, f_n\}$ is a linearly independent set of continuous functions with $n+1$ elements. Thus $C[a,b]$ must be infinite dimensional.

Example 2.5.18 The solution set of the homogeneous system

$$\begin{aligned} 2x_1 + 2x_2 - x_3 + x_5 &= 0 \\ -x_1 - x_2 + 2x_3 - 3x_4 + x_5 &= 0 \\ x_1 + x_2 - 2x_3 - x_5 &= 0 \\ x_3 + x_4 + x_5 &= 0 \end{aligned}$$

is the set of all $(x_1, x_2, x_3, x_4, x_5)$ in $\mathbf{R}^5$ satisfying the set of equations. If A is the coefficient matrix of the system, the solution set is $\{\mathbf{x} \in \mathbf{R}^5 : A\mathbf{x} = \mathbf{0}\}$. It can be shown (see the next section) that it is a subspace of $\mathbf{R}^5$. We want to determine a basis for this space, and also its dimension.

Using Gaussian elimination we get that the solution of this system is

$$x_1 = -s - t, x_2 = s, x_3 = -t, x_4 = 0, x_5 = t \quad \text{where } s, t \in \mathbf{R}.$$

We can rewrite the solution using vectors to get

$$\begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \end{pmatrix} = s \begin{pmatrix} -1 \\ 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} + t \begin{pmatrix} -1 \\ 0 \\ -1 \\ 0 \\ 1 \end{pmatrix},$$

which shows that the vectors

$$\mathbf{u}_1 = \begin{pmatrix} -1 \\ 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} \quad \text{and} \quad \mathbf{u}_2 = \begin{pmatrix} -1 \\ 0 \\ -1 \\ 0 \\ 1 \end{pmatrix}$$

span the solution space. You can check (by inspection) that $\mathbf{u}_1$ and $\mathbf{u}_2$ are linearly independent, so $\{\mathbf{u}_1, \mathbf{u}_2\}$ is a basis and the dimension of the space must be 2.

We will end this section with a look at some useful facts about linear independence and bases. We'll leave some of the proofs as (slightly challenging) exercises for you. They are all useful results and also gives one a feeling for how bases work.

Theorem 2.5.19 *Let $S = \{\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_n\}$ be a non-empty set of vectors in a vector space V.*

(a) If S is linearly independent, and if $\mathbf{v}$ is a vector in V that is not in the span of S then $S \cup \{\mathbf{v}\}$ is still linearly independent.

(b) If $\mathbf{v}$ is a vector in S that is expressible as a linear combination of other vectors in S, then $S \backslash \{\mathbf{v}\}$ spans the same set as S.

Proof: (a) We give a proof by contradiction. Suppose $S \cup \{\mathbf{v}\}$ is linearly dependent. Then there are scalars $\lambda_1, \lambda_2, \ldots, \lambda_{n+1}$, not all zero, such that

$$\lambda_1 \mathbf{u}_1 + \lambda_2 \mathbf{u}_2 + \ldots + \lambda_n \mathbf{u}_n + \lambda_{n+1} \mathbf{v} = \mathbf{0}.$$

We cannot have $\lambda_{n+1} = 0$, for this would imply that S is linearly dependent (why?), contrary to the assumption. But if $\lambda_{n+1} \neq 0$, then

$$\mathbf{v} = -\frac{1}{\lambda_{n+1}} \left(\lambda_1 \mathbf{u}_1 + \lambda_2 \mathbf{u}_2 + \ldots + \lambda_n \mathbf{u}_n \right).$$

But this contradicts the fact that $\mathbf{v} \notin \operatorname{span}(S)$, so $S \cup \{\mathbf{v}\}$ must be linearly independent.

(b) This part is left as an exercise. Keep in mind that in any linear combination containing $\mathbf{v}$, $\mathbf{v}$ can be replaced by a linear combination of the other vectors in S.

$\blacksquare$

This theorem is sometimes called the "plus/minus" theorem.

Example 2.5.20 (a) Suppose we have a set S of two linearly independent vectors in $\mathbf{R}^3$. They span a plane through the origin; if we now enlarge S by adding a vector not in the span of S, the resulting set of vectors is still linearly independent. (What does it span?)

(b) If S is a set of three non-collinear vectors (i.e. they don't all lie along the same line) in $\mathbf{R}^3$ that do lie in a common plane, then the three vectors span the plane. However, if we remove one of the vectors that is in the span of the other two, the remaining set of two vectors will still span the same plane.

Theorem 2.5.21 *If V is an n-dimensional space and if S is a set in V with exactly n vectors, then S is a basis for V if either S spans V or S is linearly independent.*

Proof: Suppose first that S is linearly independent. We need to show that it spans V. Suppose it does not, and $\mathbf{v}$ is a vector in V that is not in the span of S. Then by Theorem 2.5.19(a) $S \cup \{\mathbf{v}\}$ is still linearly independent. But this contradicts Theorem 2.5.13(a). It follows that S spans V and is therefore a basis for V.
The proof that S is a basis if it spans V uses Theorem 2.5.19(b) and Theorem 2.5.13(b), and is left as an exercise. ■

This result tells us that the three vectors mentioned in Example 2.5.20(a) must actually be a basis for $\mathbf{R}^3$ since there are three of them that are linearly independent.

Example 2.5.22 (a) The set $S = \{(-3, 7), (5, 5)\}$ in $\mathbf{R}^2$ has two vectors. Since they are clearly linearly independent and $\mathbf{R}^2$ is two dimensional, S is a basis for $\mathbf{R}^2$.

(b) The first two vectors of $T = \{(2, 0, -1), (4, 0, 7), (-1, 1, 4)\}$ span the xz-plane. (Why?) The third vector does not lie in this plane. Thus T is a linearly independent set in the three-dimensional space $\mathbf{R}^3$. It must therefore be a basis for $\mathbf{R}^3$.

Theorem 2.5.23 *Let S be a set of vectors in a finite-dimensional vector space V.*

(a) If S spans V, but is not a basis for V, then S can be reduced to a basis for V by removing, appropriately, some vectors from S.

(b) If S is a linearly independent set that is not already a basis for V, then S can be enlarged to form a basis for V by adding appropriate vectors to S.

Proof: (a) If S spans V, but is not a basis for V, then S must be linearly dependent. Hence one of the vectors in S, say $\mathbf{v}$, must be a linear combination of the remaining vectors in S. It follows from Theorem 2.5.19 that $S \setminus \{\mathbf{v}\}$ will still span V. If $S \setminus \{\mathbf{v}\}$ is linearly independent, it is a basis for V and we can stop. If it is not, we can remove a vector from $S \setminus \{\mathbf{v}\}$ and still be left with a set that spans V. This process can be continued until we obtain a linearly independent set, and hence a basis for V.

(b) The proof of this part uses the first part of Theorem 2.5.19, and is left as an exercise. ■

Example 2.5.24 Let $S = \left\{ \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 3 \end{pmatrix}, \begin{pmatrix} -2 \\ 3 \\ 8 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} \right\}$. Then clearly S cannot be linearly independent, since there are just too many vectors (four in $\mathbf{R}^3$). However, if S spans $\mathbf{R}^3$, we should be able to remove one vector to get a basis for $\mathbf{R}^3$.

We check that S spans $\mathbf{R}^3$. Let (x_1, x_2, x_3) be an arbitrary member of $\mathbf{R}^3$. We seek constants $\lambda_1, \lambda_2, \lambda_3, \lambda_4$ such that $\lambda_1 \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix} + \ldots + \lambda_4 \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix}$.
The associated augmented matrix for this system of equations is

$$\begin{pmatrix} 1 & 0 & -2 & 1 & x_1 \\ 0 & 1 & 3 & 1 & x_2 \\ 1 & 3 & 8 & 1 & x_3 \end{pmatrix}$$

This reduces to

$$\begin{pmatrix} 1 & 0 & -2 & 1 & x_1 \\ 0 & 1 & 3 & 1 & x_2 \\ 0 & 0 & 1 & -3 & x_3 - x_1 - 3x_2 \end{pmatrix},$$

which shows us two things. Firstly, it shows us that we **can** solve for $\lambda_1, \lambda_2, \lambda_3, \lambda_4$; this means that the vectors do span $\mathbf{R}^3$. Secondly, it shows us that λ_4 is a free variable. Now if we take $x_1 = x_2 = x_3 = 0$ we see that we can set $\lambda_4 = 1$ and obtain a linear combination of the original four vectors which is the zero vector. That means that we know that the last vector is a linear combination of the first three (since λ_4 is non-zero) which means that we can remove it from our set without affecting the span of the set. Thus the first three vectors form a basis for $\mathbf{R}^3$.

We end this chapter by indicating how a basis for an infinite-dimensional vector space can be defined. It is clear from our definition of an infinite-dimensional space that a basis for such a space will need to have infinitely many elements. A basis for a finite-dimensional space is a (finite) linearly independent set which spans the space. If we want to use the same definition for infinite dimensional spaces, we'll have to say what it means for an *infinite* set to be linearly independent, and to span a vector space. (You've already had a chance to look at linear dependence for infinite sets in Exercise 8 of Section 2.4.) Here are the definitions:

Definition 2.5.25 *Let V be a vector space and S a (possibly infinite) subset of V.*

(a) We say that S spans V if every element of V can be written as a ***finite*** *linear combination of elements of S.*

(b) We say that S is linearly independent if ***every finite*** *subset of S is linearly independent.*

(c) We say that S is a basis for V if it is linearly independent and spans V.

Example 2.5.26 As we've seen, the vector space P of all polynomials in x is an infinite-dimensional vector space. The set $S = \{x^n : n = 0, 1, 2, 3, \ldots\}$ is an infinite subset of P. It can be checked that S spans P and is linearly independent, and is therefore a basis for P. We ask you to check the details in the exercises.

If V is a vector space containing the non-zero vector $\mathbf{v}$, then the set $\{\mathbf{v}\}$ is linearly independent. If $\text{span}\{\mathbf{v}\} \neq V$, Theorem 2,5,19(a) allows us to enlarge $\{\mathbf{v}\}$ one vector at a time in such a way that the new sets are all still linearly independent. The process will stop once we have a linearly independent set which spans V, that is a basis for V. If the process does not stop, V is infinite dimensional. (Why?)

We can now ask whether every infinite-dimensional vector space has a basis. The answer is "yes", but the proof depends on some fairly sophisticated set theory. For the moment we'll ask you to accept this on trust.

Summary:

- A linearly independent set which spans a vector space is a basis for that space.
- Every vector in the vector space can be written in a unique way as a linear combination of the basis vectors.
- A finite-dimensional vector space is one that has a basis consisting of a finite number of vectors; other vector spaces are infinite-dimensional.
- The number of vectors in a basis for a finite-dimensional space is unique, and called the dimension of the space.

- A set of n vectors in an n-dimensional vector space is a basis for the space if it is either linearly independent, or it spans the space.

Exercises

1. Explain why the following are *not* bases for the indicated vector spaces.
   (a) $\{(1,2),(0,3),(2,7)\}$ for $\mathbf{R}^2$.
   (b) $\{(-1,3,2),(6,1,1)\}$ for $\mathbf{R}^3$.
   (c) $\{1+x+x^2,\ x-1\}$ for P_2.

2. Which of the following sets are bases for $\mathbf{R}^3$?
   (a) $\{(3,-1,4),(2,5,6),(1,4,8)\}$
   (b) $\{(1,6,4),(2,4,-1),(-1,2,5)\}$

3. (a) Find the coordinate vector of $(1,1)$ relative to the basis $B=\{(2,-4),(3,8)\}$ for $\mathbf{R}^2$.
   (b) Find the coordinate vector of $(2,-1,3)$ relative to the basis $B=\{(3,3,3),(2,2,0),(1,0,0)\}$ for $\mathbf{R}^3$.

4. Find a basis for, and the dimension of, the solution space of the system:

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

5. Find a basis for, and the dimension of, the subspace of $\mathbf{R}^3$ given by the plane with equation $x-y=0$.

6. Find a vector that can be adjoined to the set $\{(-1,2,3),(1,-2,-2)\}$ to produce a basis for $\mathbf{R}^3$.

7. Find the dimension of the vector space spanned by:
   $\{(1,2,-1,3),(2,1,1,9),(0,2,-2,-2),(2,4,-2,6)\}$ in $\mathbf{R}^4$.

8. Find a basis for, and the dimension of, the following vector spaces:
   (a) All 3×3 matrices.
   (b) All 3×3 diagonal matrices. (A diagonal matrix is one whose non-diagonal entries are all zero.)
   (c) All 3×3 symmetric matrices.

9. Complete the proofs of
   (a) Theorem 2.5.19(b);
   (b) Theorem 2.5.21;
   (c) Theorem 2.5.23(b).
10. Let V be a vector space and B be a basis for V.
    (a) Prove that if S is a linearly independent subset of V which contains B, then $S = B$. (This is sometimes expressed by saying a basis is a *maximal linearly independent* subset.)
    (b) Prove that if S is a subset of V which spans V and is contained in B, then $S = B$. (This is sometimes expressed by saying a basis is a *minimal spanning* subset.)
    (c) Prove that a maximal linearly independent set of V is a basis for V.
    (d) Prove that a minimal spanning set of V is a basis for V.
11. Check that the set S given in Example 2.5.26 is a basis for P.

2.6 Subspaces associated with a matrix

In this section, we look at some very important subspaces associated with any matrix. These are the *nullspace* (or *kernel*), the *row space* and *column space* of a matrix.

The nullspace of a matrix is the set of all vectors which when multiplied by the matrix on the left gives the zero vector. We can regard the rows of an $m \times n$ matrix as a set of m n-vectors, and ask what the subspace spanned by these vectors will be. In the same way we may think of the columns of an $m \times n$ matrix as a set of n m-vectors, and again ask for the span of this set of vectors. Since the span of any set of vectors is a subspace, this gives us two further subspaces associated with a matrix. The reasons for looking at these subspaces include the fact that we will get a deeper understanding of the relationships between the solutions of a linear system of equations and properties of its coefficient matrix.

Let's pose two questions here:

- What relationships exist between the solutions of a linear system $A\mathbf{x} = \mathbf{b}$ and the nullspace, row space and column space of the matrix A?

- What relationships exist between the nullspace, row space and column space of a matrix?

We will spend the rest of this section investigating these questions.

Definition 2.6.1 *Let A be an $m \times n$ matrix. The set $\{\mathbf{x} : A\mathbf{x} = \mathbf{0}\}$ is called the* ***null space*** *of A. We denote this by $NS(A)$. (Some textbooks refer to the null space of A as the* ***kernel*** *of A.)*

It follows from the definition that if A is an $m \times n$ real matrix, then $NS(A)$ is a *subset* of $\mathbf{R}^n$; if A is complex, it is a subspace of $\mathbf{C}^n$. We would like to show it is a *subspace* as well. But let's do some concrete examples first.

Example 2.6.2 (a) To find the null space of the matrix $A = \begin{pmatrix} 1 & 2 \\ 0 & 3 \end{pmatrix}$ we must find the set of vectors $\mathbf{x} = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$ such that $A\mathbf{x} = \mathbf{0}$. This will be the case if

$$\begin{aligned} x_1 + 2x_2 &= 0 \\ 3x_2 &= 0, \end{aligned}$$

from which you can easily see that $x_1 = 0 = x_2$, so $NS(A) = \{\mathbf{0}\}$.

(b) Let $B = \begin{pmatrix} 1 & 2 \\ 4 & 8 \end{pmatrix}$; then if $B\mathbf{x} = \mathbf{0}$ then, letting $\mathbf{x} = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$, we have

$$\begin{aligned} x_1 + 2x_2 &= 0 \\ 4x_1 + 8x_2 &= 0. \end{aligned}$$

But the second row is a multiple of the first, so we get infinitely many solutions. Let's write these down: if we let $x_2 = \lambda$ then $x_1 = -2\lambda$, so we get

$$NS(B) = \left\{ \mathbf{x} : \mathbf{x} = \lambda \begin{pmatrix} -2 \\ 1 \end{pmatrix}, \lambda \in \mathbf{R} \right\}.$$

The set of all the points in $NS(B)$ is a straight line through the origin in the direction of the vector $\begin{pmatrix} -2 \\ 1 \end{pmatrix}$.

(c) If $C = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ is the zero matrix, $C\mathbf{x} = \mathbf{0}$ for every vector $\mathbf{x} \in \mathbf{R}^2$. Thus $NS(C) = \mathbf{R}^2$.

Notice that in all the three examples considered above, each nullspace is indeed a vector subspace. We prove now that this is always the case.

Theorem 2.6.3 *If A is an $m \times n$ real matrix, then $NS(A)$ is a subspace of $\mathbf{R}^n$; if A is complex, it is a subspace of $\mathbf{C}^n$.*

Proof: As we've seen already, $NS(A)$ is certainly a subset of $\mathbf{R}^n$. Now we prove that it is a subspace; to do that we have to prove it non-empty, closed under addition and under scalar multiplication. Since $A\mathbf{0} = \mathbf{0}$ we already have $\mathbf{0}$ a member of $NS(A)$, so it's non-empty. For closure under addition, take two members, say $\mathbf{u}$ and $\mathbf{v}$, of $NS(A)$; this means that $A\mathbf{u} = \mathbf{0}$ and $A\mathbf{v} = \mathbf{0}$. Our job is to check that $\mathbf{u} + \mathbf{v} \in NS(A)$. That means we have to check that $A(\mathbf{u} + \mathbf{v}) = \mathbf{0}$. This is quite easy:

$$A(\mathbf{u} + \mathbf{v}) = A\mathbf{u} + A\mathbf{v} \text{ (why?) } = \mathbf{0} + \mathbf{0} = \mathbf{0}$$

which is what we wanted. To check closure under scalar multiplication we must show that $\lambda\mathbf{u} \in NS(A)$ whenever $\mathbf{u} \in NS(A)$ and $\lambda \in \mathbf{R}$. This is also easy:

$$A(\lambda\mathbf{u}) = \lambda A\mathbf{u} \text{ (Why?) } = \lambda\mathbf{0} = \mathbf{0}$$

as we wanted. ■

We mention here that actually calculating $NS(A)$ for any A always amounts to solving a homogeneous system of linear equations. As we have noted before, homogeneous system always has at least one solution. It is clear from what we have just proved that the set of solutions of a homogeneous system of equations does form a vector space. For this reason, it is sometimes referred to as the **solution space** of the system of equations. (The solutions of a general (non-homogeneous) system of linear equations, however, need not form a vector space.)

We now look at finding bases for the nullspace of a matrix. The following example illustrates the important ideas.

Example 2.6.4 Let

$$A = \begin{pmatrix} 0 & 0 & 1 & -4 \\ 2 & -4 & -1 & -2 \\ 4 & -8 & 0 & -12 \end{pmatrix}.$$

We want to find a basis for $NS(A)$, the nullspace of A.

We first reduce A to row echelon form U. Since A and U are row equivalent, the two equations $A\mathbf{x} = \mathbf{0}$ and $U\mathbf{x} = \mathbf{0}$ have the same solutions (Lemma 1.6.10). This means, in terms of nullspaces, that $NS(A) = NS(U)$. In this case,

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

Now we are looking for all vectors (x_1, x_2, x_3, x_4) such that

$$\begin{aligned} 2x_1 - 4x_2 - x_3 - 2x_4 &= 0 \\ x_3 - 4x_4 &= 0 \end{aligned}$$

Using the usual method for solving this, we move the free variables to the right hand side to obtain

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

We have two free variables: x_2 and x_4. Let $x_2 = s$ and $x_4 = t$ where $s, t \in \mathbf{R}$. Substituting and using backsubstitution,we get

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

We can rewrite this as

$$\begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} = s \begin{pmatrix} 2 \\ 1 \\ 0 \\ 0 \end{pmatrix} + t \begin{pmatrix} 3 \\ 0 \\ 4 \\ 1 \end{pmatrix}.$$

This tells us that $NS(U)$ and hence $NS(A)$ is spanned by the vectors

$$\begin{pmatrix} 2 \\ 1 \\ 0 \\ 0 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 3 \\ 0 \\ 4 \\ 1 \end{pmatrix}.$$

Since these two vectors are linearly independent (why?) they form a basis for $NS(A)$. From this we also get $\dim NS(A) = 2$.

The above example illustrates a useful fact:

Theorem 2.6.5 *If U is a matrix in row echelon form, then* $\dim NS(U)$ *is the number of free variables in the equation* $U\mathbf{x} = \mathbf{0}$.

Proof: We omit the details of the proof. The last example shows the basic idea of the proof. It is clear that the vectors obtained by the method in the example spans the null space. To see that they will always be linearly independent, note that there is a vector corresponding to each free variable, and that this vector has a 1 in the position corresponding to the free variable, while all the other vectors will have a 0 in this position. ∎

Definition 2.6.6 *We call* $\dim(NS(A))$ *the* ***nullity*** *of A.*

According to Theorem 2.6.5, the nullity of matrix A is just the number of free variables of the matrix equation $U\mathbf{x} = \mathbf{0}$, where U is the matrix obtained by row reducing A to row echelon form.

We now turn to the other important subspaces associated with any $m \times n$ matrix A. Let

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

The vectors

$$\begin{aligned} \mathbf{r}_1 &= (a_{11}, a_{12}, \dots, a_{1n}) \\ \mathbf{r}_2 &= (a_{21}, a_{22}, \dots, a_{2n}) \\ \vdots & \qquad \vdots \\ \mathbf{r}_m &= (a_{m1}, a_{m2}, \dots, a_{mn}) \end{aligned}$$

in $\mathbf{R}^n$ are called the **row vectors** of A. The vectors

$$\mathbf{c}_1 = \begin{pmatrix} a_{11} \\ a_{21} \\ \vdots \\ a_{m1} \end{pmatrix}, \quad \mathbf{c}_2 = \begin{pmatrix} a_{12} \\ a_{22} \\ \vdots \\ a_{m2} \end{pmatrix}, \dots, \mathbf{c}_n = \begin{pmatrix} a_{1n} \\ a_{2n} \\ \vdots \\ a_{mn} \end{pmatrix}$$

in $\mathbf{R}^m$ are called the **column vectors** of A.

Example 2.6.7 Let $A = \begin{pmatrix} 2 & 1 & 7 \\ 1 & 3 & 5 \end{pmatrix}$.
The row vectors of A are $\quad (2, 1, 7) \quad$ and $\quad (1, 3, 5)$. They are members of $\mathbf{R}^3$.
The column vectors of A are

$$\begin{pmatrix} 2 \\ 1 \end{pmatrix}, \quad \begin{pmatrix} 1 \\ 3 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 7 \\ 5 \end{pmatrix}.$$

They are members of $\mathbf{R}^2$.

Definition 2.6.8 *Let A be an $m \times n$ matrix.*

1. *The subspace of $\mathbf{R}^n$ spanned by the row vectors of A is called the **row space** of A and is denoted by $RS(A)$.*

2. *The subspace of $\mathbf{R}^m$ spanned by the column vectors of A is called the **column space** of A and is denoted by $CS(A)$.*

Example 2.6.9 Let A be as in Example 2.6.7. The row vectors are linearly independent (why?) and span $RS(A)$ so form a basis for $RS(A)$. We thus have that $\dim RS(A) = 2$. The column vectors, however, cannot all be linearly independent (why?), and $\dim CS(A) \leq 2$. On the other hand, any two of the column vectors are linearly independent, so form a basis for $CS(A)$. Thus $\dim CS(A) = 2$. In fact, it is clear that $CS(A) = \mathbf{R}^2$.

For larger matrices it will not always be so easy to find $RS(A)$ and $CS(A)$. Recall, however, that if we reduce a matrix A to its row echelon form U, then $NS(A) = NS(U)$. Fortunately the same happens to be true for the row spaces: $RS(A) = RS(U)$. However, the same is **not** true for $CS(A)$. To prove the result for $RS(A)$ we need a lemma which says that performing an elementary row operation on a matrix results in a matrix with exactly the same row space.

Lemma 2.6.10 *Elementary row operations do not change the row space of a matrix.*

Proof: We consider the case where a matrix B has been obtained from matrix A by performing one elementary row operation. Suppose B has been obtained from A by a row interchange; then it's clear that the row space of B is identical with that of A. The other possibilities are that A has been obtained from B by multiplying a row of A by a non-zero constant, or, that a multiple of one row of A has been added to another. In either case, the rows of B are linear combinations of rows of A, and so linear combinations of the rows of B are in turn still linear combinations of the rows of A. Thus, in any case, we have proved that $RS(B) \subseteq RS(A)$. The reverse inclusion is easy: if B can be obtained from A by an elementary row operation, then A can be obtained by B by an elementary row operation, which means (using the same argument) that $RS(A) \subseteq RS(B)$ and the proof is finished. ∎

The proof of the main result is now easy. One gets the row echelon form of a matrix by performing a series of elementary row operations. At each step the row space is unchanged, so the row space of the row echelon form is identical with the row space of the original matrix. We have proved:

Theorem 2.6.11 *Let U be a row echelon form of A. Then $RS(U) = RS(A)$.*

Example 2.6.12 Let $A = \begin{pmatrix} 1 & -2 & 0 & 0 & 3 \\ 2 & -5 & -3 & -2 & 6 \\ 0 & 5 & 15 & 10 & 0 \\ 2 & 6 & 18 & 8 & 6 \end{pmatrix}$. We find a basis for $RS(A)$.

Gaussian elimination reduces A to

$$U = \begin{pmatrix} 1 & -2 & 0 & 0 & 3 \\ 0 & -1 & -3 & -2 & 0 \\ 0 & 0 & -12 & -12 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

A basis for $RS(U)$ (and hence $RS(A)$) is

$$\{(1, -2, 0, 0, 3), (0, -1, -3, -2, 0), (0, 0, -12, -12, 0)\}$$

and $\dim RS(A) = 3$. You may be wondering why these three vectors are linearly independent; the reason is that the "staircase" pattern of the row echelon matrix forces the non-zero rows to be linearly independent. You can check this.

The last statement in the above example is worth highlighting:

Theorem 2.6.13 *The non-zero rows of a matrix U in row echelon form are linearly independent and form a basis for $RS(U)$. Thus the dimension of $RS(U)$ is exactly the number of non-zero rows in U or, just as well, the number of pivots of U, or equally well, the number of dependent variables in the equation $U\mathbf{x} = \mathbf{0}$.*

Example 2.6.14 Suppose we are asked to find a basis for the subspace of $\mathbf{R}^5$ spanned by the set of vectors

$$\left\{ \begin{pmatrix} 1 \\ -2 \\ 0 \\ 0 \\ 3 \end{pmatrix}, \begin{pmatrix} 2 \\ -5 \\ -3 \\ -2 \\ 6 \end{pmatrix}, \begin{pmatrix} 0 \\ 5 \\ 15 \\ 10 \\ 0 \end{pmatrix}, \begin{pmatrix} 2 \\ 6 \\ 18 \\ 8 \\ 6 \end{pmatrix} \right\}.$$

These vectors are actually just the rows of the matrix of Example 2.6.12, but written as column vectors. Thus the answer is the same as for Example 2.6.12, namely a basis is

$$\left\{ \begin{pmatrix} 1 \\ -2 \\ 0 \\ 0 \\ 3 \end{pmatrix}, \begin{pmatrix} 0 \\ -1 \\ -3 \\ -2 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ -12 \\ -12 \\ 0 \end{pmatrix} \right\}.$$

The point of this example is to give you a simple strategy for actually computing bases for spans using matrices. Knowledge of the notion of a row space has helped with a practical problem.

We will spend some time now analysing the column space of a matrix. We should point out immediately that performing elementary row operations on a matrix **does** change the column space. However, there is still some tie up between the column spaces of two matrices that are row equivalent and this turns out to be useful. First we give you an example to show that the column space of a matrix and the column space of its row echelon form are different.

Example 2.6.15 Let $A = \begin{pmatrix} 1 & 3 \\ 2 & 6 \end{pmatrix}$. The second column is a multiple of the first, so the single vector $\begin{pmatrix} 1 \\ 2 \end{pmatrix}$ is a basis for the column space, which is a line through the origin in the direction of the vector $\begin{pmatrix} 1 \\ 2 \end{pmatrix}$. Now if we row reduce A we get the matrix $U = \begin{pmatrix} 1 & 3 \\ 0 & 0 \end{pmatrix}$ which has as a basis for its column space the vector $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$. This means that the two column spaces are certainly different.

You might notice that in both matrices in the above example the relationships of linear dependence amongst the columns remain the same. In both cases we see that the second column is a multiple of the first and that the first columns can be taken for a basis for the column space of each matrix. This is not a coincidence, as the next theorem will show.

Theorem 2.6.16 *If A and B are row equivalent matrices, then:*
(a) The column vectors of A are linearly independent iff the column vectors of B are linearly independent.
(b) A given set of column vectors of A forms a basis for $CS(A)$ iff the corresponding columns of B form a basis for $CS(B)$.

Proof: (a) If we want to check that the columns of A are linearly independent, we are trying to show that $A\mathbf{x} = \mathbf{0}$ has no non-trivial solution. (Why?) But we know that, if A is row equivalent to B, then the solutions for $A\mathbf{x} = \mathbf{0}$ are exactly the same as those of $B\mathbf{x} = \mathbf{0}$. Thus if $A\mathbf{x} = \mathbf{0}$ has only the trivial solution, the same is true of $B\mathbf{x} = \mathbf{0}$.

(b) In fact, (a) holds for any subset of the columns of A and the corresponding subset of columns of B. This is enough to prove the result. In the exercises we give you hints to enable you to give a complete proof of this . ■

The way we use this theorem is as follows: suppose A has row echelon form U. Then the columns of U which contain the pivots are linearly independent and form a basis for the column space of U. (Why? If you can't see this, look at any matrix in row echelon form and try to see why.) Thus the **corresponding** columns of A form a basis for the column space of A. We should point out that this means that, although $CS(A) \neq CS(U)$ we do have that $\dim CS(A) = \dim CS(U)$.

Example 2.6.17 We find a basis for the column space of the matrix

$$A = \begin{pmatrix} 1 & -2 & 0 & 0 & 3 \\ 2 & -5 & -3 & -2 & 6 \\ 0 & 5 & 15 & 10 & 0 \\ 2 & 6 & 18 & 8 & 6 \end{pmatrix}.$$

This is the matrix of Example 2.6.12; its row echelon form is

$$U = \begin{pmatrix} 1 & -2 & 0 & 0 & 3 \\ 0 & -1 & -3 & -2 & 0 \\ 0 & 0 & -12 & -12 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

The first three columns contain the pivots, so they form a basis for $CS(U)$. The corresponding columns of A are $\begin{pmatrix} 1 \\ 2 \\ 0 \\ 2 \end{pmatrix}$, $\begin{pmatrix} -2 \\ -5 \\ 5 \\ 6 \end{pmatrix}$ and $\begin{pmatrix} 0 \\ -3 \\ 15 \\ 18 \end{pmatrix}$, so these three vectors form a basis for $CS(A)$.

We can use our new found ability to find column spaces in a new way to find special bases for row spaces:

Example 2.6.18 We show that we can find a basis for the row space of

$$A = \begin{pmatrix} 1 & -2 & 0 & 0 & 3 \\ 2 & -5 & -3 & -2 & 6 \\ 0 & 5 & 15 & 10 & 0 \\ 2 & 6 & 18 & 8 & 6 \end{pmatrix}$$

consisting entirely of rows of A.

Our first method for finding a basis for A was to row reduce A to its echelon form and then take rows containing pivots as our basis. These basis vectors would usually not be rows of the original matrix A though. To get a basis consisting of rows of A we work with the columns of A^T! The row echelon form of A^T is

$$W = \begin{pmatrix} 1 & 2 & 0 & 2 \\ 0 & -1 & 5 & 10 \\ 0 & 0 & 0 & -12 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

Columns 1,2 and 4 contain pivots, thus columns 1,2 and 4 form a basis for the column space of A^T, so rows 1, 2 and 4 of A form a basis for $RS(A)$.

We finish off this section with some very important results. Fortunately we have already done most of the work neede to prove them.

Theorem 2.6.19 *Let A be any $m \times n$ matrix. Then*

$$\dim CS(A) = \dim RS(A).$$

Proof: Let U be the row echelon form of A. The dimension of $RS(A)$ is the number of rows containing pivots of U, but the dimension of $CS(A)$ is the number of columns containing pivots of U. These are of course the same! ■

The dimension of $RS(A)$ or $CS(A)$ is an important feature of any matrix A. It gets a name:

Definition 2.6.20 *Let A be a matrix. The dimension of $RS(A)$ or $CS(A)$ is called the* ***rank*** *of A and is denoted by Rank(A).*

Theorem 2.6.21 *Let A be a matrix. Then Rank(A) = Rank(A^T).*

Proof: $\text{Rank}(A) = \dim RS(A) = \dim CS(A^T) = \text{Rank}(A^T)$. ■

The dimension of the nullspace of a matrix A is also an important feature of A; recall that it also has a name:

Definition 2.6.22 *Let A be a matrix. The dimension of $NS(A)$ is called the* ***nullity*** *of A and is denoted by Nullity(A).*

The following theorem is very important: it is sometimes called the **dimension theorem** for matrices.

Theorem 2.6.23 *If A is a matrix with n columns then*

$$\mathit{Rank}(A) + \mathit{Nullity}(A) = n.$$

Proof: Let U be the row echelon form of A. We know that $NS(A) = NS(U)$ and $RS(A) = RS(U)$ and that $\dim NS(U)$ is the number of free variables in the equation $U\mathbf{x} = \mathbf{0}$. We also know that $\dim RS(U)$ is the number of pivots in U, which is the same as the number of dependent variables in the equation $U\mathbf{x} = \mathbf{0}$. But the total number of variables in $U\mathbf{x} = \mathbf{0}$ is just the number of columns of U. This is the same as the number of columns of A, which is n. Thus we have:

$$\begin{aligned} n = \dim NS(U) + \dim RS(U) &= \dim NS(A) + \dim RS(A) \\ &= \text{Nullity}(A) + \text{Rank}(A) \end{aligned}$$

as required. ■

The following example makes use of all of the preceding results.

Example 2.6.24 Let us find bases for and dimensions of $RS(A), CS(A)$ and $NS(A)$, where

$$A = \begin{pmatrix} 3 & 2 & -4 & 1 & 5 \\ 6 & 4 & -7 & 3 & 1 \\ -3 & -2 & 6 & 1 & 2 \\ 9 & 6 & -11 & 4 & 6 \end{pmatrix}.$$

The key to this all is, of course, to find the row echelon form, U, of A; it is

$$U = \begin{pmatrix} 3 & 2 & -4 & 1 & 5 \\ 0 & 0 & 1 & 1 & -9 \\ 0 & 0 & 0 & 0 & 25 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

We thus have 3 pivots, so the rank of A is 3. We know that then the nullity of A must be 2.

The non-zero rows of U must be a basis for $RS(A)$ so it has basis

$$\{(3, 2, -4, 1, 5), (0, 0, 1, 1, -9), (0, 0, 0, 0, 25)\}.$$

The columns of U which contain pivots are columns 1,3 and 5. Thus the correrpond-ing columns of A form a basis for $CS(A)$ and they are:

$$\begin{pmatrix} 3 \\ 6 \\ -3 \\ 9 \end{pmatrix}, \begin{pmatrix} -4 \\ -7 \\ 6 \\ -11 \end{pmatrix}, \begin{pmatrix} 5 \\ 1 \\ 2 \\ 6 \end{pmatrix}.$$

Finally, to find a basis for $NS(A)$, we solve $U\mathbf{x} = \mathbf{0}$. Writing out the equations we get

$$\begin{aligned} 3x_1 + 2x_2 - 4x_3 + x_4 + 5x_5 &= 0 \\ x_3 + x_4 - 9x_5 &= 0 \\ 25x_5 &= 0 \end{aligned}$$

The free variables are x_2 and x_4; let $x_2 = s$ and $x_4 = t$, where $s, t \in \mathbf{R}$. A bit of calculation shows that for $\mathbf{x} \in NS(A)$ we have:

$$\mathbf{x} = s \begin{pmatrix} -\frac{2}{3} \\ 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} + t \begin{pmatrix} -\frac{5}{3} \\ 0 \\ -1 \\ 1 \\ 0 \end{pmatrix}.$$

This tells us that the nullity of A is 2 (which we already knew) and that a basis for $NS(A)$ is

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

We finish off this section by adding to our stock of results which tell us when a square matrix A is invertible.

Theorem 2.6.25 *Let A be an $n \times n$ matrix. Then the following are equivalent:*

(a) A is invertible.

(b) $NS(A) = \{\mathbf{0}\}$.

(c) $\dim NS(A) = 0$ (The nullity of A is 0).

(d) Rank$(A) = n$.

(e) $\dim CS(A) = n$.

(f) $\dim RS(A) = n$.

(g) The columns of A are linearly independent.

(h) The rows of A are linearly independent.

(i) $\det(A) \neq 0$.

Proof: We know that (a) is equivalent to (b). The others follow from all the results we've just proved about rank and nullity, and Theorem 2.4.13. ∎

Important Note: This theorem holds for square matrices only.

Summary:

We looked at important subspaces associated with any matrix A.

- The *nullspace* of A is the set of all vectors $\mathbf{x}$ such that $A\mathbf{x} = \mathbf{0}$. Its dimension is called the *nullity* of A. We saw that the nullity of a matrix A is just the number of free variables in the associated system of equations $A\mathbf{x} = \mathbf{0}$, which is the number of variables which do not correspond to pivots in the row echelon form of A.
- The *row space* of A is the span of the rows of A and the *column space* of A is the span of the columns of A. The dimension of both these subspaces is exactly the number of pivots in the row echelon form of A. This number is called the *rank* of A.

- In a matrix with n columns we saw, because of the above two observations about rank and nullity, that the sum of the rank and nullity is exactly n.

Exercises

1. In this exercise, you prove Theorem 2.6.16(b):
   If A and B are row equivalent matrices, then a given set of column vectors of A forms a basis for $CS(A)$ iff the corresponding columns of B form a basis for $CS(B)$.

   Suppose that the first p columns of A form a basis for $CS(A)$. (Why can we assume this?) Let B be row equivalent to A.
   (a) Deduce (from Theorem 2.6.16(a)) that the first p columns of B are independent.
   (b) It remains to show that the first p columns of B span $CS(B)$. Do this as follows:
   Take an arbitrary column of A (the kth say) and express it as a linear combination of the first p columns of A. Now apply each type of elementary row operation to A, in turn, and check that the kth column of the resulting matrix (C, say) is a linear combination of the first p columns of C. Why does that finish the proof?

2. Find the rank and nullity of these matrices. If the calculations look too tedious, try to use OCTAVE or the Linear Algebra Toolkit. (Check that your answers don't contradict Theorem 2.6.23.)

   (a) $A = \begin{pmatrix} 1 & -1 & 3 \\ 5 & -4 & -4 \\ 7 & -6 & 2 \end{pmatrix}$

   (b) $B = \begin{pmatrix} 1 & 4 & 5 & 2 \\ 2 & 1 & 3 & 0 \\ -1 & 3 & 2 & 2 \end{pmatrix}$

   (c) $C = \begin{pmatrix} 1 & -3 & 2 & 2 & 1 \\ 0 & 3 & 6 & 0 & -3 \\ 2 & -3 & -2 & 4 & 4 \\ 3 & -6 & 0 & 6 & 5 \\ -2 & 9 & 2 & -4 & -5 \end{pmatrix}$

3. In each case below, find the largest possible value for the rank of A and the smallest possible value for the nullity of A.

   (a) A is 4×4

(b) A is 3×5

(c) A is 5×3.

4. (a) Suppose that A is a 3×3 matrix whose null space is a line through the origin in $\mathbf{R}^3$. Can the row or column space of A also be a line through the origin? Explain.

   (b) Suppose that A is a 3×3 matrix whose column space is a plane through the origin in $\mathbf{R}^3$. Can the null space be a plane through the origin? Can the row space be such a plane? Explain.

5. Show that an $n \times n$ matrix is invertible iff its rank is n.

6. Let A be an $m \times n$ matrix and B be an $n \times p$ matrix.

   (a) Show that the null space of B is a subspace of the null space of AB.

   (b) Deduce that $\text{rank}(AB) \leq \text{rank}(B)$.

   (c) Show that the column space of AB is a subspace of the column space of A. (Hint: Use Theorem 2.3.7)

   (d) Deduce that $\text{rank}(AB) \leq \text{rank}(A)$.

7. For the purposes of this question, let us define a "chessboard" matrix to be a square matrix (a_{ij}) such that

$$a_{ij} = 1 \text{ if } i + j \text{ is even} \qquad \text{and} \qquad a_{ij} = 0 \text{ if } i + j \text{ is odd} .$$

   Find the rank and nullity of the 3×3, 4×4 and $n \times n$ chessboard matrices.

8. (a) Show that, if A is a 3×5 matrix, then its column vectors are linearly dependent.

   (b) Show that, if A is a 5×3 matrix, then its row vectors are linearly dependent.

9. For $A = \begin{pmatrix} 1 & 2 & -1 \\ 1 & 9 & -1 \\ -3 & 8 & 3 \\ -2 & 3 & 2 \end{pmatrix}$, find a basis for the row space of A

   (a) consisting of vectors that are *not* row vectors of A;

   (b) consisting of vectors that *are* row vectors of A.

10. For $B = \begin{pmatrix} 1 & -2 & 7 & 0 \\ 1 & -1 & 4 & 0 \\ 3 & 2 & -3 & 5 \\ 2 & 1 & -1 & 3 \end{pmatrix}$, find a basis for the column space of B:

(a) consisting of vectors that are *not* column vectors of B,

(b) consisting of vectors that *are* column vectors of B.

Revision Exercises

1. (a) Let $S = \{ax^2 + bx + c \,:\, a + b = c \text{ and } a, b, c \in \mathbf{R}\}$. Is S a subspace of P_2 or not? Give a proof for your answer.

   (b) Let $M_{2\times2}(\mathbf{R})$ be the vector space of all 2×2 matrices with real entries, with the usual addition and scalar multiplication of matrices.
   Let $S = \{A \in M_{2\times2}(\mathbf{R}) \,:\, A^2 = \mathbf{0}\}$. (Here $\mathbf{0}$ is the 2×2 zero matrix.) Is S a subspace of $M_{2\times2}(\mathbf{R})$ or not? Give a proof for your answer.

2. Answer the following questions, giving reasons for your answers.

   (a) Is $S = \{x^2 + x,\ x + 1,\ x^2 + 1\}$ a basis for P_2?

   (b) Is $B = \left\{ \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix} \right\}$ a basis for $\mathbf{R}^3$?

   (c) Is $C = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 8 & 0 \\ 0 & 9 \end{pmatrix} \right\}$ a basis for span(C)?

3. Let U and W be vector subspaces of the vector space V.

   (a) Prove that $U + W = \{\mathbf{u} + \mathbf{w} : \mathbf{u} \in U, \mathbf{w} \in W\}$ is a vector subspace of V.

   (b) Prove that $U + W$ is the smallest subspace of V containing $U \cup W$.

   (c) Prove that if $V = U + W$ and $U \cap W = \{\mathbf{0}\}$, then for every $\mathbf{v} \in V$ there are unique elements $\mathbf{u} \in U, \mathbf{w} \in W$ such that $\mathbf{v} = \mathbf{u} + \mathbf{w}$. In this case we write $V = U \oplus W$.

   (d) Let V be the vector space of all continuous functions $f : [0, 1] \to \mathbf{R}$, with its usual addition and scalar multiplication, and U be the subspace $\{f \in V : f(1) = 0\}$. Find a subspace W of V such that $V = U \oplus W$.

4. Prove or disprove each of the following. State clearly whether the statement is true or false.

   (a) If B is an $m \times n$ matrix and $B\mathbf{x} = \mathbf{b}$ has infinitely many solutions for each $\mathbf{b} \in \mathbf{R}^m$, then the columns of B are dependent.

   (b) If B is an $m \times n$ matrix and the columns of B are dependent, then $B\mathbf{x} = \mathbf{b}$ has infinitely many solutions for each $\mathbf{b} \in \mathbf{R}^m$.

   (c) Every subspace of a finite-dimensional vector space is finite-dimensional.

Chapter 3

Linear Transformations

3.1 What are Linear Transformations?

In the previous chapter we studied vector spaces, an example of an abstract mathematical structure. In this chapter we look at functions between vector spaces. Rather than studying functions between vector spaces in general, we concentrate on those functions that may be regarded as the "right" or "appropriate" functions for the context. Vector spaces come equipped with two operations: those of scalar multiplication and addition. The functions we consider are those that are well-behaved with respect to these operations. As we'll see shortly, this means that these functions, which we'll call *linear functions* or *linear transformations*, "preserve" these operations. We'll spell out exactly what this means shortly.

The idea of a function that is well-behaved with respect to an operation is not an entirely new one. The crucial concept in calculus, one could argue, is that of a limit. It therefore makes sense to work with functions that are well-behaved when it comes to limits. Continuous functions are just such functions, since it is true that if a function $f : \mathbf{R} \to \mathbf{R}$ is continuous at a point $a \in \mathbf{R}$, then

$$\lim_{x \to a} f(x) = f(a) = f(\lim_{x \to a} x).$$

We sometimes say that continuous functions "preserve limits". Continuous functions are convenient to use when you want to work with limits, and we therefore regard them as the "right" functions in this context.

Before we say exactly what a *linear* function is, it is worth pointing out that we'll be working with functions in what may perhaps be a slightly unfamiliar context. So far you have worked mostly with real-valued functions defined on $\mathbf{R}$ or a subset of

$\mathbf{R}$, or in the case of functions of two variables, defined on $\mathbf{R}^2$ or a subset of $\mathbf{R}^2$. In Section 1.4 we did briefly look at the idea that we could regard an $m \times n$ matrix as a function from $\mathbf{R}^n$ to $\mathbf{R}^m$. In this chapter we look at an even more general context: functions from one vector space to another. In Appendix C the general notion of a function is discussed in some detail. For our purposes in this section it is enough to think intuitively (if somewhat imprecisely) of a function as consisting of two sets and a rule. The rule assigns to every element of the first set (which we call the *domain* of the function) a *unique* element of the second set (which we call the *codomain* of the function). If we use the letter f for the function and X and Y respectively for its domain and codomain, then we write $f : X \to Y$ to indicate that f is a function from X to Y. The terms *transformation* and *map* are often used to mean the same thing as *function*.

The functions (or transformations as we'll mostly call them) we'll be looking at in this chapter are special in that their domains and codomains are always vector spaces, and that they preserve the vector space structure, as explained above.

With all these preliminaries out of the way, we can at last give the precise definition:

Definition 3.1.1 *Let T be a function from a vector space V to a vector space W. We say that T is a* ***linear transformation*** *if it satisfies two conditions:*

(a) $T(\mathbf{u} + \mathbf{v}) = T(\mathbf{u}) + T(\mathbf{v})$ *for* ***every*** $\mathbf{u}, \mathbf{v} \in V$.

(b) $T(\lambda \mathbf{u}) = \lambda T(\mathbf{u})$ *for* ***every*** *scalar* λ *and vector* $\mathbf{u} \in V$.

You may be surprised about two things in this definition: the fact that we call a function a *transformation*, and the fact that we use a capital letter (T in this case) to denote a function, rather than the more traditional small letters like f and g. There is no good reason for this other than that it seems a firmly established tradition to use capital letters like S, T for these linear functions, and to call them linear transformations (or even *linear maps*). You may as well get used to this tradition right from the start!

Have you seen linear transformations before? The answer is that every matrix you've seen was nothing but a linear transformation in disguise. The next example illustrates this fact.

Example 3.1.2 Let $A = \begin{pmatrix} 1 & 2 & 3 \\ 1 & -3 & 2 \end{pmatrix}$. For $\mathbf{x} = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} \in \mathbf{R}^3$, let

$$T(\mathbf{x}) = A \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} x_1 + 2x_2 + 3x_3 \\ x_1 - 3x_2 + 2x_3 \end{pmatrix}.$$

Since A acts on a 3-vector and maps it to a 2-vector, this defines T as a function from the vector space $\mathbf{R}^3$ to the vector space $\mathbf{R}^2$. Is T a linear transformation? To answer this we need to recall a few facts about matrix multiplication. If A is an $m \times n$ matrix, B and C are $n \times p$ matrices and λ is a scalar,

- $A(B + C) = AB + AC$
- $A(\lambda B) = \lambda(AB)$

These two facts apply in particular when B and C are n-vectors ($n \times 1$ matrices). In our example $m = 2$ and $n = 3$. The two facts listed tell us that T defined as above using the matrix A is indeed a linear transformation:

(a) $T(\mathbf{x} + \mathbf{y}) = A(\mathbf{x} + \mathbf{y}) = A(\mathbf{x}) + A(\mathbf{y}) = T(\mathbf{x}) + T(\mathbf{y})$

(b) $T(\lambda\mathbf{x}) = A(\lambda\mathbf{x}) = \lambda A(\mathbf{x}) = \lambda T(\mathbf{x})$.

You can see that in the above example there was nothing particularly important about which matrix A we were looking at; so what we said there applies to any matrix. Explicitly:

Theorem 3.1.3 *If A is an $m \times n$ matrix, then the function $T : \mathbf{R}^n \to \mathbf{R}^m$ defined by*

$$T(\mathbf{u}) = A\mathbf{u} \quad \textit{for every } \mathbf{u} \in \mathbf{R}^n$$

is a linear transformation.

You probably already came across the idea that one could think of a matrix as a special type of function in first year mathematics. We now know what is special about them: they are *linear* functions. In particular, you saw there that the geometrical operations of reflection, projection and rotation in the plane (i.e. in $\mathbf{R}^2$) can be represented by using matrices. We now know that they are in fact linear transformations.

Example 3.1.4 The matrices

$$\mathrm{Rot}_\theta = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} \qquad \mathrm{Proj}_x = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \qquad \mathrm{Ref}_x = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

represent respectively a rotation through an angle of θ counter-clockwise about the origin, a projection onto the x -axis and a reflection in the x-axis. Make sure that you can write down the matrices representing a projection onto the y-axis and a reflection in the y-axis as well.

When you hear "linear function", you probably immediately think of a function f of the form $f(x) = mx + c$. How does this fit in with the definition you've just seen?

Example 3.1.5 We may in fact think of $\mathbf{R}$ itself as a real vector space. In this case the vectors and scalars are the same: real numbers. Let $f : \mathbf{R} \to \mathbf{R}$ be defined by $f(x) = mx$, where m is a non-zero real number. Is f linear? For $x, y \in \mathbf{R}$ (we regard these as vectors) and $\lambda \in \mathbf{R}$ (this is a scalar) we have

$$\begin{aligned} f(x+y) &= m(x+y) = mx + my = f(x) + f(y) \quad \text{and} \\ f(\lambda x) &= m(\lambda x) = \lambda(mx) = \lambda f(x). \end{aligned}$$

Hence f is a linear transformation. Let us now look at the function $g : \mathbf{R} \to \mathbf{R}$ defined by $g(x) = mx + c$, where both m and c are non-zero real numbers. Then for $x, y \in \mathbf{R}$,

$$\begin{aligned} g(x+y) &= m(x+y) + c = mx + my + c \quad \text{but} \\ g(x) + g(y) &= mx + c + my + c = mx + my + 2c \neq g(x+y). \end{aligned}$$

This is enough to show that g is not a linear transformation. It is rather unfortunate that these functions are also called linear (probably since there graphs are lines); strictly speaking we should call them *affine functions*.

Example 3.1.6 We give another example of an important geometrical transformation, namely *translation*. Let the function $T : \mathbf{R}^2 \to \mathbf{R}^2$ be defined by

$$T\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} + \begin{pmatrix} 3 \\ -2 \end{pmatrix} = \begin{pmatrix} x_1 + 3 \\ x_2 - 2 \end{pmatrix}, \qquad \text{for } \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \in \mathbf{R}^2.$$

This means that T moves (or *translates*) a point in $\mathbf{R}^2$ 3 units in the direction of the positive x axis and 2 units in the direction of the negative y axis. We check to see whether T is linear. For $\lambda \in \mathbf{R}$,

$$T\left(\lambda\begin{pmatrix} x_1 \\ x_2 \end{pmatrix}\right) = T\left(\begin{pmatrix} \lambda x_1 \\ \lambda x_2 \end{pmatrix}\right) = \begin{pmatrix} \lambda x_1 + 3 \\ \lambda x_2 - 2 \end{pmatrix},$$

whereas

$$\lambda T\left(\left(\begin{array}{c} x_1 \\ x_2 \end{array}\right)\right) = \lambda \left(\begin{array}{c} x_1+3 \\ x_2-2 \end{array}\right) = \left(\begin{array}{c} \lambda x_1+3\lambda \\ \lambda x_2-2\lambda \end{array}\right).$$

These two expressions are not equal if for example $x_1 = x_2 = 1$ and $\lambda = 2$. Therefore T is **not** a linear transformation.

We will look now at some other functions, some of which are linear and some not. You should eventually develop the ability to check routinely whether some given function is linear or not, so work through these examples carefully.

Example 3.1.7 Let $T : P_1 \to P_2$ be defined by

$$T(ax+b) = x(ax+b), \text{ for } ax+b \in P_1.$$

To check whether T is linear, we must take two arbitrary members of P_1 and apply T to their sum:

$$T\left((ax+b)+(cx+d)\right) = T\left((a+c)x+(b+d)\right) = x\left((a+c)x+(b+d)\right).$$

On the other hand

$$T(ax+b)+T(cx+d) = x(ax+b)+x(cx+d) = x\left((a+c)x+(b+d)\right),$$

so we easily see that $T\left((ax+b)+(cx+d)\right) = T(ax+b)+T(cx+d)$ as required. We must now check the second condition; let λ be an arbitrary scalar. Then

$$T\left((\lambda(ax+b)\right) = T(\lambda ax+\lambda b) = x(\lambda ax+\lambda b) = \lambda x(ax+b) = \lambda T(ax+b)$$

so the second condition also holds. Thus T is indeed linear.

Example 3.1.8 Let $T : P_1 \to P_2$ be defined by

$$T(ax+b) = x(ax+b)+x^2 \quad \text{for } ax+b \in P_1.$$

We check again whether T is linear.

Let $ax+b, cx+d \in P_1$ then

$$\begin{aligned} T((ax+b)+(cx+d)) &= T((a+c)x+(b+d)) \\ &= x((a+c)x+(b+d))+x^2 \\ &= (a+c+1)x^2+(b+d)x, \end{aligned}$$

while

$$\begin{aligned} T(ax+b)+T(cx+d) &= x(ax+b)+x^2+x(cx+d)+x^2 \\ &= (a+c+2)x^2+(b+d)x \\ &\neq T((ax+b)+(cx+d)). \end{aligned}$$

This shows that T does not satisfy the first condition for it to be a linear transformation, and therefore T is not linear.

Note that if we want to show that a function $T : V \to W$ is not linear, it is enough to either

- find two vectors $\mathbf{u}, \mathbf{v} \in V$ such that $T(\mathbf{u}+\mathbf{v}) \neq T(\mathbf{u}) + T(\mathbf{v})$ or
- find a vector $\mathbf{u} \in W$ and a scalar λ such that $T(\lambda \mathbf{u}) \neq \lambda T(\mathbf{u})$.

For example, in the above example it would have been enough to show that $T(x+2x) \neq T(x)+T(2x)$; from this we can deduce immediately that T is not linear.

On the other hand, if you want to prove that T is linear, you have to do it as in the earlier examples. A few examples in which the conditions for linearity is satisfied are **not enough** to prove linearity.

Example 3.1.9 Let W be the vector space of all functions from $\mathbf{R}$ to $\mathbf{R}$, and let V be the subspace of all differentiable functions from $\mathbf{R} \to \mathbf{R}$. Let $T : V \to W$ be defined by $T(f) = f'$ (where as usual f' denotes the derivative of f). We check that T is linear.

Take two arbitrary members of V, say f and g. Then

$$T(f+g) = (f+g)' = f' + g' = T(f) + T(g)$$

so the first condition holds. Now let λ be an arbitrary scalar (real number, in this case) and consider

$$T(\lambda f) = (\lambda f)' = \lambda f' = \lambda T(f).$$

Thus the second condition holds and T is linear.

(Incidentally, why did we not write $T : V \to V$ in the statement of the example?)

We collect together in one theorem a few useful facts about linear transformations in general. Recall that subtraction can be defined in a vector space by putting $\mathbf{u} - \mathbf{v} = \mathbf{u} + (-\mathbf{v})$, where $-\mathbf{v}$ stands for the negative, or additive inverse, of $\mathbf{v}$.

Theorem 3.1.10 *Let $T : V \to W$ be a linear transformation, $\mathbf{u}, \mathbf{v}, \mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_n \in V$ and $\lambda_1, \lambda_2, \ldots, \lambda_n$ scalars. Then*

(a) $T(\lambda_1\mathbf{u}_1 + \lambda_2\mathbf{u}_2 + \ldots + \lambda_n\mathbf{u}_n) = \lambda_1 T(\mathbf{u}_1) + \lambda_2 T(\mathbf{u}_2) + \ldots + \lambda_n T(\mathbf{u}_n)$;

(b) $T(\mathbf{0}) = \mathbf{0}$;

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

Proof: (a) We give the proof in the case $n = 2$:

$$T(\lambda_1\mathbf{u}_1 + \lambda_2\mathbf{u}_2) = T(\lambda_1\mathbf{u}_1) + T(\lambda_2\mathbf{u}_2) = \lambda_1 T(\mathbf{u}_1) + \lambda_2 T(\mathbf{u}_2).$$

For the general case you have to run through these steps repeatedly. A proper proof would use induction. See if you can write out such a proof!
(b) We use a trick: obviously $\mathbf{0} + \mathbf{0} = \mathbf{0}$. Applying T to both sides of this equation we get

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

But using the first condition of linearity we must now have

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

Adding the negative of $T(\mathbf{0})$ to both sides gives

$$T(\mathbf{0}) = \mathbf{0}$$

as required. We should just mention that in the statement $T(\mathbf{0}) = \mathbf{0}$ the two zero-vectors on either side of the equation may be different. The one on the left is the zero vector in V whereas the zero vector on the right is the one in W. This shouldn't cause any confusion though.
(c) This is an (easy) exercise. Remember that $\mathbf{u} - \mathbf{v} = \mathbf{u} + (-\mathbf{v}) = \mathbf{u} + (-1)\mathbf{v}$. ■

The second property above can sometimes be used to show that a function between vector spaces is **not** linear.

Corollary 3.1.11 *Let V and W be linear spaces and $F : V \to W$ a function. If $F(\mathbf{0}) \neq \mathbf{0}$, then F is not a linear transformation.*

Example 3.1.12 Let $F : \mathbf{R}^2 \to \mathbf{R}^2$ be defined by

$$F\left(\begin{pmatrix} x_1 \\ x_2 \end{pmatrix}\right) = \begin{pmatrix} x_1 + 1 \\ x_2 - 2 \end{pmatrix}.$$

Then

$$F\left(\begin{pmatrix} 0 \\ 0 \end{pmatrix}\right) = \begin{pmatrix} 1 \\ -2 \end{pmatrix} \neq \begin{pmatrix} 0 \\ 0 \end{pmatrix},$$

and therefore F is not a linear transformation.

Warning: If $F : V \to W$ is a function between vector spaces and $F(\mathbf{0}) = \mathbf{0}$, then F need **not** be a linear transformation. Find an example to illustrate this yourself!

Usually when you define a function, you are obliged to give a rule which specifies "what the function does" to every member of its domain. Sometimes you can get away with providing far less information. For example, if you know that the function you are dealing with is a quadratic function, specifying function values at three distinct points is enough to determine the whole function. Linear functions are a bit like this: you only have to know what values they have on a *basis* for the domain space to specify them completely. We show why this is the case.

Suppose V is an n-dimensional vector space, $T : V \to W$ is a linear transformation and $B = \{\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_n\}$ is a basis for V. Let $\mathbf{u} \in V$. Since B is a basis for V we know that there are scalars $\lambda_1, \lambda_2, \ldots, \lambda_n$ such that

$$\mathbf{u} = \lambda_1\mathbf{u}_1 + \lambda_2\mathbf{u}_2 + \ldots + \lambda_n\mathbf{u}_n.$$

Then, by the last theorem,

$$T(\mathbf{u}) = T(\lambda_1\mathbf{u}_1 + \lambda_2\mathbf{u}_2 + \ldots + \lambda_n\mathbf{u}_n) = \lambda_1 T(\mathbf{u}_1) + \lambda_2 T(\mathbf{u}_2) + \ldots + \lambda_n T(\mathbf{u}_n).$$

This shows that as long as we know $\{T(\mathbf{u}_1), T(\mathbf{u}_2), \ldots, T(\mathbf{u}_n)\}$, we can find $T(\mathbf{u})$ for any $\mathbf{u} \in V$. We simply write $\mathbf{u}$ as a linear combination of the basis vectors in B, and then write down a linear combination of the vectors $T(\mathbf{u}_1), T(\mathbf{u}_2), \ldots, T(\mathbf{u}_n)$ using the same scalars we used to write $\mathbf{u}$ as a linear combination of basis vectors. This shows that once we know what a linear transformation "does" to the vectors in a basis for its domain, we know what it "does" to *every* vector in its domain.

We illustrate this fact in the next example.

Example 3.1.13 Suppose that T is known to be linear from P_1 to P_2, and that $T(x+1) = x^2 - 1$ and $T(x-1) = x^2 + x$. We show that this is enough information to find $T(3x+7)$, and, more generally, $T(ax+b)$.

To begin you should verify that $\{x-1, x+1\}$ is a basis for P_1. Then

$$3x + 7 = -2(x-1) + 5(x+1),$$

so

$$T(3x+7) = -2T(x-1) + 5T(x+1) = -2(x^2+x) + 5(x^2-1) = 3x^2 - 2x - 5.$$

More generally, we note that $ax + b = \dfrac{a-b}{2}(x-1) + \dfrac{a+b}{2}(x+1)$, so

$$T(ax+b) \quad = \quad T\left[\left(\frac{a-b}{2}\right)(x-1) + \left(\frac{a+b}{2}\right)(x+1)\right]$$

$$\begin{aligned} &= \frac{a-b}{2}T(x-1)+\frac{a+b}{2}T(x+1) \\ &= \frac{a-b}{2}(x^2+x)+\frac{a+b}{2}(x^2-1) \\ &= ax^2+\frac{a-b}{2}x-\frac{a+b}{2}. \end{aligned}$$

Summary:

In this section we introduced the important notion of a **linear transformation** between vector spaces.

- A linear transformation between two vector spaces is a function which *preserves* the operations of addition and scalar multiplication, in the sense that the image of a sum is the sum of the images, and the image of a scalar multiple of a vector is the same scalar multiple of the image of the vector.
- Every matrix may be regarded as a linear transformation.
- Once the effect of a linear transformation on every vector of a basis for its domain is known, its effect on every vector in the domain can be found.

Exercises

1. Let V and W be vector spaces.
   (a) Show that the function $O : V \to W$ defined by $O(\mathbf{v}) = \mathbf{0}$ for every $\mathbf{v} \in V$ is a linear transformation. (It is called the **zero linear transformation**.)
   (b) Let $V = W$ Show that $I : V \to V$ defined by $I\mathbf{v} = \mathbf{v}$ for every $\mathbf{v} \in V$ is a linear transformation. (It is called the **identity transformation**.)
   (c) Give an example to show that a function $F : V \to W$ with the property that $F(\mathbf{0}) = \mathbf{0}$ need not be a linear ransformation.
2. Which of the following are linear transformations? Justify your answers.
   (a) $T : \mathbf{R}^3 \to \mathbf{R}^2$, given by $T(a, b, c) = (2a - b + c, b - 4c)$.
   (b) $T : P_2 \to P_2$, where $T(a_0 + a_1x + a_2x^2) = a_0 + a_1(x + 1) + a_2(x + 1)^2$.
   (c) $L : P_2 \to P_2$, where $L(a_0 + a_1x + a_2x^2) = (a_0 + 1) + (a_1 + 1)x + (a_2 + 1)x^2$.
   (d) $T : M_{n\times n}(\mathbf{R}) \to \mathbf{R}$, where $M_{n\times n}(\mathbf{R})$ consists of all $n \times n$ matrices, and $T(A) = \sum_{i=1}^{n} a_{ii}$ for $A = (a_{ij})$.
   (This number, $\sum_{i=1}^{n} a_{ii}$, is called the **trace** of the matrix A.)

(e) $F : M_{n\times n}(\mathbf{R}) \to \mathbf{R}$, where
$F(A) = a_{11} \cdot a_{22} \cdot a_{33} \cdot \ldots \cdot a_{nn}$ for $A = (a_{ij})$.

(f) $T : \mathbf{R}^2 \to \mathbf{R}^2$ given by $T(x, y) = (x + y^2, \sqrt[3]{y})$.

(g) $S : \mathbf{R}^2 \to \mathbf{R}^4$ given by $T(x, y) = (3y, 4x, 0, x - y)$.

3. (a) Given a suitable function $f(t)$ we can define a function $\mathcal{L}f(s)$ by

$$\mathcal{L}f(s) = \int_0^\infty e^{-st} f(t)\, dt.$$

We call $\mathcal{L}f$ the Laplace Transform of f. Show that the operation $T(f) = \mathcal{L}f$ is a linear transformation. (You may assume that the set of "suitable functions" is a vector space with the usual addition and scalar multiplication for functions.)

(b) Given a suitable function $f(t)$ we can define a function $\mathcal{F}f(w)$ by

$$\mathcal{F}f(w) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^\infty e^{-iwt} f(t)\, dt.$$

We call $\mathcal{F}f$ the Fourier Transform of f. Show that the operation $T(f) = \mathcal{F}f$ is a linear transformation. (You may again assume that the set of "suitable functions" is a vector space with the usual addition and scalar multiplication for functions.)

4. Let $T : \mathbf{R}^3 \to \mathbf{R}^3$ be a linear transformation. Show that T maps a line in $\mathbf{R}^3$ to a point or a line in $\mathbf{R}^3$. [**Hint:** use the vector equation of a line.]
Show that T does something similar to planes in $\mathbf{R}^3$.

3.2 The kernel and range of a linear transformation

We saw in the last section that any matrix can be viewed as a linear transformation and in Chapter 2 we looked at some fundamental subspaces associated with any matrix. In this section we'll look at two fundamental subspaces associated with any linear transformation, and you will notice that the results look very similar to results that we obtained for the fundamental subspaces of a matrix.

We look first at the so-called *kernel* of a linear transformation, which is the analogue of the nullspace of a matrix.

Definition 3.2.1 *Let $T : V \to W$ be a linear transformation. The **kernel** of T is the subset of V consisting of all vectors $\mathbf{u}$ such that $T(\mathbf{u}) = \mathbf{0}$. It is often denoted by* $\ker(T)$. *In brief:*

$$ker(T) = \{\mathbf{u} \in V : T(\mathbf{u}) = \mathbf{0}\}$$

Example 3.2.2 Let A be an $m \times n$ matrix and T be the associated linear transformation from $\mathbf{R}^n \to \mathbf{R}^m$ (i.e. $T(\mathbf{u}) = A\mathbf{u}$ for $\mathbf{u} \in \mathbf{R}^n$). Then

$$\ker(T) = \{\mathbf{u} \in \mathbf{R}^n : T(\mathbf{u}) = \mathbf{0}\} = \{\mathbf{u} \in \mathbf{R}^n : A\mathbf{u} = \mathbf{0}\} = \mathrm{NS}(A),$$

where $\mathrm{NS}(A)$ is the null space of A.

We have already seen that the null space of a matrix is a subspace, and we now know that the kernel of a linear transformation defined by a matrix equals the null space of the matrix. This shows that for such linear transformations the kernel is a subspace. Is the kernel always a subspace, for any kind of linear transformation? The next theorem says that this is indeed the case. Not surprisingly, the proof is reminiscent of the same result for a null space of a matrix.

Theorem 3.2.3 *If V and W are vector spaces and $T : V \to W$ is a linear transformation, then $ker(T)$ is a subspace of V.*

Proof: Firstly, $\ker(T)$ is non-empty, since $\mathbf{0} \in \ker(T)$. (Why?) Now let $\mathbf{u}$ and $\mathbf{v}$ be arbitrary elements of $\ker(T)$. We must show that $\mathbf{u} + \mathbf{v} \in \ker(T)$. We know that, since T is linear

$$T(\mathbf{u} + \mathbf{v}) = T(\mathbf{u}) + T(\mathbf{v}) = \mathbf{0} + \mathbf{0} = \mathbf{0},$$

so $\mathbf{u} + \mathbf{v}$ is a member of $\ker(T)$, as desired. Also, if λ is an arbitrary scalar, we must show that $\lambda\mathbf{u} \in \ker(T)$. But $T(\lambda\mathbf{u}) = \lambda T(\mathbf{u}) = \lambda\mathbf{0} = \mathbf{0}$ as required. Thus $\ker(T)$ is indeed a subspace of V. ■

Example 3.2.4 Let $T : \mathbf{R}^3 \to \mathbf{R}^2$ be the transformation defined by

$$T(x, y, z) = (x + y, x - z).$$

It is straightforward to prove that T is linear; this is left as an exercise for you. We look at its kernel:

$$\begin{aligned} \ker(T) &= \{(x, y, z) : T(x, y, z) = (0, 0)\} \\ &= \{(x, y, z) : (x + y, x - z) = (0, 0)\} \\ &= \{(x, y, z) : x = t, y = -t, z = t, \text{ for } t \in \mathbf{R}\} \\ &= \{\lambda(1, -1, 1) : \lambda \in \mathbf{R}\} \end{aligned}$$

(Fill in the details missing from the above calculations.) Thus it is clear that a basis for $\ker(T)$ is $\{(1,-1,1)\}$ and $\dim\ker(T) = 1$.

There is a link between the first two examples. If we put $A = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & -1 \end{pmatrix}$, then for the T of the last example we have $T(\mathbf{u}) = A\mathbf{u}$ for all $\mathbf{u} \in \mathbf{R}^3$, and so $\mathrm{NS}(A) = \ker(T)$.

We recall that a function f is *one-to-one* (also written 1-1) or *injective* if

$$f(x) = f(y) \Rightarrow x = y.$$

An alternative way of saying this is that f is one-to-one if

$$x \neq y \Rightarrow f(x) \neq f(y);$$

a one-to-one function therefore sends different “inputs” to different “outputs”. (For more on one-to-one functions, see Appendix C.2.) Linear transformations are functions, so we can certainly ask when a linear transformation will be one-to-one. We show that there is a really nice tie-up between the kernel of a linear transformation and this question.

Theorem 3.2.5 *If V and W are vector spaces and $T : V \to W$ is a linear transformation, then T is one-to-one if and only if $\ker(T) = \{\mathbf{0}\}$.*

Proof: Let T be 1-1 and let $\mathbf{v} \in \ker(T)$. We must show that $\mathbf{v} = \mathbf{0}$. But $T(\mathbf{v}) = \mathbf{0} = T(\mathbf{0})$. (Why?) So, since T is 1-1, $\mathbf{v} = \mathbf{0}$ as we wanted to show.
For the converse, assume that $\ker(T) = \{\mathbf{0}\}$ and that $T(\mathbf{u}) = T(\mathbf{v})$. We must show that $\mathbf{u} = \mathbf{v}$. Consider the following:

$$T(\mathbf{u} - \mathbf{v}) = T(\mathbf{u}) - T(\mathbf{v}) = \mathbf{0},$$

so $\mathbf{u} - \mathbf{v} \in \ker(T)$, so $\mathbf{u} - \mathbf{v} = \mathbf{0}$, which gives us $\mathbf{u} = \mathbf{v}$ as we wanted. ■

Example 3.2.6 Let $T : \mathbf{R}^2 \to \mathbf{R}^3$ be defined by

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

Then it is easy to check that T is linear.(Do this!) To find $\ker(T)$, we note that $(x, y) \in \ker(T)$ means that $(x, x + y, x - y) = (0, 0, 0)$. But this clearly tells us that $x = 0 = y$. (Compare coordinates.) Thus $\ker(T) = \{(0, 0)\}$. We can now see in two ways that T is 1-1. Either use Theorem 3.2.5, which tells us immediately that T is 1-1, or assume $T(x, y) = T(a, b)$ and show that $x = a$ and $y = b$. We'll leave this last bit for you.

Recall that if f is a function from a set X to a set Y, we define the *range* of f as the subset $\mathrm{ran}(f) = \{f(x) : x \in X\}$ of Y. In general $\mathrm{ran}(f)$ will be a proper subset of the codomain Y. If $\mathrm{ran}(f) = Y$, we say that the function f is *onto*, or *surjective* (see Appendix C.2).

Having looked at the analogue of the null space for a matrix, we are now going to look at the analogue of the column space. Before we do that, we recall that we saw in Theorem 2.3.4 that if A is an $m \times n$ matrix then $\mathbf{v} \in \mathbf{R}^m$ is a linear combination of the columns of A (equivalently, is in the column space $CS(A)$ of A) if and only if there is a vector $\mathbf{u} \in \mathbf{R}^n$ such that $\mathbf{v} = A\mathbf{u}$. This result allows us to interpret the column space of a matrix as the range of a function.

Now let $T : \mathbf{R}^n \to \mathbf{R}^m$ be the linear transformation associated with the matrix A, i.e. $T(\mathbf{u}) = A\mathbf{u}$. The range of the function T is $\{T(\mathbf{u}) : \mathbf{u} \in \mathbf{R}^n\} = \{A\mathbf{u} : \mathbf{u} \in \mathbf{R}^n\}$, and it follows from the above remark that this is equal to $CS(A)$. It follows that a linear transformation $T : \mathbf{R}^n \to \mathbf{R}^m$ defined by an $m \times n$ matrix A will be surjective if and only if the column space $CS(A)$ of A equals $\mathbf{R}^m$.

We are now going to look at the range of an arbitrary linear transformation T, and it should come as no surprise that this range is indeed a vector space.

Definition 3.2.7 *Let V and W be vector spaces and $T : V \to W$ be a linear transformation. The* ***range*** *of T is the set ran$(T) = \{T(\mathbf{v}) : \mathbf{v} \in V\}$.*
(This is sometimes also written as $T^{\to}(V)$, or simply $T(V)$.) The transformation T is onto, or surjective, if ran$(T) = W$.

Theorem 3.2.8 *If V and W are vector spaces and $T : V \to W$ is a linear transformation, then ran(T) is a subspace of W.*

Proof: Firstly, $\mathrm{ran}(T)$ is non-empty since $T(\mathbf{0}) = \mathbf{0}$ is a member of $\mathrm{ran}(T)$. Secondly, if $\mathbf{w}_1$ and $\mathbf{w}_2$ are members of $\mathrm{ran}(T)$ then $\mathbf{w}_1 = T(\mathbf{v}_1)$ and $\mathbf{w}_2 = T(\mathbf{v}_2)$ for vectors $\mathbf{v}_1, \mathbf{v}_2 \in V$. Then

$$\mathbf{w}_1 + \mathbf{w}_2 = T(\mathbf{v}_1) + T(\mathbf{v}_2) = T(\mathbf{v}_1 + \mathbf{v}_2),$$

and $\mathbf{v}_1 + \mathbf{v}_2 \in V$, so $\mathbf{w}_1 + \mathbf{w}_2 \in \mathrm{ran}(T)$ as we wanted. Lastly, if λ is a scalar and $\mathbf{w} \in \mathrm{ran}(T)$ then $\mathbf{w} = T(\mathbf{v})$ for some $\mathbf{v} \in V$ and then

$$\lambda\mathbf{w} = \lambda T(\mathbf{v}) = T(\lambda\mathbf{v})$$

so $\lambda\mathbf{w} \in \mathrm{ran}(T)$ as needed. ■

Example 3.2.9 Let $T : \mathbf{R}^3 \to \mathbf{R}^3$ be defined by

$$T\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 1 \\ 1 & 1 & 2 \\ 2 & 1 & 3 \end{pmatrix}\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix}.$$

We first find a basis for and the dimension of $\text{ran}(T)$. Let A be the 3×3 matrix used to define T, i.e.

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

Then $\text{ran}(T) = CS(A)$. So the vectors $\begin{pmatrix} 1 \\ 1 \\ 2 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix}$ and $\begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix}$ span the range of T. However, they do not form a basis for $\text{ran}(T)$ because the last vector is the sum of the first two. The first two, however, are linearly independent (why?) so they form a basis for $\text{ran}(T)$. The dimension of $\text{ran}(T)$ is thus 2.
Recall that T will be onto if $\text{ran}(T) = \mathbf{R}^3$. But the range of T has dimension 2, whereas $\mathbf{R}^3$ has dimension 3. Thus T cannot be onto. The kernel of T is given by

$$\ker(T) = \left\{\begin{pmatrix} x \\ y \\ z \end{pmatrix} : \begin{pmatrix} 1 & 0 & 1 \\ 1 & 1 & 2 \\ 2 & 1 & 3 \end{pmatrix}\begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}\right\}.$$

Solving the resulting system of equations gives

$$\ker(T) = \{\lambda\begin{pmatrix} -1 \\ -1 \\ 1 \end{pmatrix} : \lambda \in \mathbf{R}\}.$$

We see that the kernel of T is not just $\{\mathbf{0}\}$, so T is not 1-1. In fact, dim(ker (T)=1. We notice that $\dim\ker(T) + \dim\text{ran}(T) = 1 + 2 = 3$. This is not surprising, since $\ker(T)$ and $\text{ran}(T)$ are the analogues of the null space and column space of a matrix; in this case they are the null space and column space of the given matrix A.

We gave a simple example here, and you could probably see the answers more or less by inspection. In a more complicated example you would have to use all the tools we've already developed to find the required answers.

A function is called *bijective* if it is both injective and surjective. It is shown in Appendix C.2 that a function $f : X \to Y$ is bijective if and only if it has an inverse $f^{-1} : Y \to X$. If we specialise this result to linear transformations, a natural question arises: is the inverse of a bijective linear transformation also linear?

Proposition 3.2.10 *Let V and W be vector spaces and $T : V \to W$ be a bijective linear transformation. Then the inverse T^{-1} of T is a linear map from W to V, and is also a bijection.*

Proof: We leave the proof of this result as an exercise. ∎

Definition 3.2.11 *Let V and W be vector spaces. A bijective linear transformation $T : V \to W$ is called a* **linear isomorphism**.

Example 3.2.12 The linear transformation $T : P_1 \to \mathbf{R}^2$ defined by

$$T(ax+b) = \begin{pmatrix} a \\ b \end{pmatrix}$$

is a linear isomorphism; it is easy to check that it is both injective and surjective.

A linear map preserves addition and multiplication. A linear isomorphism has an inverse which does the same. If we have a linear isomorphism between two (different) vector spaces, there is therefore justification for saying that the two vector spaces are really the same, as vector spaces. The isomorphism "relabels" the elements of the first vector space to give us elements of the second vector space, and the relabeling is done in a way that is consistent with the way addition and scalar multiplication are defined in the two spaces.

Definition 3.2.13 *We say that two vector spaces V and W are* **isomorphic** *if there exists a linear isomorphism $T : V \to W$.*

Example 3.2.14 It follows from Example 3.2.12 that P_1 and $\mathbf{R}^2$ are isomorphic vector spaces.

We end this section with a useful result for calculating bases for ranges.

Theorem 3.2.15 *Let V and W be vector spaces and $T : V \to W$ be a linear transformation and let B be a basis for V. Then $T(B) = \{T(\mathbf{b}) : \mathbf{b} \in B\}$ spans ran(T).*

Proof: Let $B = \{\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_k\}$ and $\mathbf{w}$ be an arbitrary member of ran(T); then $\mathbf{w} = T(\mathbf{v})$ for some $\mathbf{v} \in V$. Since B is a basis for V, we must have

$$\mathbf{v} = \lambda_1 \mathbf{b}_1 + \lambda_2 \mathbf{b}_2 + \ldots + \lambda_k \mathbf{b}_k$$

where the λ_i's are scalars. But then we have

$$\mathbf{w} = T(\mathbf{v}) = \lambda_1 T(\mathbf{b}_1) + \lambda_2 T(\mathbf{b}_2) + \ldots + \lambda_k T(\mathbf{b}_k)$$

which shows that the vector $\mathbf{w}$ is in the span of $T(B)$ as we claimed. ■

Remarks: (a) Note that although $T(B)$ spans $\mathrm{ran}(T)$, it need not be a basis for $\mathrm{ran}(T)$, since it need not be a linearly independent set.
(b) The method of the above proof could be used to prove that a linear transformation *preserves linear dependence*. By that, we mean that if a set $\{\mathbf{u}_1, \mathbf{u}_2, \ldots \mathbf{u}_k\}$ is a linearly dependent set in V, then it follows that $\{T(\mathbf{u}_1), T(\mathbf{u}_2), \ldots, T(\mathbf{u}_k)\}$ will be a linearly dependent set in W. We ask you to check the details in the exercises. On the other hand, the next example shows that a linear mapping need not preserve linear independence. By that we mean that, even if a set $\{\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_k\}$ is linearly independent in V, it need not be the case that $\{T(\mathbf{u}_1), T(\mathbf{u}_2), \ldots, T(\mathbf{u}_k)\}$ is linearly independent in W. This is why we couldn't claim that $T(B)$ in the above theorem forms a basis for $\mathrm{ran}(T)$.

Example 3.2.16 Let $A = \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}$ and $T : \mathbf{R}^2 \to \mathbf{R}^2$ be the associated linear map. Then we have

$$T\begin{pmatrix} 1 \\ 0 \end{pmatrix} = A\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \end{pmatrix} \quad \text{but} \quad T\begin{pmatrix} 0 \\ 1 \end{pmatrix} = A\begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 2 \\ 2 \end{pmatrix}.$$

Thus, although $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$ and $\begin{pmatrix} 0 \\ 1 \end{pmatrix}$ are linearly independent, their images under T are not.

Example 3.2.17 Let $T : P_3 \to P_3$ be defined by

$$T(ax^3 + bx^2 + cx + d) = (a - b)x^3 + (c - d)x.$$

Let us try to find a basis for $\mathrm{ran}(T)$.

We can start by finding some vectors that span $\mathrm{ran}(T)$ and then eliminate enough of them to get a linearly independent set. By the last theorem we should examine the image under T of some basis for P_3. We know that $\{1, x, x^2, x^3\}$ is a basis for P_3. For the images of these basis vectors we get

$$T(1) = -x,\ T(x) = x,\ T(x^2) = -x^3,\ T(x^3) = x^3.$$

The set $\{x^3, -x^3, x, -x\}$ therefore spans $\mathrm{ran}(T)$. However, we can see that we can eliminate both $-x^3$ and $-x$ without affecting the set spanned. Thus a basis for $\mathrm{ran}(T)$ is $\{x^3, x\}$, since these two vectors are linearly independent.

Summary:

In this section we looked at two important subspaces associated with a linear map.

- If $T : V \to W$ is a linear transformation the set $\{\mathbf{v} \in V : T(\mathbf{v}) = \mathbf{0}\}$ is called the *kernel* of T, and it is a subspace of V. It is the analogue of the null space of a matrix.
- For any linear transformation T, T is 1-1 iff $\ker(T) = \{\mathbf{0}\}$.
- The *range* of a linear transformation is the set $\{T(\mathbf{v}) : \mathbf{v} \in V\}$ and is a subspace of W. It is the analogue of the column space of a matrix.
- If B is a basis for V and $T : V \to W$ is linear, then $T(B)$ spans the range of T.

Exercises

1. The linear transformations $T : \mathbf{R}^2 \to \mathbf{R}^2$ and $S : \mathbf{R}^2 \to \mathbf{R}^3$ are defined by

$$T\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x+y \\ 3x-y \end{pmatrix} \text{ and } S\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x-y \\ 0 \\ x-y \end{pmatrix}.$$

   (a) Find $\ker(T)$ and $\ker(S)$. (b) Find $\operatorname{ran}(T)$ and $\operatorname{ran}(S)$.

2. Let $T : P_2 \to P_3$ be the linear transformation defined by $T(p(x)) = xp(x)$. Which of the following are in $\ker(T)$?
   (a) x^2 (b) 0 (c) $1 + x$.

3. Let $T : P_2 \to P_3$ be the linear transformation in the previous question. Which of the following are in $\operatorname{ran}(T)$?
   (a) $x + x^2$ (b) $1 + x$ (c) $3 - x^2$.

4. Let V be any vector space, and let $T : V \to V$ be defined by $T(\mathbf{v}) = 3\mathbf{v}$.
   (a) What is the kernel of T? (b) What is the range of T?

5. Let $L : \mathbf{R}^4 \to \mathbf{R}^3$ be defined by

$$L\begin{pmatrix} x \\ y \\ z \\ w \end{pmatrix} = \begin{pmatrix} x+y \\ y-z \\ z-w \end{pmatrix}$$

   (a) Is L onto? (b) Find the dimension of $\ker L$.

6. Let $L : \mathbf{R}^4 \to \mathbf{R}^4$ be defined by

$$L\begin{pmatrix} x \\ y \\ z \\ w \end{pmatrix} = \begin{pmatrix} 1 & 2 & 1 & 3 \\ 2 & 1 & -1 & 2 \\ 1 & 0 & 0 & -1 \\ 4 & 1 & -1 & 0 \end{pmatrix}\begin{pmatrix} x \\ y \\ z \\ w \end{pmatrix}$$

(a) Find a basis for $\ker L$. (b) Find a basis for range L.

7. Let $L : P_2 \to P_2$ be the linear transformation defined by

$$L(ax^2 + bx + c) = (a + c)x^2 + (b + c)x.$$

(a) Is $x^2 - t - 1$ in $\ker L$? (b) Is $x^2 + x - 1$ in $\ker L$?
(c) Is $2x^2 - x$ in range L? (d) Is $x^2 - x + 2$ in range L?
(e) Find a basis for $\ker L$. (f) Find a basis for range L.

8. Let V and W be the vector spaces of polynomial functions of degree at most 3 and 2 respectively, and let $T : P_3 \to P_2$ be the linear transformation defined by

$$T(p) = p',$$

where p' denotes the derivative of the polynomial function p.

(a) Find a basis for $\ker T$. (b) Find a basis for range T.

9. Let V be the vector space of all polynomial functions of degree at most 1, and let $T : P_1 \to \mathbf{R}^2$ be the function defined by the formula

$$T(p) = (p(0), p(1))$$

(a) Find $T(p)$ if $p(x) = 1 - 2x$.

(b) Show that T is a linear transformation.

(c) Show that T is one-to-one.

(d) Is T a linear isomorphism?

10. For each of the linear mappings $\mathrm{Rot}_x, \mathrm{Proj}_x$ and Ref_x defined in Example 3.1.4 determine whether it is a linear isomorphism.

11. Let $T : V \to W$ be a linear transformation, and let $S = \{\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_n\}$ be a subset of V. Show that if S is linearly dependent, so is the set $T(S) = \{T(\mathbf{u}_1), T(\mathbf{u}_2), \ldots, T(\mathbf{u}_n)\}$. (We say that linear transformations **preserve linear dependence**.)

12. Prove : If $\{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n\}$ is a basis for V and $\mathbf{w}_1, \mathbf{w}_2, \ldots, \mathbf{w}_n$ are vectors in W (not necessarily distinct), then there exists a linear transformation $T : V \to W$ such that $T(\mathbf{v}_1) = \mathbf{w}_1, T(\mathbf{v}_2) = \mathbf{w}_2, \ldots, T(\mathbf{v}_n) = \mathbf{w}_n$.
    [**Hint:** How would you define $T(\lambda_1\mathbf{v}_1 + \lambda_2\mathbf{v}_2 + \ldots + \lambda_n\mathbf{v}_n)$?]

13. Prove Proposition 3.2.10.

Remember that you can use the Linear Algebra Toolkit (or OCTAVE) to check your answers, or do the calculations if they get too tedious.

3.3 The matrix of a linear transformation

We've already seen in the last section that a matrix can be viewed as a linear transformation. In this section, we will see that there is a (partial) converse, that is, many linear transformations can actually be viewed as matrices, if you use a bit of ingenuity.

Recall that if B is a (finite) basis for a space, one can talk about the **coordinate vector** of a given vector with respect to the basis. You should refresh your memory about this idea by looking at the Section 2.5, where we discussed the notions of basis and dimension. We will use the idea of coordinate vectors to show that one can represent many linear transformations as matrices.

We'll first introduce some notation to make the statements of the ideas clearer.

Definition 3.3.1 *Let V be an n-dimensional vector space with basis B, and let $\mathbf{v}$ be a member of V. We will write $[\mathbf{v}]_B$ for the coordinate vector of $\mathbf{v}$ with respect to the (ordered) basis B.*

Example 3.3.2 Let $B_1 = \{(1,0),(0,1)\}$ and let $B_2 = \{(1,1),(1,-1)\}$. These are both bases for $\mathbf{R}^2$. We find $[(3,5)]_{B_1}$ and $[(3,5)]_{B_2}$.

We have $(3,5) = 3(1,0) + 5(0,1)$, so $[(3,5)]_{B_1}$ is again just $(3,5)$.
However we have $(3,5) = 4(1,1) - 1(1,-1)$, so $[(3,5)]_{B_2} = (4,-1)$.

We list now some useful facts about coordinate vectors.

Theorem 3.3.3 *Let B be a basis for a vector space V, $\mathbf{v}_1, \mathbf{v}_2 \in V$ and λ a scalar. Then*

(a) $[\mathbf{v}_1 + \mathbf{v}_2]_B = [\mathbf{v}_1]_B + [\mathbf{v}_2]_B$ *and*

(b) $[\lambda \mathbf{v}_1]_B = \lambda [\mathbf{v}_1]_B$.

Proof: Exercise. You will need to use the fact that every vector in a vector space has a unique representation in terms of the basis vectors. If you can write down two representations for the vector $\mathbf{v}_1 + \mathbf{v}_2$ for example, they must be equal. ■

Corollary 3.3.4 *Let B be a basis for an n-dimensional real vector space V. Then the function $F : V \to \mathbf{R}^n$ defined by $F(\mathbf{v}) = [\mathbf{v}]_B$, for $\mathbf{v} \in V$, is a linear isomorphism. Hence every n-dimensional real vector space is isomorphic to the vector space $\mathbf{R}^n$. If V is a complex vector space, the same result holds, with $\mathbf{R}^n$ replaced by $\mathbf{C}^n$.*

Proof: Theorem 3.3.3 shows that F is linear. It is an easy exercise, using the fact that B is a basis, to show that F is bijective. ■

We are ready for the main result now.

Theorem 3.3.5 *Let $T : V \to W$ be a linear transformation, and suppose that V is an n-dimensional and that W is an m-dimensional vector space. Also, let $B_V = \{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n\}$ be a basis for V and $B_W = \{\mathbf{w}_1, \mathbf{w}_2, \ldots, \mathbf{w}_m\}$ be a basis for W. Then form the matrix A whose j^{th} column is the coordinate vector $[T(\mathbf{v}_j)]_{B_W}$. A is an $m \times n$ matrix with the following property:*

$$A[\mathbf{v}]_{B_V} = [T(\mathbf{v})]_{B_W} \text{ for any vector } \mathbf{v} \in V.$$

Moreover, A is the only matrix with this property.

We say that A is the **matrix which represents T with respect to the two bases B_V and B_W**. We denote A by ${}_{B_W}[T]_{B_V}$. In the case where $V = W$, i.e. $T : V \to V$, and where we use the same basis, B, for V both times, we call A the "matrix which represents T with respect to B."

If the functions $F_V : V \to \mathbf{R}^n$ and $F_W : W \to \mathbf{R}^m$ are defined by $F_V(\mathbf{v}) = [\mathbf{v}]_{B_V}$ and $F_W(\mathbf{w}) = [\mathbf{w}]_{B_W}$, then it follows from Corollary 3.3.4 that they are both isomorphisms and the equation in Theorem 3.3.5 above becomes

$$A(F_V(\mathbf{v})) = F_W(T(\mathbf{v})).$$

The diagram below gives one a way of picturing this equation.

$$\begin{tikzcd} V \arrow[r, "T"] \arrow[d, "F_V"'] & W \arrow[d, "F_W"] \\ \mathbf{R}^n \arrow[r, "A"] & \mathbf{R}^m \end{tikzcd}$$

Before we actually do the proof, it might be as well to apply the statement of the theorem to a few cases to see it at work; the proof of the theorem will not look so daunting then.

Example 3.3.6 Let $T : P_1 \to P_2$ be the linear transformation defined by

$$T(p(x)) = x(p(x)).$$

Let's find the matrix which represents T with respect to the bases $B_1 = \{1, x\}$ and $B_2 = \{1, x, x^2\}$ for P_1 and P_2 respectively.

According to the statement of the theorem, we must calculate $[T(1)]_{B_2}$ and $[T(x)]_{B_2}$.

$$[T(1)]_{B_2} = [x]_{B_2} = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} \quad \text{and} \quad [T(x)]_{B_2} = [x^2]_{B_2} = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}.$$

Thus the theorem says that we should set

$$A = \begin{pmatrix} 0 & 0 \\ 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Let's see if it really works. We'll calculate $[T(ax+b)]_{S_2}$ and $A[ax+b]_{S_1}$ separately; the theorem says that we should get the same answer.

Firstly $T(ax+b) = x(ax+b) = ax^2 + bx$, so

$$[T(ax+b)]_{B_2} = \begin{pmatrix} 0 \\ b \\ a \end{pmatrix}.$$

Secondly,

$$A[ax+b]_{B_1} = \begin{pmatrix} 0 & 0 \\ 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} b \\ a \end{pmatrix} = \begin{pmatrix} 0 \\ b \\ a \end{pmatrix}$$

as we hoped.

Proof: (of Theorem 3.3.5) Suppose that $[\mathbf{v}]_{B_V} = (\lambda_1, \lambda_2, \ldots, \lambda_n)$. Then $\mathbf{v} = \lambda_1\mathbf{v}_1 + \lambda_2\mathbf{v}_2 + \ldots + \lambda_n\mathbf{v}_n$.
Using the linearity of T we get
$T(\mathbf{v}) = \lambda_1 T(\mathbf{v}_1) + \lambda_2 T(\mathbf{v}_2) + \ldots + \lambda_n T(\mathbf{v}_n)$. Now we have

$$\begin{aligned} [T(\mathbf{v})]_{B_W} &= \lambda_1[T(\mathbf{v}_1)]_{B_W} + \lambda_2[T(\mathbf{v}_2)]_{B_W} + \ldots + \lambda_n[T(\mathbf{v}_n)]_{B_W} \qquad \text{(Why?)} \\ &= A\begin{pmatrix} \lambda_1 \\ \lambda_2 \\ \vdots \\ \lambda_n \end{pmatrix} \end{aligned}$$

since A has $[T(\mathbf{v}_j)]_{B_W}$'s for its columns. So we have

$$[T(\mathbf{v})]_{B_W} = A[\mathbf{v}]_{B_V}$$

as we wanted. ■

Example 3.3.7 Let $A = \begin{pmatrix} 1 & 2 & 0 \\ 3 & 2 & 1 \end{pmatrix}$. Then, we know from the previous section that we can think of A as a linear mapping from $\mathbf{R}^3$ to $\mathbf{R}^2$. It is a natural to ask at this stage what the matrix representing A with respect to the usual bases for $\mathbf{R}^3$ and $\mathbf{R}^2$ is.

The theorem says we should apply the mapping to the basis vectors chosen in $\mathbf{R}^3$. We get

$$A\begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 3 \end{pmatrix}, A\begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 2 \\ 2 \end{pmatrix}, A\begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix}.$$

(Since we are working with the usual bases in $\mathbf{R}^3$ and $\mathbf{R}^2$ the coordinate vector of any vector $\mathbf{v}$ is just $\mathbf{v}$ itself.) Thus the matrix representing A with respect to the usual bases is just A itself. We could make this a general theorem, but it's pretty obvious from this example.

Example 3.3.8 Let A be the matrix of the previous example. We find the matrix ${}_{B_2}T_{B_1}$ which represents A with respect to the bases

$$B_1 = \left\{ \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix} \right\} \quad \text{and} \quad B_2 = \left\{ \begin{pmatrix} 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ -1 \end{pmatrix} \right\}$$

for $\mathbf{R}^3$ and $\mathbf{R}^2$ respectively.

The theorem says we must calculate the coordinate vectors of

$$A\begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}, \quad A\begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}, \quad A\begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix}$$

with respect to the basis B_2. We get

$$A\begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 4 \end{pmatrix}, \quad A\begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \quad A\begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 3 \\ 5 \end{pmatrix}.$$

We must now find the coordinate vectors of these vectors with respect to B_2. They are, in order,

$$\begin{pmatrix} \frac{5}{2} \\ -\frac{3}{2} \end{pmatrix}, \quad \begin{pmatrix} \frac{1}{2} \\ -\frac{1}{2} \end{pmatrix}, \quad \begin{pmatrix} 4 \\ -1 \end{pmatrix}.$$

Thus the desired matrix must be

$$\begin{pmatrix} \frac{5}{2} & \frac{1}{2} & 4 \\ -\frac{3}{2} & -\frac{1}{2} & -1 \end{pmatrix}.$$

You should check the answer by trying it out on a few coordinate vectors of some vectors in $\mathbf{R}^3$.

It is possible to work out formulae for converting a matrix which represents a linear transformation with respect to certain bases to the matrix which would represent the transformation with respect to different bases. We will not do this. It is clear from the last two examples that the matrix which represents a particular linear transformation is dependent on the bases chosen.

We end this section with a result which may not be very surprising, but is worth noting. Since any linear transformation from one finite dimensional vector space to another can be represented as a matrix, and any matrix is a linear transformation from a finite dimensional space to another, many results that hold for matrices viewed as linear transformations also hold true for general linear transformations between finite dimensional vector spaces. In particular, the following theorem is important:

Theorem 3.3.9 *Let $T : V \to W$ be a linear transformation, and let V be finite dimensional. Then*

$$\dim(ker(T)) + \dim(ran(T)) = \dim V.$$

Proof: The proof is omitted, but will appear in a tutorial. Note that we have proved the corresponding result for matrices (Theorem 2.6.23). ■

Corollary 3.3.10 *Let V be a finite dimensional vector space and $T : V \to V$ be a linear transformation. Then the following are equivalent:*

(a) T is injective.

(b) T is surjective.

(c) T is a linear isomorphism.

Proof: Exercise. Use the facts that T is injective if and only if $\ker(T) = \{\mathbf{0}\}$ and that for a subspace U of V we have dim U =dim V if and only if $U = V$. ■ .

The above result shows that a linear function from a vector space into itself is rather special: if it is *either* injective *or* surjective, then it will automatically be *both* injective *and* surjective. Convince your self that this need not be true for non-linear functions.

Summary:

Let $T : V \to W$ (where V and W are finite dimensional vector spaces) be a linear transformation. We can find a matrix A which "does the same job" as T in the following sense: let B_V be a basis for V, let B_W be a basis for W and let $\mathbf{u} \in V$. Then multiplication of the coordinate vector of $\mathbf{u}$ (with respect to the basis B_V) by A produces the coordinate vector of $T\mathbf{u}$ (with respect to the basis B_W). We say that the matrix A *represents* the linear transformation T with respect to these bases.

Exercises

1. Prove Theorem 3.3.3.
2. Let F be the function defined in Corollary 3.3.4.
   (a) Explain how it follows from Theorem 3.3.3 that F is linear.

(b) Prove that F is in fact a linear isomorphism and find its inverse.

3. Let $T : P_2 \to P_1$ be the linear transformation defined by

$$T(a_0 + a_1x + a_2x^2) = (a_0 + a_1) - (2a_1 + 3a_2)x$$

(a) Find the matrix for T with respect to the standard bases $B = \{1, x, x^2\}$ and $B' = \{1, x\}$ for P_2 and P_1.

(b) Verify that the matrix obtained in part (a) satisfies Theorem 3.3.5 for every element $c_0 + c_1x + c_2x^2$ in P_2.

4. Let $T : \mathbf{R}^2 \to \mathbf{R}^3$ be defined by

$$T\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} x_1 + 2x_2 \\ -x_1 \\ 0 \end{pmatrix}$$

Find the matrix ${}_{B'}[T]_B$ with respect to the bases $B = \{\mathbf{u}_1, \mathbf{u}_2\}$ and $B' = \{\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3\}$, where

$$\mathbf{u}_1 = \begin{pmatrix} 1 \\ 3 \end{pmatrix}, \quad \mathbf{u}_2 = \begin{pmatrix} -2 \\ 4 \end{pmatrix}, \quad \mathbf{v}_1 = \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}, \quad \mathbf{v}_2 = \begin{pmatrix} 2 \\ 2 \\ 0 \end{pmatrix}, \quad \mathbf{v}_3 = \begin{pmatrix} 3 \\ 0 \\ 0 \end{pmatrix}.$$

5. Let V be the vector space of all polynomial functions of degree at most n, and $D : V \to V$ be the linear transformation given by differentiation :

$$D(p) = p'.$$

Find the matrix for D with respect to the basis $B = \{1, x, x^2, \ldots, x^n\}$.

6. Let $L : P_1 \to P_2$ be defined by $L(p(x)) = xp(x) + p(0)$.
Let

$$B = \{x, 1\} \text{ and } B' = \{x + 1, x - 1\}$$

be bases for P_1. Let

$$C = \{x^2, x, 1\} \text{ and } C' = \{x^2 + 1, x - 1, x + 1\}$$

be bases for P_2. Find the matrix of L with respect to:
(a) B and C (b) B' and C'.

7. Let $M_{2\times2}(\mathbf{R})$ be the space of 2×2 matrices with real entries, and let $L : M_{2\times2}(\mathbf{R}) \to M_{2\times2}(\mathbf{R})$ be defined by $L(A) = A^T$. Let

$$B = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \right\}$$

and

$$C = \left\{ \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right\}$$

be bases for $M_{2\times 2}$. Find the matrix of L with respect to:
(a) B (b) B and C.

8. Show that if $T : V \to V$ is defined by $T(\mathbf{u}) = \lambda\mathbf{u}$ for some scalar λ, then the matrix of T with respect to any basis for V is a diagonal matrix.

9. Let $B = \{\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3, \mathbf{v}_4\}$ be a basis for a vector space V. Find the matrix with respect to B of the linear transformation $T : V \to V$ defined by

$$T(\mathbf{v}_1) = \mathbf{v}_2, T(\mathbf{v}_2) = \mathbf{v}_3, T(\mathbf{v}_3) = \mathbf{v}_4, T(\mathbf{v}_4) = \mathbf{v}_1.$$

10. We can now tie up some ideas mentioned earlier concerning the associativity of matrix multiplication (see Section 1.2).
(a) Suppose that A is an $m \times p$ matrix and that B is a $p \times n$ matrix. We know that AB is then an $m \times n$ matrix. Let T_A be the linear transformation from $\mathbf{R}^p \to \mathbf{R}^m$ induced by multiplication by A (and similarly for T_B and T_{AB}.) Show that $T_{AB} = T_A \circ T_B$ by considering the action of T_{AB} and $T_A \circ T_B$ on the standard basis of $\mathbf{R}^n$.
(b) Show that (for suitable C) $A(BC) = (AB)C$ by considering the j^{th} column of $A(BC)$ and using what you proved in (a) above. [Your task is to show that the j^{th} column of $A(BC)$ is identical with the j^{th} column of $(AB)C$.]

Chapter 4

Eigenvectors, eigenvalues and diagonalization

4.1 Eigenvalues and eigenvectors

In the three examples we considered at the beginning of Chapter 1 we were faced with the same problem: Given a square matrix A, we needed to know whether there there existed a scalar λ and a non-zero vector $\mathbf{x}$ such that $A\mathbf{x} = \lambda\mathbf{x}$. We mentioned that the scalar and vector were respectively called an eigenvalue and eigenvector of A. These notions were defined in Definition 1.7.17, and in Theorem 1.7.18 we saw how we could use determinants to find eigenvalues.

In this chapter we investigate eigenvalues and eigenvectors and their uses and applications in more detail. We'll see that the eigenvalues and eigenvectors of a matrix contain a great deal of important and useful information about the matrix. These concepts have applications in the study of vibrations, electrical systems, genetics, chemical reactions, quantum mechanics, economics, geometry, hand-writing analysis, image compression and in all sorts of engineering problems. There can be no doubt that they are useful!

As a reminder, let us give precise definitions again:

Definition 4.1.1 *If A is an $n \times n$ matrix, then a* ***non-zero*** *vector $\mathbf{x}$ is called an* ***eigenvector of*** *A if*

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

for some scalar λ. The scalar is called an ***eigenvalue of*** *A and $\mathbf{x}$ is said to be an eigenvector of A corresponding to (or associated with) the eigenvalue λ.*

(Why do you think did we only define eigenvectors for *square* matrices?)

We can also define eigenvectors for general linear transformations from a vector space into itself. Since we can always represent a linear transformation from a finite dimensional vector space into itself by a matrix, we will concentrate on eigenvalues and egenvectors of matrices in this section and succeeding ones. For completeness, we give the general definition:

Definition 4.1.2 *Let V be a vector space and $T : V \to V$ be a linear transformation. Then any non-zero vector $\mathbf{x} \in V$ such that*

$$T(\mathbf{x}) = \lambda \mathbf{x}$$

for some scalar λ is called an ***eigenvector*** *of T. The scalar is called an* ***eigenvalue*** *of T and $\mathbf{x}$ is said to be an eigenvector of T corresponding to (or associated with) the eigenvalue λ.*

Example 4.1.3 Let $A = \begin{pmatrix} -1 & 2 \\ 0 & 3 \end{pmatrix}$.

(a)

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

so $\begin{pmatrix} 1 \\ 2 \end{pmatrix}$ is an eigenvector of A corresponding to the eigenvalue 3.

(b)

$$\begin{pmatrix} -1 & 2 \\ 0 & 3 \end{pmatrix}\begin{pmatrix} -1 \\ -2 \end{pmatrix} = \begin{pmatrix} -3 \\ -6 \end{pmatrix} = 3\begin{pmatrix} -1 \\ -2 \end{pmatrix},$$

so $\begin{pmatrix} -1 \\ -2 \end{pmatrix}$ is another eigenvector of A corresponding to the eigenvalue 3. Note that the second eigenvector is a scalar multiple of the first.

(c) A also has an eigenvalue different to 3:

$$\begin{pmatrix} -1 & 2 \\ 0 & 3 \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} -1 \\ 0 \end{pmatrix} = (-1)\begin{pmatrix} 1 \\ 0 \end{pmatrix},$$

so $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$ is an eigenvector of A corresponding to the eigenvalue -1.

(d) Before you begin to think that all vectors are eigenvectors, consider

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

which means that $\begin{pmatrix} 1 \\ 1 \end{pmatrix}$ is not an eigenvector of A.

The first two examples suggest that any non-zero scalar multiple of an eigenvector for a matrix will also be an eigenvector, corresponding to the same eigenvalue. This is in fact true for any square matrix:

Proposition 4.1.4 L*et A be a square matrix and $\mathbf{x}$ an eigenvector of A corresponding to the eigenvalue λ. Then for every non-zero scalar μ, $\mu\mathbf{x}$ is an eigenvector of A corresponding to the eigenvalue λ.*

Proof: This is an easy exercise. ■

This implies that there are infinitely many eigenvectors corresponding to the same eigenvalue. The third example above shows that a matrix may have more than one eigenvalue.

Some obvious questions have probably occurred to you. In the above example we tested some vectors to see whether they were eigenvectors. But how do we find the eigenvalues and eigenvectors? Does every square matrix have at least one eigenvalue? Are all the eigenvectors corresponding to a particular eigenvalue linearly dependent? If there are eigenvalues, how many are there? We will see answers to these questions as we go along.

In Theorem 1.7.18 we saw how eigenvalues can be calculated. We repeat the theorem here, since we'll be making extensive use of it in this chapter.

Theorem 4.1.5 *Let A be a square matrix. Then*

$$\lambda \textit{ is an eigenvalue of } A \textit{ if and only if } \det(\lambda I - A) = 0.$$

Remark: Note that $\det(A - \lambda I) = 0$ if and only if $\det(\lambda I - A) = 0$; you can use either equation to calculate the eigenvalues of A.

In Example 1.7.19 we saw that to find the eigenvalues of a matrix, we had to find the zeros of a polynomial in λ. The polynomial is what you get when you calculate $\det(\lambda I - A)$, and is so important it gets a name of its own. A natural name would be *eigenpolynomial*, but (English) tradition favours the term **characteristic polynomial**.

Definition 4.1.6 *Let A be an $n \times n$ matrix. The determinant* $\det(\lambda I - A)$ *is a polynomial of degree n in λ and is called the* ***characteristic polynomial*** *of A. The equation* $\det(\lambda I - A) = 0$ *is called the* ***characteristic equation*** *of A.*

It's not hard to see that if A is an $n \times n$ matrix, then the characteristic polynomial of A has degree n and the coefficient of λ^n is 1. We also know that since the characteristic polynomial of A has degree n, then the characteristic equation of A has at most n distinct roots, so A has at most n distinct eigenvalues. Since there are polynomial equations with no real roots, a matrix may have no *real* eigenvalues. It is therefore easy to find real matrices which have no real eigenvalues (see Example 4.1.8). The fundamental theorem of algebra guarantees the existence of n complex roots (not necessarily distinct, of course) for every polynomial equation of degree n. It follows that if we allow complex eigenvalues, every matrix (real or complex-valued) has eigenvalues.

Let's do some more eigenvalue examples to get a bit more familiar with this idea.

Example 4.1.7 We find all the eigenvalues of the matrix

$$A = \begin{pmatrix} 5 & -7 & 7 \\ 4 & -3 & 4 \\ 4 & -1 & 2 \end{pmatrix}.$$

As a first step, we find

$$\lambda I - A = \begin{pmatrix} \lambda & 0 & 0 \\ 0 & \lambda & 0 \\ 0 & 0 & \lambda \end{pmatrix} - \begin{pmatrix} 5 & -7 & 7 \\ 4 & -3 & 4 \\ 4 & -1 & 2 \end{pmatrix} = \begin{pmatrix} \lambda-5 & 7 & -7 \\ -4 & \lambda+3 & -4 \\ -4 & 1 & \lambda-2 \end{pmatrix}.$$

The characteristic polynomial is then

$$\begin{aligned}
\left| \, \lambda I - A \, \right| &= \begin{vmatrix} \lambda-5 & 7 & -7 \\ -4 & \lambda+3 & -4 \\ -4 & 1 & \lambda-2 \end{vmatrix} \\
&= (\lambda-5)\begin{vmatrix} \lambda+3 & -4 \\ 1 & \lambda-2 \end{vmatrix} - 7\begin{vmatrix} -4 & -4 \\ -4 & \lambda-2 \end{vmatrix} - 7\begin{vmatrix} -4 & \lambda+3 \\ -4 & 1 \end{vmatrix} \\
&= (\lambda-5)(\lambda^2+\lambda-2) - 7(-4\lambda-8) - 7(4\lambda+8) \\
&= \lambda^3 - 4\lambda^2 - 7\lambda + 10
\end{aligned}$$

Thus the characteristic equation is

$$\lambda^3 - 4\lambda^2 - 7\lambda + 10 = 0$$

Having reached this stage, we are faced with solving a cubic equation. Fortunately, this one factorizes as

$$(\lambda - 1)(\lambda - 5)(\lambda + 2) = 0$$

which means that the eigenvalues are $1, 5$ and -2.

Example 4.1.8 Let

$$A = \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}.$$

The characteristic equation of A is $(1-\lambda)^2 + 1 = \lambda^2 - 2\lambda + 2 = 0$. This equation has no *real* roots, and therefore A has no real eigenvalues. The equation has two complex roots:

$$\lambda = \frac{-(-2) + \sqrt{(-2)^2 - 4 \times 1 \times 2}}{2} = 1 + i \text{ and } \lambda = \frac{2 - \sqrt{-4}}{2} = 1 - i.$$

Therefore A does have two complex eigenvalues.

Usually you are not so lucky, and must rely on numerical techniques for solving the characteristic equation . (OCTAVE does this: just type in "eig(A)" to get the eigenvalues of A.)

Some matrices have characteristic polynomials that are easy to factorize:

Example 4.1.9 We find the eigenvalues of

$$A = \begin{pmatrix} 2 & 3 & 4 \\ 0 & 5 & 6 \\ 0 & 0 & 7 \end{pmatrix}.$$

The characteristic polynomial is

$$\begin{aligned} \det(\lambda I - A) &= \begin{vmatrix} \lambda - 2 & -3 & -4 \\ 0 & \lambda - 5 & -6 \\ 0 & 0 & \lambda - 7 \end{vmatrix} \\ &= (\lambda - 2) \begin{vmatrix} \lambda - 5 & -6 \\ 0 & \lambda - 7 \end{vmatrix} \text{ (expanding along the top row)} \\ &= (\lambda - 2)(\lambda - 5)(\lambda - 7) \end{aligned}$$

Thus the eigenvalues are $2, 5$ and 7. These are exactly the entries on the diagonal of A. Note that A is an upper triangular matrix.

You should be able to see from the last example that the eigenvalues of any upper (or lower) triangular matrix will always be exactly the entries on the diagonal.

The eigenvalues of a square matrix need certainly not be distinct; we'll see some examples soon. (The characteristic equation could have repeated roots, giving repeated eigenvalues.) As we have see, it is also possible for a matrix (even one with real entries) to have complex eigenvalues.

Here are two useful checks which help with finding eigenvalues:

Theorem 4.1.10 *Let the eigenvalues of the $n \times n$ matrix A be $\lambda_1, \lambda_2, \ldots, \lambda_n$. Then*

(a) $\sum_{i=1}^{n} \lambda_i = \sum_{i=1}^{n} a_{ii}$

(b) $\lambda_1 \lambda_2 \ldots \lambda_n = \det(A)$.

Proof: We'll ask you to check these results for 2×2 and 3×3 matrices in the exercises. The proof for the general case is similar, but needs properties of determinants we have not covered ■

Remark: The number

$$\sum_{i=1}^{n} a_{ii}$$

is known as the **trace** of the matrix A and denoted by $\mathrm{tr}(A)$.

Now that we've had a bit of practice with finding eigenvalues, we can start looking at eigenvectors. An important fact that we see almost immediately is that the eigenvectors associated with an eigenvalue "almost" form a vector subspace. To see this, suppose that λ is an eigenvalue of A. A non-zero eigenvector $\mathbf{x}$, associated with λ, is a solution of the equation $(\lambda I - A)\mathbf{x} = \mathbf{0}$. This means that it is a member of the nullspace of $\lambda I - A$. Moreover, all members of this nullspace, except the zero vector, are eigenvectors corresponding to the eigenvalue λ. We have thus seen:

Theorem 4.1.11 *Let λ be an eigenvalue of the $n \times n$ matrix A. The eigenvectors of A associated with λ are the non-zero vectors in $NS(\lambda I - A)$, and hence together with the zero vector, form a subspace of $\mathbf{R}^n$ (or $\mathbf{C}^n$ if A is a complex matrix).*

It now makes sense to make the following definition:

Definition 4.1.12 *Let A and λ be as in the above theorem. Then $NS(\lambda I - A)$ is called the **eigenspace** associated with λ. We'll use the notation W_λ for this eigenspace.*

Establishing a basis for each of the eigenspaces of a given matrix is a very important business. Since you should by now be pretty good at finding nullspaces and bases for them, this shouldn't cause you any trouble. We do this in the next two examples.

Example 4.1.13 We find bases for the eigenspaces of the matrix

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

The characteristic equation of A is

$$0 = (\lambda - 4)(\lambda - 1) + 2 = \lambda^2 - 5\lambda + 6 = (\lambda - 3)(\lambda - 2).$$

Thus the eigenvalues of A are $\lambda = 2$ and $\lambda = 3$.

To find a basis for W_2 we first calculate $2I - A = \begin{pmatrix} -2 & -2 \\ 1 & 1 \end{pmatrix}$.

We can see by inspection that rank $\begin{pmatrix} -2 & -2 \\ 1 & 1 \end{pmatrix} = 1$ and so its nullity is 1 as well.

It's also easy to see by inspection that $\begin{pmatrix} 1 \\ -1 \end{pmatrix} \in NS\left(\begin{pmatrix} -2 & -2 \\ 1 & 1 \end{pmatrix}\right)$.

Hence $\left\{\begin{pmatrix} 1 \\ -1 \end{pmatrix}\right\}$ is a basis for W_2. You could check now that
$A\begin{pmatrix} 1 \\ -1 \end{pmatrix} = 2\begin{pmatrix} 1 \\ -1 \end{pmatrix}$.

To find a basis for W_3 we need $NS(3I - A) = NS\left(\begin{pmatrix} -1 & -2 \\ 1 & 2 \end{pmatrix}\right)$. As before, we can see that the rank of $\begin{pmatrix} -1 & -2 \\ 1 & 2 \end{pmatrix}$ is 1 and so its nullity is 1 too. By inspection, $\begin{pmatrix} 2 \\ -1 \end{pmatrix}$ is a member of the eigenspace. Thus $\left\{\begin{pmatrix} 2 \\ -1 \end{pmatrix}\right\}$ is a basis for W_3.

Of course, you won't always be able to spot eigenvectors as we did in the above example, but you do have the know-how to find them, if necessary. The next example is a case in point.

Example 4.1.14 We find bases for the eigenspaces of

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

The usual calculations (do them!) give the characteristic equation as

$$\lambda^3 - 5\lambda^2 + 8\lambda - 4 = (\lambda - 1)(\lambda - 2)^2 = 0.$$

Thus the eigenvalues are 1 and 2. (We say that $\lambda = 2$ is a **repeated eigenvalue** because $(\lambda - 2)^2$ is a factor of the characteristic polynomial.)

To find W_1, we find the nullspace of $I - A = \begin{pmatrix} 1 & 0 & 2 \\ -1 & -1 & -1 \\ -1 & 0 & -2 \end{pmatrix}$. We reduce $I - A$ to its row-echelon form $U = \begin{pmatrix} 1 & 0 & 2 \\ 0 & -1 & 1 \\ 0 & 0 & 0 \end{pmatrix}$. Now U has rank 2 and nullity 1, so our eigenspace W_1 will also have dimension 1. Suppose $\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix}$ is a member of the eigenspace; then it is a solution of $U\mathbf{x} = \mathbf{0}$. From the form of U we can deduce that x_3 is a free variable; let $x_3 = t$, where $t \in \mathbf{R}$; then $x_2 = t$ and $x_1 = -2t$, so

$$\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = t \begin{pmatrix} -2 \\ 1 \\ 1 \end{pmatrix}.$$

Thus $\left\{ \begin{pmatrix} -2 \\ 1 \\ 1 \end{pmatrix} \right\}$ is a basis for W_1.

W_2 is the nullspace of $\begin{pmatrix} 2 & 0 & 2 \\ -1 & 0 & -1 \\ -1 & 0 & -1 \end{pmatrix}$. This matrix has rank 1, so must have nullity 2. Any basis for W_2 must therefore have two elements. We reduce the matrix to its row-echelon form $U = \begin{pmatrix} 2 & 0 & 2 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$. If $\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix}$ is a solution of $U\mathbf{x} = \mathbf{0}$, then both x_2 and x_3 are free variables. Let $x_3 = t$ and $x_2 = s$ where $s, t \in \mathbf{R}$. Then $x_1 = -x_3 = -t$, so

$$\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = s \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} + t \begin{pmatrix} -1 \\ 0 \\ 1 \end{pmatrix}.$$

Then a basis for W_2 is $\left\{ \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} -1 \\ 0 \\ 1 \end{pmatrix} \right\}$

Example 4.1.15 We have seen that the matrix $A = \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}$ has the complex eigenvalues $1+i$ and $1-i$. The eigenspace corresponding to the eigenvalue $1+i$ is the nullspace of the matrix

$$\begin{pmatrix} 1+i-1 & 1 \\ -1 & 1+i-1 \end{pmatrix} = \begin{pmatrix} i & 1 \\ -1 & i \end{pmatrix}.$$

The second row of this matrix is i times the first row, so that we can reduce it to the matrix $U = \begin{pmatrix} i & 1 \\ 0 & 0 \end{pmatrix}$. If the vector $\begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$ is in the nullspace of U, then $ix_1 + x_2 = 0$, or $-x_1 + ix_2 = 0$. Hence $x_1 = ix_2$. The eigenspace corresponding to the eigenvalue $1+i$ is therefore

$$W_{1+i} = \left\{ \lambda \begin{pmatrix} i \\ 1 \end{pmatrix} : \lambda \in \mathbf{C} \right\}.$$

Note that in this case we have complex eigenvectors.

The eigenspace W_{1-i} can be found in the same way.

We finish off with a result which extends our list of conditions that are equivalent to the invertibility of a square matrix.

Theorem 4.1.16 *An $n \times n$ matrix A is invertible if and only if $\lambda = 0$ is not an eigenvalue of A.*

Proof: If $\lambda = 0$ is an eigenvalue, then

$$0 = \det(\lambda I - A) = \det(-A) = (-1)^n \det(A),$$

which means that $\det(A) = 0$, so A is not invertible. The converse is similar. ∎

Summary:

In this section we introduced the notions of an eigenvalue and a corresponding eigenvector for a square matrix A.

- A scalar λ is an *eigenvalue* for the matrix A if there is a *non-zero* vector $\mathbf{x}$ such that $A\mathbf{x} = \lambda\mathbf{x}$; the vector $\mathbf{x}$ is called an *eigenvector* of A corresponding to the eigenvalue λ.

- The eigenvalues of A are the solutions to the *characteristic equation* $\det(A - \lambda I) = 0$.
- An $n \times n$ matrix may have no real eigenvalues, but it will always have n complex eigenvalues.
- If λ is an eigenvalue of A, then $NS(A - \lambda I)$ is called the *eigenspace* of A associated with the eigenvector λ; it consists of all the eigenvectors of A corresponding to λ as well as the zero vector.
- A matrix may have repeated eigenvalues (correponding to repeated roots of the characteristic equation).

Exercises

The following OCTAVE commands may come in useful:

det (A) gives the determinant of the matrix A
poly (A) gives the coefficients of the characteristic polynomial of A.
eig (A) gives the eigenvalues of of A.
$[V, D]$ = **eig**(A) gives you a matrix V with columns the eigenvectors of A corresponding to the eigenvalues of A; the matrix D is a diagonal matrix with these eigenvalues on the main diagonal.

1. Find the eigenvalues and bases of the eigenspaces for the matrix $\begin{pmatrix} 3 & 0 \\ 8 & -1 \end{pmatrix}$.
2. In this section there was an example of a real matrix with no real eigenvalues. Construct another such a matrix A as follows:
   A will satisfy this condition if its characteristic polynomial is say $\lambda^2 + 1$. (Why?) Write out the characteristic polynomial of $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, and choose a, b, c, d to give $\lambda^2 + 1$ as required.
3. Find the eigenvalues and bases of the eigenspaces for the matrices:
   (a) $\begin{pmatrix} 10 & -9 \\ 4 & -2 \end{pmatrix}$ (b) $\begin{pmatrix} -2 & -7 \\ 1 & 2 \end{pmatrix}$
4. By inspection, find the eigenvalues for matrix: $\begin{pmatrix} 3 & 0 & 0 \\ -2 & 7 & 0 \\ 4 & 8 & 1 \end{pmatrix}$.

5. Prove: If λ is an eigenvalue of A, $\mathbf{x}$ is a corresponding eigenvector, and μ is a scalar, then $\lambda - \mu$ is an eigenvalue of $A - \mu I$, and $\mathbf{x}$ is a corresponding eigenvector.

6. Find the eigenvalues and bases for the eigenspaces of $A = \begin{pmatrix} -2 & 2 & 3 \\ -2 & 3 & 2 \\ -4 & 2 & 5 \end{pmatrix}$.
   Then use Question 5 above to find the eigenvalues and bases for the eigenspaces of
   (a) $A - 3I$ (b) $A + 2I$.

7. Find the eigenvalues and bases of the eigenspaces for the matrix $\begin{pmatrix} 0 & 0 & 2 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & -2 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$.

8. Let A be a 2×2 matrix, and call a line through the origin of $\mathbf{R}^2$ **invariant** under A if $A\mathbf{x}$ lies on the line when $\mathbf{x}$ does. Find equations for all lines in $\mathbf{R}^2$, if any, that are invariant under each of the given matrices below.
   (a) $A = \begin{pmatrix} 4 & -1 \\ 2 & 1 \end{pmatrix}$ (b) $A = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ (c) $A = \begin{pmatrix} 2 & 3 \\ 0 & 2 \end{pmatrix}$.

9. Let A be a 6×6 matrix with characteristic equation $\lambda^2(\lambda - 1)(\lambda - 2)^3 = 0$. What are the possible dimensions for eigenspaces of A?

10. We prove Theorem 4.1.10 for the case of a 2×2 matrix as follows:
    Write out the characteristic polynomial of $A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$ in two ways. Firstly, calculate det $(\lambda I - A)$. Secondly, assume the two eigenvalues are λ_1 and λ_2: the characteristic polynomial is then $(\lambda - \lambda_1)(\lambda - \lambda_2)$.
    To get part 1 (involving the trace of A), compare the coefficients of λ in your two expressions.
    To get part 2 (involving the determinant of A), compare the constant terms.

    If you have lots of energy and enthusiasm, check this result for the 3×3 case. In this case, compare the coefficients of λ^2, and the constant terms.

4.2 Diagonalization

Eigenvectors and eigenvalues have one of their most significant uses in the setting of diagonalization. In fact the two ideas are inseparable. At this stage the word "diagonalization" probably does not mean much to you. You may remember that a *diagonal matrix* is a square matrix with all entries **not** on the main diagonal equal to zero. Note that a diagonal matrix could even have some or all of the entries on the main diagonal equal to zero; the only thing that the definition prescribes is that if there are non-zero entries, they have to be on the diagonal. To diagonalize a square matrix means, roughly speaking, to change it into a diagonal matrix by multiplying it by invertible matrices. Since diagonal matrices are relatively simple matrices with nice properties, there are many situations where being able to diagonalize a square matrix turns out to be very useful indeed (as we'll see later in this chapter).

The questions we want to look at in this section are:

- What exactly do we mean by diagonalizing a square matrix?
- When is it possible to diagonalize a square matrix?
- If a square matrix can be diagonalized, how do we go about doing it?

We'll see that the way we define diagonalization is motivated by what we know about matrix representations for linear maps. The answer to the second question shows up the link between diagonalization and eigenvectors. Roughly speaking, a matrix is diagonalizable if it has enough "different" eigenvectors. The idea at the core of all of this is contained in the next theorem.

Theorem 4.2.1 *Let A be an $n \times n$ matrix.*

(a) If A has n linearly independent eigenvectors $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n$ and P is the matrix whose j-th column is $\mathbf{v}_j$, then $P^{-1}AP$ is a diagonal matrix D, and the entries, d_{jj}, on the main diagonal of D are exactly the eigenvalues corresponding to the eigenvectors $\mathbf{v}_j$.

(b) If there is an invertible matrix P such that $P^{-1}AP$ is a diagonal matrix $D = \left(\, d_{ij} \, \right)$, then for each j, the j-th column of P is an eigenvector of A corresponding to the eigenvalue d_{jj}, and hence A has n linearly independent eigenvectors.

Proof: (a) P is square and of rank n, since its columns are linearly independent. Now calculate AP one column at a time:

$$\begin{aligned} j\text{-th column of } AP &= A(j\text{-th column of } P) \\ &= A\mathbf{v}_j \\ &= \lambda_j \mathbf{v}_j \end{aligned}$$

Now calculate PD one column at a time, where D is as described above:

$$\begin{aligned} j\text{-th column of } PD &= P(j\text{-th column of } D) \\ &= P\begin{pmatrix} 0 \\ \vdots \\ \lambda_j \\ \vdots \\ 0 \end{pmatrix} \\ &= \lambda_j \mathbf{v}_j \end{aligned}$$

Thus $AP = PD$, so $P^{-1}AP = D$, as claimed. (By the way, how do we know that P^{-1} exists?)

(b) If $P^{-1}AP = D$, then $AP = PD$. Let $\mathbf{v}_j$ be the j-th column of P. Then comparing j-th columns on each side of the equation $AP = DP$, we see that $A\mathbf{v}_j = d_{jj}\mathbf{v}_j$. Hence $\mathbf{v}_j$ is an eigenvector of A corresponding to the eigenvalue d_{jj}. Since P is invertible, it must have rank n, and therefore the columns of P must be linearly independent. ■

Let's check the theorem by doing an example:

Example 4.2.2 Let $A = \begin{pmatrix} 0 & 0 & -2 \\ 1 & 2 & 1 \\ 1 & 0 & 3 \end{pmatrix}$. We give the essential details, and ask you to do most of the checking. We begin by calculating the characteristic equation of A. Check that this is

$$(\lambda - 1)(\lambda - 2)^2 = 0.$$

From this we can deduce that the eigenvalues of A are 1 and 2. The next step is to find the eigenspace corresponding to each eigenvalue. Check that the eigenspaces are as follows:

W_2 has as basis $\left\{ \begin{pmatrix} -1 \\ 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} \right\}$.

W_1 has as basis $\left\{ \begin{pmatrix} -2 \\ 1 \\ 1 \end{pmatrix} \right\}$.

These three vectors are in fact linearly independent (check this!), so we can form the matrix

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

which has as columns the three eigenvectors. Now check that

$$P^{-1} = \begin{pmatrix} 1 & 0 & 2 \\ 1 & 1 & 1 \\ -1 & 0 & -1 \end{pmatrix}.$$

To see that P does what is required of it, check that

$$P^{-1}AP = \begin{pmatrix} 2 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Notice that there is no preferred order for writing down the eigenvectors of A as columns of P. Once you have decided on the order though, the matrix D will have eigenvalues on the diagonal *in the order that you wrote down the eigenvectors in P*. This means that you can diagonalize A in different ways, depending on the order in which you do things. This is not a problem as long as you remember to write down eigenvectors and eigenvalues in the same order.

It is time to make precise the notion of diagonalizability:

Definition 4.2.3 *We say that a square matrix A is* ***diagonalizable*** *if there is an invertible matrix P such that $P^{-1}AP = D$ where D is a diagonal matrix; this P is then said to* ***diagonalize*** *A.*

Let's have a brief summary of what we know now. Let A be an $n \times n$ matrix. In what follows we'll assume that A is a real matrix, but everything we say also holds for complex matrices, as long as we replace $\mathbf{R}^n$ by $\mathbf{C}^n$.

- A is diagonalizable if A has n linearly independent eigenvectors.
- If A has n linearly independent eigenvectors, then they form a basis for $\mathbf{R}^n$. Thus A is diagonalizable if there is a basis for $\mathbf{R}^n$ consisting of eigenvectors of A.

- If there is an invertible matrix P and a diagonal matrix D such that $P^{-1}AP = D$, then the columns of P must be eigenvectors of A, and therefore A must have n linearly independent eigenvectors.

As a result of the above discussion, we have, for an $n \times n$ matrix A:

$$\begin{aligned} A \text{ is diagonalizable } &\iff A \text{ has } n \text{ linearly independent eigenvectors} \\ &\iff \mathbf{R}^n \text{ has a basis consisting of eigenvectors of } A \end{aligned}$$

Our knowledge of matrix representations of linear transformations enables us to interpret this result in a very satisfactory way. Let us suppose that the $n \times n$ matrix A is diagonalizable. Then A has n linearly independent eigenvectors; let's call these $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n$ and the associated eigenvalues $\lambda_1, \lambda_2, \ldots, \lambda_n$ (these need not all be distinct). The eigenvectors form a basis of $\mathbf{R}^n$; let's call it B. We can use A to define a linear transformation T from $\mathbf{R}^n$ to $\mathbf{R}^n$: put $T(\mathbf{u}) = A\mathbf{u}$ for every $\mathbf{u} \in \mathbf{R}^n$. Let's find the matrix ${}_B[T]_B$ representing T with respect to the basis B. Now we have

$$T(\mathbf{v}_1) = A\mathbf{v}_1 = \lambda_1 \mathbf{v}_1, \quad \ldots \quad , T(\mathbf{v}_n) = A\mathbf{v}_n = \lambda_n \mathbf{v}_n.$$

The coordinate vectors of the vectors $T(\mathbf{v}_i)$ with respect to B are

$$[T(\mathbf{v}_1)]_B = (\lambda_1, 0, \ldots, 0), \quad \ldots \quad , [T(\mathbf{v}_n)]_B = (0, 0, \ldots, 0, \lambda_n).$$

These coordinate vectors are the columns of ${}_B[T]_B$. It follows that ${}_B[T]_B$ is a diagonal matrix D with the eigenvalues $\lambda_1, \lambda_2, \ldots, \lambda_n$ on the main diagonal.

If we write F_B for the linear transformation which maps a vector in $\mathbf{R}^n$ to its coordinate vector with respect to the basis B (i.e. $F_B(\mathbf{v}) = [\mathbf{v}]_B$) and recall that F_B is a bijection and therefore has an inverse F_B^{-1}, we get the following picture:

$$\begin{tikzcd} \mathbf{R}^n \arrow[r, "A"] \arrow[d, "F_B"'] & \mathbf{R}^n \\ \mathbf{R}^n \arrow[r, "D =_B [T]_B"] & \mathbf{R}^n \arrow[u, "F_B^{-1}"'] \end{tikzcd}$$

We have therefore shown that if an $n \times n$ matrix A is diagonalizable, and T is the linear transformation associated with A, then there is a basis B of $\mathbf{R}^n$ such that the matrix ${}_B[T]_B$ representing T with respect to this basis is a diagonal matrix. The converse of this statement is also true. As a challenge, see if you can prove it. This comment also bears out the claim we made earlier, in Chapter 2, that it can sometimes be very useful to work with specially chosen bases, rather than simply the standard ones.

Warning: Not all square matrices are diagonalizable; it's a pity, but there it is!

Example 4.2.4 Let $A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. A is not diagonalizable; it has only one eigenvalue, which is 1. The eigenspace associated with 1 is $NS\begin{pmatrix} 0 & -1 \\ 0 & 0 \end{pmatrix}$ which is just $\{t\begin{pmatrix} 1 \\ 0 \end{pmatrix} : t \in \mathbf{R}\}$. So A does not have two linearly independent eigenvectors, so cannot be diagonalized.

This obviously raises the question as to which matrices are diagonalizable. The answer is not simple. We will content ourselves with a partial answer.

The partial answer that we provide here centres around the eigenvalues of the matrix. We will prove a theorem that says that if you look at eigenvectors associated with different eigenvalues, then they will form a linearly independent set. Of course this doesn't help if you don't have enough different eigenvalues to start with.

Theorem 4.2.5 *If $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_m$ are all eigenvectors of a square matrix A, associated with distinct eigenvalues $\lambda_1, \lambda_2, \ldots, \lambda_m$, then $S = \{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_m\}$ is linearly independent.*

Proof: Suppose that S is not linearly independent ; we'll derive a contradiction. We certainly know that $\{\mathbf{v}_1\}$ is linearly independent (why?) so let k be the first integer such that $\{\mathbf{v}_1, \mathbf{v}_2, \ldots \mathbf{v}_k\}$ is linearly dependent. Then there are scalars $\mu_1, \ldots, \mu_k$ **not all zero** such that

$$\mu_1\mathbf{v}_1 + \mu_2\mathbf{v}_2 + \ldots + \mu_k\mathbf{v}_k = \mathbf{0}. \qquad (1)$$

Now multiply both sides of the above equation (on the left) by A remembering that the $\mathbf{v}_j$'s are eigenvectors; we get

$$\mu_1\lambda_1\mathbf{v}_1 + \mu_2\lambda_2\mathbf{v}_2 + \ldots + \mu_k\lambda_k\mathbf{v}_k = \mathbf{0}. \qquad (2)$$

Now multiply (1) by λ_k; we get:

$$\mu_1\lambda_k\mathbf{v}_1 + \mu_2\lambda_k\mathbf{v}_2 + \ldots + \mu_k\lambda_k\mathbf{v}_k = \mathbf{0}. \qquad (3)$$

If we now subtract (2) from (3) we get:

$$\mu_1(\lambda_k - \lambda_1)\mathbf{v}_1 + \mu_2(\lambda_k - \lambda_2)\mathbf{v}_2 + \ldots + \mu_{k-1}(\lambda_k - \lambda_{k-1})\mathbf{v}_{k-1} = \mathbf{0}.$$

But the vectors $\{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_{k-1}\}$ are linearly independent (why?) so, since none of the $\lambda_k - \lambda_i$ are zero, we must have all the μ_i zero for $1 \le i \le k-1$. Going back to equation (1) this leaves us with $\mu_k \mathbf{v}_k = \mathbf{0}$ and since $\mathbf{v}_k \neq \mathbf{0}$, we must have $\mu_k = 0$. But this contradicts the fact that we knew that the μ_i's were not all zero. We have a contradiction, and the proof is finished. ■

The upshot of this theorem is that the thing to hope for is that any $n \times n$ matrix you want to diagonalize has n distinct eigenvalues. If this is the case, any n associated eigenvectors will be linearly independent and you are away. However, even if you don't have enough eigevalues, all is not lost. Have a look at Example 4.2.2. There the 3×3 matrix A had only two eigenvalues, but luckily one of these eigenvalues had two linearly independent eigenvectors. Putting them together with the third eigenvector from the other eigenvalue gave us a linearly independent set of 3 eigenvectors for a 3×3 matrix, and again we were in business.

Let's have a last example to illustrate these ideas.

Example 4.2.6 We determine whether the two matrices

(a) $A = \begin{pmatrix} 5 & -7 & 7 \\ 4 & -3 & 4 \\ 4 & -1 & 2 \end{pmatrix}$ (b) $B = \begin{pmatrix} -6 & 12 & -1 \\ -6 & 11 & 0 \\ 0 & 0 & 2 \end{pmatrix}$

are diagonalizable.

(a) You should check that the characteristic equation is

$$(\lambda - 1)(\lambda + 2)(\lambda - 5) = 0$$

so A has 3 distinct eigenvalues. It must therefore have three linearly independent eigenvectors and so must be diagonalizable.

(b) The characteristic equation of B is

$$(\lambda - 2)^2(\lambda - 3).$$

So B has only two distinct eigenvalues. It all now depends on the dimensions of the eigenspaces. Both these eigenspaces have dimension 1, which you should check; that means that we can only get at most two linearly independent eigenvectors, so B is not diagonalizable.

Summary:

In this section we looked at the possibility of diagonalizing an $n \times n$ matrix A.

- We say A is *diagonalizable* if there is an invertible matrix P such that $P^{-1}AP$ is a diagonal matrix.
- Not all square matrices are diagonalizable.
- A is diagonalizable if and only if it has n linearly independent eigenvectors.
- If A has n distinct eigenvalues, it is diagonalizable. However, A may be diagonalizable even if it has fewer than n distinct eigenvalues, as long as it has n linearly independent eigenvectors.

Exercises

1. Let
$$A = \begin{pmatrix} 4 & 0 & 1 \\ 2 & 3 & 2 \\ 1 & 0 & 4 \end{pmatrix}.$$
   (a) Find the eigenvalues of A.
   (b) For each eigenvalue λ find the rank of the matrix $\lambda I - A$.
   (c) Is A diagonalizable? Justify your conclusion.

2. In each case below, determine whether A is diagonalizable. If so, find a matrix P that diagonalizes A, and determine $P^{-1}AP$.

   (a) $A = \begin{pmatrix} -14 & 12 \\ -20 & 17 \end{pmatrix}$ (b) $A = \begin{pmatrix} 2 & 0 & -2 \\ 0 & 3 & 0 \\ 0 & 0 & 3 \end{pmatrix}$

   (c) $A = \begin{pmatrix} 19 & -9 & -6 \\ 25 & -11 & -9 \\ 17 & -9 & -4 \end{pmatrix}$

3. Find A^{10}, where $A = \begin{pmatrix} 1 & 0 \\ -1 & 2 \end{pmatrix}$ (**Hint:** Diagonalize !)

4. Let A be an $n \times n$ matrix and $T : \mathbf{R}^n \to \mathbf{R}^n$ be defined by $T(\mathbf{u}) = A\mathbf{u}$. Show that if there is a basis B of $\mathbf{R}^n$ such that ${}_B[T]_B$ is a diagonal matrix, then A has n linearly independent eigenvectors.

4.3 Applications of diagonalization

Diagonalization and the use of eigenvectors probably constitute the single most useful tool in linear algebra. We will give you an idea of two applications in this section, but there are many! We start off by having a look at the kind of problem that we considered at the start of this course.

Markov Matrices

Recall that in Example 1.1.1 we set up a matrix which described, in terms of percentages, what happened each month to the transport preferences of UCT students commuting to campus. The matrix was

$$M = \begin{pmatrix} 0.8 & 0.1 \\ 0.2 & 0.9 \end{pmatrix}.$$

This is an example of a **stochastic**, **Markov**, or **probability** matrix. We give the general definition now.

Definition 4.3.1 *A square ($n \times n$) matrix $M = \begin{pmatrix} m_{ij} \end{pmatrix}$ is called a **Markov matrix** if*

(a) $m_{ij} \geq 0$ for all i and j (all the entries of M are non-negative) and

(b) for each j,

$$m_{1j} + m_{2j} + \ldots + m_{kj} = 1$$

(the entries in each column add up to 1).

Such matrices occur in many situations; you will see a small selection in the exercises. They are also, under certain circumstances, referred to as *transition matrices.*

Example 4.3.2 Let's look now at some of the features of the matrix M that describes the transport preferences. We adapt the notation we used in Example 1.1.1 slightly and write $x_1(n)$ for the fraction of students using the Jammie Shuttle in month n, $x_2(n)$ for the fraction of students using their own transport in month n, and $\mathbf{x}(n) = \begin{pmatrix} x_1(n) \\ x_2(n) \end{pmatrix}$. The matrix equation modelling the situation then becomes $\mathbf{x}(n+1) = M\mathbf{x}(n)$.

We start of by finding the eigenvalues and eigenvectors of

$$M = \begin{pmatrix} 0.8 & 0.1 \\ 0.2 & 0.9 \end{pmatrix}$$

and then use this information to diagonalize M.

The characteristic equation is

$$0 = \lambda^2 - 1.7\lambda + 0.7 = (\lambda - 1)(\lambda - 0.7)$$

and therefore the eigenvalues are $\lambda = 1$ and $\lambda = 0.7$. We find the corresponding eigenspaces:

W_1: $1I - M = \begin{pmatrix} 0.2 & -0.1 \\ -0.2 & 0.1 \end{pmatrix}$, so the eigenspace W_1 has dimension 1 with a basis vector $\begin{pmatrix} 1 \\ 2 \end{pmatrix}$; if we rewrite this as a vector with components fractions of the population, we get $\frac{1}{3}\begin{pmatrix} 1 \\ 2 \end{pmatrix}$.

$W_{0.7}$: $0.7I - M = \begin{pmatrix} -0.1 & -0.1 \\ -0.2 & -0.2 \end{pmatrix}$ so the eigenspace $W_{0.7}$ has dimension 1 with a basis vector $\begin{pmatrix} 1 \\ -1 \end{pmatrix}$.

The fact that one of the eigenvalues is 1 is interesting: it means that, for the eigenvectors corresponding to 1, multiplication of these vectors by M leaves them unchanged. This has significance for the transport preferences. If at a particular time the distribution of transport preferences were in fact an eigenvector corresponding to 1, then the *distribution* of transport preferences would remain unchanged from month to month. (This is sometimes called a **steady-state** distribution.) Since we are working with distributions of transport preferences expressed as fractions of the total student population, the sum of the fractions would have to be 1, and the steady state distribution (expressed as a vector) would be $\frac{1}{3}\begin{pmatrix} 1 \\ 2 \end{pmatrix}$.

We use the basis vectors in the usual way to diagonalize M. Thus we get:

$$P^{-1}MP = D$$

where

$$P = \begin{pmatrix} 1 & 1 \\ 2 & -1 \end{pmatrix}, \quad P^{-1} = \frac{1}{3}\begin{pmatrix} 1 & 1 \\ 2 & -1 \end{pmatrix} \quad D = \begin{pmatrix} 1 & 0 \\ 0 & 0.7 \end{pmatrix}.$$

Now that we have diagonalized M, it is easy to calculate powers of M:

$$M^n = (PDP^{-1})^n = PD^nP^{-1} = \begin{pmatrix} 1 & 1 \\ 2 & -1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & (.7)^n \end{pmatrix}\frac{1}{3}\begin{pmatrix} 1 & 1 \\ 2 & -1 \end{pmatrix}.$$

If we let $n \to \infty$ then $(.7)^n \to 0$ so we see that

$$M^n \to \frac{1}{3}\begin{pmatrix} 1 & 1 \\ 2 & -1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 2 & -1 \end{pmatrix} = \begin{pmatrix} 1/3 & 1/3 \\ 2/3 & 2/3 \end{pmatrix}.$$

We point out that the columns of this limit matrix are identical and moreover that they are rather special: each one is the steady state distribution described above!

If we start with a and b students using the Jammie Shuttle and their own transport respectively, then

$$\lim_{n\to\infty} M^n \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} 1/3 & 1/3 \\ 2/3 & 2/3 \end{pmatrix}\begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} 1/3(a+b) \\ 2/3(a+b) \end{pmatrix}.$$

Since $a+b = 10000$ is just the total student population, we see that, no matter what the starting distribution of preferences, over a period of many months (an infinitely long academic year?) the distribution of preferences tends towards the steady-state distribution.

None of what we observed in the above example is coincidental. You will prove in Exercise 5 that a Markov matrix always has 1 as an eigenvalue. It can also be proved (although this is a somewhat deeper result) that the other eigenvalues have absolute value at most 1. For a large class of Markov matrices it is true that as $n \to \infty$ the n^{th} power of the Markov matrix tends to a matrix A, all of whose columns are identical. This result (the proof of which unfortunately is beyond the scope of this course) holds for Markov matrices whose entries are positive, or Markov matrices that have a power whose entries are all positive. In practice many Markov matrices do satisfy this condition. They are called **regular** Markov matrices in the literature. Given that the n^{th} power of a regular Markov matrix does tend to this rather special matrix A, it is possible to prove that the columns are all the so-called steady-state eigenvector whose entries add up to 1. The fact that any (population) distribution heads, over a period of time, to the steady-state distribution is also easy to see. (The reason is clear in this example and similar reasoning applies to other Markov matrices.) This is important from an applications point of view: if you know that you are examining a situation or process governed by a regular Markov matrix, then over a period of time, no matter what, your distribution tends to a steady-state.

Rankings

The problem of ranking web sites that we considered in Example 1.1.2 also reduces to an eigenvalue problem, as can be seen by looking at the matrix form of the system of linear equations we had to solve there. What is special about this problem is that we are interested in a *positive* eigenvalue (the constant of proportionality k)

and a corresponding eigenvector with *positive* components (the rankings r_i of the sites). Do we have any guarantee that it will always be possible to find such a positive eigenvalue and corresponding positive eigenvector? It can be shown that if all the entries of the matrix are positive, we'll always be able to find such an eigenvalue and eigenvector. (This result is known as Perron's Theorem.) However, the matrix in our example has some entries equal to 0, and it is clear that in general we cannot expect all the entries to be positive. Fortunately there is a generalization of Perron's theorem (known as the Perron-Frobenius theorem) which says that if all the entries of the matrix are non-negative and some power of the matrix has only positive entries, then there will still be a positive eigenvalue and a corresponding positive eigenvector. We can use this result to show that the method illustrated in the example will always work. The proofs of these results are beyond the scope of this course.

Differential Equations

Our second application is more traditional. You may remember from your first-year course that the differential equation

$$\frac{dy}{dx} = ky$$

has as general solution $y = Ce^{kx}$, where C is an arbitrary constant. If we are also given an initial condition, for instance, $y(0) = 2$, then we can evaluate the constant C; in this example it would be 2.

It is common in many situations to have not just one dependent variable y, but possibly many interlinked variables which all depend on, say, a single variable x or t. For instance, in a chemical experiment, you might have a number of chemicals interacting over a period of time, or in an economics model, you might have various parameters (share prices, interest rates etc.) interacting over a period of time, and their interaction could well be described by a system of linked differential equations. In Section 1.1 we had an example showing how such linked differential equations could be used to model the interaction between rabbits and foxes on an island.

How does one solve such a system? Diagonalization can sometimes come to the rescue. We'll give you an example right now, which is purely mathematical, but you will be able to apply the basic method to whatever example you might be faced with in your particular field. We'll give a selection of these in the exercise sheets.

Example 4.3.3 We try to solve the system of differential equations

$$\begin{aligned} x_1'(t) &= x_1(t) - x_2(t) \\ x_2'(t) &= 2x_1(t) + 4x_2(t) \end{aligned}$$

Writing $\mathbf{x}(t)$ for $\begin{pmatrix} x_1(t) \\ x_2(t) \end{pmatrix}$ and $\mathbf{x}'(t)$ for $\begin{pmatrix} x_1'(t) \\ x_2'(t) \end{pmatrix}$, we could rewrite this equation in the form

$$\mathbf{x}'(t) = \begin{pmatrix} 1 & -1 \\ 2 & 4 \end{pmatrix} \mathbf{x}(t). \tag{1}$$

Now the matrix $A = \begin{pmatrix} 1 & -1 \\ 2 & 4 \end{pmatrix}$ has eigenvalues 2 and 3 associated with the eigenvectors $\mathbf{v}_1 = \begin{pmatrix} 1 \\ -1 \end{pmatrix}$ and $\mathbf{v}_2 = \begin{pmatrix} 1 \\ -2 \end{pmatrix}$ respectively (check this!). Since the eigenvalues are distinct, the associated eigenvectors are linearly independent, and we can form the matrix P as usual by taking the vectors $\mathbf{v}_1$ and $\mathbf{v}_2$ as columns of P. We then know that

$$P^{-1}AP = \begin{pmatrix} 2 & 0 \\ 0 & 3 \end{pmatrix}.$$

Now we introduce a change of variable, to enable us to bring in the diagonal matrix. Let

$$\begin{pmatrix} u_1(t) \\ u_2(t) \end{pmatrix} = \mathbf{u}(t) = P^{-1}\mathbf{x}(t);$$

then if $\mathbf{u}'(t)$ is defined in the same way as $\mathbf{x}'(t)$ we get

$$\mathbf{u}'(t) = P^{-1}\mathbf{x}'(t).$$

This can be rewritten as

$$\mathbf{x}'(t) = P\mathbf{u}'(t),$$

and it is this that we now use in the equation (1). We get

$$P\mathbf{u}'(t) = AP\mathbf{u}(t),$$

so

$$\mathbf{u}'(t) = P^{-1}AP\mathbf{u}(t),$$

which gives

$$\begin{pmatrix} u_1'(t) \\ u_2'(t) \end{pmatrix} = \begin{pmatrix} 2 & 0 \\ 0 & 3 \end{pmatrix} \begin{pmatrix} u_1(t) \\ u_2(t) \end{pmatrix}.$$

Looking at this carefully, we see that we now have two very simple differential equations to solve; simple because we have managed to "unhook" $u_1(t)$ from $u_2(t)$. The equations are

$$\begin{aligned} u_1'(t) &= 2u_1(t) \\ u_2'(t) &= 3u_2(t) \end{aligned}$$

Both of these differential equation are of the you have already dealt with in first year. The general solutions for u_1 and u_2 are

$$\begin{aligned} u_1(t) &= b_1 e^{2t} \\ u_2(t) &= b_2 e^{3t}, \end{aligned}$$

where b_1 and b_2 are arbitrary constants. We must now convert this solution to a solution for x_1 and x_2 to finish the problem. We can do this as follows: we know that

$$\mathbf{u} = \begin{pmatrix} b_1 e^{2t} \\ b_2 e^{3t} \end{pmatrix} = \begin{pmatrix} b_1 \\ 0 \end{pmatrix} e^{2t} + \begin{pmatrix} 0 \\ b_2 \end{pmatrix} e^{3t}.$$

But $\mathbf{x}(t) = P\mathbf{u}(t)$, so we get

$$\begin{aligned} \mathbf{x}(t) &= \begin{pmatrix} 1 & 1 \\ -1 & -2 \end{pmatrix} \left[\begin{pmatrix} b_1 \\ 0 \end{pmatrix} e^{2t} + \begin{pmatrix} 0 \\ b_2 \end{pmatrix} e^{3t} \right] \\ &= b_1 \begin{pmatrix} 1 \\ -1 \end{pmatrix} e^{2t} + b_2 \begin{pmatrix} 1 \\ -2 \end{pmatrix} e^{3t} \end{aligned}$$

It's not hard to see how the final solution has turned out: the eigenvalues of A crop up as the constants k in the e^{kt} terms and the columns of P occur as "vector" coefficients of the corresponding e^{kt} terms. One can develop this theory quite far, but the above example illustrates all the important points.

Of course, if the matrix A **cannot** be diagonalized, then this method fails. There are methods to get round this problem. One of them involves using special invertible matrices (called orthogonal matrices) to "upper triangularize" A, and then some more theory of differential equations can get you to solutions. You may see this approach in a course on differential equations.

We have presented only two applications of diagonalization. There are many, many more. We hope that these examples will convey something of the usefulness of eigenvalues, eigenvectors and diagonalization, and that you will be able to appreciate these ideas when you meet them again in other disciplines.

Summary:

In this section we have considered two applications of diagonalization:

- *Markov matrices* are square matrices with non-negative entries which have the property that the sum of the entries in each column is 1. Such matrices always have 1 as an eigenvalue, and the corresponding eigenvector describes a *steady state* of the process described by the matrix.

- If a system of differential equations has a coefficient matrix that can be diagonalized, diagonalization can be used to "separate" the variables and hence to solve the system as a set of single differential equations.

Historical notes

Andrei Andreyevich Markov (1856–1922)

Andrei Markov was born in Ryazan, Russia and grew up in St Petersburg. As a child his health was poor and he had to walk with crutches. He showed outstanding ability in mathematics (although he performed poorly in other subjects). His younger brother Vladimir was also an outstanding mathematician, but died at the age of 25 from tuberculosis. Andrei wrote his first paper in mathematics while still at school, and went on to study Mathematics and Physics at the University of St Petersburg. He studied under the Chebyshev, who thought highly of him. In 1880 he started teaching at the university and was appointed a professor there in 1893. He formally retired in 1905, but kept on teaching for most of his life.

Markov's early work was in number theory and analysis, but he is best remembered for his ground-breaking work in probability theory, and particularly for his work on Markov chains, which was the beginning of the theory of stochastic processes. He was interested in poetry as well, and applied some of his mathematical ideas to the study of poetic styles.

Markov lived during a turbulent time in Russia and held strong views which he expressed without fear. It was only his high standing as an academician and his age which saved him from severe punishment by the Tsarist authorities. During the Russian Revolution he insisted on being sent to a small country town to teach mathematics in the secondary school there, without receiving any pay. He returned to St Petersburg when his health deteriorated, and kept on lecturing at the university until his death.

Exercises

1. If
$$A = \begin{pmatrix} 1 & -2 & 8 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix},$$
find
(a) A^{1000} (b) A^{-1000} (c) A^{2301} (d) A^{-2301}.

2. Given $M = \begin{pmatrix} \frac{1}{3} & \frac{1}{2} \\ \frac{2}{3} & \frac{1}{2} \end{pmatrix}$.

   (a) Diagonalize M.

   (b) Find $\lim_{n\to\infty} M^n$ and $\lim_{n\to\infty} M^n \begin{pmatrix} x_0 \\ y_0 \end{pmatrix}$.

3. (**Genetics**) Consider a plant that can have red flowers (R), pink flowers (P), or white flowers (W) depending upon the genotypes RR, RW, and WW. When we cross each of these genotypes with a genotype RW, we obtain the transition matrix

		Flowers	of parent	plant
		R	P	W
Flowers of	R	0.5	0.25	0.0
offspring	P	0.5	0.50	0.5
plant	W	0.0	0.25	0.5

   Suppose that each successive generation is produced by crossing only with plants of RW genotype. When the process reaches equilibrium, what percentage of the plants will have red, pink, or white flowers?

4. **(Mass Transport)** A new mass transport system (using busses, trains, taxis) has just gone into operation. The transport authority has made studies that predict the percentage of commuters who will change to mass transport (M) or continue driving their cars (C). The following transition matrix has been obtained:

		This	year
		M	C
Next	M	0.7	0.2
year	C	0.3	0.8

   Suppose that the population of the area remains constant, and that initially 30 percent of the commuters use mass transport and 70 percent use their cars.

(a) What percentage of the commuters will be using the mass transport system after 1 year? After 2 years?

(b) What percentage of the commuters will be using the mass transport system in the long run?

5. (a) Show that, for any square matrix A, A and A^T have the same eigenvalues.

   (b) Show that any Markov matrix has $\lambda = 1$ as an eigenvalue. [**Hint:** Consider the product $A^T\mathbf{x}$, where $\mathbf{x}$ is a vector all of whose entries are 1, and use (a).]

6. Find the general solution to the homogeneous linear system of differential equations
$$\begin{pmatrix} x_1' \\ x_2' \\ x_3' \end{pmatrix} = \begin{pmatrix} 4 & 0 & 0 \\ 3 & -5 & 0 \\ 2 & 1 & 2 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix}.$$

7. Consider two competing species that live in the same forest and let $x_1(t)$ and $x_2(t)$ denote the respective populations of the species at time t. Suppose that the initial populations are $x_1(0) = 500$ and $x_2(0) = 200$. If the growth rates of the species are given by
$$\begin{aligned} x_1'(t) &= -3x_1(t) + 6x_2(t) \\ x_2'(t) &= x_1(t) - 2x_2(t), \end{aligned}$$
what is the population of each species at time t?

Revision Exercises

1. Let $A = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 3 & 0 & 1 \end{pmatrix}$.

   (a) Find the eigenvalues and associated eigenvectors of A. Show your working.

   (b) Find a matrix P which diagonalizes A; give also the diagonalized form, D, of A.

   (c) Is there a basis for $\mathbf{R}^3$ consisting of eigenvectors of this matrix A? Justify your answer.

   (d) We call a line through the origin in $\mathbf{R}^3$ *invariant under a matrix B* if, whenever $\mathbf{x}$ lies on the line, $B\mathbf{x}$ also lies on the line. Does $\mathbf{R}^3$ have any lines that are invariant under the given matrix A? If so, find them; if not, explain why not.

2. Prove that, if G and H are invertible $n \times n$ matrices such that $GH = HG$, then, if $\mathbf{x}$ is an eigenvector of G, it follows that $H\mathbf{x}$ is an eigenvector of G.

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

   (a) Find all the eigenvalues of A, and the eigenspace corresponding to each eigenvalue.

   (b) Is A diagonalizable? If it is, give an invertible matrix P which diagonalizes A; if not, say why not.

   (c) Let the linear transformation $T : \mathbf{R}^3 \to \mathbf{R}^3$ be defined by $T\mathbf{x} = A\mathbf{x}$. Is there a basis B for $\mathbf{R}^3$ such that ${}_B[T]_B$ is a diagonal matrix D? If so, give B and D; if not, say why not.

Chapter 5

Inner product spaces

5.1 Inner product spaces

One of the useful features about working in $\mathbf{R}^2$ and $\mathbf{R}^3$ is the ability to talk about angles between vectors. In particular, it is really useful to know when two vectors are perpendicular. This knowledge enables us to resolve a given vector into vectors parallel and perpendicular to another given vector. The applications of being able to resolve vectors in this way are quite numerous. (If you've forgotten about this, read your first-year notes on vectors and components again.)

The fundamental idea underlying all these techniques was the notion of the *dot product* of two vectors. Recall that for two vectors (x_1, x_2, x_3) and (y_1, y_2, y_3) in $\mathbf{R}^3$ the their dot product is given by

$$(x_1, x_2, x_3) \cdot (y_1, y_2, y_3) = x_1y_1 + x_2y_2 + x_3y_3.$$

(For convenience we'll sometimes write the elements of $\mathbf{R}^3$, and more generally $\mathbf{R}^n$, as row vectors rather than column vectors.)

Can we talk about dot products in other vector spaces? Fortunately there are many vector spaces in which we can do this in quite natural ways. It is these ideas that we want to explore in this chapter. We'll set up the basic idea in this section and look more specifically at orthogonality in the next section.

Now how do we go about setting up an idea of a dot product in a general vector space? The approach we use is quite common in any field of mathematics, when faced with a similar question. You have already seen something of this in the section on vector spaces. Here is the gist of it. We have a useful concept in a specific situation (in this case that of a dot product in $\mathbf{R}^3$). We look at what we use most often when working with this concept in the particular situation. In the present case we look at the useful properties of the dot product in $\mathbf{R}^3$. The next step is to see if we can't set up a definition of the concept (in this case the dot product) in more general situations (in this case in general vector spaces) which embodies all these useful properties.

What properties of dot products do we use most often? The following list provides an answer. You should check that the dot product of two vectors $\mathbf{u}$ and $\mathbf{v}$ in $\mathbf{R}^2$ or $\mathbf{R}^3$ satisfies all these properties.

1. The dot product of two vectors is a *number* that depends on the two vectors. The dot product of $\mathbf{u}$ and $\mathbf{v}$ is a number denoted by $\mathbf{u} \cdot \mathbf{v}$. To put it more precisely, the dot product on $\mathbf{R}^3$ is a function from $\mathbf{R}^3 \times \mathbf{R}^3$ to $\mathbf{R}$.
2. $\mathbf{u} \cdot \mathbf{v} = \mathbf{v} \cdot \mathbf{u}$ for any two vectors $\mathbf{u}, \mathbf{v}$.
3. $(\mathbf{u} + \mathbf{v}) \cdot \mathbf{w} = \mathbf{u} \cdot \mathbf{w} + \mathbf{v} \cdot \mathbf{w}$ for any three vectors $\mathbf{u}, \mathbf{v}$ and $\mathbf{w}$.
4. $(\lambda \mathbf{u}) \cdot \mathbf{v} = \lambda(\mathbf{u} \cdot \mathbf{v}) = \mathbf{u} \cdot (\lambda \mathbf{v})$ for any scalar λ and any two vectors $\mathbf{u}, \mathbf{v}$.
5. $\mathbf{v} \cdot \mathbf{v} \geq 0$ for any vector $\mathbf{v}$ and $\mathbf{v} \cdot \mathbf{v} = 0$ iff $\mathbf{v} = \mathbf{0}$.

Since the above five conditions seem to be what one uses all the time when working with dot products, as mathematicians, we turn it all round and say that anything that satisfies the above five conditions ought to be called a dot product. It is common in a general vector space, though, to talk about *inner products* rather than dot products, and to write $\langle \mathbf{u}, \mathbf{v} \rangle$ for the inner product of $\mathbf{u}$ and $\mathbf{v}$, rather than $\mathbf{u} \cdot \mathbf{v}$. Here is the definition:

Definition 5.1.1 *An* ***inner product*** *on a vector space V over* $\mathbf{R}$ *is a function that associates a real number $\langle \mathbf{u}, \mathbf{v} \rangle$ with each ordered pair of vectors* $\mathbf{u}$ *and* $\mathbf{v}$ *in V in such a way that the following conditions are satisfied for all vectors* $\mathbf{u}, \mathbf{v}$ *and* $\mathbf{w}$ *in V and all scalars (real numbers) λ:*

1. $\langle \mathbf{u}, \mathbf{v} \rangle = \langle \mathbf{v}, \mathbf{u} \rangle$ *(Symmetry)*
2. $\langle \mathbf{u} + \mathbf{v}, \mathbf{w} \rangle = \langle \mathbf{u}, \mathbf{w} \rangle + \langle \mathbf{v}, \mathbf{w} \rangle$ *(Additivity)*
3. $\langle \lambda \mathbf{u}, \mathbf{v} \rangle = \lambda \langle \mathbf{u}, \mathbf{v} \rangle$
4. $\langle \mathbf{v}, \mathbf{v} \rangle \geq 0$*, and* $\langle \mathbf{v}, \mathbf{v} \rangle = 0$ *iff* $\mathbf{v} = \mathbf{0}$*.*

If there is an inner product defined on a vector space, we say the vector space is equipped *with an inner product. Any vector space equipped with an inner product is called an* ***inner product space****.*

We made a bit of a fuss about the fact that the scalars were real in the above definition. In the case where the scalars are complex numbers, one of the above conditions have to be modified slightly to be useful. An inner product on a complex vector space is a function that associates a *complex* number $\langle \mathbf{u}, \mathbf{v} \rangle$ with each ordered pair of vectors $\mathbf{u}$ and $\mathbf{v}$ in V in such a way that the same conditions as in the definition above are satisfied, except that the first one is replaced by

$1'$. $\langle \mathbf{u}, \mathbf{v} \rangle = \overline{\langle \mathbf{v}, \mathbf{u} \rangle}$.

(Recall that the complex conjugate of a complex number $z = a + ib$ is given by $\overline{z} = a - ib$.) This means that the inner product on a complex inner product space is no longer symmetric. You may be somewhat surprised by this condition and wonder what the motivation is for this. Here is part of the story: If we take $\mathbf{v} = \mathbf{u}$ in the condition 1' above, we get

$$\langle \mathbf{u}, \mathbf{u} \rangle = \overline{\langle \mathbf{u}, \mathbf{u} \rangle},$$

from which we can deduce that $\langle \mathbf{u}, \mathbf{u} \rangle \in \mathbf{R}$; if this were not the case, the condition 4 would not hold.

Much of the theory of real and complex inner product spaces is the same as that for real inner product spaces. In what follows we'll point out specifically where there is a difference between the real and complex case. In the examples in the rest of this chapter we'll concentrate mainly on real inner product spaces, but will mention complex spaces occasionally.

We look now at some examples of inner products in different settings.

Example 5.1.2 In $\mathbf{R}^2$, we can put

$$\langle (x_1, y_1), (x_2, y_2) \rangle = x_1 x_2 + y_1 y_2$$

and this satisfies all the conditions of an inner product, and the same is true for the dot product in $\mathbf{R}^3$ defined at the start of the section. (This is where the original idea came from!) Similarly, in $\mathbf{R}^n$, let $\mathbf{u} = (u_1, u_2, \ldots, u_n)$ and $\mathbf{v} = (v_1, v_2, \ldots, v_n)$. Then, if we put

$$\langle \mathbf{u}, \mathbf{v} \rangle = u_1 v_1 + u_2 v_2 + \ldots + u_n v_n,$$

this defines an inner product. The proof is an exercise.

In the complex vector space $\mathbf{C}^n$ (see Example 4.2.1.) we can define an inner product as follows: for $\mathbf{u} = (u_1, u_2, \ldots, u_n)$ and $\mathbf{v} = (v_1, v_2, \ldots, v_n)$ in $\mathbf{C}^n$, put

$$\langle \mathbf{u}, \mathbf{v} \rangle = u_1\overline{v_1} + u_2\overline{v_2} + \ldots + u_n\overline{v_n}.$$

Then you can check that this is indeed an inner product on the complex vector space $\mathbf{C}^n$.

Example 5.1.3 In $\mathbf{R}^2$ define $\langle (x_1, y_1), (x_2, y_2) \rangle = 3x_1x_2 + 5y_1y_2$. This defines an inner product on $\mathbf{R}^2$, since it satisfies all the conditions. Let's just check, say, the second one: let $\mathbf{u} = (x_1, y_1)$, $\mathbf{v} = (x_2, y_2)$ and $\mathbf{w} = (x_3, y_3)$. Then

$$\begin{aligned} \langle \mathbf{u}, \mathbf{v} + \mathbf{w} \rangle &= \langle (x_1, y_1), (x_2 + x_3, y_2 + y_3) \rangle \\ &= 3x_1(x_2 + x_3) + 5y_1(y_2 + y_3) \\ &= 3x_1x_2 + 3x_1x_3 + 5y_1y_2 + 5y_1y_3 \end{aligned}$$

and

$$\langle \mathbf{u}, \mathbf{v} \rangle + \langle \mathbf{u}, \mathbf{w} \rangle = 3x_1x_2 + 5y_1y_2 + 3x_1x_3 + 5y_1y_3$$

so the second condition is indeed satisfied.

Example 5.1.4 We can define an inner product on $C[a, b]$ (the vector space of all continuous functions $f : [a, b] \to \mathbf{R}$) as follows: let

$$\langle f, g \rangle = \int_a^b f(t)g(t)\,dt.$$

This is certainly a real number, and we can now check the four conditions needed. For instance, it's pretty clear that $\langle f, g \rangle = \langle g, f \rangle$. Also,

$$\begin{aligned} \langle f + g, h \rangle &= \int_a^b (f(t) + g(t))(h(t))\,dt \\ &= \int_a^b (f(t)h(t) + g(t)h(t))\,dt \\ &= \int_a^b f(t)h(t)\,dt + \int_a^b g(t)h(t)\,dt \\ &= \langle f, h \rangle + \langle g, h \rangle \end{aligned}$$

The third condition is also easy to check. To check condition (4) you will need to know that if the integral of a non-negative continuous function is zero, the function must be the function which equals zero at every point. The proof of this is beyond the scope of this course, but those of you doing real analysis may well get to prove this there.

Here now are some useful facts about inner products which follow directly from the definition:

Theorem 5.1.5 *Let* $\mathbf{u}, \mathbf{v}$ *and* $\mathbf{w}$ *be vectors in a real inner product space* V *and let* λ *be a scalar (a real number). Then:*

(a) $\langle \mathbf{0}, \mathbf{v} \rangle = \langle \mathbf{v}, \mathbf{0} \rangle = 0$

(b) $\langle \mathbf{u}, \mathbf{v} + \mathbf{w} \rangle = \langle \mathbf{u}, \mathbf{v} \rangle + \langle \mathbf{u}, \mathbf{w} \rangle$

(c) $\langle \mathbf{u}, \lambda\mathbf{v} \rangle = \lambda\langle \mathbf{u}, \mathbf{v} \rangle$

(d) $\langle \mathbf{u} - \mathbf{v}, \mathbf{w} \rangle = \langle \mathbf{u}, \mathbf{w} \rangle - \langle \mathbf{v}, \mathbf{w} \rangle$

(e) $\langle \mathbf{u}, \mathbf{v} - \mathbf{w} \rangle = \langle \mathbf{u}, \mathbf{v} \rangle - \langle \mathbf{u}, \mathbf{w} \rangle$

(f) If $\langle \mathbf{v}, \mathbf{w} \rangle = 0$ **for all** $\mathbf{w} \in V$, then $\mathbf{v} = \mathbf{0}$.

Proof: We'll prove only (b), (c) and (f):
(b) $\langle \mathbf{u}, \mathbf{v} + \mathbf{w} \rangle = \langle \mathbf{v} + \mathbf{w}, \mathbf{u} \rangle = \langle \mathbf{v}, \mathbf{u} \rangle + \langle \mathbf{w}, \mathbf{u} \rangle = \langle \mathbf{u}, \mathbf{v} \rangle + \langle \mathbf{u}, \mathbf{w} \rangle$
You can see that the trick was to use commutativity of the inner product to get what we wanted. The same idea is used to prove (c):
(c) $\langle \mathbf{u}, \lambda\mathbf{v} \rangle = \langle \lambda\mathbf{v}, \mathbf{u} \rangle = \lambda\langle \mathbf{v}, \mathbf{u} \rangle = \lambda\langle \mathbf{u}, \mathbf{v} \rangle$.
(f) If $\langle \mathbf{v}, \mathbf{w} \rangle = 0$ for all $\mathbf{w} \in V$, then, in particular, $\langle \mathbf{v}, \mathbf{v} \rangle = 0$, but we know this means $\mathbf{v} = \mathbf{0}$, which is what we wanted. ■

With the exception of the third one, the facts proved above for real inner product spaces also hold for complex inner product spaces. The third one has to be modified as follows: If $\mathbf{u}$ and $\mathbf{v}$ are vectors in a complex inner product space and λ is a complex scalar, then $\langle \mathbf{u}, \lambda\mathbf{v} \rangle = \overline{\lambda}\langle \mathbf{u}, \mathbf{v} \rangle$. This follows from

$$\langle \mathbf{u}, \lambda\mathbf{v} \rangle = \overline{\langle \lambda\mathbf{v}, \mathbf{u} \rangle} = \overline{\lambda\langle \mathbf{v}, \mathbf{u} \rangle} = \overline{\lambda}\,\overline{\langle \mathbf{v}, \mathbf{u} \rangle} = \overline{\lambda}\langle \mathbf{u}, \mathbf{v} \rangle.$$

We move on to two famous inequalities which hold in any inner product space. You've met them both before in the context of dot products in $\mathbf{R}^2$ and $\mathbf{R}^3$. Before we get to the two inequalities, let's remind ourselves about lengths of vectors. In $\mathbf{R}^2$ we know that the length of $\mathbf{v} = (x, y)$ is just $\sqrt{x^2 + y^2}$; this can also be written as $\sqrt{\langle \mathbf{v}, \mathbf{v} \rangle}$. The same is true in $\mathbf{R}^3$. This leads us to define a length of a vector in $\mathbf{R}^n$, for any n, and, in fact, for any vector in an inner product space, in a similar way. In this setting, we talk about the *norm* of a vector.

Definition 5.1.6 *Let V be an inner product space and let $\mathbf{v} \in V$. The* ***norm*** *of* $\mathbf{v}$*, written $\|\mathbf{v}\|$ is given by*

$$\|\mathbf{v}\| = \sqrt{\langle \mathbf{v}, \mathbf{v} \rangle}.$$

In $\mathbf{R}^2$ and $\mathbf{R}^3$, the norm of a vector is just the length of the vector as we said earlier; in higher dimensions, one struggles to visualize length, but you won't be far wrong if you think of the norm of a vector as specifying its "size".

We now give you the two inequalities promised.

Theorem 5.1.7 *Let $\mathbf{u}$ and $\mathbf{v}$ be vectors in an inner product space. Then we have:*

(a) $|\langle \mathbf{u}, \mathbf{v} \rangle| \leq \|\mathbf{u}\| \, \|\mathbf{v}\|$ *(Cauchy-Schwarz inequality.)*

(b) $\|\mathbf{u} + \mathbf{v}\| \leq \|\mathbf{u}\| + \|\mathbf{v}\|$ *(Triangle inequality.)*

Proof: We include the proofs for the sake of completeness, but mention that they are identical to the proofs you saw last year in your first year course.

(a) If either $\mathbf{u}$ or $\mathbf{v}$ is $\mathbf{0}$ then both $\langle \mathbf{u}, \mathbf{v} \rangle$ and $\|\mathbf{u}\|\|\mathbf{v}\|$ are zero. So suppose both $\mathbf{u}$ and $\mathbf{v}$ are non-zero. Let $\mathbf{w} = \mathbf{u} - \lambda \mathbf{v}$ where λ is a scalar. We know that $\langle \mathbf{w}, \mathbf{w} \rangle \geq 0$ so:

$$\begin{aligned}
0 &\leq \langle \mathbf{u} - \lambda \mathbf{v}, \mathbf{u} - \lambda \mathbf{v} \rangle \\
&= \langle \mathbf{u}, \mathbf{u} \rangle - \lambda \langle \mathbf{v}, \mathbf{u} \rangle - \overline{\lambda} \langle \mathbf{u}, \mathbf{v} \rangle + |\lambda|^2 \langle \mathbf{v}, \mathbf{v} \rangle \\
&= \langle \mathbf{u}, \mathbf{u} \rangle - \lambda \langle \mathbf{v}, \mathbf{u} \rangle - \overline{\lambda \langle \mathbf{v}, \mathbf{u} \rangle} + |\lambda|^2 \langle \mathbf{v}, \mathbf{v} \rangle \\
&= \langle \mathbf{u}, \mathbf{u} \rangle - 2\mathrm{Re}(\lambda \langle \mathbf{v}, \mathbf{u} \rangle) + |\lambda|^2 \langle \mathbf{v}, \mathbf{v} \rangle \\
&= ||\mathbf{u}||^2 - 2\mathrm{Re}(\lambda \langle \mathbf{v}, \mathbf{u} \rangle) + |\lambda|^2 ||\mathbf{v}||^2
\end{aligned}$$

Now let $\lambda = \dfrac{\overline{\langle \mathbf{v}, \mathbf{u} \rangle}}{\langle \mathbf{v}, \mathbf{v} \rangle}$ in the above. Then

$$\begin{aligned}
0 &\leq ||\mathbf{u}||^2 - 2\mathrm{Re}\left(\frac{|\langle \mathbf{v}, \mathbf{u} \rangle|^2}{||\mathbf{v}||^2} \right) + \frac{|\langle \mathbf{v}, \mathbf{u} \rangle|^2}{||\mathbf{v}||^4} ||\mathbf{v}||^2 \\
&= ||\mathbf{u}||^2 - \frac{|\langle \mathbf{v}, \mathbf{u} \rangle|^2}{||\mathbf{v}||^2}
\end{aligned}$$

Thus we have

$$0 \leq ||\mathbf{u}||^2 ||\mathbf{v}||^2 - |\langle \mathbf{v}, \mathbf{u} \rangle|^2$$

which can be written as

$$|\langle \mathbf{u}, \mathbf{v}\rangle|^2 = |\langle \mathbf{v}, \mathbf{u}\rangle|^2 \leq \|\mathbf{u}\|^2 \|\mathbf{v}\|^2$$

Taking positive square roots gives the result we want.

(b) By the Cauchy-Schwartz inequality,

$$\langle \mathbf{u}, \mathbf{v}\rangle \leq |\langle \mathbf{u}, \mathbf{v}\rangle| \leq \|\mathbf{u}\| \, \|\mathbf{v}\|.$$

Thus

$$\begin{aligned} \|\mathbf{u}+\mathbf{v}\|^2 &= \langle \mathbf{u}+\mathbf{v}, \mathbf{u}+\mathbf{v}\rangle \\ &= \langle \mathbf{u}, \mathbf{u}\rangle + 2\langle \mathbf{u}, \mathbf{v}\rangle + \langle \mathbf{v}, \mathbf{v}\rangle \\ &\leq \|\mathbf{u}\|^2 + 2\|\mathbf{u}\| \, \|\mathbf{v}\| + \|\mathbf{v}\|^2 \\ &= (\|\mathbf{u}\| + \|\mathbf{v}\|)^2 \end{aligned}$$

Thus $\|\mathbf{u}+\mathbf{v}\|^2 \leq (\|\mathbf{u}\| + \|\mathbf{v}\|)^2$ and taking positive square roots gives us the desired result. ■

Summary:

In this section we

- used the properties of the dot product in $\mathbf{R}^2$ and $\mathbf{R}^3$ to motivate and give the definition of an *inner product* in a vector space (and noted the difference between real and complex inner products);
- derived some useful identities and inequalities (including the Cauchy-Swartz and triangle inequalities) that hold in any inner product space.

Historical notes

Augustin Louis Cauchy (1789–1857)

Cauchy was born in Paris at the time of the French Revolution. When he was four, conditions in Paris became so dangerous that the family moved to Arcuiel. There conditions were so hard that they soon returned to Paris. Cauchy's father took an active interest in his son's education, and sought advice from the mathematicians Laplace and Lagrange. Cauchy's formal education started with two years devoted to classical languages, after which he studied mathematics at the Ecole Polytechnique and engineering at the Ecole des Ponts et Chaussèes. After graduation he took on a job at Cherbourg, where he worked on harbour facilities for Napoleon's fleet. Although he worked extremely hard, he made time for mathematical research and published his first paper.

In September 1812 Cauchy became ill and returned to Paris. While recuperating he continued his research and published a further paper. He did not want to return to Cherbourg, and managed to obtain a posting to the Ourcq Canal project, where he worked as a student earlier. Cauchy wanted an academic position, but failed in a number of applications. He did manage to obtain further sick leave, and a stoppage on the canal project caused by political events gave him two years in which to do research. One of the important achievements of this time was a memoir on integration which became the basis of his theory of complex functions.

In 1815 he did manage to secure a position at the Ecole Polytechnique, and the next year was awarded a prize by the French Academy of Sciences for a paper on waves. This was followed by a solution to a problem posed by Fermat, and election to the French Academy of Sciences.

In 1817 he obtained a post at the Collège de France. His textbook *Cours d'analyse* of 1821 attempted to establish a rigorous foundation for the study of the calculus. This included a rigorous definition of the notion of an integral, and a rigorous treatment of convergence of infinite series.

Cauchy's relations with his fellow scientists were not particularly good. He was a staunch Catholic and tended to bring religion into his work. He supported the Jesuits in their attack on the Academy of Sciences. His manner was often abrupt and very critical, and the young mathematicians Abel and Galois amongst others were treated badly by him.

After the revolution of 1830, Cauchy decided to leave Paris and he spent some time in Switzerland. When he returned to Paris, he was asked to swear an oath of allegiance to the new government. When he refused to do this, he lost all his positions. He went to Turin, and was appointed professor of theoretical physics there in 1832. The next year he went from there to Prague to tutor the grandson of Charles

X, but Cauchy's quick temper and the prince's lack of interest meant that this was not a particularly successful venture. Cauchy returned to Paris in 1838, but could not teach because he still refused to take the oath of allegiance. This even meant that he could not take up a new position to which he was appointed. His religious and political views also resulted in him not being appointed to a professorship at the Collège de France, even though he was the best candidate. He continued to do research in mathematical physics, astronomy and differential equations.

Political changes in France in 1848 led to Cauchy regaining his old appointments. When he applied for the chair at the Collège de France in 1850, he narrowly lost out to Liouville, and this soured relations between them. Another dispute (in which Cauchy was proved to be wrong) led to a great deal of bitterness in the last years of Cauchy's life. He died in 1857. His name lives on in many terms in mathematics, like Cauchy sequences, the Cauchy-Schwarz inequality, the Cauchy-Riemann equations and the Cauchy integral formula. He contributed to all the then-known areas of mathematics, and his contributions show an amazing creativity and insight.

Hermann Amandus Schwarz (1843–1921)

Hermann Schwarz was born in Hermsdorf (now in Poland), the son of an architect. When he left school he started studying chemistry in Berlin. There he was soon won over to mathematics by the famous mathematicians Weierstrass and Kummer. He became interested in the links between geometry and analysis and obtained a doctorate under Weierstrass in 1864. After that he obtained his teacher's training qualification and was appointed at the University of Halle. From there he moved to Zurich, and in 1875 he was appointed as professor at the University of Göttingen. In 1892 he succeeded Weierstrass in Berlin, where he taught until 1918.

Schwarz's earlier work was in the calculus of variation, and particular in the study of minimal surfaces. He made import contributions to the study of conformal mappings (in complex analysis), and discovered a special case of the inequality now known as the Cauchy-Schwarz inequality.

Exercises

1. Show that
$$\langle A, B\rangle = a_{11}b_{11} + a_{12}b_{12} + a_{21}b_{21} + a_{22}b_{22},$$
defines an inner product on $M_{2\times 2}$, where $A = \begin{pmatrix} a_{ij} \end{pmatrix}, B = \begin{pmatrix} b_{ij} \end{pmatrix}$.

2. Let $\mathbf{u} = (u_1, u_2, u_3)$ and $\mathbf{v} = (v_1, v_2, v_3)$. Determine if
$$\langle \mathbf{u}, \mathbf{v}\rangle = u_1^2v_1^2 + u_2^2v_2^2 + u_3^2v_3^2$$
defines an inner product on $\mathbf{R}^3$. If not, list the axioms that do not hold. Remember to give counterexamples for those axioms that do not hold.

3. Let $p(x) = a_0 + a_1x + a_2x^2$ and $q(x) = b_0 + b_1x + b_2x^2$ be in P_2. For each of the following, decide whether it defines an inner product on P_2. If not, what fails?
   (a) $\langle p, q\rangle = p(0)q(0) + p(1)q(1) + p(2)q(2)$.
   (b) $\langle p, q\rangle = p(0)q(0)$.

4. Let $p(x) = a_0 + a_1x$ and $q(x) = b_0 + b_1x$. Decide if $\langle p, q\rangle = \int_{-1}^{1} p(x)q(x)\ dx$ defines an inner product on P_1. If not, what fails?

5. Suppose that $\mathbf{u}, \mathbf{v}$ and $\mathbf{w}$ are vectors such that
$$\langle \mathbf{u}, \mathbf{v}\rangle = 2,\ \langle \mathbf{v}, \mathbf{w}\rangle = -3,\ \langle \mathbf{u}, \mathbf{w}\rangle = 5, \|\mathbf{u}\| = 1, \|\mathbf{v}\| = 2, \|\mathbf{w}\| = 7$$
Evaluate each of the following using this information:
(a) $\langle \mathbf{u}+\mathbf{v}, \mathbf{v}+\mathbf{w}\rangle$ (b) $\langle \mathbf{u}-\mathbf{v}-2\mathbf{w}, 4\mathbf{u}+\mathbf{v}\rangle$ (c) $\|2\mathbf{w}-\mathbf{v}\|$

6. Prove: $\|\lambda\mathbf{u}\| = |\lambda|\|\mathbf{u}\|$, for any scalar λ and vector $\mathbf{u}$ in an inner product space.

7. Check that $\mathbf{C}^n$ is a complex inner product space with the inner product defined in Example 4.1.2.

8. Show that the following identity holds for vectors $\mathbf{u}$ and $\mathbf{v}$ in any inner product space.
$$\|\mathbf{u}+\mathbf{v}\|^2 + \|\mathbf{u}-\mathbf{v}\|^2 = 2\|\mathbf{u}\|^2 + 2\|\mathbf{v}\|^2.$$

9. Let P_2 be equipped with the inner product defined by
$$\langle a_0 + a_1x + a_2x^2, b_0 + b_1x + b_2x^2\rangle = a_0b_0 + a_1b_1 + a_2b_2.$$
Verify that the Cauchy-Schwartz inequality holds for the vectors $p(x) = -1 + 2x + x^2$ and $q(x) = 2 - 4x^2$

5.2 Orthogonality and orthonormal bases.

We turn now to something you are already familiar with, that is, the idea of an angle between vectors. In fact, the idea of an angle between vectors is not as important in general vector spaces as it is in $\mathbf{R}^2$ or $\mathbf{R}^3$. What does remain of great importance though, is the notion of *perpendicularity* or *orthogonality*. Recall from your first year course that two vectors in $\mathbf{R}^2$ or $\mathbf{R}^3$ are perpendicular if their dot product is zero. We extend this idea to any inner product space.

Definition 5.2.1 *Let* $\mathbf{u}$ *and* $\mathbf{v}$ *be vectors in an inner product space* V*. We say that* $\mathbf{u}$ *and* $\mathbf{v}$ *are* ***orthogonal*** *if and only if* $\langle \mathbf{u}, \mathbf{v} \rangle = 0$*, i.e. if and only if their inner product is zero. We write this as* $\mathbf{u} \perp \mathbf{v}$*, i.e.*

$$\mathbf{u} \perp \mathbf{v} \quad \textit{if and only if} \quad \langle \mathbf{u}, \mathbf{v} \rangle = 0.$$

You are used to the idea of orthogonality or perpendicularity of vectors in $\mathbf{R}^2$ and $\mathbf{R}^3$, but it comes as quite a surprise that we can talk about orthogonality of polynomials for instance. We have a quick look at this in the next example.

Example 5.2.2 Let P_2 have the inner product

$$\langle p, q \rangle = \int_{-1}^{1} p(t)q(t)\,dt$$

and let $p(t) = t$ and $q(t) = t^2$. Then

$$\langle p, q \rangle = \int_{-1}^{1} tt^2\,dt = \int_{-1}^{1} t^3\,dt = 0$$

so the two polynomials are orthogonal. We also have

$$\|p\| = \sqrt{\langle p, p \rangle} = \sqrt{\int_{-1}^{1} t^2\,dt} = \sqrt{\frac{2}{3}}$$

and

$$\|q\| = \sqrt{\langle q, q \rangle} = \sqrt{\int_{-1}^{1} t^4\,dt} = \sqrt{\frac{2}{5}}.$$

It is easy to prove an analogue of the theorem of Pythagoras in an inner product space. Here it is:

Theorem 5.2.3 *Let* $\mathbf{u}$ *and* $\mathbf{v}$ *be vectors in an inner product space* V *such that* $\mathbf{u} \perp \mathbf{v}$ *. Then*

$$\|\mathbf{u}\|^2 + \|\mathbf{v}\|^2 = \|\mathbf{u} + \mathbf{v}\|^2.$$

Proof: We have

$$\begin{aligned} \|\mathbf{u} + \mathbf{v}\|^2 &= \langle \mathbf{u} + \mathbf{v}, \mathbf{u} + \mathbf{v} \rangle \\ &= \langle \mathbf{u}, \mathbf{u} \rangle + 2\langle \mathbf{u}, \mathbf{v} \rangle + \langle \mathbf{v}, \mathbf{v} \rangle \\ &= \langle \mathbf{u}, \mathbf{u} \rangle + \langle \mathbf{v}, \mathbf{v} \rangle \\ &= \|\mathbf{u}\|^2 + \|\mathbf{v}\|^2 \end{aligned}$$

(Where did we use $\mathbf{u} \perp \mathbf{v}$?) ■

Now that we know what it means to say that two vectors are orthogonal, we can extend the definition to any set of vectors.

Definition 5.2.4 *Let* S *be a set of distinct vectors in an inner product space* V*.*

1. *S is said to be* ***orthogonal*** *if every pair of distinct vectors in the set S is orthogonal.*
2. *A vector* $\mathbf{v}$ *is said to be* ***normal*** *if* $\|\mathbf{v}\| = 1$*.*
3. *S is* ***orthonormal*** *if S is orthogonal and each member of S is normal.*

The standard basis $\{(1, 0, 0), (0, 1, 0), (0, 0, 1)\}$ in $\mathbf{R}^3$ (and more generally the standard basis in $\mathbf{R}^n$) is particularly convenient to work with. This can be attributed mainly to the fact that this basis forms an orthonormal set. Conversely, we'll see that in general orthogonal (and orthonormal) sets of vectors have many of the desirable properties of the standard basis in $\mathbf{R}^n$.

Theorem 5.2.5 *If* $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n$ *are non-zero orthogonal vectors, then they are linearly independent.*

Proof: Suppose $\lambda_1, \lambda_2, \ldots, \lambda_n$ are scalars such that

$$\lambda_1\mathbf{v}_1 + \lambda_2\mathbf{v}_2 + \ldots + \lambda_n\mathbf{v}_n = \mathbf{0}.$$

We want to show that each λ_i is zero. Pick any $\mathbf{v}_i$. Then:

$$\begin{aligned} 0 = \langle \mathbf{0}, \mathbf{v}_i \rangle &= \langle (\lambda_1\mathbf{v}_1 + \lambda_2\mathbf{v}_2 + \ldots + \lambda_n\mathbf{v}_n), \mathbf{v}_i \rangle \\ &= \lambda_1\langle \mathbf{v}_1, \mathbf{v}_i \rangle + \lambda_2\langle \mathbf{v}_2, \mathbf{v}_i \rangle + \ldots + \lambda_n\langle \mathbf{v}_n, \mathbf{v}_i \rangle \\ &= \lambda_i\langle \mathbf{v}_i, \mathbf{v}_i \rangle \text{ since } \langle \mathbf{v}_j, \mathbf{v}_i \rangle = 0 \text{ whenever } i \neq j. \end{aligned}$$

But $\langle \mathbf{v}_i, \mathbf{v}_i \rangle \neq 0$ so $\lambda_i = 0$. Since i was arbitrary, we've proved that all the λ_i's are zero, so the vectors $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n$ are indeed linearly independent. ■

It's quite natural to talk now about orthonormal or orthogonal bases for a vector space, and they turn out to be really easy bases to work with.

Definition 5.2.6 *A basis B for a vector space V is **orthogonal** if the set B is orthogonal; it is **orthonormal** if B is orthonormal.*

Example 5.2.7 The standard basis for $\mathbf{R}^n$ is an orthonormal basis.

The set of vectors

$$S = \{(1,1,1,1), (-1,-1,1,1), (-1,1-1,1), (-1,1,1,-1)\}$$

in $\mathbf{R}^4$ is orthogonal (check it yourself) but is not orthonormal since each vector in S has norm 2. By the last theorem, this set is linearly independent. It is therefore an orthogonal basis for $\mathbf{R}^4$. We could modify S to make it an orthonormal basis for $\mathbf{R}^4$ by dividing each vector by its norm. Thus

$$B = \left\{ \frac{1}{2}(1,1,1,1), \frac{1}{2}(-1,-1,1,1), \frac{1}{2}(-1,1,-1,1), \frac{1}{2}(-1,1,1,-1) \right\}$$

is an orthonormal basis for $\mathbf{R}^4$.

We look now at an algorithm for transforming any (finite) basis of an inner product space into an orthonormal basis. The fact that we *can* do this means that any finite-dimensional inner product space space has an orthonormal basis. The procedure we use is known as the **Gram-Schmidt algorithm**.

Theorem 5.2.8 *Every (non-zero) finite-dimensional inner product space V has an orthonormal basis.*

Proof: We give the algorithm promised above:
Let $B = \{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n\}$ be any basis for V. We give a rule for determining a set $\{\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_n\}$ ($\mathbf{u}$ for "unit") of orthonormal vectors (which must then be an orthonormal basis).

STEP 1: $\mathbf{v}_1 \neq \mathbf{0}$ so we set $\mathbf{u}_1 = \dfrac{\mathbf{v}_1}{\|\mathbf{v}_1\|}$. Then $\mathbf{u}_1$ is surely normal.

STEP 2: Recall the projection of $\mathbf{v}_2$ onto $\mathbf{u}_1$ is

$$\frac{\langle \mathbf{v}_2, \mathbf{u}_1 \rangle}{\langle \mathbf{u}_1, \mathbf{u}_1 \rangle}\mathbf{u}_1 = \langle \mathbf{v}_2, \mathbf{u}_1 \rangle \mathbf{u}_1$$

since $\|\mathbf{u}_1\| = 1$. Then

$$\mathbf{w}_2 = \mathbf{v}_2 - \langle \mathbf{v}_2, \mathbf{u}_1 \rangle \mathbf{u}_1$$

is orthogonal to $\mathbf{u}_1$. (Check this if you like by taking the inner product, but this is the whole idea behind orthogonal projections.) Also, $\mathbf{w}_2$ is non-zero, since if it were zero, we would have a non-trivial linear combination of $\mathbf{v}_1$ and $\mathbf{v}_2$ yielding the zero vector, which contradicts the linear independence of the $\mathbf{v}_i$'s. We set

$$\mathbf{u}_2 = \frac{\mathbf{w}_2}{\|\mathbf{w}_2\|}.$$

This will be normal and still orthogonal to $\mathbf{u}_1$.

STEP 3: The projections of $\mathbf{v}_3$ onto $\mathbf{u}_1$ and $\mathbf{u}_2$ are respectively

$$\langle \mathbf{v}_3, \mathbf{u}_1 \rangle \mathbf{u}_1 \quad \text{and} \quad \langle \mathbf{v}_3, \mathbf{u}_2 \rangle \mathbf{u}_2.$$

If we subtract these two projections from $\mathbf{v}_3$ the resulting vector, $\mathbf{w}_3$, will be orthogonal to both $\mathbf{u}_1$ and $\mathbf{u}_2$, but only because $\mathbf{u}_1$ and $\mathbf{u}_2$ are orthonormal. Let's see why:

$$\begin{aligned}
\langle \mathbf{w}_3, \mathbf{u}_1 \rangle &= \langle \mathbf{v}_3 - \langle \mathbf{v}_3, \mathbf{u}_1 \rangle \mathbf{u}_1 - \langle \mathbf{v}_3, \mathbf{u}_2 \rangle \mathbf{u}_2 \,,\, \mathbf{u}_1 \rangle \\
&= \langle \mathbf{v}_3, \mathbf{u}_1 \rangle - \langle \mathbf{v}_3, \mathbf{u}_1 \rangle \langle \mathbf{u}_1, \mathbf{u}_1 \rangle - \langle \mathbf{v}_3, \mathbf{u}_2 \rangle \langle \mathbf{u}_2, \mathbf{u}_1 \rangle \\
&= 0.
\end{aligned}$$

The check for $\mathbf{u}_2$ is similar. Also $\mathbf{w}_3$ cannot be the zero vector because of the linear independence of $\mathbf{v}_1, \mathbf{v}_2$ and $\mathbf{v}_3$. We set

$$\mathbf{u}_3 = \frac{\mathbf{w}_3}{\|\mathbf{w}_3\|}.$$

STEPS 4 to n: Repeat as above with the obvious modifications.

The result is a set of n orthonormal vectors, which must be a basis for the original space. (Why?) ■

From the way the vectors $\mathbf{u}_i$ are defined, the following corollary is clear:

Corollary 5.2.9 *With the notation of Theorem 5.2.8, for each k such that $1 \le k \le n$ the set $\{\mathbf{u}_1, \ldots, \mathbf{u}_k\}$ spans the same subspace as the set $\{\mathbf{v}_1, \ldots, \mathbf{v}_k\}$.*

Let's do an example to see the Gram-Schmidt algorithm at work. The idea of the algorithm itself is quite simple; the calculations become rather messy, as you will notice. (You could write a macro for OCTAVE that does it for you, if you wanted to...)

Example 5.2.10 We apply the Gram-Schmidt procedure to the set of vectors

$$S = \{\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3\} \text{ in } \mathbf{R}^3, \text{ where } \mathbf{v}_1 = (1,1,1,1), \mathbf{v}_2 = (0,1,1,1), \mathbf{v}_3 = (0,0,1,1)\}.$$

Notice first that S is a linearly independent set in $\mathbf{R}^4$. It must be a basis for $V = \mathrm{span}(S)$, but $V \neq \mathbf{R}^4$ (why?). We find an orthonormal basis for V.

Since $\|\mathbf{v}_1\| = 2 \neq 1$, $\mathbf{v}_1$ is not normal. Put $\mathbf{u}_1 = \frac{1}{2}(1,1,1,1) = (\frac{1}{2}, \frac{1}{2}, \frac{1}{2}, \frac{1}{2})$. Then $\|\mathbf{u}_1\| = 1$.

Put

$$\begin{aligned}
\mathbf{w}_2 &= (0,1,1,1) - \left\langle \left(\frac{1}{2}, \frac{1}{2}, \frac{1}{2}, \frac{1}{2}\right), (0,1,1,1) \right\rangle \left(\frac{1}{2}, \frac{1}{2}, \frac{1}{2}, \frac{1}{2}\right) \\
&= (0,1,1,1) - \left(\frac{3}{4}, \frac{3}{4}, \frac{3}{4}, \frac{3}{4}\right) = \left(-\frac{3}{4}, \frac{1}{4}, \frac{1}{4}, \frac{1}{4}\right)
\end{aligned}$$

Now $\|\mathbf{w}_2\| = \dfrac{1}{2}\sqrt{3}$, so

$$\mathbf{u}_2 = \frac{\mathbf{w}_2}{\|\mathbf{w}_2\|} = \frac{\sqrt{3}}{6}(-3,1,1,1).$$

For $\mathbf{u}_3$, first compute $\langle (0,0,1,1), \mathbf{u}_1 \rangle$ and $\langle (0,0,1,1), \mathbf{u}_2 \rangle$. They are, respectively, 1 and $\dfrac{1}{3}\sqrt{3}$. Then

$$\begin{aligned}
\mathbf{w}_3 &= \mathbf{v}_3 - \langle \mathbf{v}_3, \mathbf{u}_1 \rangle \mathbf{u}_1 - \langle \mathbf{v}_3, \mathbf{u}_2 \rangle \mathbf{u}_2 \\
&= (0,0,1,1) - 1\left(\frac{1}{2}, \frac{1}{2}, \frac{1}{2}, \frac{1}{2}\right) - \left(\frac{1}{3}\sqrt{3}\right)\left(-\frac{1}{2}\sqrt{3}, \frac{1}{6}\sqrt{3}, \frac{1}{6}\sqrt{3}, \frac{1}{6}\sqrt{3}\right) \\
&= (0,0,1,1) - \left(\frac{1}{2}, \frac{1}{2}, \frac{1}{2}, \frac{1}{2}\right) - \left(-\frac{1}{2}, \frac{1}{6}, \frac{1}{6}, \frac{1}{6}\right) \\
&= \left(0, -\frac{2}{3}, \frac{1}{3}, \frac{1}{3}\right)
\end{aligned}$$

You can check that $\|\mathbf{w}_3\| = \dfrac{1}{3}\sqrt{6}$, so set

$$\mathbf{u}_3 = \frac{\mathbf{w}_3}{\|\mathbf{w}_3\|} = \frac{1}{\sqrt{6}}(0,-2,1,1).$$

The three orthonormalized vectors are $\mathbf{u}_1, \mathbf{u}_2$ and $\mathbf{u}_3$.

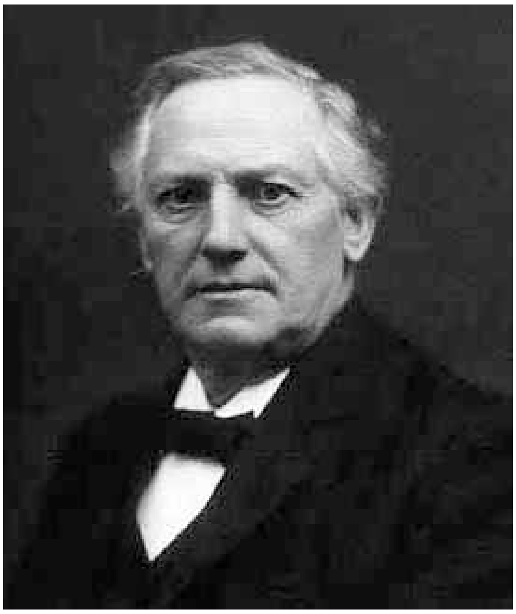
Summary:

In this section the important notions of *orthogonality* and *orthonormality* for two or more vectors in an inner product space was introduced. We saw

- that an analogue of Pythagoras's theorem holds in inner product spaces;
- that a set of orthogonal vectors is linearly independent;
- that every finite dimensional inner product space has an orthonormal basis. This result follows by an application of the Gramm-Schmidt orthonormalization algorithm to a basis for the space.

Historical notes

Jorgen Pedersen Gram (1850–1916)



Jorgen Gram was born in Nustrup in Denmark, the son of a farmer. He obtained a Master's degree in Mathematics in 1874. Even before this he published his first paper in algebra, on invariant theory. In 1875 he started working for an insurance company and soon his work there led him back to mathematics research, in particular in the areas of probability theory and numerical analysis. He also became fascinated by problems in forestry management and developed mathematical models which were later widely used. His work in number theory and numerical analysis led to an interest and substantial contributions to number theory.

Gram founded his own insurance company in 1884. He was the the Chairman of the Danish Insurance Council from 1910 until his death. Although he never held a university position and therefore never had any students, he had a positive influence on young Danish mathematicians. He was editor of a mathematics journal and highly regarded by the Danish mathematical community. Although he used the orthogonalisation process now known as the Gram-Schmidt algorithm, he was not the first to use it. He died tragically when struck and killed by a bicycle.

Erhard Schmidt (1876–1959)

Erhard Scmidt was born in what is now Tartu in Estonia, the son of a medical biologist. After attending his local university, he went to Berlin, where he studied under Schwarz. He then went to Göttingen where he obtained a doctorate under Hilbert on integral equations. After this he went to Bonn, and then had positions in Zurich, Erlangen and Breslau. In 1917 he succeeded Schwarz as professor in Berlin. It was he who was mainly responsible for the founding of the Institute for Applied Mathematics in Berlin. His talents were recognised outside his own field, and he was first appointed Dean in 1921, and then vice-chancellor of the university for the period 1929 – 1930. He stayed on in Berlin under very difficult circumstances during the Nazi era. After the war he was appointed as Director of the Mathematics research Institute of the German Academy of Sciences, where he remained until 1958.

Schmidt's main contribution to mathematics was in the area of integral equations and was responsible for the introduction of the notion of a Hilbert space. He made extensive use of eigenvalues and eigenfunctions in his solutions of integral equations. In a paper of 1907 he described the orthonormalisation process named after him. It was, however, Laplace who first used this method, before Gram or Schmidt. Later in his life Schmidt became interested in topology, and made contributions in this field as well.

Exercises

1. Let $\mathbf{u}$ and $\mathbf{v}$ be vectors in an inner product space.
   (a) Prove that $\|\mathbf{u}\| = \|\mathbf{v}\|$ if and only if $\mathbf{u}+\mathbf{v}$ and $\mathbf{u}-\mathbf{v}$ are orthogonal.
   (b) Give a geometric interpretation of this result in $\mathbf{R}^2$ with the usual inner product.
2. Let $\mathbf{R}^4$ have the usual inner product, and let $\mathbf{u} = (-1, 1, 0, 2)$. Determine

whether $\mathbf{u}$ is orthogonal to the set of vectors $S = \{\mathbf{w}_1, \mathbf{w}_2, \mathbf{w}_3\}$, where $\mathbf{w}_1 = (0, 0, 0, 0)$, $\mathbf{w}_2 = (1, -1, 3, 0)$, and $\mathbf{w}_3 = (4, 0, 9, 2)$.

3. Let V be an inner product space. Show that if $\mathbf{w}$ is orthogonal to each of the vectors $\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_r$, then it is orthogonal to every vector in span $\{\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_r\}$.

4. Let $\mathbf{R}^4$ have its usual inner product. In each case below, determine whether the given vectors form an orthogonal set.

   (a) $\mathbf{u}_1 = (1, 1, 1, 1)$, $\mathbf{u}_2 = (1, -1, 0, 0)$, $\mathbf{u}_3 = (1, 1, -2, 0)$, $\mathbf{u}_4 = (1, 1, 1, -3)$.

   (b) $\mathbf{w}_1 = (1, 2, 3, 4)$, $\mathbf{w}_2 = (-9, 1, 1, 1)$, $\mathbf{w}_3 = (1, -8, 1, 1)$, $\mathbf{w}_4 = (0, 1, -2, 1)$.

5. Let $\mathbf{x} = (\frac{1}{\sqrt{5}}, -\frac{1}{\sqrt{5}})$ and $\mathbf{y} = (\frac{2}{\sqrt{30}}, \frac{3}{\sqrt{30}})$.

   Show that $\{\mathbf{x}, \mathbf{y}\}$ is orthonormal if $\mathbf{R}^2$ has the inner product defined by $\langle \mathbf{u}, \mathbf{v} \rangle = 3u_1v_1 + 2u_2v_2$, for $\mathbf{u} = (u_1, u_2)$ and $\mathbf{v} = (v_1, v_2)$, but is not orthonormal if $\mathbf{R}^2$ has the usual inner product.

6. In each case below, a set of vectors in an an inner product space is given. Apply the Gram-Schmidt procedure to find an orthonormal basis for the span of the set.

   (a) $\begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 2 \\ 2 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}$ in $\mathbf{R}^3$ with its usual inner product.

   (b) $\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} -2 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}$ in the vector space $M_{2\times 2}$ of all 2×2 matrices with the inner product defined by

   $$\langle A, B \rangle = a_{11}b_{11} + a_{12}b_{12} + a_{21}b_{21} + a_{22}b_{22}.$$

   (c) 1, x, x^2 in P_2 with the inner product defined by

   $$\langle p, q \rangle = p(-1).q(-1) + p(0).q(0) + p(1).q(1).$$

   (You need not show that this is an inner product on P_2.)

Appendix A

Sets

A.1 Basics: sets, elements, subsets and Cartesian products

Intuitively, we think of a set as a collection of objects or elements that belong together in some way. This idea is a good enough notion for our purposes, but causes significant problems when you get to more advanced mathematics. We won't worry about this, but we warn you that we are looking at what has been called the "friendly face" of naive set theory.

So, we provide no definition of what a set is; we trust you have a reasonable idea yourself. A set consists of **elements**; if the item x is a member of a particular set, A, we say "x is an element of A" and write $x \in A$. If x is not an element of A, we write $x \notin A$. Given any item x and any set A, it's reasonable to feel that x either is or is not an element of A but not both.

Example A.1.1 The collection of prime numbers is a set; the elements of this set are the prime numbers. If we denote this set by P, then $7 \in P$, but $8 \notin P$.

There is quite a well-established tradition of using capital letters for sets and small letters for the elements of sets.

A set of the form $\{x\}$ (that is, with exactly one element) is called a **singleton** set.

There are various ways of describing sets, or describing their elements, but two are common:

- A complete list of all elements.
- A description of the property that any element must have to be a member of the set in question.

We give examples below. Inevitably, there is some notation to get used to.

Example A.1.2 To indicate that the set A has precisely the elements $1, 3, 5$ and 7 we write:

$$A = \{1, 3, 5, 7\}.$$

We can deduce from this list of elements all sorts of (uninteresting) facts such as: $3 \in A$ but $9 \notin A$.

Clearly this listing technique has its limitations; you might waste a lot of time trying to list the elements of a large (or infinite!) set. A common practise (not without its dangers) is to describe an infinite set with elements that follow some kind of pattern by listing enough of the elements to make clear what the pattern is, followed by $\ldots$ to indicate that this pattern is continued indefinitely. An example would be to write

$$\{0, 1, 2, 3, 4, \ldots\}$$

to denote the set of natural numbers. A very common abbreviation for this set is the symbol $\mathbf{N}$; we'll use it in the next example, which gives a more rigorous way of describing infinite sets.

Example A.1.3 We know that an even natural number is one that has a factor 2. Let us denote the set of all even natural numbers by B. We could write this set as follows:

$$B = \{x \in \mathbf{N} : x = 2k \text{ for some } k \in \mathbf{N}\}.$$

You would read the above as follows: B is the set of all x chosen from $\mathbf{N}$ *such that* $x = 2k$ for some natural number k.

Once again we can deduce all sorts of things from this description of B: for instance $0 \in B$ but $23 \notin B$.

There are other ways of saying that $x \in A$ in informal English; for instance "x is a member of A", "x belongs to A"; we'll generally use the words "element" or "member".

We turn now to the idea of subsets, which are sometimes easily confused with elements.

Definition A.1.4 (Subset, equality) *Let A and B be sets. We say*

- *B is a* ***subset*** *of A if every member of B is a member of A. We write $B \subseteq A$. We then say that B* **is contained in** A or A **contains** B. (Don't confuse "element of" with "contained in".)
- $A = B$ if $A \subseteq B$ and $B \subseteq A$.

Warning: it is very easy to confuse the ideas of "being an element" of a set and "being a subset" of a set. Even the notation is confusing. Remember that $\in$ relates elements of a set to a set but that $\subseteq$ refers to subcollections of a set.

The above is all fairly reasonable and maybe you feel it is not worth writing down, but experience shows that you may be missing the point. The definition of equality of sets, for instance, is telling you precisely how to check whether two sets are equal; you must prove that any element of the one set is an element of the other and vice versa. To prove that $A \subseteq B$ you must show that every element of A is an element of B. Obvious enough? Well remember you have been warned!

We start with some easy examples:

Example A.1.5 Let $A = \{1, 2, 3\}$, $B = \{2, 3\}$, and $C = \{1, 1, 2, 3\}$. Then $B \subseteq A$ or $A \supseteq B$ but $A \not\subseteq B$. It is also clear that $A = C$, since every element of A is an element of C and vice versa. (So repeating elements in the list of elements of a set is a silly thing to do.)

Example A.1.6 Let P be the set of prime numbers, E the set of even prime numbers, F the set of odd prime numbers, H the set of positive even natural numbers and $G = \{2\}$. Then $2 \in P$ and 2 is the only element in E, so $E = G \subseteq P$. However, $G \neq P$. Also $F \subseteq P$ but $P \neq F$. Finally, E is not contained in F and H is not contained in P. Make sure that you can prove these statements using the definitions.

One rather surprising fact when one first looks at sets is that it is very convenient to have a set with **no** elements. This may seem counter-intuitive, but you get used to it. We take it as an *axiom* (something that we do not need to prove) that there is an empty set (i.e. a set with no elements). This is just saying that we are allowed to view a collection with no elements as a legitimate collection. It turns out that any two empty sets are equal, as you will see, so there is in fact only one empty set, and the notation for this set is either $\emptyset$ or $\{\,\}$.

We can prove some things about empty sets:

Proposition A.1.7 *(a) If B is an empty set, then, for any set A, $B \subseteq A$.*
(b) If B and C are empty sets, then $B = C$.

Proof: (a) Suppose that B is not contained in A. Then there must be an element x in B which is not in A. But B does not contain any elements, so we have a contradiction. Therefore we must have $B \subseteq A$.

(b) We know from (a) that $B \subseteq C$ and $B \supseteq C$, so, by definition of equality of sets, we have $B = C$. ■

In the exercises you will be asked to prove the following:

Proposition A.1.8 *(a) For any set A, $A \subseteq A$.*
(b) Let $A \subseteq B$ and $B \subseteq C$, then $A \subseteq C$.

We now give a list of sets that we use frequently, as well as the symbols we use for them:

$\mathbf{N} = \{0, 1, 2, 3, \ldots\}$	Natural numbers
$\mathbf{N}^+ = \{1, 2, 3, \ldots\}$	Positive natural numbers
$\mathbf{Z} = \{\ldots - 2, -1, 0, 1, 2, \ldots\}$	Integers
$\mathbf{Q}$	Rational numbers
$\mathbf{Q}^+$	Positive rational numbers
$\mathbf{R}$	Real numbers
$\mathbf{R}^+$	Positive real numbers
$\mathbf{C}$	Complex numbers

You may have grown up *not* thinking of 0 as a natural number. In this course 0 *is* a natural number.

The following notation will be used in this course (and is widespread):

For $a, b \in \mathbf{R}$, $a \leq b$:

$[a, b] = \{x \in \mathbf{R} : a \leq x \leq b\}$

$[a, b) = \{x \in \mathbf{R} : a \leq x < b\}$

$(a, b] = \{x \in \mathbf{R} : a < x \leq b\}$

$(a, b) = \{x \in \mathbf{R} : a < x < b\}$

$[a, \infty) = \{x \in \mathbf{R} : x \geq a\}$

$(a, \infty) = \{x \in \mathbf{R} : x > a\}$

$(-\infty, b] = \{x \in \mathbf{R} : x \leq b\}$

$(-\infty, b) = \{x \in \mathbf{R} : x < b\}$

$(-\infty, \infty) = \mathbf{R}$

We finish this section with a way of combining two (or more) sets to form a third. You have already seen an example of this at school (probably without realising it!) when you were first introduced to the idea of using *ordered pairs* of real numbers to locate points in the plain. There is a way of thinking of the plane as a *product* of the set of real numbers with itself. It is this idea which motivates the more general notion of a Cartesian product of two (not necessarily equal) sets.

The idea of the Cartesian product $A \times B$ of the sets A and B is that it is a set consisting of all ordered pairs of the form (a, b) where a is any element from A and b is any element from B. You have seen ordered pairs as coordinates of points in the plane. In this context we can think of the plane as $A \times B$, with $A = \mathbf{R}$ and $B = \mathbf{R}$, and so the ordered pairs (a, b) are ordered pairs of real numbers, representing points in the plane. This means that you are really already familiar with the Cartesian product $\mathbf{R} \times \mathbf{R}$ (which we usually write simply as $\mathbf{R}^2$): it can be thought of as the set of all the points in the plane.

We've talked about *ordered pairs* above without giving a precise definition. We can do this rigorously (see the note below), but for our purposes it is enough to think of it in a rather intuitive way as two elements in a definite order (so that we know which one comes first and which comes second).

The most important facts about ordered pairs seem to be:

- $(a, b) = (c, d)$ if and only if $a = c$ and $b = d$
- $(a, b) \neq (b, a)$ except when $a = b$.

A note for the purists:
You might perhaps wonder how we define an ordered pair in the first place. The answer is that we certainly can define an ordered pair just in terms of fairly simple sets, but that it doesn't really improve our understanding of them. On the other hand, it's perhaps reassuring that we can do it. Here is the definition:

Definition A.1.9 (Ordered pair) *The ordered pair* (a, b) *is defined to be the set* $\{\{a\}, \{a, b\}\}$

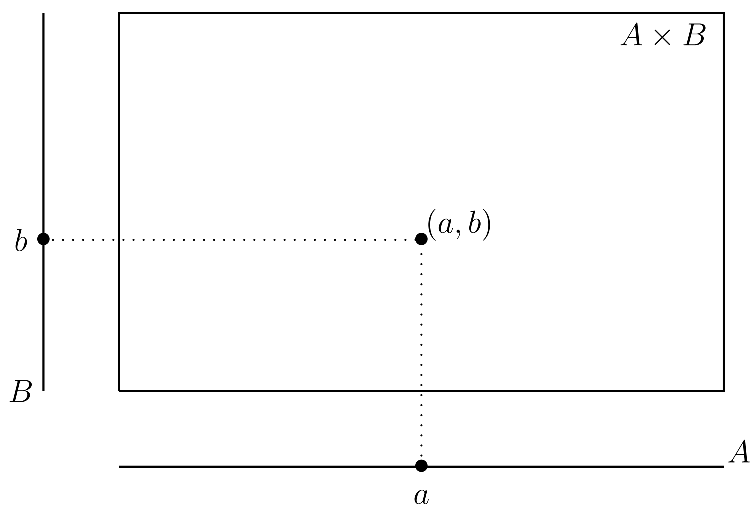
This looks intimidating, but don't worry. We can use this definition to prove the facts above and after that we forget the definition completely and work with (a, b) as before.
Here ends the note for purists.

Definition A.1.10 (Cartesian product) *Let A and B be sets. The* ***Cartesian product of*** *A* ***and*** *B is written $A \times B$ and consists of all ordered pairs of the form (a, b) where $a \in A$ and $b \in B$. That is:*

$$A \times B = \{(a, b) : a \in A, b \in B\}.$$

Example A.1.11 If $A = \mathbf{R}$ and $B = \mathbf{R}$, then $A \times B = \mathbf{R} \times \mathbf{R}$ is usually denoted by $\mathbf{R}^2$ and can be pictured as the Cartesian plane (the "xy-plane"). We can also think of $\mathbf{R}^2$ as the set of all real 2-vectors; if we do this we usually (but not always!) write the ordered pair (x, y) as $\begin{pmatrix} x \\ y \end{pmatrix}$.

If A and B are intervals in $\mathbf{R}$, the Cartesian product $A \times B$ can be represented as follows:



This is a useful picture to keep in mind for a Cartesian product, even when the sets are not intervals.

Example A.1.12 If $A = \mathbf{Z} = B$, then $A \times B$ can be thought of as the lattice of all points in the plane with integer cooordinates.

It is also possible to look at *ordered triples, ordered quadruples* and more generally *ordered* n-*tuples*, where $n \geq 2$ is an integer. A rigorous definition of this concept is somewhat technical; we'll rely on our intuitive understanding of the idea. Given this, we can then define the Cartesian product of the sets A, B and C as

$$A \times B \times C = \{(a, b, c) : a \in A, B \in B, c \in C\}.$$

Similar definitions can be given for products of more than three sets.

Example A.1.13 If $A = B = C = \mathbf{R}$, then $A \times B \times C = \mathbf{R} \times \mathbf{R} \times \mathbf{R}$ is usually denoted by $\mathbf{R}^3$ and

$$\mathbf{R}^3 = \{(x, y, z) : x, y, z \in \mathbf{R}\}.$$

More generally, for any integer $n \geq 2$,

$$\mathbf{R}^n = \{(x_1, x_2, \ldots, x_n) : x_i \in \mathbf{R} \text{ for } i = 1, 2, \ldots, n\}.$$

Example A.1.14 If A, B and C are bounded intervals in $\mathbf{R}$, then the Cartesian product $A \times B \times C$ can be pictured as a rectangular box in space, with its edges parallel to the coordinate axes.

Exercises

1. Determine which of the following statements are true :
   (a) $\emptyset \in \{\emptyset\}$
   (b) $\emptyset \subseteq \{\emptyset\}$
   (c) $\pi/4 \in \{\pi/4\}$
   (d) $\emptyset \in \{\pi/4\}$
   (e) $\pi/4 \in \{\{\pi/4\}\}$
   (f) $\{\pi/4\} \subseteq \{\{\pi/4\}\}$
   (g) $\{\pi/4\} \in \{\{\pi/4\}\}$
   (h) $\emptyset \subseteq \{\{\pi/4\}\}$
   (i) $\{\pi/4\} \subseteq \{\pi/4, \{\pi/2\}\}$
2. Determine which of the following statements are true:
   (a) The empty set is a subset of every set.

(b) If $A \subseteq B$, then $A = B$.

(c) If $A = B$, then $A \subseteq B$.

(d) Since $\emptyset$ is a member of $\{\emptyset\}$, $\emptyset = \{\emptyset\}$.

3. Consider the statement:
   For any two sets A and B, at least one of the following statements is true:
   (a) $A \subseteq B$ (b) $B \subseteq A$ (c) $A = B$
   Is this statement true? If so, prove it, otherwise give a counter-example.

4. Find three sets, A, B and C such that $A \in B$, $B \in C$ and $A \in C$.

5. Let A, B and C be sets. Prove:

   (a) $A \subseteq A$.

   (b) If $A \subseteq B$ and $B \subseteq C$, then $A \subseteq C$.

6. Let $A = \{1, 2, 3, 4\}$ and $B = \{2, 3, 5\}$. Write down all the elements of $A \times B$.

A.2 New Sets from Old: Power sets, unions, intersections and complements

We are now about to embark on a fairly systematic investigation of what we can do with sets, and what rules are useful when working with sets. In doing so, we'll see quite a few ways of constructing new sets from given sets. Our first example is very important.

Definition A.2.1 (Power Set) *Given any set, A, we can form the* ***power set*** *of A which we write as $\mathcal{P}(A)$. The elements of the power set of A are precisely all the subsets of A. Another way of saying this: the power set of A consists of the collection of all subsets of A. We could write this as follows:*

$$\mathcal{P}(A) = \{B : B \subseteq A\}$$

(In a sense, the above definition is saying that it makes sense to consider the collection of all subsets of any given set. In a formal course in set theory this would be an axiom.)

Example A.2.2 Let $A = \{0, 1\}$ The subsets of A are $\emptyset, \{0\}, \{1\}$ and $\{0, 1\}$.Thus

$$\mathcal{P}(A) = \{\emptyset, \{0\}, \{1\}, \{0, 1\}\}.$$

You should at this stage work out the power set of a set with one element and the power set of a set with three elements; the *numbers* of elements in these power sets follow an obvious pattern.

We turn now to operations on sets; you have probably seen some of these before.

Definition A.2.3 (Union, Intersection) *Let A and B be sets; then*

*(a) the set $A \cup B = \{x : x \in A \text{ or } x \in B\}$ is called the **union** of A with B.*

*(b) the set $A \cap B = \{x : x \in A \text{ and } x \in B\}$ is called the **intersection** of A with B.*

We think of $\cup$ and $\cap$ as operations on sets (in the same way that we think of $+$ and $\times$ as operations on numbers).

(In a formal course in set theory, you would see axioms asserting that it makes sense to talk about unions and intersections.)

It is worth emphasising here that in mathematics the word "or" is used in an *inclusive* sense. In the definition of union above, this means that an element x is in the union $A \cup B$ if it is in either in A, or in B, or in both A and B. This is rather different to the way we use "or" in everyday English.

Here are some simple examples involving unions and intersections.

Example A.2.4

(a) Let $A = \{2, 3, 4, 5, 6\}$ and $B = \{3, 4, 7, 10\}$. Then

$$A \cup B = \{2, 3, 4, 5, 6, 7, 10\}$$

and

$$A \cap B = \{3, 4\}.$$

(b) Let $A = [1, 3)$ and let $B = (2, 5]$. (That means that $A = \{x \in \mathbf{R} : 1 \leq x < 3\}$ and $B = \{x \in \mathbf{R} : 2 < x \leq 5\}$.) Then $A \cup B = [1, 5]$ and $A \cap B = (2, 3)$.

Example A.2.5 Let E, F, P and H be as in Example A.1.6. Then

$$E \cup F = P, E \cap F = \emptyset, H \cap P = E.$$

We list now some useful identities concerning the operations $\cap$ and $\cup$. Once proved, these identities can be used at any time when working with sets. They are time-savers.

Proposition A.2.6 *For any sets A, B and C:*

(a)	$\emptyset \cap A = \emptyset$	*(e)*	$A \cap (B \cap C) = (A \cap B) \cap C$
	$A \cup \emptyset = A$		$A \cup (B \cup C) = (A \cup B) \cup C$
(b)	$A \cap B \subseteq A, B$	*(f)*	$A \cup A = A = A \cap A$
(c)	$A, B \subseteq A \cup B$	*(g)*	*If* $A \subseteq B$ *then*
(d)	$A \cup B = B \cup A$		$A \cup C \subseteq B \cup C$
	$A \cap B = B \cap A$		$A \cap C \subseteq B \cap C$

Proof: The proofs are all easy as long as you remember the definitions and how to prove two sets equal or one set a subset of another. We'll prove the first part of (g); the proof is fairly typical, so use this as a guiding example:

Suppose that $A \subseteq B$; we must show that $A \cup C \subseteq B \cup C$. To do this let $x \in A \cup C$: there are two possibilities to consider

(i) $x \in A$: but then $x \in B$ by our assumption that $A \subseteq B$, so, by definition of unions, $x \in B \cup C$.

(ii) $x \in C$: but then $x \in B \cup C$ by definition of union again.

In either case, we get $x \in B \cup C$ so we are finished. ■

It is often the case that the sets or subsets one is working with are all subsets of some given set U; this set is then referred to as the **universe of discourse** or sometimes just the **universal** set. Clearly different problems will need or use different universal sets.

Definition A.2.7 (Complements) *Let A and B be subsets of a universal set U.*

*(a) The **complement of** A **relative to** B is the set*

$$\{x \in B : x \notin A\}.$$

This is written $B \backslash A$ or sometimes $B - A$ and usually referred to informally as "B minus A". (There are situations where the notation $B - A$ could also mean something else and therefore we'll tend to avoid it in this course.)

(b) The set $U \setminus A$ is usually called the ***complement*** *of A; this is denoted by A', $A^{\sim}$ or by $\mathbf{C}A$. We'll stick to the first version. Of course we have that*

$$A' = \{x \in U : x \notin A\}.$$

A few simple examples should sort out complements:

Example A.2.8 Let $U = \{1, 2, 3\}, A = \{1, 2\}, B = \{2, 3\}$.
Then $B \setminus A = \{3\}$ (not just 3!), $A \setminus B = \{1\}$, $A' = \{3\}$, $(A')' = \{3\}' = \{1, 2\} = A$, $U' = \emptyset$, $\emptyset' = U$.

Example A.2.9 Let E, F, P and H be as in Example A.1.6, K be the set of odd natural numbers and let $U = \mathbf{N}^+$ be the universal set. Then $P \setminus F = E$, $P \setminus H = F$, $H \setminus P = \{4, 6, 8, \ldots\}$, $H' = K, K' = H$.

The next proposition contains some useful identities concerning complements. Parts (b) and (c), which relates unions, intersections and complements, are sometimes referred to as *De Morgan's Laws*.

The proofs of the identities below are best done using some elementary ideas from logic. You will have to look at Appendix B to make sense of the proofs below.

Proposition A.2.10 *Let A and B be subsets of some universal set U. Then:*

(a) $(A')' = A$

(b) $(A \cup B)' = A' \cap B'$

(c) $(A \cap B)' = A' \cup B'$

(d) $A \setminus B = A \cap B'$

(e) $A \subseteq B \Leftrightarrow B' \subseteq A'$

Proof: We won't prove them all; you should try the ones we don't do here or in lectures. Here we just prove (a) and (e).

For (a), since we are trying to show two sets equal, we must show that every element of the one is an element of the other and vice versa. Let $x \in (A \cup B)'$. That means that

$$\begin{array}{ll} & \neg(x \in A \cup B), \\ \text{so} & \neg(x \in A \ \vee \ x \in B), \\ \text{so} & \neg(x \in A) \ \wedge \ \neg(x \in B),\ (*) \\ \text{so} & x \in A' \ \wedge \ x \in B', \\ \text{so} & x \in A' \cap B'. \end{array}$$

So far, we have proved that if $x \in (A \cup B)'$ then $x \in A' \cap B'$. We still need to prove the converse, but you should try that yourself. We point out now that although the above proof looks straightforward, many people do not understand what we did to obtain $(*)$. We in fact used the logical law we established in Appendix B which states that the proposition $\neg(P \vee Q)$ is logically equivalent to the proposition $\neg P \wedge \neg Q$; we used it in the case where P is the statement $x \in A$ and Q is the statement $x \in B$. Make sure you understand every single step of the above proof.

(e) Since this statement is an if and only if statement we will need to prove two things: first, we prove that if $A \subseteq B$ then $B' \subseteq A'$; then we prove the converse. For the first assertion, *assume* that $A \subseteq B$; we want to *prove* that then $B' \subseteq A'$. To prove this, we assume that $x \in B'$ and show that then $x \in A'$. So if $x \in B'$, then $x \notin B$, so $x \notin A$ (since, if it were, then $x \in B$ since $A \subseteq B$). But if $x \notin A$ then $x \in A'$, as we hoped to show. We'll leave the converse to you, since its proof is rather similar to what we've just done. You should do it yourself. ■

We finish this section with some useful identities concerning $\cup$ and $\cap$; they interact in a very good way with each other. The identities you'll see below are often referred to as the **distributive laws** for $\cap$ and $\cup$.

Proposition A.2.11 *For any sets A, B and C the following identities hold:*

(a) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.

(b) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$.

Proof: We'll prove just (some of) the first identity; the proof of the second is similar. The strategy for the proof is really determined by what we're trying to do, which is, to prove two sets equal. So we assume $x \in A \cap (B \cup C)$ and show that this implies that $x \in (A \cap B) \cup (A \cap C)$.

So let $x \in A \cap (B \cup C)$; that means that

$$x \in A \ \text{ and } (x \in B \text{ or } x \in C).$$

We can replace this sentence by a logically equivalent on. You will see in Appendix B that $P \wedge (Q \vee R) \quad \equiv \quad (P \wedge Q) \vee (P \wedge R)$. If we do so, we have that

$$(x \in A \text{ and } x \in B) \text{ or } (x \in A \text{ and } x \in C).$$

But this just means that

$$x \in (A \cap B) \text{ or } x \in (A \cap C)$$

which gives us

$$x \in (A \cap B) \cup (A \cap C)$$

as we needed. The reverse implication (converse) has a similar proof, which you should do yourself. ■

Exercises

1. Let $X = \{a, b, c\}$. List all the members of $\mathcal{P}(\mathcal{X})$. Do you know how many sets you have listed? Repeat the question for $X = \{a, b, c, d\}$.

2. Is there a set with exactly 12 subsets? Explain.

3. Prove that $A \cup B = A$ if and only if $B \subseteq A$.

4. Prove that $A \cap B = A$ if and only if $A \subseteq B$.

5. Give a proof of, or a counterexample to, each of the following statements.

   (a) Prove or find a counterexample to the following statement. For any sets P, Q, and R,
   $$(P \cap Q) \cup R = P \cap (Q \cup R)$$

   (b) A student is asked to prove that for any sets A, B, and C,
   $$(A \setminus (B \cup C)) = (A \setminus B) \cap (A \setminus C).$$
   The student writes: "Let $x \in A \setminus (B \cup C)$. Then $x \in A$ and $x \notin B$ or $x \notin C$. Therefore $x \in A \setminus B$ and $x \in A \setminus C$. Thus $A \setminus (B \cup C) = (A \setminus B) \cap (A \setminus C)$."
   What, if anything, is wrong with this proof?

   (c) For any three sets A, B, and C,
   $$A \times (B \cup C) = (A \times B) \cup (A \times C)$$

   (d) For any three sets A, B, and C,
   $$A \times (B \cap C) = (A \times B) \cap (A \times C)$$

A.3 Families of Sets

It is easy to extend our idea of a union or intersection of two sets to, say, three or four sets (using the associative law to keep the brackets under control); for example:

$$A \cup B \cup C \cup D = ((A \cup B) \cup C) \cup D.$$

But we sometimes want to do even better than that; we may have a large (possibly infinite) collection whose union we might be interested in. For instance, we might be interested in the collection of subsets of $\mathbf{R}$ of the form $[0,1)$, $[0,\frac{1}{2})$, $[0,\frac{1}{3}),\ldots,[0,\frac{1}{n})$ etc. How would we describe its union? How would we describe its intersection? You probably have an intuitive idea of how this might work, but we want a precise version too.

The first thing to settle is: how do we *talk* about these collections of sets? What notation should we use? Let's look at the above example:

Example A.3.1 We are considering the sets $[0,\frac{1}{n})$, for each positive natural number n. If we let the set $[0,\frac{1}{n})$ be denoted by the symbol A_n, say, then we might well refer to the whole collection of sets as

$$\mathcal{C} = \{A_n : n \in \mathbf{N}^+\}$$

where for each n, $A_n = [0,\frac{1}{n})$. ($\mathcal{C}$ is a set of sets.) It is common to think of the set $\mathbf{N}^+$ as playing a sort of indexing, or labeling, job in this example; it keeps track of all the sets under consideration. For that reason it is referred to as the **index** set that indexes the collection we are working with. We also refer to the whole collection of sets as an **indexed family** of sets. In cases such as the one above where the indexing set is the set of natural numbers, the indexed family $(A_n)_{n\in\mathbf{N}}$ of sets is usually simply called a *sequence* of sets.

Let's try another example of a collection or family of sets.

Example A.3.2 For each real number x, we are interested (for some or other reason) in the set $[-x,x]$. That means that we are considering a huge number of sets, one for each real number. It would make sense to label each set $[-x,x]$ as, say, B_x; then we would refer to the whole family as the collection

$$\{B_x : x \in \mathbf{R}\}.$$

The index set would be $\mathbf{R}$.

Example A.3.3 For each natural number, n we are interested in the factors of n. Thus the set of factors of twelve is the set $\{1, 2, 3, 4, 6, 12\}$. It would make good sense to label the set of factors of any particular n as, say, F_n. Thus the set above gets the label F_{12}. The collection of all these sets, one for each n, would then be sensibly indexed by $\mathbf{N}$. We could refer to the whole collection as the indexed family $\{F_n : n \in \mathbf{N}\}$.

In what follows, we'll often use the notation

$$\{A_i : i \in I\}$$

to talk about some general indexed family. Don't be put off by this; it just means a collection of sets, which we've indexed using some appropriate set I, so there's one set, A_i, for each $i \in I$. (The symbol I stands for whatever index set we're using; it could be doing duty for $\mathbf{N}^+$ or $\mathbf{R}$ or whatever; we don't know what it is and it doesn't matter; it's just some index set.)

In virtually all the examples we deal with, it will usually be pretty clear what to use as a sensible index set, but there are occasions where you might not want to refer to a particular index set, or perhaps not be sure which to use. Here is an example:

Example A.3.4 Let $\mathcal{C}$ be the family of all subsets of $\mathbf{N}$ containing the number 0. Then there is no obvious indexing set, but we could write

$$\mathcal{C} = \{A \subseteq \mathbf{N} : 0 \in A\}.$$

We consider now how to handle unions and intersections of indexed families. Let's try unions first. A union of two sets was easy: an element is in a union if it is in either (alternatively: at least one) of the two sets. Now it is a little tricky to talk about "either" set when we are talking about a (possibly infinite) collection of sets. On the other hand, saying that an element is in *at least one of* the sets under consideration still makes good sense. That's the approach we'll take.

Definition A.3.5 (Arbitrary unions) *Let $\{A_i : i \in I\}$ be an indexed family of sets. Then*

$$\bigcup\{A_i : i \in I\} = \{x : x \in A_i \textit{ for at least one } i \in I\}.$$

This means that $x \in \bigcup\{A_i : i \in I\}$ if and only if there is an $i \in I$ such that $x \in A_i$. There is an alternative notation for this union; we often write it more conveniently as

$$\bigcup_{i \in I} A_i.$$

Now that looks a bit daunting, but let's try to unpack the definition: it is saying that x is in the union of the A_i's (that's the bit before the "if and only if") if there is (at least) one i (from I) with x in the corresponding A_i (which is the bit after the "if and only if"). That's exactly what we wanted; x is in the union if it is in at least one of the sets under consideration.

We first give a simple example, where the indexing set is finite.

Example A.3.6 Let $A_1 = \{12, 13, 14\}$, $A_2 = \{13, 14, 15\}$, $A_3 = \{14, 15, 16\}$. We could then refer to the family $\{A_i : i \in \{1, 2, 3\}\}$. It is an indexed family of sets, with indexing set $\{1, 2, 3\}$. Now we can also talk about

$$\bigcup\{A_i : i \in \{1, 2, 3\}\}.$$

This must be

$$A = \{12, 13, 14, 15, 16\}$$

since each of the elements in the set A is in the union and conversely.

It probably won't come as too much of a surprise now how we're going to define the intersection of an indexed family. Here is the definition:

Definition A.3.7 (Arbitrary intersections) *Let $\{A_i : i \in I\}$ be an indexed family of sets. Then*

$$\bigcap\{A_i : i \in I\} = \{x : x \in A_i \text{ for every } i \in I\}.$$

this means that $x \in \bigcap\{A_i : i \in I\}$ if and only if for every $i \in I$ we have $x \in A_i$. The alternative notation for the above intersection is

$$\bigcap_{i \in I} A_i.$$

This one should be easier to unpack: we're saying that x is in an intersection of sets if it is in every single one.

Example A.3.8 Let's take the sets of example A.3.6; then

$$\bigcap\{A_i : i \in \{1, 2, 3\}\} = \{14\}$$

since only the element 14 is in each of the A_i's.

Experience tells us that working with these unions and intersections of collections of sets is something you may take some time to get used to. We'll go through a few examples to help you get used to these beasts. It may be useful to remind you that:

- $x \in \bigcup\{A_i : i \in I\}$ means that **there is** an i such that $x \in A_i$.
- $x \in \bigcap\{A_i : i \in I\}$ means that **for every** i, $x \in A_i$.

Please avoid the temptation to think that $x \in \bigcap\{A_i : i \in I\}$ means that "$x \in A_1$ and $x \in A_2$ and ..."; that may be roughly what you feel intuitively, but really doesn't make any sense, *so don't* do it. Whenever you want to use unions or intersections just think about the definition before you start; after that it's quite easy.

You may have noticed that we have, at the beginning of the definitions, referred to these unions and intersections as *arbitrary* unions and intersections. That's just a phrase we sometimes use to indicate that we're talking about a union of a possibly infinite collection of sets. This is rather common informal language, which you will hear us use from time to time.

Example A.3.9 Let $A_n = [0, \frac{1}{n})$ for each $n \in \mathbf{N}^+$. We find $\bigcap\{A_n : n \in \mathbf{N}^+\}$ and $\bigcup\{A_n : n \in \mathbf{N}^+\}$.

It seems plausible that $\bigcap\{A_n : n \in \mathbf{N}^+\} = \{0\}$, but we should be able to prove this. To prove that $\{0\} = \bigcap\{A_n : n \in \mathbf{N}^+\}$ we have to prove that two sets are equal.

Let's do the usual thing: first, since 0 is the only element of $\{0\}$ we should prove that it is an element of $\bigcap\{A_n : n \in \mathbf{N}^+\}$; this is easy, since $0 \in [0, \frac{1}{n})$ for each $n \in \mathbf{N}^+$, and so 0 is in the intersection, as needed. This shows that $\{0\} \subseteq \bigcap\{A_n : n \in \mathbf{N}^+\}$.

Conversely, we need to show that $\bigcap\{A_n : n \in \mathbf{N}^+\} \subseteq \{0\}$.Instead of showing that $x \in \bigcap\{A_n : n \in \mathbf{N}^+\} \Rightarrow x \in \{0\}$, we'll use a contrapositive argument and show that if $x \notin \{0\}$ then $x \notin \bigcap\{A_n : n \in \mathbf{N}^+\}$. So assume that $x \notin \{0\}$. There are (in this case) really only two possibilities for x;

$x < 0$: If this is the case then clearly $x \notin [0, \frac{1}{2})$, say, so

$$x \notin \bigcap\{A_n : n \in \mathbf{N}^+\}.$$

$x > 0$: If this is the case then there is some $k \in \mathbf{N}^+$ such that $\frac{1}{k} < x$. But then $x \notin [0, \frac{1}{k})$ so $x \notin \bigcap\{A_n : n \in \mathbf{N}^+\}$, so we have finished the proof.

It seems plausible that

$$\bigcup\{A_n : n \in \mathbf{N}^+\} = [0, 1),$$

but then a proof of this should be possible.

If $x \in [0, 1)$ then $x \in \bigcup\{A_n : n \in \mathbf{N}^+\}$ since, in fact, $[0, 1)$ is one of the members of the indexed family ($n = 1$). Conversely, if $x \in \bigcup\{A_n : n \in \mathbf{N}^+\}$ then for some $k \in \mathbf{N}^+$ we must have $x \in [0, \frac{1}{k})$, but then $0 \leq x < \frac{1}{k}$, so $0 \leq x < 1$, so $x \in [0, 1)$ as claimed. The proof is now finished.

Notice the strategy in both the above examples; we "guess" the answer, using our intuition, and then we use more formal means to prove that our answer is in fact correct. Drawing diagrams of the sets you are working with also helps. You should get used to thinking informally about what you are doing first, but then converting everything to a more formal version which uses definitions, logic and clear language to explain things fully. Your proofs should be clearly understandable by (say) a friend.

We now prove some useful facts that help when handling collections of sets, intersections, unions and so on. We've already proved similar facts for unions and intersections involving just two sets.

Proposition A.3.10 *Let $\{A_i : i \in I\}$ be some (arbitrary) family of sets, let k be some particular member of I, and let B be some set.*

(a) $A_k \subseteq \bigcup\{A_i : i \in I\}$

(b) $\bigcap\{A_i : i \in I\} \subseteq A_k$

(c) $B \cap (\bigcup\{A_i : i \in I\}) = \bigcup\{B \cap A_i : i \in I\}$

(d) $B \cup (\bigcap\{A_i : i \in I\}) = \bigcap\{B \cup A_i : i \in I\}$

Proof: (a) and (b) are similar; we'll do (a). Let $x \in A_k$. Then there is an $i \in I$ such that $x \in A_i$ (it is k), so, by definition, $x \in \bigcup\{A_i : i \in I\}$, as we needed.

(c) and (d) are similar; we'll do (c). We lay out the proof in a way that we haven't used as yet:

$$\begin{aligned} & x \in B \cap \left(\bigcup\{A_i : i \in I\}\right) \\ \text{iff} \quad & x \in B \text{ and } x \in \bigcup\{A_i : i \in I\} \end{aligned}$$

$$\begin{aligned}
&\text{iff} \quad x \in B \text{ and there is an } i \in I \text{ such that } x \in A_i \\
&\text{iff} \quad \text{there is an } i \in I \text{ such that } x \in B \cap A_i \\
&\text{iff} \quad x \in \bigcup\{B \cap A_i : i \in I\}
\end{aligned}$$

which is exactly what we wanted. You should make absolutely sure that you understand why each line holds if and only if the next line holds before you accept this proof. ■ In the last result of this section we look the De Morgan rules for complementation for arbitrary unions and intersections. The proofs of these rules are most easily done using quantifiers and and negation of statements involving quantifiers. To be able to do this, we note that we could have written the definitions for arbitrary unions and intersections using quantifiers in the following way:

$$\bigcup\{A_i : i \in I\} = \{x : (\exists i \in I)(x \in A_i)\}$$

and

$$\bigcap\{A_i : i \in I\} = \{x : (\forall i \in I)(x \in A_i)\}.$$

Proposition A.3.11 L*et* $\{A_i : i \in I\}$ *be some (arbitrary) family of sets. Then*

(a) $(\bigcap\{A_i : i \in I\})' = \bigcup\{A_i' : i \in I\}$

(b) $(\bigcup\{A_i : i \in I\})' = \bigcap\{A_i' : i \in I\}$.

Proof: (a) and (b) are similar; we'll do the proof of (a).

$$\begin{aligned}
& x \in (\bigcap\{A_i : i \in I\})' \\
\text{iff} \quad & x \notin (\bigcap\{A_i : i \in I\}) \\
\text{iff} \quad & \neg[(\forall i \in I)(x \in A_i)] \\
\text{iff} \quad & (\exists i \in I)(x \notin A_i) \\
\text{iff} \quad & (\exists i \in I)(x \in A_i') \\
\text{iff} \quad & x \in \bigcup\{A_i' : i \in I\}
\end{aligned}$$

which is just what we needed to show. Once again, we ask you to make absolutely sure you understand why we can use "iff" repeatedly above. ■

Exercises

1. For each natural number n, let $A_n = \{k \in \mathbf{N} : k \geq n\}$.

   (a) Find $\cup\{A_n : n \in \mathbf{N}\}$ and $\cap\{A_n : n \in \mathbf{N}\}$.

(b) Prove that your answers are correct.

2. Give an example of a family $\{C_n : n \in \mathbf{N}^+\}$ such that

$$\cap\{C_n : n \in \mathbf{N}^+\} = \emptyset \text{ but, for each } n \in \mathbf{N}^+, \quad \cap\{C_k : 1 \leq k \leq n\} \neq \emptyset.$$

3. Prove Proposition A.3.10 (b) and (d).

4. Prove Proposition A.3.11.

Appendix B

Logic

B.1 Statements and connectives

Logic is the underlying language of mathematics. When we prove things in mathematics, this is the language we use. It is therefore important to understand the basic ideas in logic, and to learn to use these in the proofs of results. This appendix gives a very brief introduction to those parts of logic you will need this year, and later. The module 2DS explores some of these ideas in more depth.

Here is a typical mathematical statement:

If n is an even integer, then n^2 is an even integer.

It's structure *could* be analysed as follows: it is a statement built up from two sub-statements with something linking the two substatements. The one sub-statement is "n is an even integer" and the other substatement is "n^2 is an even integer". The link is the use of the "if–then" idea. We will find that many statements in mathematics follow the above pattern, that is, statements linked to other statements in various ways. We first try to give a (not very precise) explanation of what a statement is.

Definition B.1.1 (Proposition/Statement) *A **proposition** or **statement** is a sentence of which it makes sense to say that it is true or false but not both.*

This is not quite satisfactory. What, for example, is the meaning of the word "sentence"? A rigorous answer to this question lies outside the scope of this appendix. For the moment we'll assume that we all know what a sentence is.

Example B.1.2 Here are some examples of propositions or statements:
(a) $2 + 3 = 6$ (b) $2 + 3 \neq 6$

Here are some examples of non-propositions:
(c) $2 + 3$ (d) What time is it? (e) This statement is false.

We now turn to the idea of *linking* propositions to make what we might call **compound** propositions: a compound proposition is one which comprises one or more propositions and *connectives*. You may not have seen the word "connective"; it is the technical term for a link.

Example B.1.3 The following are compound propositions:

(a) $5 > 4$ and $2 \geq 3$

(b) If π is a rational number, then π^2 is a rational number.

(c) $5 \neq 6$.

In (a) the sub-statements are $5 > 4$, $2 \geq 3$ and the connective is the word "and"; in (b) the sub statements are "π is a rational number" and "π^2 is a rational number" and the connective is "if – then"; (c) is a bit different; it is usually analysed as follows: the sub-statement is $5 \geq 6$ and the connective is the symbol $\neg$ which changes the meaning of the substatement (negates it).

We now give you a list of the most commonly used connectives, the corresponding English words that we usually use for them and the symbols which we will use to represent them:

Connective	Associated English word	Common Symbol
Conjuction	and	$\wedge$
Disjunction	or	$\vee$
Implication	if ... then	$\Rightarrow$
Biconditional	if and only if	$\Leftrightarrow$
Negation	not, not the case that	$\neg$

Having isolated the idea of sub-statements and connectives it is now possible to represent the structure of statements in a simple way, as we do in the next example.

Example B.1.4 Let us consider the statement:
"If Thandi has a credit for MAM1000W then Thandi cannot get credit for MAM1005H". We could represent the sub-statement "Thandi has a credit for MAM1000W" using the letter P; we could also represent the sub-statement "Thandi can get a credit for MAM1005H" using the letter Q. The original compound sentence can then be represented by the symbols

$$P \Rightarrow (\neg Q).$$

Similarly, the sentence "If $x \geq 1$ or $x \leq -1$ then $x^2 \geq 2$" could be represented by the symbols

$$(P \vee Q) \Rightarrow R$$

where P stands for $x \geq 1$, Q stands for $x \leq -1$ and R stands for $x^2 \geq 2$. (We will see later that our analysis of this sentence is not as useful as it might be.)

We will now turn to the meaning of the various connectives and try to make them more precise. Some connectives cause no trouble, but some are notoriously tricky. We use a pretty standard method of doing this, commonly referred to as **truthtables**.

Definition B.1.5 (Negation)*: If a sentence P (no matter what P represents) is true then the sentence $\neg P$ must be false; similarly if the sentence P is false then the sentence $\neg P$ is true. We summarize this idea in a truthtable:*

P	$\neg P$
T	F
F	T

where T stands for "true" and F stands for "false". We usually use 1 instead of T and 0 instead of F. With this convention the truthtable for negation becomes:

P	$\neg P$
1	*0*
0	*1*

Definition B.1.6 (Conjunction) *For the statement "P and Q" to be true, both P and Q must be true, otherwise the statement is false. This is summarized in the truthtable below, which in some sense we take as the* ***definition*** *of the meaning of the connective "and":*

P	Q	$P \wedge Q$
1	1	1
1	0	0
0	1	0
0	0	0

Use of conjunction usually causes no problem; it's pretty clear what it means both in everyday usage and in mathematics.

Example B.1.7 The statement "The earth is flat and $\pi > 3$" is false since (it is generally accepted) the earth is not flat. Similarly the statement "The earth is round(ish) and $\pi > 3$" is true since both substatements are true.

We move on to deciding precisely what the connective "or" is to mean; this is not quite as clear cut as for conjunction. When you say "Either I'm going to town or I'm going to the beach" you don't usually think "But maybe I'll do both". On the other hand if someone says "In cricket you've got to be a good bowler or a good batsman" it's understood that someone could well be good at both activities. In mathematics we opt for the second interpretation of the word "or".

Definition B.1.8 (Disjunction) *The following is the truthtable for disjunction:*

P	Q	$P \vee Q$
1	1	1
1	0	1
0	1	1
0	0	0

Example B.1.9 ''The earth is flat or π is rational" is a false statement, but "The earth is flat or π is irrational" is true.

We come now to one of the most commonly used connectives in mathematics: implication. Unfortunately the commonly accepted truth table looks a bit odd at first and even counter-intuitive. We'll try to motivate it with a (very carefully chosen) example:

Example B.1.10 A large company has given you life insurance; the terms are: *If* you die before the age of 60 *then* they will pay your estate a large amount of money. Under what conditions would your lawyers sue them for breach of contract? (In other words, when would you regard them as having made a false claim?) Answer: surely only in the case where you died before 60 and they didn't pay your estate. (Would you really sue them if you *didn't* die and they paid you the money?) That's the position that we take in mathematics too: a statement that involves implication is only regarded as false if the "if" part is true but the "then" part is false.

Definition B.1.11 (Implication) *The following is the truthtable for implication:*

P	Q	$P \Rightarrow Q$
1	1	1
1	0	0
0	1	1
0	0	1

We need a bit of terminology here: in the statement $P \Rightarrow Q$, P is called the **hypothesis, condition** or **antecedent**; Q is called the **conclusion** or **consequent**. We could thus say: $P \Rightarrow Q$ is false only when the hypothesis (antecedent) is true and the conclusion (consequent) is false.

Example B.1.12 Consider the following statements:

If the earth is flat then the moon is round.

If the earth is flat then the moon is made of green cheese.

If it is raining the plants outside will get wet.

If it is raining the plants outside will not get wet.

The first three statements are all true, according to our truthtable, whereas the last statement is false.

Did you feel somewhat uneasy about saying whether the first two statements above were true? In fact in mathematics and "real life"we seldom consider statements which involve an implication where the antecedent is false. (There are some notable exceptions though!) They don't seem very useful, to say the least.

Because implication turns out to be a very common component of logical thinking it wont come as a surprise to you that there are many different ways of talking about it in the English language. Here is a list of some of them:

- If P then Q.
- P is sufficient for Q.
- Q if P
- P only if Q. (A nasty way of saying it!)
- Q is necessary for P. (Also a bit confusing.)

All the above have the same meaning. (But mind your P's and Q's.)

One very important thing to notice is that the truthtable for $P \Rightarrow Q$ and $Q \Rightarrow P$ are **not** the same. In fact we call $Q \Rightarrow P$ the **converse** of $P \Rightarrow Q$.

We give now the truthtable for the last connective that we need:

Definition B.1.13 (Biconditional) *The following is the truthtable for biconditional:*

P	Q	$P \Leftrightarrow Q$
1	1	1
1	0	0
0	1	0
0	0	1

Exercises

1. Which of the following are propositions?

   (a) $2^2 + 3^2 = 17$

   (b) $8x^3 + 6x^2 - 4x + 2$

(c) If n is a positive integer, then the sum of the first n positive integers is given by $n(n+1)/2$.

(d) Every non-zero square matrix is invertible.

(e) $\arctan 1$

2. Identify the hypothesis and the conclusion in each of the following compound propositions.

(a) If Mary is 24 years old, then I am a monkey's uncle.

(b) n^2 is odd whenever n is an odd integer.

(c) When a is irrational, $a^2 + a$ is irrational.

(d) In order to pass the driver's test, the candidate must be able to parallel park.

(e) In order to pass the vision test, it is sufficient for the candidate to read the line $Q\ S\ Z\ P\ W\ M$ 4.

B.2 Tautologies, Contradictions and Equivalence

Some statements turn out to be automatically true. Here is a very simple example:

Example B.2.1 $P \vee \neg P$ is automatically true; this makes sense intuitively, but our truthtables support our intuition:

P	$\neg P$	$P \vee \neg P$
1	0	1
0	1	1

While we're thinking about these, some statements also turn out to be automatically false:

Example B.2.2 The statement $P \wedge \neg P$ is automatically false, as a quick check of its truthtable shows:

P	$\neg P$	$P \wedge \neg P$
1	0	0
0	1	0

It is perhaps amusing to notice that for every automatically true statement there is a corresponding automatically false one. (Why?) We give you a bit of terminology now concerning the above ideas.

Definition B.2.3 (Tautology, Contradiction, Contingency)*If a statement has a truth table in which only 1's appear, it is called a* ***tautology****. If a statement has a truthtable in which only 0's appear it is called a* ***contradiction****. Any other kind of statement is called a* ***contingency****.*

Here is a list of some important tautologies:

(a) $P \vee \neg P$

(b) $(P \Rightarrow Q) \Rightarrow (\neg Q \Rightarrow \neg P)$

(c) $(\neg Q \Rightarrow \neg P) \Rightarrow (P \Rightarrow Q)$

(d) $[P \wedge (P \Rightarrow Q)] \Rightarrow Q$

(e) $[P \Rightarrow (Q \wedge \neg Q)] \Rightarrow \neg P$

It's worth thinking about the intuitive content of the above tautologies. The first one, (a), almost defines how we feel about negation: if something is false then its negation is true and vice versa. The tautologies (b) and (c) together tell us something very important: $P \Rightarrow Q$ implies and is implied by $\neg Q \Rightarrow \neg P$ so the two implications are somehow equivalent. (We'll see this again later.) In (d) we see one of the most common forms of reasoning: if we know that P implies Q and we also know that P is true then we know that Q is true. The last tautology is the heart of what we call "proof by contradiction"; if P implies a contradiction $(Q \wedge \neg Q)$ then P must be false, so $\neg P$ must be true.

We now return to the idea mentioned in the paragraph above that, in some sense, the two statements $P \Rightarrow Q$ and $\neg Q \Rightarrow \neg P$ are equivalent; they are clearly two different statements but seem to have roughly the same meaning. Truthtables make this more precise: if you draw up the truthtables for each statement, you see that they are essentially the same. It seems reasonable to agree that two statements that have the same truthtable are logically saying the same thing and that's exactly the view we take. This idea is expressed in the following definition:

Definition B.2.4 (Logical equivalence) *Two statements P and Q are said to be* ***logically equivalent*** *if $P \Leftrightarrow Q$ is a tautology (which is really saying that P and Q have the "same" truthtable). We then write $P \equiv Q$.*

It's a rather boring little exercise to show that $P \vee Q \equiv Q \vee P$, but do it if you are worried about it.

Example B.2.5 Let's use our definition to show that $P \Rightarrow Q \equiv \neg Q \Rightarrow \neg P$.

You could draw up a truthtable for

$$(P \Rightarrow Q) \Leftrightarrow (\neg Q \Rightarrow \neg P)$$

as follows:

P	Q	$P \Rightarrow Q$	$\neg P$	$\neg Q$	$\neg Q \Rightarrow \neg P$	$(P \Rightarrow Q) \Leftrightarrow (\neg Q \Rightarrow \neg P)$
1	1	1	0	0	1	1
1	0	0	0	1	0	1
0	1	1	1	0	1	1
0	0	1	1	1	1	1

The columns for $P \Rightarrow Q$ and $\neg Q \Rightarrow \neg P$ are the same and the final column has only ones in it, so we get the equivalence desired.

Note: It is common to refer to $\neg Q \Rightarrow \neg P$ as the **contrapositive** of $P \Rightarrow Q$. We remind you that $P \Rightarrow Q$ and its contrapositive are logically equivalent.

We give you a list now of some other useful and important equivalences. Please take especial note of the first two; they are really important and (perhaps at first) a bit surprising.

(a) $P \Rightarrow Q \quad \equiv \quad \neg P \vee Q$

(b) $\neg(P \Rightarrow Q) \quad \equiv \quad P \wedge \neg Q$

(c) $\neg(P \vee Q) \quad \equiv \quad \neg P \wedge \neg Q$

(d) $\neg(P \wedge Q) \quad \equiv \quad \neg P \vee \neg Q$

(e) $\neg(\neg P) \quad \equiv \quad P$

(f) $P \vee (Q \wedge R) \quad \equiv \quad (P \vee Q) \wedge (P \vee R)$

(g) $P \wedge (Q \vee R) \quad \equiv \quad (P \wedge Q) \vee (P \wedge R)$

We give a brief discussion of some of these below:

(a) is perhaps a bit surprising, but is useful sometimes. Remember it!

(b) is important; it really tells you how to think about what a false implication means: it says that to show that P does **not** imply Q, you can show P is true and Q is not.

(c) and (d) are important; in set theory they give us the so-called De Morgan laws. Please take note of them; it is a *very* common error at this stage to think that to negate a conjunction (disjunction) you just negate the individual propositions and then stick a conjunction (disjunction) in between. Negating is not that simple!

The last two equivalences are sometimes referred to as the **distributive rules** for conjunction and disjunction.

Exercises

1. Write the converse and the contrapositive of each of the following propositions.
   (a) If $\sqrt{2} < \sqrt{5}$, then $2 < 5$.
   (b) If $2 \geq 5$, then $\sqrt{2} \geq \sqrt{5}$.

2. Let A and B be square matrices. Consider the following statement:

   If AB is non-singular, B is invertible. (1)

   (a) Write this compound statement in symbolic form, using connectives, and letters for statements (say what the statements are). Use the word "singular", not the word "non-singular", in your statement(s).
   (b) Write the converse of the statement (1), both in symbolic form and in English.

B.3 Open Sentences and Quantifiers

We reveal a big secret here: what we did in the last two sections is not particularly useful as it stands for the purposes of proving most results in mathematics! But it is a necessary preamble to really useful things, where it certainly gets used. Let's look at the very first sentence that we analysed: it was

"If n is an even integer, then n^2 is an even integer."

Which n are we referring to in this sentence? Or are we using n to stand for any even integer? What are we actually claiming? Whether consciously or not, we were probably claiming that the statement was true for *all* possible n, but this is not clear from the form of the sentence. It seems reasonable to say that we were using the symbol n as a sort of variable.

Here's another sentence which causes a bit more trouble than the last:

$$x \geq 2.$$

Is it true or false or both? Your answer is probably "Well, that depends." Quite rightly so; the sentence is true for some values of x (e.g. 3) and false for others (e.g. 1 or $1+i$). Once again, the sentence seems to involve some sort of variable.

The above sentences are examples of something which we will call an **open** sentence; one which involves a variable (at least one) and whose truth seems to depend on the values given for the variable. They certainly don't seem to qualify as propositions, since they might be both true and false, depending on what you replace the variable by. Here are some more examples:

Example B.3.1 More examples of open sentences:

(a) He is the president of South Africa.

(b) $z \leq 2$ and $z \geq -2$.

(c) f is increasing.

The three examples above all have (implicit) variables in them; sentence (a) is false unless "He" happens to be one particular person. Similar comments apply to (b) and (c).

We won't try to define an open sentence in this course. When you do a proper course on logic this idea would get taken care of in a way which would take us too long to cover here. We hope you get the idea from the above examples.

Given an open sentence, it is important to also specify those objects which could sensibly be substituted for the variables. This is often referred to as the **universe** appropriate for the given sentence.

Example B.3.2 The universe for (a) in example B.3.1 could be the set of South African citizens, but certainly not the set of real numbers! In (b) above, the universe might be integers, real numbers or even complex numbers.The universe for (c) could be the set of all real valued functions.

Associated with any open sentence and universe is something we call its **truth set**: it is the collection of all members of the universe which when substituted for the variable(s) produce a true proposition or statement.

Example B.3.3 The truth set for (a) in example B.3.1 is the set consisting of one person, well known to us all. The truth set for (b) is the interval $[-2, 2]$ (if our universe is the set of real numbers). The truth set for (c) is huge and includes functions like $f(x) = x^3$.

Now let's look at a sentence that looks as though it might be open but in fact is not:

$$x + 2 = 2 + x \text{ for any real } x.$$

The sentence involves a variable x but also includes the important phrase "for any real x". This sentence really is a proposition since it makes sense to say that it is true or false, but not both. (It is in fact true.) In other situations you will see phrases like

"for every x",

" for some x",

"there exists an x such that" or

"there are x and y"

which coupled with some open sentence turn it into a proposition. We call these phrases **quantifiers**, and they are said to **bind** the variables to which they refer. It turns out that we need only two kinds of quantifiers for most purposes.

Definition B.3.4 (Universal Quantifiers) *Phrases such as*

- *for each x*
- *for any x*
- *for all x*

*are called **universal quantifiers**.*

Example B.3.5 Each of the following propositions contains universal quantifiers:

(a) For each real number x, $x^2 \geq x$.

(b) For any real number x, $x^2 \geq 0$.

(c) For all real numbers x and y, $x + y \geq -2$.

We introduce a convenient symbolization of the phrase "for all"; it is $\forall$. We can now write the propositions in B.3.5 more concisely: here is (a)

$$(\forall x)(x^2 \geq x),$$

where it is understood that our universe is the set of real numbers. If some confusion about the universe might arise, we could write

$$(\forall x \in \mathbf{R})(x^2 \geq x).$$

Similarly (c) could be written as

$$(\forall x)(\forall y)(x + y \geq -2)$$

where, again, we are assuming x and y refer to real numbers.

So, in general then, given an open sentence $P(x)$, i.e., a sentence that involves the variable x,

we agree that

$$\boxed{(\forall x)P(x) \text{ stands for the proposition `` for every } x,\ P(x)\text{''}.}$$

We handle the phrases "there is an x" similarly:

Definition B.3.6 (Existential Quantifiers) *Phrases such as*

- *for some x*
- *there exists an element x*
- *there is an x*

are called ***existential quantifiers****.*

Example B.3.7 Each of the following propositions contains at least one existential quantifier.

(a) There is a real number x such that $x + 2 = 5$.

(b) There are real numbers x and y such that $x + y = 2$.

Again, we introduce a convenient symbol for the phrase "there is": it is $\exists$. We can now rewrite the propositions of B.3.7 more concisely: (a) becomes

$$(\exists x)(x + 2 = 5)$$

or, if necessary

$$(\exists x \in \mathbf{R})(x + 2 = 5),$$

(b) becomes $(\exists x \in \mathbf{R})(\exists y \in \mathbf{R})(x + y = 2)$.

You must develop the skill of translating sentences involving quantifiers into the concise form we've used above. This will help you to understand the structure of sentences, and increase your ability to work with complicated sentences. In particular, many mathematical sentences involve hidden or implicit quantifiers and trying to write them using the concise symbolization we've just set up will often reveal such problems.

Example B.3.8 We translate the following sentences using quantifier symbols:

(a) $\sin^2 x + \cos^2 x = 1$

(b) An integer n is even provided that there is an integer k such that $n = 2k$.

(c) There is a least natural number.

(a) There is a hidden quantifier here because we are really claiming that the equation is true for any real number x; so here is the proper translation:

$$(\forall x \in \mathbf{R})(\sin^2 x + \cos^2 x = 1).$$

(b) The phrase "provided that" is tricky; here it seems to mean "if and only if". A first attempt at translating the proposition might be

$$(n \text{ is even }) \Leftrightarrow (\exists k)(n = 2k)$$

where the understanding is that k must be an integer. But looking at our translation again, we see that there is an unbound variable, n; we still have an open sentence. Presumably what we are claiming is true for any integer n, so a final translation might be:

$$(\forall n \in \mathbf{N})\left[(n \text{ is even }) \Leftrightarrow (\exists k \in \mathbf{N})(n = 2k)\right].$$

(Why did we put the square brackets in in the last line?)

(c) This is a true statement, since 0 is the least natural number, but that isn't the point; how do we translate the above? As a start we could write

$$(\exists n \in \mathbf{N})(n \text{ is the least natural number})$$

but we can do better: consider

$$(\exists n \in \mathbf{N})(\forall m \in \mathbf{N})(n \leq m).$$

This proposition says exactly what we want; there is a natural number less than or equal to every natural number. Make sure you understand this.

Translation of a mathematical proposition using quantifiers etc into informal English (or whatever language you're using) is also an important skill. We may frequently have to give definitions of new ideas or statements of theorems in a precise way using all the symbols we have developed so far; you should be able to unravel these into acceptable English so that you get an intuitive understanding of them.

Example B.3.9 We translate the following into informal English.

(a) $(\forall m \in \mathbf{Z})(\exists n \in \mathbf{Z})(n > m)$

(b) $(\exists n \in \mathbf{Z})(\forall m \in \mathbf{Z})(n > m)$

(a) This could be translated as: for any integer m there is an integer n larger than m. This is true, since, for instance $m + 1$ is bigger than m, so $m + 1$ will do as the n claimed to exist. More informally, this proposition states that there is no largest integer.

(b) On the face of it, you might think there is not much difference between (a) and (b), but there is a world of difference. This is how we might translate (b): there is some integer n, such that any integer m is less than n. In fact this proposition claims that *there is a largest integer*, which is false.

The above two examples highlight an important fact: be careful about the order in which you write down quantifiers; **swopping universal and existential quantifiers changes the meaning of your statement**.

We turn now to another important question; how do quantifiers interact with negation? For instance if you negate the statement "All swans are black", you get the statement "Not all swans are black" (Surprise!) But the latter statement can be written more intuitively and usefully as “There is a swan that is not black”. While these two statements are not identical, they have the same meaning; we would describe them as being logically equivalent to each other. Similar comments apply when negating a sentence involving an existential quantifier. We summarize these facts below:

$$\begin{aligned} \neg(\forall x)(P(x)) &\equiv (\exists x)(\neg P(x)) \\ \neg(\exists x)(P(x)) &\equiv (\forall x)(\neg P(x)). \end{aligned}$$

We won't attempt to prove these facts; they seem clear enough at this level. In a course on logic you would see a proper discussion of these ideas.

Example B.3.10 We want to write out a useful negation of:

For every real number x there is a real number y such that $2^y = x$.

We first write out the sentence using quantifiers: it is

$$(\forall x)(\exists y)(2^y = x)$$

where the universe is clearly the set of real numbers. If we negate this we get:

$$\begin{aligned} \neg(\forall x)(\exists y)(2^y = x) &\equiv (\exists x)\neg[(\exists y)(2^y = x)] \\ &\equiv (\exists x)(\forall y)\neg(2^y = x) \\ &\equiv (\exists x)(\forall y)(2^y \neq x). \end{aligned}$$

Can you see how we used the two facts about negating quantifiers in the above? We can now translate the final proposition back into English to get: There is some x such that for all y, $2^y \neq x$. This happens to be true; try $x = -1$.

With that under our belt, we turn to the idea of **counterexamples**. Many mathematical statements involve universal quantifiers; we are always trying to find statements that are true of all the objects under consideration. To prove such claims, one has to come up with a proof that works for all possible objects under consideration; a tough job! On the other hand, to disprove such a claim one has to disprove a statement like $(\forall x)P(x)$, which means that you have to be able to show that $\neg(\forall x)P(x)$ is true; but this amounts to showing that $(\exists x)\neg P(x)$ is true, i.e. you need to find just one x such that $P(x)$ is false. This particular x is called a **counterexample** to the assertion that $(\forall x)P(x)$ is true.

Example B.3.11 The statement: "Every perfect square is divisible by 3" is false; a counterexample to the statement is the number 4; it is a perfect square that is not divisible by 3.

In fact, we might as well look at counterexamples for a fairly common type of mathematical statement right now: many statements have the form

$$(\forall x)(P(x) \Rightarrow Q(x)).$$

(Examples: look at the example above; if we let $P(x)$ stand for "x is a perfect square" and $Q(x)$ stand for "x is divisible by 3" then the statement in example 3.11 is translated exactly as $(\forall x)(P(x) \Rightarrow Q(x))$.)

To disprove such a statement we must show that $(\exists x)\neg(P(x) \Rightarrow Q(x))$ is true. But we know from the last chapter that $\neg(P(x) \Rightarrow Q(x))$ is logically equivalent to $P(x) \wedge \neg Q(x)$, so we are actually trying to show $(\exists x)(P(x) \wedge \neg Q(x))$. That tells us that we must find an x such that $P(x)$ is true, but (and) $Q(x)$ is not. (This is exactly what we did in the last example.)

What's the point of all we have done in this chapter? The answer is that the language we've developed so far will do very nicely for just about all the mathematics that we need to look at. Quantifiers, variables and connectives are all we need.

In a course on logic you might well learn similar things to what we've looked at so far, but presented in a far more precise way. You would in all likelihood learn first about Propositional Calculus, which is what we did, more or less, in the first two sections of this appendix. You would then move on to so-called First Order Logic which handles variables and quantifiers, as we did in this section.

We've finished our crash course in logic and it's time to put it to use, which we do in the next section of this appendix.

Exercises

1. Find the truth set of the open sentence $(x^2+1)(x-3)(x^2-2)(2x-3)=0$, when it is given that the universe of this open sentence is each of the following:

   (a) $\mathbf{Z}$ (b) $\mathbf{Q}$ (c) $\mathbf{R}$ (d) $\mathbf{C}$.

2. If both of the following statements have the set of positive real numbers as their universe, which statement is true?

(a) $(\forall x)(\exists y)(x < y^2)$ (b) $(\exists y)(\forall x)(x < y^2)$

3. Write a *useful* negation of each of the following propositions.

    (a) For all a and b, if $a < b$, then $a^2 < b^2$.

    (b) For all a and b, if $ab = 0$, then $a = 0$ or $b = 0$.

4. Write the contrapositive of each of the following propositions.

    (a) For all a and b, if $ab \neq 0$, then $a = 0$ or $b = 0$,

    (b) For all a and b, if $a \neq 0$ or $b \neq 0$, then $ab \neq 0$.

5. A group G is **cyclic** provided that there is a member a of G such that for each member g of G, there is an integer n such that $a^n = g$.

    (a) Write this definition using connectives and quantifiers.

    (b) Explain in a useful way what it means to say that a group G is not cyclic.

    (You do not need to have the slightest idea what a group is!)

B.4 Methods of Proof

We now have a reasonable grasp of logic, and can use this to develop techniques for proving things. It is a fact of life that you will discover as we go along that most statements in mathematics involve proving statements of the form "If P then Q" or, as we can now write: "$P \Rightarrow Q$". There may indeed be a variable in the sentence, in which case we may be trying to prove something that has the form $(\forall x)(P(x) \Rightarrow Q(x))$. Nonetheless, this still involves us with proving $P(x) \Rightarrow Q(x)$.

Our knowledge of implication leads us to various strategies for proving implications.

(1) **Direct Proof**: We assume that P is true and show that Q is then true. (Why don't we bother to check the case where P is false?)

(2) **Contrapositive proof**: We prove that $\neg Q \Rightarrow \neg P$ is true, since we know this is logically equivalent to $P \Rightarrow Q$. To do so, we begin by assuming Q is false and show that P is then false. (Why?) [Note: we haven't explicitly said what the contrapositive of $(\forall x)(P(x) \Rightarrow Q(x))$ is yet; strictly speaking there isn't one, but the statement
$(\forall x)(\neg Q(x) \Rightarrow \neg P(x))$ will do.]

(3) **Proof by Contradiction**: Assume that P is true and that Q is false; if you find that this leads you to a contradiction, then you know that one of your assumptions is false. Since you are trying to prove $P \Rightarrow Q$, you are only interested in the case where P is true, so your assumption that Q is false must be incorrect. Thus Q is true, and you've proved that $P \Rightarrow Q$.

We'll illustrate each of these methods with some simple proofs concerning facts well known to you. Before we do that, we remind you of a few simple definitions: recall that a natural number n is **even** if there is a natural number k such that $n = 2k$ (in other words n is divisible by 2 or has 2 as a factor). Similarly, a natural number n is **odd** if there is a natural number k such that $n = 2k+1$. (Exercise: Write these statements using quantifiers.) Taking this a bit further, we say that the integer a **divides** the integer b if there is an integer k such that $b = ka$. (Alternatives: a is a factor or divisor of b; b is a multiple of a.) A **prime** number p is a positive integer greater than 1 whose only divisors are p itself and 1.

Example B.4.1 (*Use of direct method of proof*) Prove that if n is an odd natural number then so is n^2.

Proof: You might think that at this stage we try to write a proof that uses only quantifiers and is all very formal, but that, in fact, is not at all what we're about here. The quantifiers and connectives are there to help you be precise if necessary, but no mathematician ever resorts to that sort of thing unless he/she absolutely has to. What follows is a typical proof.

Assume that n is odd. Then there is a natural number k such that $n = 2k + 1$. That means that $n^2 = (2k+1)^2 = 4k^2+4k+1$ which we can rewrite as $2(2k^2+2k)+1$. This shows that n^2 is odd, since it has been written in the form $2m + 1$ where m is a natural number. ■

Please try to imitate the sort of style we used above when you are writing out a proof; notice that we *do* use English; we also try to make it read in a sensible way. Avoid trying to use just mathematical symbols and no explanation. While you may be able to get away with this, it usually doesn't read well and is difficult for anyone (but yourself) to understand. Remember: writing mathematics involves communicating with other people!

Example B.4.2 a (*Use of contrapositive method of proof*) Suppose m and b are real numbers with $m \neq 0$. Let $f(x) = mx+b$. Show that if $x \neq y$ then $f(x) \neq f(y)$.

Proof: The contrapositive of

$$x \neq y \Rightarrow f(x) \neq f(y)$$

is

$$f(x) = f(y) \Rightarrow x = y.$$

We try to show that this is true. Assume $f(x) = f(y)$; then

$$mx + b = my + b.$$

Subtracting b from both sides shows

$$mx = my.$$

Finally multiplying both sides by $\frac{1}{m}$ yields

$$x = y,$$

as we needed. (Where did we use the fact that $m \neq 0$?)

A slightly more concise proof might go as follows:

$$\begin{aligned} f(x) = f(y) &\Rightarrow mx + b = my + b \\ &\Rightarrow mx = my \quad \text{(Subtract } b \text{ from both sides.)} \\ &\Rightarrow x = y \quad \text{(Multiply both sides by } \tfrac{1}{m}\text{.)} \end{aligned}$$

as needed. ∎

We come now to proof by contradiction; this is a slippery customer and must be treated with care. The example we give to illustrate this type of proof is a classic one and is part of your general mathematical education.

Example B.4.3 If r is a real number such that $r^2 = 2$ then r is not rational. (So we are claiming that $\sqrt{2}$ is not rational.)

Proof: We assume r is real and that $r^2 = 2$. Now assume that r is indeed rational (!) [Note: in these notes, we'll indicate when we have assumed something that should lead to a contradiction by the symbol (!)] Then we may write $r = \frac{m}{n}$ where m and n are positive integers and we may also assume that m and n have no common factors. (Why?) Then we also must have:

$$r^2 = \frac{m^2}{n^2} = 2,$$

so

$$m^2 = 2n^2.$$

Now $2n^2$ is even, so m^2 is even, but this is only possible if m is even. (Why?) So $m = 2k$ for some integer k. Thus

$$4k^2 = m^2 = 2n^2,$$

so

$$n^2 = 2k^2.$$

By a similar argument to the one above we must have n even as well. We now have reached the situation where both m and n are even which contradicts the fact that m and n had no common factors. Thus our assumption that r was rational was false and we reach the conclusion that r is not rational. ∎

The fact that there *are* non-rational numbers (which we call **irrational numbers** these days) was something discovered by the Greeks and in particular by the followers of Pythagoras. It caused a major crisis for the Greek mathematicians as they had assumed that all numbers were ratios of whole numbers and many of their proofs depended on this "fact". Many of their proofs of geometric facts had to be overhauled in the light of this alarming discovery and it was Euclid who was instrumental in saving the day (some years later). Nonetheless, the Greeks were so shocked by this problem that they they tended to avoid algebra altogether after that. It was the Hindu and Arabic school of Mathematics that eventually spurred more exploration of algebra.

We give you a last example using proof by contradiction:

Example B.4.4 There do not exist prime numbers a, b and c such that

$$a^3 + b^3 = c^3.$$

Proof: Suppose that there are primes a, b and c such that $a^3 + b^3 = c^3$. (!) If a and b are both odd, then $a^3 + b^3$ must be even (Why?) so c^3 must be even. That in turn means that c is even and prime, so $c = 2$. This is impossible, since a and b, being odd primes, are both greater than 2.

So at least one of a and b must be even; let's assume it's b, so $b = 2$. Therefore

$$b^3 = 8 = c^3 - a^3 = (c - a)(a^2 + ac + c^2).$$

But since a and c are primes, each of a^2, ac and c^2 must be greater than or equal to 4. This means that $(a^2 + ac + c^2)$ is greater than or equal to 12, which forces $c^3 - a^3$ to be greater than or equal to 12. (Why can't we have $c - a = 0$?) This contradicts $c^3 - a^3 = 8$. So we get a contradiction and we have proved what we wanted. ∎

We have now shown you some examples illustrating the three methods of proving the truth of an implication. Mathematics is not a spectator sport and it is up to you to now try the exercises at the end of the section to get used to thinking about how to prove things. You will also see proofs using these ideas in linear algebra, and be asked to prove things yourself..

Exercises

1. Let m, n, and r be integers. Prove that if m divides n and n divides r, then m divides r.

2. Let m be an even integer and n be an odd integer. Prove that $m + n$ is odd and mn is even.

3. Consider the statement

   "If n is any prime, then $2^n + 1$ is prime."

   (a) Is this statement true? If your answer is yes, prove the statement. Otherwise find a counterexample to the statement.

   (b) Is the converse of this the statement true? If your answer is yes, prove the statement. Otherwise find a counterexample to the statement.

Appendix C

Relations and functions

C.1 Functions

You have worked with functions for a large part of your mathematical career, and may well feel that you have a pretty good understanding of them and what they are about. You have probably also discovered that functions are very important and useful, and that sooner or later you come across them in every kind of mathematics. It is exactly because they are so important that is essential to have a solid understanding of the basic facts about functions. You will soon discover that there are a few tricky ideas that you have to get your head around.

What is a function? Most of us have an intuitive idea of a function as some kind of rule. Here is an informal definition:

Definition C.1.1 (Function – informal definition) *Let A and B be sets. A **function** f from A to B is a rule that assigns to every $a \in A$ a* unique *element $b \in B$. We write $b = f(a)$; this makes sense since f assigns only one element to a. We call A the **domain** of f (denoted by $dom(f)$) and B the **codomain** of f (denoted by $cod(f)$). We write $f : A \to B$ as a shorthand for "f is a function from A to B". We often express the fact that $b = f(a)$ by saying that f **maps** a to b.*

It is important to realise that there are three things needed to make up a function: sets A and B and a rule f. When a function is defined, all three need to be specified.

Why is this only an "informal" definition? The problem lies with the word "rule". What is a rule? You may feel that you know, but if you are honest, you'll soon discover that it is very difficult to give the word a precise meaning. Fortunately, there is a way of doing it, and in the next paragraphs we'll give a brief explanation for the purists. Most of the time the informal definition is good enough, and probably a better reflection of the way most of us think about functions. So if you are not a purist, you can skip the next paragraph, and be comfortable in the knowledge that our intuition can be made precise.

[**Note for the purists:** We want to make precise the idea of a rule assigning elements of B to every element of A. One way of saying exactly what such a rule is, is to make a comprehensive list of ordered pairs: for each $a \in A$, we write down a and the element $b \in B$ that is assigned to a to get an ordered pair (a, b). The set of all such ordered pairs says exactly what the rule is. We have agreed to write $f(a)$ for the element in B that the rule f assigns to a. We could say that the set $\{(a, f(a)) : a \in A\}$ *is* the rule. But this set is a subset of the Cartesian product $A \times B$. It is, however, not just any old subset of $A \times B$. The rule is special in the sense that it assigns to every $a \in A$ a *unique* element in B – there cannot be two different elements of B assigned to the same $a \in A$.

These ideas is the motivation for the following rigorous definitions:

A **relation** from A to B is a subset of $A \times B$.

A **function** f from A to B is a subset f of $A \times B$ such that

(a) for every $a \in A$ there is a $b \in B$ such that $(a, b) \in f$ and

(b) if $(a, b) \in f$ and $(a, c) \in f$ then $b = c$.

It follows at once from these definitions that every function is also a relation, but that not every relation will be a function.

Example C.1.2 Let $A = B = \mathbf{R}$. The subset $\{(x, y) : x = y^2\}$ of $\mathbf{R} \times \mathbf{R}$ is a relation from $\mathbf{R}$ to $\mathbf{R}$, but not a function. It fails to be so for two reasons. Firstly, there is no $y \in \mathbf{R}$ such that $(-1, y) \in \{(x, y) : x = y^2\}$. Secondly, it's clear that $(1, -1)$ and $(1, 1)$ are both in $\{(x, y) : x = y^2\}$, but $-1 \neq 1$.

On the other hand the subset $\{(x, y) : y = x^2\}$ of $\mathbf{R} \times \mathbf{R}$ is a function: firstly for every $x \in \mathbf{R}$, there is a $y \in \mathbf{R}$ such that $y = x^2$, and secondly, if (x, y) and (x, z) are members of $\{(x, y) : y = x^2\}$, then $y = x^2 = z$, so $y = z$. We have checked that both conditions of the definition of a function are satisfied.

Now that we know it can be done properly, we can relax and return to a more informal way of doing things. Here ends the note for purists.]

A function $f : A \to B$ assigns elements of B to elements of A. But there is nothing in the definition that says that *all* the elements of B must be so assigned.

It is quite possible that the set of elements of B that are assigned to elements of A forms a proper subset of B.

Definition C.1.3 (Range) *Let $f : A \to B$ be a function. We define the* ***range*** *of f to be the subset $\{b \in B : f(a) = b$ for some $a \in A\}$ of B, or more concisely the set $\{f(a) : a \in A\}$. This set is denoted by ran(f), so that*

$$ran(f) = \{b \in B : f(a) = b \textit{ for some } a \in A\} = \{f(a) : a \in A\}.$$

The next examples show that the range can be different from the codomain.

Example C.1.4 Let $A = \mathbf{R} = B$ and the function $f : A \to B$ be defined by $f(x) = |x|$. Then f is a function with $\mathrm{dom}(f) = \mathbf{R}, \mathrm{ran}(f) = [0, \infty)$. The codomain ofquare matrices of the same size f is $\mathbf{R}$, and this is different from range of f.

Definition C.1.5 (Function equality) *Suppose that we have two functions $f : A \to B$ and $g : C \to D$. These functions are* ***equal*** *if*

(a) $A = C$

(b) $B = D$

(c) for every $a \in A = C, f(a) = g(a)$.

Example C.1.6 Let f be the function in Example C.1.4 and define the function $g : \mathbf{R} \to \mathbf{R}$ by $g(x) = y$ where $x^2 = y^2$ and $y \geq 0$. Then g is equal to f.

quare matrices of the same size

Definition C.1.7 (Identity function) *For any set A, we can always define the* ***identity function*** *from A to A. We use id_A to denote this function and it is defined by*

$$id_A(a) = a$$

for every $a \in A$.

The next definition tells us how to "hook up" two functions to form a third one.

Definition C.1.8 (Composition of functions) *Let $f : X \to Y$ and $g : Y \to Z$ be functions. For every $x \in X$, let*

$$(g \circ f)(x) = g(f(x)).$$

Then the function $g \circ f : X \to Z$ is called the ***composition*** *of f and g.*

Example C.1.9 Let $f : \mathbf{R} \to \mathbf{R}$ be defined by $f(x) = x + 1$ and let $g : \mathbf{R} \to \mathbf{R}$ be defined by $g(x) = x^2$. Then

$$(f \circ g)(x) = f(g(x)) = f(x^2) = x^2 + 1.$$

On the other hand

$$(g \circ f)(x) = g(f(x)) = g(x + 1) quarematricesofthesamesize = (x + 1)^2.$$

Notice that $g \circ f$ need not equal $f \circ g$ even when both are defined.

Exercises

1. Let $f : A \to B$, $g : B \to C$ and $h : C \to D$ be functions. Prove that $(h \circ g) \circ f = h \circ (g \circ f)$.

C.2 Bijections and inverses

We can think of a function as a rule which takes us from one set to another. Is it always possible to find another function that will "undo" what the original function has done? More precisely, given a function $f : X \to Y$, can we always find a function $g : Y \to X$ such that if we start with an $x \in X$, apply f to it to get $f(x) \in Y$ and then apply g to $f(x)$, we get back to x (i.e. $g(f(x)) = x$)? quare matrices of the same size Let's explore this question with a familiar example.

Example C.2.1 Let the function $f : \mathbf{R} \to \mathbf{R}$ be defined by $f(x) = x^2$. Then $\mathrm{dom}(f) = \mathbf{R}$, $\mathrm{cod}(f) = \mathbf{R}$ and $\mathrm{ran}(f) = [0, \infty)$. Let's see if we can define a function $g : \mathbf{R} \to \mathbf{R}$ such that $g(f(x)) = x$, that is, such that $g(x^2) = x$, for every $x \in \mathbf{R}$. The obvious thing to do seems to be to define, for $y \in \mathbf{R}$, $g(y) = \sqrt{y}$. But if we do this, two problems arise:

1. $g(y)$ does not make sense for all$y \in \mathbf{R}$, but only for $y \geq 0$;
2. if, for example, $x = -2$, then $f(x) = (-2)^2 = 4$ and $g(f(x)) = \sqrt{f(x)} = \sqrt{4} = 2 \neq -2 = x$.

For this f, there is clearly no function that will "undo" what f has done.

We want to identify those functions for which we can find a function that will undo what it has done. We certainly need to avoid the problems shown up by the example above. The first problem is easy to avoid: it is necessary to avoid functions for which the codomain and range are different.

Definition C.2.2 (Surjective or onto functions) *Let $f : X \to Y$ be a function. We say that f is **onto**, or a **surjective** function, if ran$(f) = Y$.*

Warning: You have undoubtedly heard the term "onto" before. We point out that it seems to be a common error to confuse the words "onto" and "into"; saying that a function is "into" a particular set just means that the "output" values the function produces lie in that set. Saying that a function $f : X \to Y$ is "onto" means something far stronger: it means that *every* member of Y is an "output". Of course, what we have just said is far less precise than what we said in the definition, but it may help to alert you to a problem.

To avoid the second problem shown up in Example C.2.1 we need to make sure that the function does not produce the same output for two different inputs.

Definition C.2.3 (One-one or injective function) *f is **one-to-one** or **injective** if $f(x_1) = f(x_2)$ implies that $x_1 = x_2$. Equivalently (using the contrapositive of the above implication) f is injective if for any $x_1, x_2 \in X$, $x_1 \neq x_2$ implies that $f(x_1) \neq f(x_2)$. If f is one-to-one we often write " f is $1 - 1$".*

We point out now the general strategies you might adopt to prove that a function is onto or $1 - 1$:

> **Onto**: If $f : X \to Y$ is a function and you want to prove that it is onto, you must start by taking an arbitrary element y of Y and convincing yourself (and us) that you can find an element x of X such that $f(x) = y$. It is certainly no good starting with an arbitrary element x of X and showing that $f(x)$ is a member of Y since that is known already!

One-to-one: There are (at least) two strategies possible here: you can start by assuming that $x_1 \neq x_2$ and show that $f(x_1) \neq f(x_2)$,or you could assume that $f(x_1) = f(x_2)$ and prove that that implies that $x_1 = x_2$. This second strategy is surprisingly useful.

Example C.2.4 (a) Let $f : \mathbf{R} \to \mathbf{R}$ be the function defined in Example C.2.1 i.e. $X = Y = \mathbf{R}$, $f(x) = x^2$. Then f is neither onto nor $1-1$. To show that f is not onto, it is enough to note that $-1 \in \mathbf{R}$, but there is no $x \in \mathbf{R}$ such that $f(x) = x^2 = -1$. To see that f is not $1-1$, note that $2 \neq -2$, but $f(2) = 4 = f(-2)$.

(b) Let $X = \mathbf{R}$ and let $Y = [0, \infty)$. Let $g : X \to Y$ be defined by $g(x) = x^2$. (Note that $g \neq f$.) Then g is onto but not $1-1$. To see that g is onto, let y be an arbitrary element of Y. That means that $y \geq 0$ and so $\sqrt{y}$ exists; let $x = \sqrt{y}$. Then $f(x) = (\sqrt{y})^2 = y$, so f is onto. To see that g is not $1-1$, we can use the same argument as we used for f in (a).

(c) Let $X = Y = [0, \infty)$ and define $h : X \to Y$ by $h(x) = x^2$. Note that $h \neq f$ and $h \neq g$. Then h is both onto and $1-1$. The proof that h is onto is as for g in (b). To see that h is $1-1$, let $h(x_1) = h(x_2)$, with $x_1, x_2 \in X = [0, \infty)$. Then $x_1^2 = x_2^2$. Since x_1 and x_2 are both positive, this implies that $x_1 = x_2$ (take square roots).

.

Definition C.2.5 (Bijection) *A function $f : X \to Y$ which is both injective and surjective (both $1-1$ and onto) is called a **bijection** or a **one to one correspondence**.*

Any $1-1$ and onto function from X to Y "pairs off" corresponding elements of X and Y. If such a function exists, there is a sense in which we can think of X and Y as the same *sets*, with the elements and X and Y having different "labels" or "names'.

We point out that there is always an obvious bijection from any set X to itself, namely the identity function id_X.

We need to make precise the notion of a function that "undoes" what another function has done.

Definition C.2.6 (Inverse function) *Let $f : X \to Y$ be a function. We say that f is **invertible**, or that f **has an inverse**, if there is a function $g : Y \to X$ such that $g \circ f = id_X$ and $f \circ g = id_Y$, that is, such that*

$$g(f(x)) = x \text{ for every } x \in X \text{ and } f(g(y)) = y \text{ for every } y \in Y.$$

*If such a function g exists, we call it an **inverse** of f.*

We now bring together the last two definitions in a rather neat way:

Theorem C.2.7 *A function $f : X \to Y$ has an inverse if and only if f is a bijection.*

Proof: Suppose that f is a bijection. We need to show that we can define a function $g : Y \to X$ that will be an inverse for f. Now if $y \in Y$, there is an $x \in X$ such that $y = f(x)$, since f is onto. There is, in fact, only one such x. To see this suppose that we also have $y = f(x')$, for some $x' \in X$. Then $f(x) = y = f(x')$. But then we must have $x = x'$, since f is also one-to-one. This means that there is a unique $x \in X$ such that $f(x) = y$, and therefore we can put $g(y) = x$. Since we can do this for every $y \in Y$, we have succeeded in defining a function $g : Y \to X$, and this function clearly has the property that $g(f(x)) = x$ for every $x \in X$. Also, if $y \in Y$, then there is an $x \in X$ such that $y = f(x)$, and then $f(g(y)) = f(g(f(x)) = f(x) = y$. It follows that g is an inverse of f.

Conversely, suppose that g is an inverse of f. To show that f is onto, let $y \in Y$ and put $x = g(y)$. Then $f(x) = f(g(y)) = y$, as we wanted. To show that f is one-to-one, suppose $f(x_1) = f(x_2)$. Then $x_1 = g(f(x_1)) = g(f(x_2)) = x_2$, and we are done. ∎

Example C.2.8 Let $f : [0, \infty) \to [0, \infty)$ be defined by $f(x) = x^2$. We have seen in Example C.2.4 that f is one-to-one and onto, hence a bijection. The function $g : [0, \infty) \to [0, \infty)$ defined by $g(x) = \sqrt{x}$ is an inverse of f.

So far we have talked about *an* inverse of a function. But can a function have more than one inverse? The answer is no:

Theorem C.2.9 *Let $f : X \to Y$ be a bijection. Then the inverse of f is unique.*

Proof: We already know that f has at least one inverse $g : Y \to X$, with the property that $g(f(x)) = x$ for every $x \in X$. Suppose there is another function $h : Y \to X$ such that $h(f(x)) = x$ for every $x \in X$. Since g and h have the same domains and codomains, we only have to show that $h(y) = g(y)$ for every $y \in Y$. So let $y \in Y$. Since f is onto, there is an $x \in X$ such that $y = f(x)$. Then $h(y) = h(f(x)) = x = g(f(x)) = g(y)$, and we are done. ∎

Since the inverse of an invertible function f is unique, it makes sense to have a special symbol for it. Not surprisingly, we write f^{-1} for the inverse of f. So if $f : X \to Y$ is a bijection, then its inverse is the function $f^{-1} : Y \to X$ such that $f^{-1}(f(x)) = x$ for every $x \in X$ and $f(f^{-1}(y)) = y$ for every $y \in Y$.

The following example is a bit surprising: it shows how to pair off all the elements of $\mathbf{R}$ with $(-\frac{\pi}{2}, \frac{\pi}{2})$.

Example C.2.10 The function $f : \mathbf{R} \to (-\frac{\pi}{2}, \frac{\pi}{2})$ defined by $f(x) = \arctan(x)$ is both an injection and a bijection, and hence a bijection.

f is $1 - 1$: Suppose $\arctan(x_1) = \arctan(x_2)$; then

$$\tan(\arctan(x_1)) = \tan(\arctan(x_2))$$

which gives

$$x_1 = x_2$$

as we needed. (Make sure you understand the last step.)

f is onto: Let $y \in (-\frac{\pi}{2}, \frac{\pi}{2})$. We must find $x \in \mathbf{R}$ such that $f(x) = y$. But $\tan(y) \in \mathbf{R}$ and, because $y \in (-\frac{\pi}{2}, \frac{\pi}{2})$, we have $\arctan(\tan(y)) = y$, so we let $x = \tan(y)$ and we are finished. (Again, make sure you understand each step.)

Exercises

1. Which of the following functions are: (i) one-to-one (ii) onto?
   (a) $f : \mathbf{R} \to \mathbf{R}$ defined by $f(x) = 2x + 1$.
   (b) $f : \mathbf{Z} \to \mathbf{Z}$ defined by $f(x) = 2x + 1$.
   (c) $f : \mathbf{R} \to \mathbf{R}$ defined by $f(x) = (x - 3)^2$.
   (d) $f : [0, \infty) \to [0, \infty)$ defined by $f(x) = (x - 3)^2$.
   (e) $f : \mathbf{R}^2 \to \mathbf{R}^2$ defined by $f((x, y)) = (2x - y, x + y)$.
   (f) $f : \mathbf{R}^2 \to \mathbf{R}$ defined by $f(x, y) = xe^y$.
2. Suppose that $f : X \to Y$ and $g : Y \to Z$ are functions.
   (a) Show that, if f and g are both one-to-one, then $g \circ f : X \to Z$ is also one-to-one.
   (b) Show that, if f and g are both onto, then $g \circ f : X \to Z$ is also onto.
3. Show that the inverse of a bijection is also a bijection.

4. Let $h : A \to B$ and $k : B \to C$ be functions. Prove that if $k \circ h : A \to C$ is a one-to-one function, then $h : A \to B$ is a one-to-one function.
   Show by example that the converse does not hold.

5. (a) Give an example of a one-to-one function $f : \mathbf{N} \to \mathbf{N}$ that maps $\mathbf{N}$ onto $\mathbf{N}$.
   (b) Give an example of a one-to-one function $f : \mathbf{N} \to \mathbf{N}$ that does not map $\mathbf{N}$ onto $\mathbf{N}$.
   (c) Give an example of a function f mapping $\mathbf{N}$ onto $\mathbf{N}$ that is not a one-to-one function.
   (d) Give an example of a function $f : \mathbf{N} \to \mathbf{N}$ that is not one-to-one and does not map onto $\mathbf{N}$.

C.3 Relations

We do not explicitly make use of relations in the Linear Algebra course. This section is therefore for those who are interested in learning something more about relations and the way they relate (dreadful pun!) to functions. You will need to be more familiar with this material if you do the second semester module in algebra. We remind you of the definition of a relation:

Definition C.3.1 (Relation) *A **relation** from A to B is just a set of ordered pairs of $A \times B$. That is, a relation from A to B is just some subset R of $A \times B$. (Some books talk about a relation **between** A and B.) To indicate that $(a, b) \in R$, we can also write $a\, R\, b$, and we say " a is related to b (via the relation R).*

Definition C.3.2 (Domain and range) *Let R be a relation from A to B.*

*The **domain** of R is the set $\{a \in A :$ there is a $b \in B$ such that $(a, b) \in R\}$. It is a subset of $A$and is denoted by dom R.*

*The **range** of R is the set $\{b \in B :$ there is a $a \in A$ such that $(a, b) \in R\}$. It is a subset of B and is denoted by ran R.*

Example C.3.3 The sets

$$R = \{(x, y) \in \mathbf{R}^2 : x^2 + y^2 = 1\} \text{ and } S = \{(x, y) \in \mathbf{R}^2 : y \geq 0, x^2 + y^2 \leq 1\}$$

are both relations from $\mathbf{R}$ to $\mathbf{R}$, with $\operatorname{dom} R = \operatorname{dom} S = [-1, 1]$ and $\operatorname{ran} R = [-1, 1], \quad \operatorname{ran} S = [0, 1]$.

Example C.3.4 Let $M_{3\times 4}$ be the set of all 3×4 real matrices. Let

$$\mathcal{R} = \{(A, B) \in M_{3\times 4} \times M_{3\times 4} : A \text{ is row eqiuvalent to } B\}.$$

Then $\mathcal{R}$ is a relation from $M_{3\times 4}$ to $M_{3\times 4}$ with domain and range both equal to $M_{3\times 4}$.

Definition C.3.5 (Inverse relation) *If R is a relation from A to B, the inverse relation R^{-1} of R is the relation from B to A defined by*

$$R^{-1} = \{(b, a) : (a, b) \in R\}.$$

Note that $\operatorname{dom} R^{-1} = \operatorname{ran} R$ and $\operatorname{ran} R^{-1} = \operatorname{dom} R$.

Example C.3.6 If S is the relation from $\mathbf{R}$ to $\mathbf{R}$ defined by

$$S = \{(x, y) \in \mathbf{R}^2 : y \geq 0, x^2 + y^2 \leq 1\},$$

then

$$S^{-1} = \{(y, x) \in \mathbf{R}^2 : x \geq 0, x^2 + y^2 \leq 1\} = \{(x, y) \in \mathbf{R}^2 : y \geq 0, x^2 + y^2 \leq 1\}.$$

Definition C.3.7 (Composition) *Let R be a relation from A to B and S be a relation from B to C. Then the composition $S \circ R$ of the relations R and S is the relation from A to C defined by*

$$S \circ R = \{(a, c) \in A \times C : \textit{ there is a } b \in B \textit{ such that } (a, b) \in R \textit{ and } (b, c) \in S\}.$$

The definition looks daunting and perhaps needs some informal explanation: it really says that you can "get to" c from a via the relation $S \circ R$ if you can get from a to *some* b via the relation R and then get from that b to c via the relation S. We also talk about the relation R *followed by* S. So $S \circ R$ is the relation which captures the idea of "doing" R first followed by "doing" S.

Example C.3.8 Let $S = \{(x, y) : x \leq y\} \subseteq \mathbf{R} \times \mathbf{R}$ and let
$T = \{(x, y) : x + y = 3\} \subseteq \mathbf{R} \times \mathbf{R}$. We find $S \circ T$ and $T \circ S$.

$$\begin{aligned} S \circ T &= \{(x, z) : \text{ for some } y \in \mathbf{R}, (x, y) \in T \text{ and } (y, z) \in S\} \\ &= \{(x, z) : \text{ for some } y \in \mathbf{R}, x + y = 3 \text{ and } y \leq z\} \\ &= \{(x, z) : z \geq 3 - x\} \end{aligned}$$

On the other hand

$$\begin{aligned} T \circ S &= \{(x,z) : \text{ for some } y \in \mathbf{R}, (x,y) \in S \text{ and } (y,z) \in T\} \\ &= \{(x,z) : \text{ for some } y \in \mathbf{R}, x \leq y \text{ and } y + z = 3\} \\ &= \{(x,z) : z \leq 3 - x\} \end{aligned}$$

Notice that $S \circ T \neq T \circ S$.

A function is a special kind of relation. The next definition makes this precise. There is a tradition of using small letters (such as f, g), rather than capital letters, to denote relations that are functions.

Definition C.3.9 (Function) *A function f from A to B is a relation from A to B (i.e. f is a subset of $A \times B$) such that:*

(a) dom$(f) = A$ and

(b) If $(a,b) \in f$ and $(a,c) \in f$ then $b = c$ (for any $a \in A$ and any $b, c \in B$.)

Of course, if we stick to our relation notation, given some function f, instead of saying $(a,b) \in f$ we might write $a\,f\,b$, but nobody does that! We always write the familiar $f(a) = b$ instead of $a\,f\,b$; this does make sense now because, as f is a function, any $a \in A$ will be related to exactly one $b \in B$.

We have defined composition for functions and relations. Since functions are relations, this means that we could have two ways of defining composition for functions. Fortunately they turn out to be the same:
If $f : X \to Y$ and $g : Y \to Z$ are functions, then they are relations, and their composition (as relations) is the relation given by

$$\begin{aligned} g \circ f &= \{(x,z) \in X \times Z : \text{ there is a } y \in Y \text{ such that } (x,y) \in f \text{ and } (y,z) \in g]\} \\ &= \{(x,z) : f(x) = y \text{ and } g(y) = z \text{ for some } y \in Y\} \\ &= \{(x,z) : z = g(f(x))\} \end{aligned}$$

This relation is a function (check this!), and is the same function as the composition of the functions f and g we defined before.

Since functions are relations, every function has an inverse relation. But this inverse relation need not be a function. When will this inverse relation be a function? The answer is perhaps not that surprising, if you keep in mind what we have discovered about the existence of inverse functions before.

Theorem C.3.10 *Let $f : X \to Y$ be a function. Then the inverse relation f^{-1} is a function from Y to X if and only if f is a bijection.*

Proof: Suppose that f is a bijection. Since f is onto, we know that f^{-1} is a relation with domain Y, so all that remains is to show that if (y, x_1) and (y, x_2) are members of f^{-1} then $x_1 = x_2$. So suppose that (y, x_1) and (y, x_2) are members of f^{-1}. Then we must have (x_1, y) and (x_2, y) members of f, that is, $f(x_1) = y = f(x_2)$. Since f is $1-1$ we get $x_1 = x_2$ as we wanted.

Conversely, suppose that f^{-1} is a function from Y to X. This implies that $\operatorname{ran} f = \operatorname{dom} f^{-1} = Y$, so that f is onto. To show that f is $1-1$, suppose that $f(x_1) = f(x_2)$ $(= y$, say). Then, since $(x_1, y) \in f$, we have that $(y, x_1) \in f^{-1}$; similarly, $(y, x_2) \in f^{-1}$. But f^{-1} is assumed to be a function, forcing $x_1 = x_2$ as we wanted. ■

Exercises

1. Sketch the graph of each of the following relations. For each relation, state its domain and range.

   (a) $S = \{(x, y) \in \mathbf{R} \times \mathbf{R} : x^2 + y^2 = 16\}$

   (b) $S = \{(x, y) \in \mathbf{R} \times \mathbf{R} : |x| \leq 1 \text{ and } |y| > 3\}$

   (c) $S = \{(x, y) \in \mathbf{R} \times \mathbf{R} : |x| = 1 \text{ and } 3 < y \leq 5\}$

   Now do the same for the inverse of each of these relations.

2. Let R be a relation from A to B. If $a \in \operatorname{dom} R$, we write $R[a]$ for the set of all elements in B related to a, i.e.

   $$R[a] = \{b \in B : (a, b) \in R\}.$$

   For the relation

   $$R = \{(a, b) \in \mathbf{N}^+ \times \mathbf{N}^+ : a \text{ divides } b\},$$

   list five members of $R[7]$, and list five members of $R[14]$. For which $n \in \mathbf{N}^+$ is it true that $R[n] = \mathbf{N}^+$?

Appendix D

The Greek Alphabet

Small	*Capital*	*Pronounced*
α	A	alpha
β	B	beta
γ	Γ	gamma
δ	Δ	delta
ϵ	E	epsilon
ζ	Z	zeta
η	H	eta
θ	Θ	theta
ι	I	iota
κ	K	kappa
λ	Λ	lambda
μ	M	mu
ν	N	nu
ξ	Ξ	xi
o	O	omicron
π	Π	pi
ρ	P	rho
σ	Σ	sigma
τ	T	tau
υ	Υ	upsilon
ϕ	Φ	phi
χ	X	chi
ψ	Ψ	psi
ω	Ω	omega

Appendix E

Introduction to OCTAVE

OCTAVE is a powerful programming language, well suited to manipulation of vectors and matrices. This handout is very brief: it shows you how to get started and some basic functions.

How to get started: OCTAVE is an open source program, and can be downloaded for free at `https://www.gnu.org/software/octave/`.

When you open OCTAVE, you will see a *Command Window* with some inormation and disclaimers, and below it the symbol >> followed by a flashing cursor. This indicates that OCTAVE is waiting for a command. This line is called the *command line*. You may also see *Workspace* and *Command History* windows; you can close thes if you do not need them.

To get out of OCTAVE you can type "quit" on the command line.

Entering matrices. To enter the matrix $A = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{pmatrix}$, type in:

A = [1 space 2 space 3;4 space 5 space 6]. The spaces separate the entries; the semi-colons indicate the end of a row; the brackets [and] mark the beginning and end of the matrix. Now press enter; if you've entered it as above, you should see the matrix A nicely arrayed in matrix form. OCTAVE checks that your matrix has rows of the same length and columns of the same length. It also now stores your matrix for as long as you want. After entering this matrix, you just need to type A whenever you want to use it. OCTAVE is case sensitive, so you can enter a different matrix for a if you want, and OCTAVE will distinguish between a and A. If you want to change A, just enter another matrix after typing $A =$ and OCTAVE stores your new matrix A and discards the old one.

Useful timesavers:

- Pressing $\uparrow$ gives you the last command typed; pressing it repeatedly gives you all the previous commands you typed. This can save you a lot of typing if you want to change some previous command: recall it using $\uparrow$, edit it, and press enter.
- Typing "who" gives you a list of variables currently in use.
- Typing "whos" gives a list of variables in use, as well as what they are (size of matrix, etc.)

Operations with matrices: Let's assume you've typed in matrices A and B. Typing in

- $A + B$ and enter returns $A + B$ if this is defined.
- $A - B$ and enter returns $A - B$ if this is defined.
- $A * B$ and enter returns the product AB if it is defined.
- $A\hat{}n$ and enter (n a positive integer) returns the n-th power of A.
- $A \backslash B$ and enter returns the matrix $A^{-1}B$ if this is defined. In general, it gives a solution for the equation $AX = B$, but you must use it with care: if the system is inconsistent, it returns the so-called "least squares" solution (more about that later in the course); if the system is indeterminate, it returns one solution of the system, without telling you that the system is indeterminate, otherwise it returns the unique solution of the system.
- inv(A) and enter returns the inverse of A if it exists.
- A' and enter returns the transpose A^T of A.
- det(A) and enter returns the determinant of A.
- poly(A) and return gives the coefficients of the characteristic polynomial of A.
- eig(A) and return gives you the eigenvalues of A (including the complex ones).
- $[V, D] = \text{eig}(A)$ and return gives you a matrix V with columns the eigenvectors of A corresponding to the eigenvalues of A; the matrix D is a diagonal matrix with these eigenvalues on the main diagonal.

The colon operator: This has a tremendous number of uses. We illustrate its use in matrices:

Entering $A(:,2)$ will give you the second column of matrix A; the colon is telling OCTAVE to look at all rows. Similarly entering $A(3,:)$ will get you the third row of A; the colon is telling OCTAVE to look at all columns. Thus, if you want to do a row operation on matrix A (say, 2×row 2 added to row 3), you could type in

$$A(3,:) = A(3,:) + 2A(2,:)$$

which will result in the new row 3 of A being twice row 2 added to the old row 3.

How to get help: If you want help on a specific command, say the "det" command, type "help det" in the command line. Typing "doc"in the command line, or using the "Help" button on the OCTAVE taskbar, will take you to the instruction manual.

We have already mentioned the program MATLAB, which is very similar to OCTAVE. Most of the OCTAVE commands described above are exactly the same in MATLAB.