Contents

Chapter A

Introduction

This chapter is a quick introduction to the whole course. The first section is all about abstraction: what it is, and why it's your friend. The second and third are brisk summaries of facts about two important mathematical concepts: first vectors, then matrices. You may know much of what's there—in which case, make sure you don't glaze over and miss the few things you don't know. Or much of it may be new to you.

In either case, you should work through the material in detail, making sure you understand everything. If you're shaky on anything in these sections, it will come back to bite you later!

It's in the nature of these accelerated courses that there's quite a lot to work through. It's also part of the deal that you may need to put in significant time looking up details in books or other sources.

A1 The power of abstraction

For the lecture of Monday, 28 September 2015; part one of five

Learning mathematics involves getting used to higher and higher levels of abstraction. This section explains what abstraction is, why 'abstract' isn't a negative word (or shouldn't be), and what kind of abstract concepts we'll meet in this course.

A thing, and another thing, but no more things

Once upon a time, human beings realized that it would be useful to have a quick way of saying 'a thing, and another thing, but no more things'. So they invented a nonsense word: *two*. This saved early human beings from having to go round saying 'I have a parent, and another parent, but no more parents' or 'I have a leg, and another leg, but no more legs'. Instead, they could just say 'I have two parents' and 'I have two legs'.

But what does 'two' on its own mean—not 'two parents', or 'two legs', but just 'two'? It's a made-up word, an abstraction. It's not attached to any particular real-world objects, such as parents or legs. It lives in the same idealized mathematical world that contains mythical concepts such as perfect circles.

But exactly *because* the concept of 'two' isn't attached to any real-world objects, it's extremely useful and flexible. If you've shown that adding two cows to two cows gives you the same result as adding one cow to three cows, that's only of interest to people who count cows. But if you've shown that $2+2 = 1+3$, that's a general, abstract result that applies to any kind of object you might want to count: cows, trees, parents, legs, and so on.

People sometimes use the word *abstract* in a negative way, to mean something like 'divorced from reality' or 'having no practical application'. But abstraction is exactly what gives mathematics its power. It's what makes maths applicable to an enormous range of real-world situations, rather than tied to one in particular. It's what enables maths to cross geographical and cultural boundaries.

Mathematics tends to get more and more abstract the further you go. Even in this course, you'll see a gradual ratcheting-up of the level of abstraction. But why is it useful?

Spaghetti

Maybe the first dish you learned to cook was spaghetti. Maybe you asked someone how to cook it, or you read the packet; anyway, you learned that the way to do it is to boil some water in a pan, add the dry spaghetti, and simmer vigorously until it's done.

Then you bought a packet of penne (the hollow tubes). How do you cook those? You boil some water in a pan, add the dry penne, and simmer vigorously until it's done.

At this point, if not sooner, you'll have understood that there is a general concept of *pasta*. There's no need to clutter up your mind with memorized methods for cooking spaghetti, and cooking penne, and cooking fusilli, and cooking fettuccine, and so on. You only have to remember one single thing: how to cook pasta.

But after a while, you get fed up with pasta and feel like some rice. How do you cook that? Well, one easy way is to boil some water in a pan, add the rice, and simmer vigorously until it's done. Or maybe you feel like some bulghur, or barley, or couscous, or quinoa. How do you cook those? You boil some water in a pan, add the bulghur or whatever, and simmer vigorously until it's done.

Eventually, after you've gained some experience of cooking, you realize the common thread: all these types of food cooked in the same way are *grains*. And that's a useful thought to have, because now, whenever you meet some unfamiliar grain, you can take a pretty good guess at how to cook it.

So generalizing from the very particular concept of spaghetti to the more general concept of pasta, and then to the even more general concept of grain, is useful in your development as a cook. Something similar is true in mathematics. Although as a novice cook (or mathematician) you might initially feel more comfortable with very particular types of food (or mathematical object), part of learning to grow as a cook (or mathematician) is expanding your repertoire—familiarizing yourself with the unfamiliar.

Warning Don't get intoxicated on generality! Suppose someone asks you to make toast. Armed with your knowledge about the general theory of cooking grains, you say to yourself 'Bread is made of wheat, which is a grain; so I shall make toast by boiling some water in a pan, adding the bread, and simmering vigorously until it's done'.

Of course, you wouldn't really say that, but there *is* a risk of doing something similar in a mathematical context. General, abstract statements still have to be stated in precise mathematical language, taking care to make sure that everything is clear and correct. It is the precision of language that enables us to navigate safely through unfamiliar abstract territory without doing the mathematical equivalent of boiling bread.

Climbing the ladder of abstraction

One way to explain this course is that it involves four different levels of abstraction, each higher than the last.

We begin with systems of simultaneous linear equations, or *linear systems* for short. A linear system looks something like this:

$$\begin{aligned} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n &= b_1 \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n &= b_2 \\ &\vdots \\ a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n &= b_m, \end{aligned}$$

where the numbers a_{ij} and b_j are treated as known and the numbers x_i as unknown.

We'll see that if we want to think about linear systems, it's easier if we do it at a higher level of abstraction, using the concept of *matrix*. As we'll see, the whole linear system above can be encapsulated in a single, simple equation:

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

where A is a matrix (treated as known), $\mathbf{b}$ is a vector (also treated as known), and $\mathbf{x}$ is another vector (treated as unknown). Obviously we've gained in simplicity, reducing m long equations to one short equation. The price to pay is a higher level of abstraction, since we're now dealing with matrices and vectors rather than just numbers.

But actually, the higher level of abstraction is immediately useful. Simply writing down the equation '$A\mathbf{x} = \mathbf{b}$' suggests a possible way of solving it. For if A, $\mathbf{x}$ and $\mathbf{b}$ were numbers, the solution would be $\mathbf{x} = \mathbf{b}/A$ (at least assuming that $A \neq 0$). Now for matrices and vectors, the right-hand side doesn't make sense, but it does give a useful clue as to how to proceed—again, something we'll come back to later in the course.

After we've worked with matrices for a while, we'll see that in many situations, the most important thing about an $m \times n$ matrix A is the mapping $T \colon \mathbb{R}^n \to \mathbb{R}^m$ defined by $T(\mathbf{x}) = A\mathbf{x}$ (for $\mathbf{x} \in \mathbb{R}^n$). Mappings like this have special properties, such as $T(\mathbf{x}+\mathbf{y}) = T(\mathbf{x})+T(\mathbf{y})$, and a special name: they're called *linear maps* or *linear transformations*. This is the third level of abstraction.

Even then, we're not done. As we'll see when we're working with linear maps $T\colon \mathbb{R}^n \to \mathbb{R}^m$, it's often not important that the domain and codomain are $\mathbb{R}^n$ and $\mathbb{R}^m$ specifically. In the theory of linear maps, only a few key features of $\mathbb{R}^n$ really matter; for instance, that one can add together two elements of $\mathbb{R}^n$ to get another element of $\mathbb{R}^n$. We'll write down a general definition of *vector space*, encapsulating all the key features of $\mathbb{R}^n$. So $\mathbb{R}^n$ is a vector space for each n, but there are other vector spaces besides. That's our fourth and final level of abstraction.

Ultimately, then, we'll understand linear algebra as the study of vector spaces and linear maps between them. That's all this course has time for, but the theme is taken up again in the Year 3 course Honours Algebra, as well as being widely useful in many other areas of mathematics.

A2 Vectors

For the lecture of Monday, 28 September 2015; part two of five

Let $\mathbb{R}$ denote the set of real numbers. We sometimes refer to real numbers as **scalars**.

Let $n \geq 0$. An n-dimensional **vector** is simply a list of n real numbers $x_1, x_2, \ldots, x_n$, which we write in a column:

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

We write $\mathbb{R}^n$ for the set of all n-dimensional vectors. Often elements of $\mathbb{R}^n$ are written in the horizontal notation

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

instead. It makes no real difference which notation we use, but in this course we are going to use column notation.

It saves space if we write

$$\mathbf{x} = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix}, \qquad \mathbf{y} = \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{pmatrix},$$

and so on. The convention is to use bold typeface for vectors. In handwriting, it's hard to write bold symbols like $\mathbf{x}$, so we write $\underline{x}$ instead.

Algebraic operations on vectors

Any two vectors $\mathbf{x}, \mathbf{y} \in \mathbb{R}^n$ can be added together to get a third vector $\mathbf{x} + \mathbf{y} \in \mathbb{R}^n$:

$$\mathbf{x} + \mathbf{y} = \begin{pmatrix} x_1 + y_1 \\ x_2 + y_2 \\ \vdots \\ x_n + y_n \end{pmatrix}.$$

Any vector $\mathbf{x}$ in $\mathbb{R}^n$ can be multiplied by any scalar $a \in \mathbb{R}$ to get another vector $a\mathbf{x} \in \mathbb{R}^n$:

$$a\mathbf{x} = \begin{pmatrix} ax_1 \\ ax_2 \\ \vdots \\ ax_n \end{pmatrix}.$$

One especially important vector in $\mathbb{R}^n$ is the **zero vector**

$$\mathbf{0} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}.$$

Here are some basic properties of addition and scalar multiplication of vectors.

Lemma A2.1 *Let* $\mathbf{x}, \mathbf{y}, \mathbf{z} \in \mathbb{R}^n$ *and* $a, b \in \mathbb{R}$. *Then:*

i. $(\mathbf{x} + \mathbf{y}) + \mathbf{z} = \mathbf{x} + (\mathbf{y} + \mathbf{z})$*;*

ii. $\mathbf{x} + \mathbf{y} = \mathbf{y} + \mathbf{x}$*;*

iii. $\mathbf{x} + \mathbf{0} = \mathbf{x}$*;*

iv. $a(b\mathbf{x}) = (ab)\mathbf{x}$*;*

v. $1\mathbf{x} = \mathbf{x}$*;*

vi. $a(\mathbf{x} + \mathbf{y}) = a\mathbf{x} + a\mathbf{y}$*;*

vii. $(a + b)\mathbf{x} = a\mathbf{x} + b\mathbf{x}$*;*

viii. $0\mathbf{x} = \mathbf{0}$.

Proof This is a series of routine checks using the definitions. (You should do a few of them, until you're confident you could do them all.) □

We write $(-1)\mathbf{x}$ as $-\mathbf{x}$; it is the vector whose ith entry is $-x_i$. We have $-\mathbf{x} + \mathbf{x} = \mathbf{0}$, either by direct calculation or using Lemma A2.1 (how?).

The dot product

Any two vectors $\mathbf{x}, \mathbf{y} \in \mathbb{R}^n$ have a **dot product** or **scalar product** $\mathbf{x} \cdot \mathbf{y} \in \mathbb{R}$, defined by

$$\mathbf{x} \cdot \mathbf{y} = \sum_{i=1}^{n} x_i y_i.$$

(On the right-hand side, we have used summation notation; it means $x_1 y_1 + x_2 y_2 + \cdots + x_n y_n$.) Note that $\mathbf{x} \cdot \mathbf{y}$ is a scalar, not a vector—hence the name 'scalar product'.

The **length** of a vector $\mathbf{x} \in \mathbb{R}^n$ is

$$\|\mathbf{x}\| = \sqrt{\sum_{i=1}^{n} x_i^2} = \sqrt{\mathbf{x} \cdot \mathbf{x}}.$$

Let us record some basic properties of the dot product and length.

Lemma A2.2 *Let* $\mathbf{x}, \mathbf{y}, \mathbf{z} \in \mathbb{R}^n$ *and* $a \in \mathbb{R}$. *Then:*

i. $\mathbf{x} \cdot \mathbf{y} = \mathbf{y} \cdot \mathbf{x}$*;*

ii. $\mathbf{x} \cdot (\mathbf{y} + \mathbf{z}) = \mathbf{x} \cdot \mathbf{y} + \mathbf{x} \cdot \mathbf{z}$*;*

iii. $\mathbf{x} \cdot \mathbf{0} = 0$*;*

iv. $\mathbf{x} \cdot (a\mathbf{y}) = a(\mathbf{x} \cdot \mathbf{y})$*;*

v. $\|\mathbf{x}\| \geq 0$*, with equality if and only if* $\mathbf{x} = \mathbf{0}$*;*

vi. $\|a\mathbf{x}\| = |a| \, \|\mathbf{x}\|$.

Proof Again, these are routine checks using the definitions. $\square$

For nonzero vectors $\mathbf{x}$ and $\mathbf{y}$ in $\mathbb{R}^2$ or $\mathbb{R}^3$, it can be shown that

$$\mathbf{x} \cdot \mathbf{y} = \|\mathbf{x}\| \, \|\mathbf{y}\| \cos \theta$$

where θ is the angle between the vectors $\mathbf{x}$ and $\mathbf{y}$. It follows that

$$|\mathbf{x} \cdot \mathbf{y}| \leq \|\mathbf{x}\| \, \|\mathbf{y}\|$$

in $\mathbb{R}^2$ and $\mathbb{R}^3$. We now show that this inequality holds in $\mathbb{R}^n$ for all $n \geq 0$.

Lemma A2.3 (Cauchy–Schwarz inequality) *For all* $\mathbf{x}, \mathbf{y} \in \mathbb{R}^n$*,*

$$|\mathbf{x} \cdot \mathbf{y}| \leq \|\mathbf{x}\| \|\mathbf{y}\|$$

with equality if and only if $\mathbf{x}$ *is a scalar multiple of* $\mathbf{y}$ *or vice versa.*

Intuitively, the condition '$\mathbf{x}$ is a scalar multiple of $\mathbf{y}$ or vice versa' means that $\mathbf{x}$ and $\mathbf{y}$ point in the same or opposite directions. The 'or vice versa' condition is needed in order to cover the possibility that $\mathbf{x}$ or $\mathbf{y}$ is $\mathbf{0}$.

Proof In the case $\mathbf{y} = \mathbf{0}$, both sides of the inequality are 0 and $\mathbf{y}$ is a scalar multiple of $\mathbf{x}$ (namely, $0\mathbf{x}$), so the result holds. Now assume that $\mathbf{y} \neq \mathbf{0}$.

If $\mathbf{y}$ is a scalar multiple of $\mathbf{x}$ then $\mathbf{x}$ is a scalar multiple of $\mathbf{y}$ (since $\mathbf{y} \neq \mathbf{0}$). But if $\mathbf{x} = a\mathbf{y}$ for some scalar a, then $\mathbf{x} \cdot \mathbf{y} = a\mathbf{y} \cdot \mathbf{y} = a\|\mathbf{y}\|^2$, and so $a = \mathbf{x} \cdot \mathbf{y} / \|\mathbf{y}\|^2$. Hence the condition '$\mathbf{x}$ is a scalar multiple of $\mathbf{y}$ or vice versa' is equivalent to the condition

$$\mathbf{x} = \frac{\mathbf{x} \cdot \mathbf{y}}{\|\mathbf{y}\|^2} \mathbf{y}.$$

Now

$$\begin{aligned}
0 &\leq \left\| \mathbf{x} - \frac{\mathbf{x} \cdot \mathbf{y}}{\|\mathbf{y}\|^2} \mathbf{y} \right\|^2 \\
&= \left(\mathbf{x} - \frac{\mathbf{x} \cdot \mathbf{y}}{\|\mathbf{y}\|^2} \mathbf{y} \right) \cdot \left(\mathbf{x} - \frac{\mathbf{x} \cdot \mathbf{y}}{\|\mathbf{y}\|^2} \mathbf{y} \right) \\
&= \|\mathbf{x}\|^2 - 2 \frac{(\mathbf{x} \cdot \mathbf{y})^2}{\|\mathbf{y}\|^2} + \frac{(\mathbf{x} \cdot \mathbf{y})^2}{\|\mathbf{y}\|^2} \\
&= \frac{1}{\|\mathbf{y}\|^2} \left(\|\mathbf{x}\|^2 \, \|\mathbf{y}\|^2 - (\mathbf{x} \cdot \mathbf{y})^2 \right),
\end{aligned}$$

or equivalently

$$(\mathbf{x} \cdot \mathbf{y})^2 \leq \|\mathbf{x}\|^2 \, \|\mathbf{y}\|^2.$$

Taking square roots on both sides gives the result. Equality holds if and only if $\mathbf{x} - \frac{\mathbf{x} \cdot \mathbf{y}}{\|\mathbf{y}\|^2} \mathbf{y} = \mathbf{0}$; but we have already seen that this is equivalent to the condition that $\mathbf{x}$ is a scalar multiple of $\mathbf{y}$ or vice versa. $\square$

Lemma A2.4 (Triangle inequality) *For all* $\mathbf{x}, \mathbf{y} \in \mathbb{R}^n$*,*

$$\|\mathbf{x} + \mathbf{y}\| \leq \|\mathbf{x}\| + \|\mathbf{y}\|.$$

To see why it's called the 'triangle inequality', draw a picture: it says that the length of each side of a triangle is at most the sum of the lengths of the other two sides. This is visually obvious in $\mathbb{R}^2$ and $\mathbb{R}^3$, but can you really claim that it's obvious in $\mathbb{R}^{14382}$?

Proof Using the Cauchy–Schwarz inequality,

$$\begin{aligned}\|\mathbf{x}+\mathbf{y}\|^2 &= (\mathbf{x}+\mathbf{y})\cdot(\mathbf{x}+\mathbf{y})\\ &= \|\mathbf{x}\|^2 + 2\mathbf{x}\cdot\mathbf{y} + \|\mathbf{y}\|^2\\ &\leq \|\mathbf{x}\|^2 + 2|\mathbf{x}\cdot\mathbf{y}| + \|\mathbf{y}\|^2\\ &\leq \|\mathbf{x}\|^2 + 2\|\mathbf{x}\|\,\|\mathbf{y}\| + \|\mathbf{y}\|^2\\ &= \big(\|\mathbf{x}\| + \|\mathbf{y}\|\big)^2.\end{aligned}$$

Taking square roots on both sides gives the result. □

What is the angle between two nonzero vectors in $\mathbb{R}^n$? We know the answer for $n = 2, 3$. For general n, let us take our inspiration from the 2- and 3-dimensional cases. In other words, for nonzero $\mathbf{x}, \mathbf{y} \in \mathbb{R}^n$, define the **angle** θ between them by

$$\theta = \cos^{-1} \frac{\mathbf{x}\cdot\mathbf{y}}{\|\mathbf{x}\|\,\|\mathbf{y}\|} \in [0, \pi].$$

(Notation: for real numbers $a \leq b$, we write $[a, b] = \{x \in \mathbb{R} : a \leq x \leq b\}$.)

Let's check that this 'definition' of θ really does make sense. The Cauchy–Schwarz inequality implies that $\frac{\mathbf{x}\cdot\mathbf{y}}{\|\mathbf{x}\|\,\|\mathbf{y}\|} \in [-1, 1]$. Every number in $[-1, 1]$ has a unique inverse cosine in $[0, \pi]$. So, the definition of θ does indeed make sense. And the definition immediately implies that

$$\mathbf{x}\cdot\mathbf{y} = \|\mathbf{x}\|\,\|\mathbf{y}\| \cos\theta$$

for all nonzero $\mathbf{x}, \mathbf{y} \in \mathbb{R}^n$, extending the pattern we've already seen for $n = 2$ and $n = 3$.

We say that $\mathbf{x}$ and $\mathbf{y}$ are **orthogonal** if $\mathbf{x}\cdot\mathbf{y} = 0$. (Other ways of saying orthogonal are 'perpendicular' and 'at right angles'.) This happens exactly when $\mathbf{x} = \mathbf{0}$ or $\mathbf{y} = \mathbf{0}$ or $\theta = \pi/2$.

The cross product

There is a further kind of product defined on $\mathbb{R}^3$ only—not $\mathbb{R}^n$ in general. Any two vectors $\mathbf{x}\times\mathbf{y}$ have a **cross product** or **vector product** $\mathbf{x}\times\mathbf{y} \in \mathbb{R}^3$, defined by

$$\mathbf{x}\times\mathbf{y} = \begin{pmatrix} x_2y_3 - x_3y_2 \\ x_3y_1 - x_1y_3 \\ x_1y_2 - x_2y_1 \end{pmatrix}.$$

As the name suggests, $\mathbf{x}\times\mathbf{y}$ is a vector, not a scalar.

Geometrically, $\mathbf{x}\times\mathbf{y}$ is a vector orthogonal to both $\mathbf{x}$ and $\mathbf{y}$. This is the main point of the construction. So if someone hands you two vectors in $\mathbb{R}^3$, you now know how to immediately write down a vector at right angles to both.

Here are some basic properties of the cross product.

Lemma A2.5 *Let $\mathbf{x}, \mathbf{y}, \mathbf{z} \in \mathbb{R}^3$ and $a \in \mathbb{R}$. Then:*

i. $\mathbf{x} \times \mathbf{y} = -\mathbf{y} \times \mathbf{x}$;

ii. $\mathbf{x} \times \mathbf{x} = \mathbf{0}$;

iii. $\mathbf{x} \times (\mathbf{y} + \mathbf{z}) = (\mathbf{x} \times \mathbf{y}) + (\mathbf{x} \times \mathbf{z})$;

iv. $\mathbf{x} \times (a\mathbf{y}) = a(\mathbf{x} \times \mathbf{y})$;

v. $(\mathbf{x} \times \mathbf{y}) \cdot \mathbf{x} = 0 = (\mathbf{x} \times \mathbf{y}) \cdot \mathbf{y}$.

Proof Once more, these are straightforward algebraic exercises. $\square$

Part (v) states that $\mathbf{x} \times \mathbf{y}$ is orthogonal to both $\mathbf{x}$ and $\mathbf{y}$, as claimed above.

When $\mathbf{x}$ and $\mathbf{y}$ are nonzero, knowing that $\mathbf{x} \times \mathbf{y}$ is orthogonal to $\mathbf{x}$ and $\mathbf{y}$ tells us what direction it points in. But what is its length? The following result gives the answer.

Lemma A2.6 *Let* $\mathbf{x}$ *and* $\mathbf{y}$ *be nonzero vectors in* $\mathbb{R}^3$*. Then*

$$\|\mathbf{x} \times \mathbf{y}\| = \|\mathbf{x}\|\, \|\mathbf{y}\| \sin\theta$$

where $\theta \in [0, \pi]$ *is the angle between* $\mathbf{x}$ *and* $\mathbf{y}$*.*

Proof We have

$$\begin{aligned}
\|\mathbf{x} \times \mathbf{y}\|^2 + (\mathbf{x} \cdot \mathbf{y})^2 &= (x_2y_3 - x_3y_2)^2 + (x_3y_1 - x_1y_3)^2 + (x_1y_2 - x_2y_1)^2 \\
&\quad + (x_1y_1 + x_2y_2 + x_3y_3)^2 \\
&= (x_1^2 + x_2^2 + x_3^2)(y_1^2 + y_2^2 + y_3^2) \\
&= \|\mathbf{x}\|^2 \|\mathbf{y}\|^2
\end{aligned}$$

where the second equality is a routine calculation. Hence

$$\begin{aligned}
\|\mathbf{x} \times \mathbf{y}\|^2 &= \|\mathbf{x}\|^2 \|\mathbf{y}\|^2 - (\mathbf{x} \cdot \mathbf{y})^2 \\
&= \|\mathbf{x}\|^2 \|\mathbf{y}\|^2 - (\|\mathbf{x}\|\|\mathbf{y}\| \cos\theta)^2 \\
&= \big(\|\mathbf{x}\|\|\mathbf{y}\| \sin\theta\big)^2.
\end{aligned}$$

Finally, $\sin\theta \geq 0$ for all $\theta \in [0, \pi]$, so taking square roots on both sides gives the result. $\square$

A3 Matrices

For the lecture of Monday, 28 September 2015; part three of five

Take integers $m, n \geq 0$. An $m \times n$ real **matrix** consists of a real number a_{ij} for each $i \in \{1, \ldots, m\}$ and $j \in \{1, \ldots, n\}$. We visualize them arranged in a grid:

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

and we write $A = (a_{ij})$ for the matrix as a whole. We refer to a_{ij} as the **(i, j)-entry** of A.

A vector is just an $m \times 1$ matrix. Given this, it's a little inconsistent that we write vectors in bold typeface and matrices in ordinary typeface; but it's a common convention and we'll stick with it.

A 1×1 matrix is just a real number.

Algebraic operations on matrices

There are several algebraic operations on matrices:

- **Addition**. Given $m \times n$ matrices $A = (a_{ij})$ and $B = (b_{ij})$, we define an $m \times n$ matrix $A + B = (c_{ij})$ by

  $$c_{ij} = a_{ij} + b_{ij}$$

  $(1 \leq i \leq m,\ 1 \leq j \leq n)$.

- **Scalar multiplication**. Given an $m \times n$ matrix $A = (a_{ij})$ and a scalar $c \in \mathbb{R}$, we define an $m \times n$ matrix $cA = (b_{ij})$ by

  $$b_{ij} = ca_{ij}$$

  $(1 \leq i \leq m,\ 1 \leq j \leq n)$.

- **Matrix multiplication**. Given an $m \times n$ matrix $A = (a_{ij})$ and an $n \times p$ matrix $B = (b_{jk})$, we define an $m \times p$ matrix $AB = (c_{ik})$ by

  $$c_{ik} = \sum_{j=1}^{n} a_{ij} b_{jk}$$

  $(1 \leq i \leq m,\ 1 \leq k \leq p)$.

One particularly important matrix is the $m \times n$ matrix all of whose entries are 0; we call this matrix 0, too. Another important matrix is the $n \times n$ **identity matrix** I_n, whose (i, j)-entry is 1 for $i = j$ and 0 for $i \neq j$.

Here are some basic facts about matrix algebra.

Lemma A3.1 *i.* $(A + B) + C = A + (B + C)$ *if* A, B *and* C *are* $m \times n$ *matrices;*

ii. $A + B = B + A$ *if* A *and* B *are* $m \times n$ *matrices;*

iii. $A + 0 = A$*;*

iv. $c(A + B) = cA + cB$ *if* A *and* B *are* $m \times n$ *matrices and* c *is a scalar;*

v. $(AB)C = A(BC)$ *if* A *is an* $m \times n$ *matrix,* B *is an* $n \times p$ *matrix and* C *is a* $p \times q$ *matrix;*

vi. $AI_n = A = I_m A$ *if* A *is an* $m \times n$ *matrix;*

vii. $A(B + C) = AB + AC$ *if* A *is an* $m \times n$ *matrix and* B *and* C *are* $n \times p$ *matrices;*

viii. $(A + B)C = AC + BC$ *if* A *and* B *are* $m \times n$ *matrices and* C *is an* $n \times p$ *matrix;*

ix. $c(AB) = (cA)B = A(cB)$ *if* A *is an* $m \times n$ *matrix,* B *is an* $n \times p$ *matrix, and* c *is a scalar.*

Proof Again, the proofs are straightforward checks using the definitions. □

However, matrix multiplication is not **commutative**, that is, $AB \neq BA$ in general.

The **transpose** of an $m \times n$ matrix A is the $n \times m$ matrix A^T whose (j, i)-entry is the (i, j)-entry of A (for $1 \leq i \leq m$, $1 \leq j \leq n$).

A matrix A is **symmetric** if $A^T = A$, that is, $a_{ji} = a_{ij}$ for all i, j. It is **antisymmetric** (or **skew symmetric**) if $A^T = -A$, that is, $a_{ji} = -a_{ij}$ for all i, j. A matrix can only be symmetric or antisymmetric if it is square ($m = n$).

We can express the dot product in terms of matrix multiplication and transpose. Indeed, given column vectors $\mathbf{x}, \mathbf{y} \in \mathbb{R}^n$, we have a row vector $\mathbf{x}^T$ (a $1 \times n$ matrix), so we can form the matrix product $\mathbf{x}^T \mathbf{y}$. This is a 1×1 matrix, that is, a scalar, and it is exactly the dot product:

$$\mathbf{x}^T \mathbf{y} = \mathbf{x} \cdot \mathbf{y}.$$

Here are some elementary properties of transpose:

Lemma A3.2 *Let* A *and* B *be matrices and* c *a scalar. Then:*

i. $(A + B)^T = A^T + B^T$*;*

ii. $(cA)^T = cA^T$*;*

iii. $(AB)^T = B^T A^T$*.*

Proof Again, these are elementary checks. Note the reversal of order in (iii). □

Any matrix can be viewed as a sequence of column vectors placed next to each other, or alternatively as a pile of row vectors placed on top of each other. It is sometimes useful to think about matrix multiplication in those terms, as follows.

Let A be an $m \times n$ matrix and B an $n \times p$ matrix, so that the matrix product AB is defined. Write the ith row of A as $\mathbf{x}_i \in \mathbb{R}^n$ (for $1 \leq i \leq m$) and the kth column of B as $\mathbf{y}_k \in \mathbb{R}^n$ (for $1 \leq k \leq p$). Then the (i, k)-entry of AB is $\mathbf{x}_i \mathbf{y}_k$ (which is a 1×1 matrix, that is, a real number). The ith row of AB is $\mathbf{x}_i B$, and the kth column of AB is $A\mathbf{y}_k$.

Inverse matrices

An $m \times n$ matrix A is **invertible** if there exists an $n \times m$ matrix B such that $AB = I_m$ and $BA = I_n$.

Let A be an invertible matrix. Then there can be only one matrix B with the properties just mentioned, since if B' is another one then

$$B = BI_m = B(AB') = (BA)B' = I_n B' = B'.$$

We call B the **inverse** of A and write B as A^{-1}.

Proposition A3.3 *i. Every invertible matrix is square. That is, if A is an invertible $m \times n$ matrix then $m = n$.*

ii. Let A and B be $n \times n$ matrices. Then $AB = I_n \iff BA = I_n$.

Neither of these facts is obvious. We will prove them later, once we have developed more theory. Note that (ii) is only true for square matrices: e.g. you should be able to find a 1×2 matrix A and a 2×1 matrix B with $AB = I_1$ but $BA \neq I_2$.

Examples A3.4 i. Take scalars $a, b, c \neq 0$. Then

$$\begin{pmatrix} a & 0 & 0 \\ 0 & b & 0 \\ 0 & 0 & c \end{pmatrix}^{-1} = \begin{pmatrix} 1/a & 0 & 0 \\ 0 & 1/b & 0 \\ 0 & 0 & 1/c \end{pmatrix}.$$

ii. Consider a 2×2 matrix $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$. If $ad - bc \neq 0$ then A is invertible and

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

Write B for the right-hand side. To check that B really is the inverse of A, in principle we need to check that $AB = I_2$ and $BA = I_2$. However, Proposition A3.3(ii) means that we only need to check one of these. This is straightforward (try it!).

The number $ad - bc$ is called the **determinant** of A. (Questions: what happens if $ad - bc = 0$? Is A invertible? If so, why? If not, why not?)

Lemma A3.5 *Let A and B be invertible $n \times n$ matrices. Then AB is also invertible, and $(AB)^{-1} = B^{-1}A^{-1}$.*

Proof We have

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

Also $(B^{-1}A^{-1})(AB) = I_n$, either by a similar argument or by Proposition A3.3(ii). $\square$

Chapter B

Simultaneous linear equations

B1 Introduction to linear systems

For the lecture of Monday, 28 September 2015; part four of five

A system of simultaneous linear equations—or 'linear system' for short—is a collection of equations like this:

$$\begin{aligned}
2x - 3y &= z + 6 \\
y + 5 &= -2z - 3(x - 2) \\
x + y + z &= 0 \\
3x + 4 &= 2y
\end{aligned}$$

'Simultaneous' means that we're interested in values of x, y and z that satisfy all the equations at once. 'Linear' means that terms such as xy, x^2 and 2^x do not appear anywhere: the equations involve only constants and scalar multiples of variables, added and subtracted from each other.

We might as well tidy up the equations so that all the variables are on the left and all the constants are on the right. Thus, a linear system is a collection of equations of the following form:

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

Here a_{ij}, b_j and x_i all represent real numbers, but we think of a_{ij} and b_j as 'known' and x_i as 'unknown'. So, we have m equations in n unknowns. We are interested in finding the values of $x_1, \ldots, x_n$ that satisfy all the equations.

Here are some fundamental questions about linear systems:

- Are there any solutions?

- Is there are a *unique* solution?
- If there is more than one solution, how many are there?
- How can we calculate all the solutions?

Examples of linear systems

To get us started on answering these questions, let us consider systems of two equations in two unknowns.

Example B1.1 A 2×2 linear system consists of equations

$$\begin{aligned} a_{11}x + a_{12}y &= b_1 \\ a_{21}x + a_{22}y &= b_2 \end{aligned}$$

in x and y. Assuming that a_{11} and a_{12} are not both zero, the first equation represents a straight line in the (x, y)-plane. Assuming that a_{21} and a_{22} are not both zero, the second represents a straight line too.

The set of solutions is the set of points lying on both lines. There are several possibilities:

- The lines intersect at a single point. Then the system has exactly one solution.
- The lines are parallel but not the same. Then the system has no solutions.
- The lines are the same. Then the system has infinitely many solutions.

How can we actually solve the equations? Multiply the first by a_{21} and the second by a_{11}, then subtract. This gives

$$(a_{11}a_{22} - a_{12}a_{21})y = a_{11}b_2 - a_{21}b_1.$$

Assuming that $a_{11}a_{22} - a_{12}a_{21} \neq 0$, this gives

$$y = \frac{a_{11}b_2 - a_{21}b_1}{a_{11}a_{22} - a_{12}a_{21}}$$

from which it follows that

$$x = \frac{a_{22}b_1 - a_{12}b_2}{a_{11}a_{22} - a_{12}a_{21}}.$$

So in the case $a_{11}a_{22} - a_{12}a_{21} \neq 0$, there is a unique solution. (Exercise: investigate the case $a_{11}a_{22} - a_{12}a_{21} = 0$.)

(If this example reminds you of Example A3.4(ii), that's good! We'll see later exactly what the connection is.)

Example B1.2 We want a methodical way to calculate the solutions of any linear system, one that we could program a computer to do. A 2×2 system isn't really big enough to illustrate how to do this. Let's try a 3×3 system: e.g.

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

We start by trying to eliminate the xs from all but one equation. We could do this by subtracting suitable multiples of the first equation from each of the other two, but the numbers will be easier if we use the second equation instead. So let's begin by swapping the first two equations:

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

(Obviously, this makes no difference to the solutions!) Now let's subtract $2\times$ the first equation from the second equation and subtract $3\times$ the first equation from the third equation. This gives:

$$\begin{aligned} x + y + z &= 4 \\ 0x + y - 3z &= -5 \\ 0x - 7y - 2z &= -11. \end{aligned}$$

Doing this doesn't change the solutions either: numbers x, y and z satisfy the old equations if and only if they satisfy the new ones.

We're now done with x, having eliminated it from all but one row. Next let's eliminate y, by subtracting $1\times$ the second equation from the first and adding $7\times$ the second equation to the third. This gives:

$$\begin{aligned} x + 0y + 4z &= 9 \\ 0x + y - 3z &= -5 \\ 0x + 0y - 23z &= -46. \end{aligned}$$

Again, this has the same solutions as the original equations. We might as well simplify the third equation by taking out a factor of -23:

$$\begin{aligned} x + 0y + 4z &= 9 \\ 0x + y - 3z &= -5 \\ 0x + 0y + z &= 2. \end{aligned}$$

Finally, we eliminate the z by subtracting $4\times$ the third equation from the first equation and adding $3\times$ the third to the second. This gives

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

or equivalently $x = 1$, $y = 1$ and $z = 2$. So this particular linear system has a unique solution.

Remark B1.3 You might think that the method above misses out a common move used for solving simultaneous equations: make one variable (x, say) the subject of an equation and then substitute it into the other equations in order to eliminate x. But in fact, this is really the same as the move we used repeatedly above, where we eliminated a variable by subtracting suitable multiples of one equation from all the others. It only looks different because we are insisting on keeping all the variables on the left-hand side and all the constants on the right.

Example B1.4 Let's consider a different 3×3 linear system:

$$\begin{aligned} x + 2y + 3z &= 1 \\ 3x + 5y - 2z &= 2 \\ 4x + 7y + z &= 3. \end{aligned}$$

Subtract $3\times$ the first equation from the second, and $4\times$ the first from the third, to get:

$$\begin{aligned} x + 2y + 3z &= 1 \\ 0x - y - 11z &= -1 \\ 0x - y - 11z &= -1. \end{aligned}$$

To eliminate y, first multiply the second equation by -1:

$$\begin{aligned} x + 2y + 3z &= 1 \\ 0x + y + 11z &= 1 \\ 0x - y - 11z &= -1. \end{aligned}$$

Now subtract $2\times$ the second equation from the first and add the second equation to the third:

$$\begin{aligned} x + 0y - 19z &= -1 \\ 0x + y + 11z &= 1 \\ 0x + 0y + 0z &= 0. \end{aligned}$$

The last equation tells us nothing and can therefore be deleted. In the first two, we can choose z freely, say by putting $z = t$ for an arbitrary scalar t, and then the solutions are given by $x = -1 + 19t,\ \ y = 1 - 11t,\ \ z = t$. We call z a **free variable** (since we can choose it freely) and x and y **leading variables**.

Matrix notation for linear systems

We will save ourselves a lot of writing if we adopt the matrix notation for linear systems. Given a linear system (B:1) (above), define

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

Then the system (B:1) is equivalent to the single equation

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

in $\mathbb{R}^m$.

Homogeneous and non-homogeneous systems

It is useful to consider the special kind of linear system where all the constants on the right-hand side are 0:

$$
\begin{aligned}
a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n &= 0 \\
a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n &= 0 \\
&\vdots \\
a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n &= 0,
\end{aligned}
\tag{B:2}
$$

or equivalently

$$A\mathbf{x} = \mathbf{0}.$$

A linear system with this property is called **homogeneous**.

We saw in Example B1.1 that a linear system need not have any solutions at all. But a homogeneous linear system always has at least one, the **trivial solution $\mathbf{x} = \mathbf{0}$**.

Now consider an arbitrary linear system $A\mathbf{x} = \mathbf{b}$, not necessarily homogeneous. I claim that if we can find just one solution of the system, then all other solutions can be obtained by adding to it any solution of the homogeneous system $A\mathbf{x} = \mathbf{0}$. That is:

Lemma B1.5 *Consider a linear system* (B:1)*. Let $\mathbf{x} = \mathbf{u}$ be a solution. Then the set of all solutions to* (B:1) *is*

$$\{\mathbf{u} + \mathbf{w} : \mathbf{w} \in \mathbb{R}^m \textit{ with } A\mathbf{w} = \mathbf{0}.\}$$

Proof We have to prove two things: that every element of this set is a solution, and that every solution belongs to this set.

First, let $\mathbf{w} \in \mathbb{R}^m$ with $A\mathbf{w} = \mathbf{0}$; we must prove that $\mathbf{x} = \mathbf{u} + \mathbf{w}$ satisfies $A\mathbf{x} = \mathbf{b}$. And indeed,

$$A(\mathbf{u} + \mathbf{w}) = A\mathbf{u} + A\mathbf{w} = \mathbf{b} + \mathbf{0} = \mathbf{b}.$$

Second, let $\mathbf{x} \in \mathbb{R}^m$ with $A\mathbf{x} = \mathbf{b}$; we must prove that $\mathbf{x} = \mathbf{u} + \mathbf{w}$ for some $\mathbf{w} \in \mathbb{R}^m$ such that $A\mathbf{w} = \mathbf{0}$. Put $\mathbf{w} = \mathbf{x} - \mathbf{u} \in \mathbb{R}^m$. Then of course $\mathbf{x} = \mathbf{u} + \mathbf{w}$, and

$$A\mathbf{w} = A(\mathbf{x} - \mathbf{u}) = A\mathbf{x} - A\mathbf{u} = \mathbf{b} - \mathbf{b} = \mathbf{0},$$

as required. □

Example B1.6 Suppose that our system consists of a single equation in two variables,

$$2x - 3y = 7.$$

The associated homogeneous system is

$$2x - 3y = 0.$$

One solution to the original system is $x = 5$, $y = 1$. The general solution to the homogeneous system is $x = 3t$, $y = 2t$, where t is any scalar. So by Lemma B1.5, the general solution to the original system is

$$\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 5 \\ 1 \end{pmatrix} + \begin{pmatrix} 3t \\ 2t \end{pmatrix} = \begin{pmatrix} 5 + 3t \\ 1 + 2t \end{pmatrix}.$$

(Suggestion: draw a picture!)

The number of solutions

In the example we just did, the homogeneous system had infinitely many solutions. There are other examples of homogeneous systems that have only one solution, namely, the trivial solution $\mathbf{0}$. (Can you think of an example?)

Lemma B1.7 *A homogeneous linear system either has just one solution (the trivial solution* $\mathbf{0}$*) or has infinitely many solutions.*

Proof Suppose that $A\mathbf{x} = \mathbf{0}$ has a nontrivial solution $\mathbf{x} = \mathbf{u}$. Then for all $c \in \mathbb{R}$, the vector $c\mathbf{u}$ is also a solution, since $A(c\mathbf{u}) = c(A\mathbf{u}) = c\mathbf{0} = \mathbf{0}$. But the vectors $c\mathbf{u}$ are different for different values of $c \in \mathbb{R}$, since $\mathbf{u} \neq \mathbf{0}$. □

We saw in Example B1.1 that some non-homogeneous linear systems have no solutions, some have exactly one solution, and some have infinitely many solutions. In fact, these are the only possibilities.

Lemma B1.8 *A linear system has no solutions, exactly one solution, or infinitely many solutions.*

Proof Consider a linear system $A\mathbf{x} = \mathbf{b}$ (where as usual A is an $m \times n$ matrix and $\mathbf{b}$ is an m-dimensional vector). If it has any solutions at all, then by Lemma B1.5, the set of all solutions has exactly as many elements as the set of solutions to the homogeneous system $A\mathbf{x} = \mathbf{0}$. But by Lemma B1.7, this set has either one element or infinitely many. □

The fundamental questions, revisited

In a sense, the lemmas we have just proved miss the point. The system

$$x + 2y + 3z = 4$$

and the system

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

both have infinitely many solutions, but you'd probably agree that in some sense, the first has 'more' solutions than the second. Indeed, the set of solutions to the first system is a plane (2-dimensional), whereas the set of solutions to the second is a line (1-dimensional).

So a more interesting question is not literally 'how many solutions are there?' but 'what is the dimension of the set of solutions?'. In order to make this precise, we need to say exactly what we mean by 'dimension'. We will do this later.

Roughly speaking, the more equations you have, the smaller you expect the dimension of the set of solutions to be. A little more exactly: for a homogeneous system, we expect each new equation to reduce by 1 the dimension of the set of solutions. (Other ways of looking at the dimension of the set of solutions are 'number of degrees of freedom in choosing a solution' or 'number of independent solutions'.)

For instance, the linear system in 3 variables with no equations at all has the 3-dimensional space $\mathbb{R}^3$ as its solution-set. When we impose one equation

$ax + by + cz = 0$, the set of solutions is 2-dimensional (a plane), at least as long as a, b and c are not all zero. When we impose two equations, the set of solutions is usually a line, and so on.

So we might guess that for any homogeneous linear system,

$$\begin{aligned}&\text{dimension of the set of solutions}\\&= \text{number of variables} - \text{number of equations.}\end{aligned}$$

But this isn't quite right. The problem is with 'number of equations'. Consider, for instance, the system

$$\begin{aligned}3x - 2y + 4z &= 0\\30x - 20y + 40z &= 0.\end{aligned}$$

Clearly the two equations are equivalent; so should we count this as one equation or two? Or, consider a less obvious example: the system

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

The third equation is -2 times the first equation plus -1 times the second equation, so it contributes nothing: the set of solutions would be the same if we deleted it entirely. Effectively, there are only two equations here, even though that's not obvious at first glance.

So a more plausible guess would be that for homogeneous systems,

$$\begin{aligned}&\text{dimension of the set of solutions}\\&= \text{number of variables} - \text{number of \textit{independent} equations.}\end{aligned}$$

We will see that once we've given precise definitions for all these terms, this guess is in fact correct. This result is one version of the *rank theorem* (also called the *rank and nullity theorem*), which we will meet repeatedly in various disguises.

B2 Solving linear systems using matrices

For the lecture of Monday, 28 September 2015; part five of five

In Examples B1.2 and B1.4, we solved some linear systems in a more or less methodical way. We used three operations repeatedly:

- interchange two equations;
- multiply an equation by a nonzero scalar (on both sides);
- add a multiple of one equation to another equation.

Just after those examples, we introduced the matrix notation for linear systems, and we saw that it saved us a lot of writing. So, let's now translate these operations into matrix terms.

In the matrix notation, a linear system

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

is written as a single equation $A\mathbf{x} = \mathbf{b}$. It is often convenient to write the $m \times n$ matrix A next to the m-dimensional vector $\mathbf{b}$, as a single matrix with a vertical bar in it:

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

(In terms of the original equations, the bar separates the left-hand side from the right-hand side.) This is called the **augmented matrix** of the linear system.

The equations of the linear system correspond to the rows of the augmented matrix. The three operations on equations correspond to the following three operations on a matrix, which are called the **elementary row operations**:

- interchange two rows;
- multiply a row by a nonzero scalar;
- add a scalar multiple of one row to another row.

Since we will be using these operations repeatedly, we set up some notation for them. Interchanging rows i and j will be written as $R_i \leftrightarrow R_j$, multiplying row i by a nonzero scalar c will be written as $R_i \to cR_i$, and adding c times row j to row i will be written as $R_i \to R_i + cR_j$.

Example B2.1 The augmented matrix of the linear system in Example B1.2 is

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

When we solved the system in Example B1.2, everything we did can be expressed in terms of elementary row operations, as follows:

$$
\begin{aligned}
\left(\begin{array}{ccc|c} 2 & 3 & -1 & 3 \\ 1 & 1 & 1 & 4 \\ 3 & -4 & 1 & 1 \end{array}\right)
&\xrightarrow[R_1 \leftrightarrow R_2]{}
\left(\begin{array}{ccc|c} 1 & 1 & 1 & 4 \\ 2 & 3 & -1 & 3 \\ 3 & -4 & 1 & 1 \end{array}\right) \\
&\xrightarrow[R_2 \to R_2 - 2R_1,\ R_3 \to R_3 - 3R_1]{}
\left(\begin{array}{ccc|c} 1 & 1 & 1 & 4 \\ 0 & 1 & -3 & -5 \\ 0 & -7 & -2 & -11 \end{array}\right) \\
&\xrightarrow[R_1 \to R_1 - R_2,\ R_3 \to R_3 + 7R_2]{}
\left(\begin{array}{ccc|c} 1 & 0 & 4 & 9 \\ 0 & 1 & -3 & -5 \\ 0 & 0 & -23 & -46 \end{array}\right) \\
&\xrightarrow[R_3 \to (-1/23)R_3]{}
\left(\begin{array}{ccc|c} 1 & 0 & 4 & 9 \\ 0 & 1 & -3 & -5 \\ 0 & 0 & 1 & 2 \end{array}\right) \\
&\xrightarrow[R_1 \to R_1 - 4R_3,\ R_2 \to R_2 + 3R_3]{}
\left(\begin{array}{ccc|c} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 2 \end{array}\right).
\end{aligned}
$$

We conclude that the unique solution to the linear system is

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

(It's maybe not completely clear what justifies this conclusion. We'll come back to this point.)

Example B2.2 The augmented matrix of the linear system in Example B1.4 is

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

The reductions performed in Example B1.4 can be translated into row operations. (How? Try it!) The end result is

$$
\left(\begin{array}{ccc|c} 1 & 0 & -19 & -1 \\ 0 & 1 & 11 & 1 \\ 0 & 0 & 0 & 0 \end{array}\right).
$$

As in Example B1.4, we conclude that the set of solutions is

$$
\left\{ \begin{pmatrix} -1 \\ 1 \\ 0 \end{pmatrix} + \begin{pmatrix} 19t \\ -11t \\ t \end{pmatrix} : t \in \mathbb{R} \right\}.
$$

The matrices we ended up with in both of the last two examples were of a certain special type. Here is the terminology.

Definition B2.3 A matrix is in **row echelon form (REF)** if:

i. any rows consisting entirely of zeros are at the bottom; and

ii. in each nonzero row, the first nonzero entry (called the **leading entry**) is to the left of all the leading entries below it.

For example, the matrix

$$\begin{pmatrix} \underline{1} & 2 & 3 & 4 & 5 \\ 0 & \underline{6} & 7 & 8 & 9 \\ 0 & 0 & 0 & \underline{10} & 11 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

is in row echelon form. The leading entries are underlined.

Remarks B2.4 i. The definition begins 'A matrix is in **row echelon form** if ...'. It's a convention of mathematical writing that the 'if' here really means 'if and only if'. The same applies whenever you read a definition like 'A splodge is said to be **purple** if such-and-such'.

ii. The word *echelon* comes from the Latin word for staircase, which also gives rise to modern English words like *escalator*.

Definition B2.5 A matrix is in **reduced row echelon form (RREF)** if it is in row echelon form, and:

i. all leading entries are equal to 1; and

ii. each column containing a leading 1 has zeros everywhere else.

For example, the final matrices in Examples B2.1 and B2.2 are both in reduced row echelon form, as is

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

It is a fact that by repeatedly performing elementary row operations, any matrix can be put into reduced row echelon form.

It is also a fact that the reduced row echelon form is unique. In other words, if you give the same matrix M to two different people and tell them to put it into reduced row echelon form, then they might use different elementary row operations to get there, but they will both arrive at the same final result.

Remark B2.6 What's the point of (not necessarily reduced) row echelon form? The answer is practical: it can be a useful intermediate stage on the way to solving a linear system. For example, suppose we have used elementary row operations to reduce our system to

$$\left(\begin{array}{ccc|c} 1 & 1 & 4 & 6 \\ 0 & 1 & -5 & -3 \\ 0 & 0 & 2 & 8 \end{array}\right).$$

This is in REF. It is not in RREF, but still, we can use it to write down the (unique) solution quickly, as follows. This matrix corresponds to the linear system

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

The third equation gives $z = 4$. Then substituting this into the second equation gives $y = 17$. Then substituting these into the first equation gives $x = -27$.

Unlike the RREF of a matrix, the REF is not unique. However, it is a fact that any two row echelon forms of a matrix have the same number of nonzero rows.

In the next sections, we will begin to say something about the dimension of the set of solutions of a linear system, as promised at the very end of Section B1.

Chapter C

Subspaces of $\mathbb{R}^n$

In Chapter B, we considered some of the fundamental questions about linear systems, and we found a practical method for solving them: write down the augmented matrix of the system, perform elementary row operations until it is in reduced row echelon form, then read off the solutions.

However, we were unable to *answer* some of the fundamental questions because of a lack of precise definitions. At the end of Section B1, I claimed that for homogeneous linear systems,

$$\begin{aligned} &\text{dimension of the set of solutions} \\ &= \text{number of variables} - \text{number of independent equations}, \end{aligned}$$

but also noted that the terms 'dimension' and 'number of independent equations' are so far undefined.

Part of the job of this chapter is to define them. Once that's done, we'll go back to linear systems with these definitions in hand.

This chapter is also important for reasons that have nothing to do with linear systems. Giving precise meanings to basic geometric concepts such as 'dimension' is of interest in itself, and the results that we prove in this chapter will come up again and again in other courses that you will take in years to come.

C1 The definition of subspace

For the lecture of Monday, 12 October 2015; part one of five

Roughly speaking, a subspace of $\mathbb{R}^n$ is a plane, line, etc., *through the origin.*

Definition C1.1 A **linear subspace** of $\mathbb{R}^n$ is a subset V of $\mathbb{R}^n$ with the following properties:

i. $\mathbf{0} \in V$;

ii. if $\mathbf{x}, \mathbf{y} \in V$ then $\mathbf{x} + \mathbf{y} \in V$;

iii. if $\mathbf{x} \in V$ and $c \in \mathbb{R}$ then $c\mathbf{x} \in V$.

Linear subspaces are also called **vector subspaces**. We will usually just call them 'subspaces' for short.

Examples C1.2 i. $\{\mathbf{0}\}$ is a subspace of $\mathbb{R}^n$ (the **trivial subspace**), and $\mathbb{R}^n$ is a subspace of $\mathbb{R}^n$ too.

ii. The subspaces of $\mathbb{R}^2$ are $\{\mathbf{0}\}$, the lines through the origin, and $\mathbb{R}^2$ itself.

iii. The subspaces of $\mathbb{R}^3$ are $\{\mathbf{0}\}$, the lines through the origin, the planes through the origin, and $\mathbb{R}^3$ itself.

Definition C1.3 Let A be an $m \times n$ real matrix. The **kernel** of A is

$$\ker(A) = \{\mathbf{x} \in \mathbb{R}^n : A\mathbf{x} = \mathbf{0}\}.$$

Some people (such as Poole) call the kernel the **null space**, and write it as $\mathrm{null}(A)$.

Lemma C1.4 *For any $m \times n$ matrix A, the kernel $\ker(A)$ is a linear subspace of $\mathbb{R}^n$.*

Proof We have to check that the three conditions of Definition C1.1 are satisfied.

(i): we have $A\mathbf{0} = \mathbf{0}$, so $\mathbf{0} \in \ker(A)$.

(ii): if $\mathbf{x}, \mathbf{y} \in \ker(A)$ then

$$A(\mathbf{x} + \mathbf{y}) = A\mathbf{x} + A\mathbf{y} = \mathbf{0} + \mathbf{0} = \mathbf{0},$$

so $\mathbf{x} + \mathbf{y} \in \ker(A)$.

(iii): if $\mathbf{x} \in \ker(A)$ and $c \in \mathbb{R}$ then

$$A(c\mathbf{x}) = c(A\mathbf{x}) = c\mathbf{0} = \mathbf{0},$$

so $c\mathbf{x} \in \ker(A)$.

(Here we have used some of the algebraic laws in Lemma A3.1.) □

In terms of linear systems, the kernel of A is the set of solutions $\mathbf{x}$ of the homogeneous system $A\mathbf{x} = \mathbf{0}$.

Here is another way of making subspaces of $\mathbb{R}^n$.

Definition C1.5 Let $\mathbf{v}_1, \dots, \mathbf{v}_m$ be a list of vectors in $\mathbb{R}^n$.

i. We say that $\mathbf{y} \in \mathbb{R}^n$ is a **linear combination** of $\mathbf{v}_1, \dots, \mathbf{v}_m$ if there exist $c_1, \dots, c_m \in \mathbb{R}$ such that

$$\mathbf{y} = c_1\mathbf{v}_1 + \cdots + c_m\mathbf{v}_m.$$

ii. The **span** of $\mathbf{v}_1, \dots, \mathbf{v}_m$ is the set

$$\mathrm{span}\{\mathbf{v}_1, \dots, \mathbf{v}_m\} = \{\mathbf{y} \in \mathbb{R}^n : \mathbf{y} \text{ is a linear combination of } \mathbf{v}_1, \dots, \mathbf{v}_m\}.$$

When $V = \mathrm{span}\{\mathbf{v}_1, \dots, \mathbf{v}_m\}$, we sometimes say that $\mathbf{v}_1, \dots, \mathbf{v}_m$ **spans** V.

If V is a subspace of $\mathbb{R}^n$ and $\mathbf{v}_1, \dots, \mathbf{v}_m$ belong to V, then any linear combination $c_1\mathbf{v}_1 + \cdots + c_m\mathbf{v}_m$ also belongs to V. This follows by induction from the definition of subspace.

Example C1.6 In $\mathbb{R}^3$, we have

$$\operatorname{span}\left\{\begin{pmatrix}1\\-1\\0\end{pmatrix}, \begin{pmatrix}0\\1\\-1\end{pmatrix}\right\} = \{\mathbf{x} \in \mathbb{R}^3 : x_1 + x_2 + x_3 = 0\}$$

since every point on the plane defined by $x_1+x_2+x_3 = 0$ is a linear combination of $\left(\begin{smallmatrix}1\\-1\\0\end{smallmatrix}\right)$ and $\left(\begin{smallmatrix}0\\1\\-1\end{smallmatrix}\right)$.

It is also true that

$$\operatorname{span}\left\{\begin{pmatrix}1\\-1\\0\end{pmatrix}, \begin{pmatrix}0\\1\\-1\end{pmatrix}, \begin{pmatrix}2\\5\\-7\end{pmatrix}, \begin{pmatrix}-4\\1\\3\end{pmatrix}\right\} = \{\mathbf{x} \in \mathbb{R}^3 : x_1 + x_2 + x_3 = 0\}.$$

Exercise: why?

Lemma C1.7 *Let* $\mathbf{v}_1, \dots, \mathbf{v}_m \in \mathbb{R}^n$. *Then* $\operatorname{span}\{\mathbf{v}_1, \dots, \mathbf{v}_m\}$ *is a linear subspace of* $\mathbb{R}^n$.

Proof Again, we verify the three conditions of Definition C1.1. Write $V = \operatorname{span}\{\mathbf{v}_1, \dots, \mathbf{v}_m\}$.

(i): we have $\mathbf{0} = \sum_{i=1}^m 0\mathbf{v}_i$, so $\mathbf{0} \in V$.

(ii): let $\mathbf{x}, \mathbf{y} \in V$. Then $\mathbf{x} = \sum_{i=1}^m c_i\mathbf{v}_i$ and $\mathbf{y} = \sum_{i=1}^m d_i\mathbf{v}_i$ for some scalars $c_1, \dots, c_m, d_1, \dots, d_m$. Hence

$$\mathbf{x} + \mathbf{y} = \sum_{i=1}^m c_i\mathbf{v}_i + \sum_{i=1}^m d_i\mathbf{v}_i = \sum_{i=1}^m (c_i\mathbf{v}_i + d_i\mathbf{v}_i) = \sum_{i=1}^m (c_i + d_i)\mathbf{v}_i,$$

so $\mathbf{x} + \mathbf{y} \in V$.

(iii): let $\mathbf{x} \in V$ and $c \in \mathbb{R}$. We have $\mathbf{x} = \sum_{i=1}^m d_i\mathbf{v}_i$ for some scalars $d_1, \dots, d_m$. Hence

$$c\mathbf{x} = c\sum_{i=1}^m d_i\mathbf{v}_i = \sum_{i=1}^m cd_i\mathbf{v}_i,$$

so $c\mathbf{x} \in V$. □

So we can manufacture subspaces of $\mathbb{R}^n$ simply by choosing a few elements and taking their span. The span is the smallest linear subspace containing those elements, in the following sense:

Lemma C1.8 *Let* $\mathbf{v}_1, \dots, \mathbf{v}_m \in \mathbb{R}^n$. *Then any subspace of* $\mathbb{R}^n$ *containing each of* $\mathbf{v}_1, \dots, \mathbf{v}_m$ *also contains* $\operatorname{span}\{\mathbf{v}_1, \dots, \mathbf{v}_m\}$.

Proof Let V be a subspace of $\mathbb{R}^n$ such that $\mathbf{v}_1, \dots, \mathbf{v}_m \in V$. As noted above, any linear combination of $\mathbf{v}_1, \dots, \mathbf{v}_m$ also belongs to V. So V contains the set of all such linear combinations, which is exactly $\operatorname{span}\{\mathbf{v}_1, \dots, \mathbf{v}_m\}$. □

Let A be an $m \times n$ matrix. The **row space** of A, written as $\operatorname{row}(A)$, is the span of the m rows of A; it is a linear subspace of $\mathbb{R}^n$. (Strictly speaking, the rows of A are *row* vectors and the elements of $\mathbb{R}^n$ are *column* vectors, so we should take transposes. But it does little harm if we blur the distinction slightly.) The **column space** of A, written as $\operatorname{col}(A)$, is the span of the n columns of A; it is a linear subspace of $\mathbb{R}^m$.

Lemma C1.9 *Let A be an $m \times n$ matrix. Then*

$$\mathrm{col}(A) = \{A\mathbf{x} : \mathbf{x} \in \mathbb{R}^n\}.$$

Proof Write the columns of A as $\mathbf{v}_1, \ldots, \mathbf{v}_n \in \mathbb{R}^m$. Then

$$A\mathbf{x} = x_1\mathbf{v}_1 + \cdots + x_n\mathbf{v}_n.$$

(Exercise: why?) But by definition,

$$\mathrm{col}(A) = \{x_1\mathbf{v}_1 + \cdots + x_n\mathbf{v}_n : x_1, \ldots, x_n \in \mathbb{R}\},$$

so $\mathrm{col}(A) = \{A\mathbf{x} : \mathbf{x} \in \mathbb{R}^n\}$. $\square$

So we can describe the column space in terms of linear systems: $\mathrm{col}(A)$ is the set of vectors $\mathbf{b} \in \mathbb{R}^m$ such that the equation $A\mathbf{x} = \mathbf{b}$ has at least one solution.

C2 The dimension of a subspace

For the lecture of Monday, 12 October 2015; part two of five

Although planet Earth lives in three-dimensional space, the *surface* of the earth is best thought of as two-dimensional. That's because it is possible to specify a point on the earth's surface by two numbers only: longitude and latitude. Similarly, the fact that the subspace

$$V = \{\mathbf{x} \in \mathbb{R}^3 : x_1 + x_2 + x_3 = 0\}$$

of $\mathbb{R}^3$ is two-dimensional (a plane) corresponds to the fact that every element of V can be expressed as a linear combination

$$c_1 \begin{pmatrix} 1 \\ -1 \\ 0 \end{pmatrix} + c_2 \begin{pmatrix} 0 \\ 1 \\ -1 \end{pmatrix}$$

of *two* vectors, $\left(\begin{smallmatrix} 1 \\ -1 \\ 0 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} 0 \\ 1 \\ -1 \end{smallmatrix}\right)$.

We are going to state a definition of the dimension of a subspace of $\mathbb{R}^n$. However, some preparation is needed first.

Definition C2.1 A list $\mathbf{v}_1, \ldots, \mathbf{v}_m$ of vectors in $\mathbb{R}^m$ is **linearly independent** if for all $c_1, \ldots, c_m \in \mathbb{R}$,

$$c_1\mathbf{v}_1 + \cdots + c_m\mathbf{v}_m = \mathbf{0} \implies c_1 = \cdots = c_m = 0.$$

If $\mathbf{v}_1, \ldots, \mathbf{v}_m$ are not linearly independent, they are said to be **linearly dependent**.

So $\mathbf{v}_1, \ldots, \mathbf{v}_m$ are linearly dependent if and only if there exist scalars $c_1, \ldots, c_m$, not all zero, such that $\sum_i c_i\mathbf{v}_i = 0$.

Lemma C2.2 *Let $\mathbf{v}_1, \ldots, \mathbf{v}_m \in \mathbb{R}^n$. The following are equivalent:*

i. $\mathbf{v}_1, \ldots, \mathbf{v}_m$ *are linearly independent;*

ii. for all $i \in \{1, \ldots, m\}$, *we have* $\mathbf{v}_i \notin \operatorname{span}\{\mathbf{v}_1, \ldots, \mathbf{v}_{i-1}, \mathbf{v}_{i+1}, \ldots, \mathbf{v}_m\}$*;*

iii. for all $\mathbf{x} \in \operatorname{span}\{\mathbf{v}_1, \ldots, \mathbf{v}_m\}$, *there are* unique $c_1, \ldots, c_m \in \mathbb{R}$ *such that* $\mathbf{x} = \sum_{i=1}^m c_i\mathbf{v}_i$.

(Jargon: 'the following are equivalent' means that (i) holds if and only if (ii) holds if and only if (iii) holds.)

Proof We prove that (iii)$\Longrightarrow$(ii)$\Longrightarrow$(i)$\Longrightarrow$(iii).

(iii)$\Longrightarrow$(ii): assume (iii). Let $i \in \{1, \ldots, m\}$ and suppose for a contradiction that $\mathbf{v}_i \in \operatorname{span}\{\mathbf{v}_1, \ldots, \mathbf{v}_{i-1}, \mathbf{v}_{i+1}, \ldots, \mathbf{v}_m\}$. Then we can write

$$\mathbf{v}_i = c_1\mathbf{v}_1 + \cdots + c_{i-1}\mathbf{v}_{i-1} + c_{i+1}\mathbf{v}_{i+1} + \cdots + c_m\mathbf{v}_m$$

for some scalars $c_1, \ldots$. But then

$$\begin{aligned} &0\mathbf{v}_1 + \cdots + 0\mathbf{v}_{i-1} + 1\mathbf{v}_i + 0\mathbf{v}_{i+1} + \cdots + 0\mathbf{v}_m \\ = {} &c_1\mathbf{v}_1 + \cdots + c_{i-1}\mathbf{v}_{i-1} + 0\mathbf{v}_i + c_{i+1}\mathbf{v}_{i+1} + \cdots + c_m\mathbf{v}_m, \end{aligned}$$

and the coefficients of $\mathbf{v}_i$ are different on the left- and right-hand sides, contradicting the uniqueness in (iii).

(ii)$\Longrightarrow$(i): assume (ii). Let $c_1, \ldots, c_m \in \mathbb{R}$ with $\sum_i c_i \mathbf{v}_i = \mathbf{0}$, and assume for a contradiction that $c_i \neq 0$ for some i. Then for that i, we have

$$\mathbf{v}_i = -\frac{1}{c_i}(c_1\mathbf{v}_1 + \cdots + c_{i-1}\mathbf{v}_{i-1} + c_{i+1}\mathbf{v}_{i+1} + \cdots + c_m\mathbf{v}_m)$$

and so $\mathbf{v}_i \in \operatorname{span}\{\mathbf{v}_1, \ldots, \mathbf{v}_{i-1}, \mathbf{v}_{i+1}, \ldots, \mathbf{v}_m\}$, a contradiction.

(i)$\Longrightarrow$(iii): let $\mathbf{x} \in \operatorname{span}\{\mathbf{v}_1, \ldots, \mathbf{v}_m\}$, and suppose that $\mathbf{x} = \sum_i c_i\mathbf{v}_i = \sum_i d_i\mathbf{v}_i$. Subtracting, $\sum_i(c_i - d_i)\mathbf{v}_i = 0$. But then by linear independence, $c_i - d_i = 0$ for all i, or equivalently $c_i = d_i$ for all i. $\square$

Definition C2.3 Let V be a subspace of $\mathbb{R}^n$. A **basis** of V is a list $\mathbf{v}_1, \ldots, \mathbf{v}_m$ of elements of V that is linearly independent and spans V.

In other words, a basis for V is a linearly independent spanning set. In other words still (using the last lemma), $\mathbf{v}_1, \ldots, \mathbf{v}_m \in V$ is a basis if and only if every element of V can be expressed as a linear combination of $\mathbf{v}_1, \ldots, \mathbf{v}_m$ in exactly one way.

The plural of basis is **bases** (pronounced 'base-eez'). Sometimes the word **base** is used instead of basis.

Examples C2.4

i. Take V to be $\mathbb{R}^n$ itself. The **standard basis** of $\mathbb{R}^n$ is the list of vectors

$$\mathbf{e}_1 = \begin{pmatrix}1\\0\\0\\\vdots\\0\end{pmatrix}, \quad \mathbf{e}_2 = \begin{pmatrix}0\\1\\0\\\vdots\\0\end{pmatrix}, \quad \ldots, \quad \mathbf{e}_n = \begin{pmatrix}0\\0\\0\\\vdots\\1\end{pmatrix}.$$

You should check that this really is a basis for $\mathbb{R}^n$.

ii. For any nonzero $x \in \mathbb{R}$, the one-element list x is a basis for $\mathbb{R}$. It is linearly independent because if $cx = 0$ then $c = 0$ (for scalars c). It spans $\mathbb{R}$ because every element of $\mathbb{R}$ is a multiple of x.

iii. Let $V = \{\mathbf{x} \in \mathbb{R}^3 : x_1 + x_2 + x_3 = 0\}$. The two-element list

$$\begin{pmatrix}1\\-1\\0\end{pmatrix}, \quad \begin{pmatrix}0\\1\\-1\end{pmatrix}$$

is a basis. So too is the two-element list

$$\begin{pmatrix}1\\0\\-1\end{pmatrix}, \quad \begin{pmatrix}3\\5\\-8\end{pmatrix}.$$

Warning C2.5 The last two examples demonstrate that the same subspace can have many bases. It's almost never correct to write '*the* basis of V'!

Although the same subspace V can have multiple bases, these examples suggest that all the bases of V have the same number of elements. We would like to define the dimension of V to be that number, in keeping with the longitude/latitude idea described above. In order to be sure that this definition makes sense, we have to do two things. First, we have to prove that any two bases of V do indeed have the same number of elements. Second, we have to prove that V has at least one basis.

Proposition C2.6 *Let V be a subspace of $\mathbb{R}^n$. Let $\mathbf{v}_1, \ldots, \mathbf{v}_k$ be linearly independent vectors in V and let $\mathbf{w}_1, \ldots, \mathbf{w}_m \in V$ be vectors spanning V. Then $k \leq m$.*

Proof In fact, we prove something stronger: that it is possible to choose k members of the list $\mathbf{w}_1, \ldots, \mathbf{w}_m$ in such a way that when these members are replaced by $\mathbf{v}_1, \ldots, \mathbf{v}_k$, the resulting list still spans V. (For instance, if $k = 3$ and $m = 5$ then it may be that $\mathbf{w}_1, \mathbf{v}_1, \mathbf{v}_2, \mathbf{w}_4, \mathbf{v}_3$ spans V.)

We choose the members to be replaced one by one. Let $0 \leq i < k$, and suppose inductively that we have chosen i members of the list $\mathbf{w}_1, \ldots, \mathbf{w}_m$ in such a way that when these members are replaced by $\mathbf{v}_1, \ldots, \mathbf{v}_i$, the resulting list spans V. (Clearly this is possible when $i = 0$.) We may assume without loss of generality that the i members of the list replaced so far are the first i; thus, we are assuming that $\mathbf{v}_1, \ldots, \mathbf{v}_i, \mathbf{w}_{i+1}, \ldots, \mathbf{w}_m$ span V.

(The phrase 'without loss of generality' means that although it looks as if we've made an unjustified assumption, we haven't really. It's just a matter of notation: although the vectors replaced so far might not be the first i, we could rename them so that they were. Making this assumption helps to keep the notation simple.)

Since $\mathbf{v}_{i+1} \in V$ and $V = \text{span}\{\mathbf{v}_1, \ldots, \mathbf{v}_i, \mathbf{w}_{i+1}, \ldots, \mathbf{w}_m\}$, we can write

$$\mathbf{v}_{i+1} = c_1\mathbf{v}_1 + \cdots + c_i\mathbf{v}_i + c_{i+1}\mathbf{w}_{i+1} + \cdots + c_m\mathbf{w}_m \qquad \text{(C:1)}$$

for some scalars $c_1, \ldots, c_m$. Since $\mathbf{v}_1, \ldots, \mathbf{v}_k$ are linearly independent, not all of $c_{i+1}, \ldots, c_m$ can be zero (by Lemma C2.2(ii)). Assume without loss of generality that $c_{i+1} \neq 0$. Then we can rearrange equation (C:1) to show that

$$\mathbf{w}_{i+1} \in \text{span}\{\mathbf{v}_1, \ldots, \mathbf{v}_i, \mathbf{v}_{i+1}, \mathbf{w}_{i+2}, \ldots, \mathbf{w}_m\}.$$

Write $W = \text{span}\{\mathbf{v}_1, \ldots, \mathbf{v}_i, \mathbf{v}_{i+1}, \mathbf{w}_{i+2}, \ldots, \mathbf{w}_m\}$. Then W is a linear subspace of V containing each of $\mathbf{v}_1, \ldots, \mathbf{v}_i, \mathbf{w}_{i+1}, \mathbf{w}_{i+2}, \ldots, \mathbf{w}_m$. By Lemma C1.8, W therefore contains the span of this list, which is V. So W is a subspace of V containing V; that is, $W = V$. Hence $\mathbf{v}_1, \ldots, \mathbf{v}_i, \mathbf{v}_{i+1}, \mathbf{w}_{i+2}, \ldots, \mathbf{w}_m$ span V, completing the induction. □

Corollary C2.7 *Let $m > n$. Then any m vectors in $\mathbb{R}^n$ are linearly dependent.*

Proof Let $\mathbf{v}_1, \ldots, \mathbf{v}_m \in \mathbb{R}^n$, and suppose for a contradiction that they are linearly independent. The standard basis $\mathbf{e}_1, \ldots, \mathbf{e}_n$ spans $\mathbb{R}^n$, so by Proposition C2.6 (with $V = \mathbb{R}^n$), we have $m \leq n$, a contradiction. □

So, if A is an $m \times n$ matrix with $m > n$ (a matrix that is taller than it is wide) then the rows must be linearly dependent.

Corollary C2.8 *Let V be a linear subspace of $\mathbb{R}^n$. Then any two bases of V have the same number of elements.*

Proof Let $\mathbf{v}_1, \ldots, \mathbf{v}_k$ and $\mathbf{w}_1, \ldots, \mathbf{w}_m$ be bases of V. Since any basis of V is linearly independent *and* spans V, Proposition C2.6 implies that both $k \leq m$ and $m \leq k$. Hence $k = m$. $\square$

We have not yet shown that a subspace of $\mathbb{R}^n$ has any basis at all! But we will.

Lemma C2.9 (Shrinking) *Let V be a subspace of $\mathbb{R}^n$ and let $\mathbf{v}_1, \ldots, \mathbf{v}_m \in V$ be a list of vectors spanning V. Then some subset of $\mathbf{v}_1, \ldots, \mathbf{v}_m$ is a basis of V.*

This subset could consist of all, some or none of $\mathbf{v}_1, \ldots, \mathbf{v}_m$. 'All' would be the case if $\mathbf{v}_1, \ldots, \mathbf{v}_m$ was already a basis. 'None' would be the case if $V = \{\mathbf{0}\}$, since the empty list is a basis for $\{\mathbf{0}\}$. (Poole wrongly states that $\{\mathbf{0}\}$ has no basis. It does; it's just empty.)

Proof Consider all subsets of $\mathbf{v}_1, \ldots, \mathbf{v}_m$ that span V. Choose one with the smallest possible number of elements: k, say. Without loss of generality, we may assume that it is of the form $\mathbf{v}_1, \ldots, \mathbf{v}_k$.

I claim that $\mathbf{v}_1, \ldots, \mathbf{v}_k$ is a basis for V. Certainly it spans V, so it only remains to show that it is linearly independent. Suppose not. Then by Lemma C2.2, there exists $i \in \{1, \ldots, k\}$ such that $\mathbf{v}_i \in \operatorname{span}\{\mathbf{v}_1, \ldots, \mathbf{v}_{i-1}, \mathbf{v}_{i+1}, \ldots, \mathbf{v}_k\}$. But then $\mathbf{v}_1, \ldots, \mathbf{v}_{i-1}, \mathbf{v}_{i+1}, \ldots, \mathbf{v}_k$ span V. (Why?) This is a subset of $\mathbf{v}_1, \ldots, \mathbf{v}_m$ that spans V and has fewer than k elements, a contradiction. $\square$

Examples C2.10 Let $V = \{\mathbf{x} \in \mathbb{R}^3 : x_1 + x_2 + x_3 = 0\}$, a subspace of $\mathbb{R}^3$.

i. The vectors

$$\mathbf{v}_1 = \begin{pmatrix} 1 \\ 2 \\ -3 \end{pmatrix}, \quad \mathbf{v}_2 = \begin{pmatrix} 1 \\ 0 \\ -1 \end{pmatrix}, \quad \mathbf{v}_3 = \begin{pmatrix} 1 \\ 4 \\ -5 \end{pmatrix}$$

span V. Any two of them form a basis of V. (Check!)

ii. The vectors

$$\mathbf{w}_1 = \begin{pmatrix} 1 \\ 2 \\ -3 \end{pmatrix}, \quad \mathbf{w}_2 = \begin{pmatrix} 1 \\ 0 \\ -1 \end{pmatrix}, \quad \mathbf{w}_3 = \begin{pmatrix} 2 \\ 0 \\ -2 \end{pmatrix}$$

also span V. This time, $\mathbf{w}_1, \mathbf{w}_2$ is a basis and $\mathbf{w}_1, \mathbf{w}_3$ is a basis, but $\mathbf{w}_2, \mathbf{w}_3$ is not a basis (why not?).

Lemma C2.11 (Growing) *Let V be a subspace of $\mathbb{R}^n$ and let $\mathbf{v}_1, \ldots, \mathbf{v}_k$ be linearly independent vectors in V. Then there is some basis of V containing $\mathbf{v}_1, \ldots, \mathbf{v}_k$ as a subset.*

Proof Consider all lists of linearly independent vectors in V containing $\mathbf{v}_1, \ldots, \mathbf{v}_k$. By Corollary C2.7, no such list contains more than n elements.

We can therefore choose one with the largest number of elements (m, say) and call it $\mathbf{v}_1, \ldots, \mathbf{v}_k, \mathbf{v}_{k+1}, \ldots, \mathbf{v}_m$.

I claim that $\mathbf{v}_1, \ldots, \mathbf{v}_m$ is a basis of V. Certainly it is linearly independent, so it only remains to show that it spans V. Let $\mathbf{v} \in V$. There is no list of linearly independent elements of V of length greater than m, so the vectors $\mathbf{v}_1, \ldots, \mathbf{v}_m, \mathbf{v}$ are linearly dependent. That is, there exist scalars $c_1, \ldots, c_m, c$, not all zero, such that

$$c_1\mathbf{v}_1 + \cdots + c_m\mathbf{v}_m + c\mathbf{v} = 0.$$

Since $\mathbf{v}_1, \ldots, \mathbf{v}_m$ are linearly independent, we must have $c \neq 0$. Rearranging the equation then shows that $\mathbf{v}$ is a linear combination of $\mathbf{v}_1, \ldots, \mathbf{v}_m$, as required.□

Example C2.12 Let $V = \mathbb{R}^3$, and put

$$\mathbf{v}_1 = \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix}, \quad \mathbf{v}_2 = \begin{pmatrix} 4 \\ 5 \\ 6 \end{pmatrix}.$$

Then $\mathbf{v_1}, \mathbf{v_2}$ are linearly independent. To extend it to a basis, we simply pick any vector $\mathbf{v}_3$ not in $\operatorname{span}\{\mathbf{v}_1, \mathbf{v}_2\}$ (such as $\mathbf{v}_3 = \left(\begin{smallmatrix} 1 \\ 0 \\ 0 \end{smallmatrix}\right)$); then $\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3$ is a basis.

Proposition C2.13 *Every linear subspace of* $\mathbb{R}^n$ *has at least one basis.*

Proof This follows immediately from Lemma C2.11 by taking $\mathbf{v}_1, \ldots, \mathbf{v}_k$ to be the empty list (i.e. the list with $k = 0$), which is linearly independent. □

Remark C2.14 Interpreting the definitions of 'linearly independent' and 'span' for the empty list can seem tricky, but if you think through it carefully then you should be able to persuade yourself that the empty list *is* linearly independent and that its span is $\{\mathbf{0}\}$. Alternatively, you can just interpret these statements as definitions.

So every linear subspace V of $\mathbb{R}^n$ has at least one basis, and all bases of V have the same number of elements. We can now state the definition that we've been wanting to state all along:

Definition C2.15 Let V be a linear subspace of $\mathbb{R}^n$. The **dimension** of V, written as $\dim V$, is the number of elements in any basis of V.

Examples C2.16 i. $\dim(\mathbb{R}^n) = n$, since $\mathbb{R}^n$ has a basis $\mathbf{e}_1, \ldots, \mathbf{e}_n$ (Example C2.4(i)) with n elements.

ii. $\dim(\{\mathbf{0}\}) = 0$, since the empty list is a basis for $\{\mathbf{0}\}$. (See Remark C2.14.)

iii. The subspace
$$V = \{\mathbf{x} \in \mathbb{R}^3 : x_1 + x_2 + x_3 = 0\}$$
of $\mathbb{R}^3$ has dimension 2 (it's a plane), since we already saw in Example C2.4(ii) that it has a basis with 2 elements.

iv. The subspace
$$V = \{\mathbf{x} \in \mathbb{R}^3 : x_1 + x_2 + x_3 = 0,\ x_1 = x_2\}$$
of $\mathbb{R}^3$ has dimension 1 (it's a line), since the one-element list $\left(\begin{smallmatrix} 1 \\ 1 \\ -2 \end{smallmatrix}\right)$ is a basis.

The following result can be useful when trying to show that some list of vectors is a basis.

Lemma C2.17 *Let V be a linear subspace of $\mathbb{R}^n$. Write $m = \dim V$ and let $\mathbf{v}_1, \ldots, \mathbf{v}_m \in V$. If $\mathbf{v}_1, \ldots, \mathbf{v}_m$ are linearly independent* or *span V then they form a basis for V.*

Proof First suppose that they are linearly independent. By Lemma C2.11 ('growing'), there is some basis containing $\mathbf{v}_1, \ldots, \mathbf{v}_m$. But V is m-dimensional, so any basis has exactly m elements, so $\mathbf{v}_1, \ldots, \mathbf{v}_m$ *is* a basis.

The proof in the case that $\mathbf{v}_1, \ldots, \mathbf{v}_m$ span V is very similar, using Lemma C2.9 ('shrinking') instead. □

Let V and W be subspaces of $\mathbb{R}^n$ with $V \subseteq W$. Then we would expect that $\dim V$ is at most $\dim W$. Moreover, $\dim V$ should be equal to $\dim W$ only when $V = W$; for instance, you can't have one plane in $\mathbb{R}^3$ being a proper subset of another. The last result of this section states that our intuition is, on this occasion, correct:

Lemma C2.18 *Let V and W be linear subspaces of $\mathbb{R}^n$ with $V \subseteq W$. Then $\dim V \leq \dim W$, with equality if and only if $V = W$.*

I should explain the expression 'with equality if ...'. The lemma states two things about V and W: (i) that $\dim V \leq \dim W$, and (ii) that $\dim V = \dim W$ if and only if $V = W$.

Proof Choose a basis $\mathbf{x}_1, \ldots, \mathbf{x}_k$ for V. Then $\mathbf{x}_1, \ldots, \mathbf{x}_k$ are linearly independent vectors in W, so by Lemma C2.11, we can extend this list to a basis $\mathbf{x}_1, \ldots, \mathbf{x}_k, \mathbf{x}_{k+1}, \ldots, \mathbf{x}_m$ for W. Hence $k \leq m$, that is, $\dim V \leq \dim W$. If $\dim V = \dim W$ then $k = m$, so $\mathbf{x}_1, \ldots, \mathbf{x}_k$ is a basis for both V and W. Hence

$$V = \operatorname{span}\{\mathbf{x}_1, \ldots, \mathbf{x}_k\} = W.$$

Conversely, if $V = W$ then $\dim V = \dim W$ immediately. □

C3 A first look at the rank theorem

For the lecture of Monday, 12 October 2015; part three of five

We have seen that an $m \times n$ matrix A gives rise to various subspaces of $\mathbb{R}^m$ and $\mathbb{R}^n$: the column space $\mathrm{col}(A) \subseteq \mathbb{R}^m$, the row space $\mathrm{row}(A) \subseteq \mathbb{R}^n$, and the kernel $\ker(A) \subseteq \mathbb{R}^n$. We can think about the dimensions of these subspaces. These have names:

Definition C3.1 Let A be an $m \times n$ matrix.

i. The **column rank** of A is $\dim(\mathrm{col}(A))$.

ii. The **row rank** of A is $\dim(\mathrm{row}(A))$.

iii. The **nullity** of A is $\dim(\ker(A))$.

So, given an $m \times n$ matrix A, we get five different numbers: m, n, the column rank, the row rank and the nullity. Are there any relationships between them?

The answer is yes: there are two relationships. First, the row-rank turns out to be equal to the column-rank. (This is perhaps a surprise, since $\mathrm{row}(A)$ is a subspace of $\mathbb{R}^n$ and $\mathrm{col}(A)$ is a subspace of $\mathbb{R}^m$.) Once we've proved this, we'll just call it the 'rank'. So there are really only four numbers in play.

Second, it turns out that $\mathrm{rank} + \mathrm{nullity} = n$. This is called the rank theorem (or the rank and nullity theorem). That name has been mentioned before in the context of linear systems, at the end of Section B1. Later, we'll look at the relationship between the result just mentioned and the result on linear systems that we were fumbling towards before.

We'll prove the second relationship first. Because we don't know yet that row rank and column rank are the same, we have to be careful for now to say which one we mean.

Theorem C3.2 (Rank theorem, first version) *For any matrix A,*

$$\textit{column-rank}(A) + \textit{nullity}(A) = \textit{number of columns of } A.$$

Proof Let A be an $m \times n$ matrix. Choose a basis $\mathbf{w}_1, \ldots, \mathbf{w}_\ell$ for $\mathrm{col}(A)$ and a basis $\mathbf{v}_1, \ldots, \mathbf{v}_k$ for $\ker(A)$. Then ℓ is the column-rank of A and k is the nullity of A, so we have to prove that $\ell + k = n$.

By Lemma C1.9, we can choose $\mathbf{v}_{k+1}, \ldots, \mathbf{v}_{k+\ell} \in \mathbb{R}^n$ such that

$$A\mathbf{v}_{k+1} = \mathbf{w}_1,\ A\mathbf{v}_{k+2} = \mathbf{w}_2,\ \ldots,\ A\mathbf{v}_{k+\ell} = \mathbf{w}_\ell.$$

I claim that $\mathbf{v}_1, \ldots, \mathbf{v}_k, \mathbf{v}_{k+1}, \ldots, \mathbf{v}_{k+\ell}$ is a basis for $\mathbb{R}^n$. If we can show this then it will follow that $k + \ell = n$ (since all bases for $\mathbb{R}^n$ have n elements), and so the proof will be finished.

First we prove that it spans $\mathbb{R}^n$. Let $\mathbf{x} \in \mathbb{R}^n$. Then $A\mathbf{x} \in \mathrm{col}(A)$ by Lemma C1.9. But $\mathbf{w}_1, \ldots, \mathbf{w}_\ell$ spans $\mathrm{col}(A)$, so

$$A\mathbf{x} = \sum_{i=1}^{\ell} d_i \mathbf{w}_i$$

for some scalars $d_1, \ldots, d_\ell$. Hence

$$A\mathbf{x} = \sum_{i=1}^{\ell} d_i A\mathbf{v}_{k+i} = A(d_1\mathbf{v}_{k+1} + \cdots + d_\ell \mathbf{v}_{k+\ell}).$$

Put $\hat{\mathbf{x}} = d_1\mathbf{v}_{k+1} + \cdots + d_\ell\mathbf{v}_{k+\ell} \in \mathbb{R}^n$. Then $A\mathbf{x} = A\hat{\mathbf{x}}$, so $A(\mathbf{x} - \hat{\mathbf{x}}) = \mathbf{0}$, or equivalently $\mathbf{x} - \hat{\mathbf{x}} \in \ker(A)$. But $\mathbf{v}_1, \ldots, \mathbf{v}_k$ spans $\ker(A)$, so

$$\mathbf{x} - \hat{\mathbf{x}} = c_1\mathbf{v}_1 + \cdots + c_k\mathbf{v}_k$$

for some scalars $c_1, \ldots, c_k$. Substituting in the definition of $\hat{\mathbf{x}}$ and rearranging gives

$$\mathbf{x} = c_1\mathbf{v}_1 + \cdots + c_k\mathbf{v}_k + d_1\mathbf{v}_{k+1} + \cdots + d_\ell\mathbf{v}_{k+\ell}.$$

So $\mathbf{x} \in \operatorname{span}\{\mathbf{v}_1, \ldots, \mathbf{v}_{k+\ell}\}$, as required.

Second, we prove that $\mathbf{v}_1, \ldots, \mathbf{v}_{k+\ell}$ are linearly independent. Let $c_1, \ldots, c_k, d_1, \ldots, d_\ell$ be scalars such that

$$c_1\mathbf{v}_1 + \cdots + c_k\mathbf{v}_k + d_1\mathbf{v}_{k+1} + \cdots + d_\ell\mathbf{v}_{k+\ell} = \mathbf{0}. \tag{C:2}$$

Multiplying each side by A on the left gives

$$c_1A\mathbf{v}_1 + \cdots + c_kA\mathbf{v}_k + d_1A\mathbf{v}_{k+1} + \cdots + d_\ell A\mathbf{v}_{k+\ell} = \mathbf{0}$$

or equivalently

$$d_1\mathbf{w}_1 + \cdots + d_\ell\mathbf{w}_\ell = \mathbf{0}$$

since $\mathbf{v}_1, \ldots, \mathbf{v}_k \in \ker(A)$ and $A\mathbf{v}_{k+i} = \mathbf{w}_i$. But $\mathbf{w}_1, \ldots, \mathbf{w}_\ell$ are linearly independent, so $d_1 = \cdots = d_\ell = 0$. Hence equation (C:2) reduces to

$$c_1\mathbf{v}_1 + \cdots + c_k\mathbf{v}_k = \mathbf{0}.$$

But $\mathbf{v}_1, \ldots, \mathbf{v}_k$ are also linearly independent, so $c_1 = \cdots = c_k = 0$. We have now shown that all the c_is and d_is are zero. Hence $\mathbf{v}_1, \ldots, \mathbf{v}_{k+\ell}$ are linearly independent, completing the proof. □

C4 Orthogonality

For the lecture of Monday, 12 October 2015; part four of five

Perhaps unexpectedly, our proof that row rank equals column rank will use some results about orthogonality. (Recall that 'orthogonal' means 'perpendicular' or 'at right angles'.) Even if we weren't trying to prove anything about rank, it is geometrically very natural to think about orthogonality, so the results here are of interest in their own right.

In Section A2, we defined two vectors $\mathbf{x}, \mathbf{y} \in \mathbb{R}^n$ to be orthogonal if $\mathbf{x} \cdot \mathbf{y} = 0$. Now we extend this definition to lists of any number of vectors.

Definition C4.1 Let $\mathbf{v}_1, \ldots, \mathbf{v}_m \in \mathbb{R}^n$.

i. We say that $\mathbf{v}_1, \ldots, \mathbf{v}_m$ are **orthogonal** if $\mathbf{v}_i \cdot \mathbf{v}_j = 0$ for all $i, j \in \{1, \ldots, m\}$ with $i \neq j$.

ii. We say that they are **orthonormal** if they are orthogonal and $\|\mathbf{v}_i\| = 1$ for all $i \in \{1, \ldots, m\}$.

Examples C4.2 i. The standard basis $\mathbf{e}_1, \ldots, \mathbf{e}_n$ of $\mathbb{R}^n$ is orthonormal.

ii. The vectors $\binom{1}{1}, \binom{1}{-1} \in \mathbb{R}^2$ are orthogonal but not orthonormal. The vectors $\binom{\sqrt{2}/2}{\sqrt{2}/2}, \binom{\sqrt{2}/2}{-\sqrt{2}/2} \in \mathbb{R}^2$ are orthonormal.

The next lemma states that orthonormality implies linear independence. (The converse is false. Why?)

Lemma C4.3 *Let $\mathbf{v}_1, \ldots, \mathbf{v}_m \in \mathbb{R}^n$. If $\mathbf{v}_1, \ldots, \mathbf{v}_m$ are orthonormal then $\mathbf{v}_1, \ldots, \mathbf{v}_m$ are linearly independent.*

Proof Let $c_1, \ldots, c_m$ be scalars such that $\sum_{i=1}^m c_i \mathbf{v}_i = \mathbf{0}$. For each $j \in \{1, \ldots, m\}$, taking the dot product of each side of this equation with $\mathbf{v}_j$ gives

$$\left(\sum_{i=1}^m c_i \mathbf{v}_i\right) \cdot \mathbf{v}_j = \mathbf{0} \cdot \mathbf{v}_j.$$

By the identities in Lemma A2.2 (and induction), the left-hand side is equal to $\sum_i c_i(\mathbf{v}_i \cdot \mathbf{v}_j)$. But then by orthonormality, the left-hand side is c_j. Also, the right-hand side is 0. Hence $c_j = 0$. This holds for all j, so $\mathbf{v}_1, \ldots, \mathbf{v}_m$ are linearly independent. $\square$

Let V be a subspace of $\mathbb{R}^n$. An **orthonormal basis** of V is a list $\mathbf{v}_1, \ldots, \mathbf{v}_m$ of vectors in V that is both orthonormal and a basis of V. By the last lemma, an equivalent statement is that the vectors are orthonormal and span V. Geometrically, an orthonormal basis of an m-dimensional subspace V consists of m unit-length vectors in V all at right angles to each other.

When $\mathbf{v}_1, \ldots, \mathbf{v}_m$ is a basis of V, we can write any $\mathbf{x} \in V$ as a linear combination $\sum_i c_i \mathbf{v}_i$ (uniquely). How do we find the c_is? When the basis is orthonormal, it's easy:

Lemma C4.4 *Let V be a linear subspace of $\mathbb{R}^n$ and let $\mathbf{v}_1, \ldots, \mathbf{v}_m$ be an orthonormal basis of V. Then for all $\mathbf{x} \in V$,*

$$\mathbf{x} = \sum_{i=1}^{m} (\mathbf{x} \cdot \mathbf{v}_i)\mathbf{v}_i.$$

Proof By definition of basis, we have $\mathbf{x} = \sum_i c_i \mathbf{v}_i$ for some scalars $c_1, \ldots, c_m$. Let $j \in \{1, \ldots, m\}$. Taking the dot product of each side of this equation with $\mathbf{v}_j$ gives

$$\mathbf{x} \cdot \mathbf{v_j} = \Bigl(\sum_i c_i \mathbf{v}_i\Bigr) \cdot \mathbf{v}_j = \sum_i c_i (\mathbf{v}_i \cdot \mathbf{v}_j) = c_j,$$

as required. □

Examples C4.5 i. Take $V = \mathbb{R}^n$ with its standard basis $\mathbf{e}_1, \ldots, \mathbf{e}_n$, which is orthonormal. For $\mathbf{x} = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} \in \mathbb{R}^n$, we have $\mathbf{x} \cdot \mathbf{e}_i = x_i$. So in this case, Lemma C4.4 simply states that $\mathbf{x} = \sum_{i=1}^{n} x_i \mathbf{e}_i$.

ii. As in Example C4.2(ii), take the orthonormal basis

$$\mathbf{v}_1 = \bigl(\begin{smallmatrix} \sqrt{2}/2 \\ \sqrt{2}/2 \end{smallmatrix}\bigr), \ \mathbf{v}_2 = \bigl(\begin{smallmatrix} \sqrt{2}/2 \\ -\sqrt{2}/2 \end{smallmatrix}\bigr)$$

of $\mathbb{R}^2$. Put $\mathbf{x} = \bigl(\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\bigr)$. Then $\mathbf{x} \cdot \mathbf{v}_1 = \sqrt{2}/2 = \mathbf{x} \cdot \mathbf{v}_2$, so

$$\mathbf{x} = \frac{\sqrt{2}}{2}\mathbf{v}_1 + \frac{\sqrt{2}}{2}\mathbf{v}_2.$$

Having an orthonormal bases makes life easier. It's good to know, then, that any basis can be 'improved' to an orthonormal basis, in the following sense:

Theorem C4.6 (Gram–Schmidt) *Let V be a linear subspace of $\mathbb{R}^n$, and let $\mathbf{w}_1, \ldots, \mathbf{w}_m$ be a basis of V. Then there is an orthonormal basis $\mathbf{v}_1, \ldots, \mathbf{v}_m$ of V with the property that for each $i \in \{0, \ldots, m\}$,*

$$\operatorname{span}\{\mathbf{v}_1, \ldots, \mathbf{v}_i\} = \operatorname{span}\{\mathbf{w}_1, \ldots, \mathbf{w}_i\}. \tag{C:3}$$

Proof We construct the vectors $\mathbf{v}_1, \ldots, \mathbf{v}_m$ one by one. Let $0 \leq i < m$, and suppose inductively that we have constructed orthonormal vectors $\mathbf{v}_1, \ldots, \mathbf{v}_i$ satisfying equation (C:3). (When $i = 0$, this just means that we have not constructed any yet.) Put

$$\mathbf{x} = \mathbf{w}_{i+1} - \bigl((\mathbf{w}_{i+1} \cdot \mathbf{v}_1)\mathbf{v}_1 + \cdots + (\mathbf{w}_{i+1} \cdot \mathbf{v}_i)\mathbf{v}_i\bigr). \tag{C:4}$$

Since $\mathbf{w}_1, \ldots, \mathbf{w}_m$ are linearly independent,

$$\mathbf{w}_{i+1} \notin \operatorname{span}\{\mathbf{w}_1, \ldots, \mathbf{w}_i\} = \operatorname{span}\{\mathbf{v}_1, \ldots, \mathbf{v}_i\}.$$

Hence $\mathbf{x} \neq \mathbf{0}$. We can therefore define $\mathbf{v}_{i+1} = \mathbf{x}/\|\mathbf{x}\|$. Evidently $\|\mathbf{v}_{i+1}\| = 1$. Also, for $1 \leq j \leq i$, we have

$$\begin{aligned}
\mathbf{v}_{i+1} \cdot \mathbf{v}_j &= \frac{1}{\|\mathbf{x}\|} \mathbf{x} \cdot \mathbf{v}_j \\
&= \frac{1}{\|\mathbf{x}\|} \Big(\mathbf{w}_{i+1} \cdot \mathbf{v}_j - \big((\mathbf{w}_{i+1} \cdot \mathbf{v}_1) \mathbf{v}_1 \cdot \mathbf{v}_j + \cdots + (\mathbf{w}_{i+1} \cdot \mathbf{v}_i) \mathbf{v}_i \cdot \mathbf{v}_j \big) \Big) \\
&= \frac{1}{\|\mathbf{x}\|} \Big(\mathbf{w}_{i+1} \cdot \mathbf{v}_j - \mathbf{w}_{i+1} \cdot \mathbf{v}_j \Big) = 0
\end{aligned}$$

(using the orthonormality of $\mathbf{v}_1, \ldots, \mathbf{v}_i$). Hence $\mathbf{v}_1, \ldots, \mathbf{v}_i, \mathbf{v}_{i+1}$ are orthonormal. Finally, equation (C:4) and the inductive hypothesis (C:3) together imply that $\operatorname{span}\{\mathbf{v}_1, \ldots, \mathbf{v}_{i+1}\} = \operatorname{span}\{\mathbf{w}_1, \ldots, \mathbf{w}_{i+1}\}$. (Exercise: why exactly do they imply this?)

This completes the induction. It remains to show that $\mathbf{v}_1, \ldots, \mathbf{v}_m$ is an orthonormal basis for V. By (C:3) with $i = m$, these vectors span V, and by Lemma C4.3, they are linearly independent. Hence they are a basis. (Alternatively, we could prove just spanning *or* linear independence, then use Lemma C2.17.) □

Corollary C4.7 *Every linear subspace of $\mathbb{R}^n$ has at least one orthonormal basis.*

Proof By Proposition C2.13, every subspace V has at least one basis. By Theorem C4.6, V therefore has an orthonormal basis. □

The proof of the theorem gives us an actual *algorithm* for constructing an orthonormal basis $\mathbf{v}_1, \ldots, \mathbf{v}_m$ out of any old basis $\mathbf{w}_1, \ldots, \mathbf{w}_m$. This algorithm is called **Gram–Schmidt orthogonalization**. (It should really be called 'Gram–Schmidt orthonormalization', but it's not.) Here is an example.

Example C4.8 When V is 3-dimensional, we start with a basis $\mathbf{w}_1, \mathbf{w}_2, \mathbf{w}_3$ and construct from it an orthonormal basis $\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3$ as follows:

$$\begin{aligned}
\mathbf{v}_1 &= \frac{\mathbf{w}_1}{\|\mathbf{w}_1\|}, \\
\mathbf{v}_2 &= \frac{\mathbf{w}_2 - (\mathbf{w}_2 \cdot \mathbf{v}_1)\mathbf{v}_1}{\|\mathbf{w}_2 - (\mathbf{w}_2 \cdot \mathbf{v}_1)\mathbf{v}_1\|}, \\
\mathbf{v}_3 &= \frac{\mathbf{w}_3 - \big((\mathbf{w}_3 \cdot \mathbf{v}_1)\mathbf{v}_1 + (\mathbf{w}_3 \cdot \mathbf{v}_2)\mathbf{v}_2\big)}{\|\mathbf{w}_3 - \big((\mathbf{w}_3 \cdot \mathbf{v}_1)\mathbf{v}_1 + (\mathbf{w}_3 \cdot \mathbf{v}_2)\mathbf{v}_2\big)\|}.
\end{aligned}$$

(This is exactly the method of the proof, written out explicitly.) For instance, if we start with the (non-orthonormal) basis

$$\mathbf{w}_1 = \begin{pmatrix} 2 \\ 0 \\ 0 \end{pmatrix}, \quad \mathbf{w}_2 = \begin{pmatrix} 2 \\ 2 \\ 0 \end{pmatrix}, \quad \mathbf{w}_3 = \begin{pmatrix} 2 \\ 2 \\ 2 \end{pmatrix}$$

then after some calculation, we find that $\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3$ is the standard basis $\mathbf{e}_1, \mathbf{e}_2, \mathbf{e}_3$.

Given a line through the origin in $\mathbb{R}^3$, you can take the plane through the origin orthogonal to it. Similarly, given a plane through the origin in $\mathbb{R}^3$, you can take the line through the origin orthogonal to it. Here is the general definition.

Definition C4.9 Let V be a linear subspace of $\mathbb{R}^n$. The **orthogonal complement** of V is

$$V^\perp = \{\mathbf{x} \in \mathbb{R}^n : \mathbf{x} \cdot \mathbf{v} = 0 \text{ for all } \mathbf{v} \in V\}.$$

$V^\perp$ is pronounced 'V-perp'. It consists of the vectors perpendicular to *everything* in V.

Lemma C4.10 *Let V be a linear subspace of $\mathbb{R}^n$. Then $V^\perp$ is also a linear subspace of $\mathbb{R}^n$.*

Proof We verify the three conditions of Definition C1.1.

For (i), certainly $\mathbf{0} \cdot \mathbf{v} = 0$ for all $\mathbf{v} \in V$.

For (ii), let $\mathbf{x}, \mathbf{y} \in V^\perp$. Then for each $\mathbf{v} \in V$, we have

$$(\mathbf{x} + \mathbf{y}) \cdot \mathbf{v} = \mathbf{x} \cdot \mathbf{v} + \mathbf{y} \cdot \mathbf{v} = 0 + 0 = 0,$$

so $\mathbf{x} + \mathbf{y} \in V^\perp$.

The proof of (iii) is similar, and left as an exercise. □

Lemma C4.11 *Let V be a linear subspace of $\mathbb{R}^n$ and let $\mathbf{v}_1, \ldots, \mathbf{v}_m \in V$ be vectors spanning V. Then*

$$V^\perp = \{\mathbf{x} \in \mathbb{R}^n : \mathbf{x} \cdot \mathbf{v}_1 = \cdots = \mathbf{x} \cdot \mathbf{v}_m = 0\}.$$

Proof Exercise. □

Proposition C4.12 *Let V be a linear subspace of $\mathbb{R}^n$. Then:*

i. $V \cap V^\perp = \{\mathbf{0}\}$*;*

ii. every element of $\mathbb{R}^n$ can be expressed as $\mathbf{v} + \mathbf{w}$ for some $\mathbf{v} \in V$ and $\mathbf{w} \in V^\perp$;

iii. $\dim V + \dim V^\perp = n$.

Proof For (i), certainly $\mathbf{0} \in V \cap V^\perp$, since both V and $V^\perp$ are subspaces. Now take any element $\mathbf{x} \in V \cap V^\perp$. Then $\mathbf{x} \cdot \mathbf{v} = 0$ for all $\mathbf{v} \in V$, and in particular this holds when $\mathbf{v} = \mathbf{x}$. Hence $\mathbf{x} \cdot \mathbf{x} = 0$, that is, $\|\mathbf{x}\|^2 = 0$, so $\mathbf{x} = \mathbf{0}$.

For (ii), let $\mathbf{x} \in \mathbb{R}^n$. By Corollary C4.7, we can choose an orthonormal basis $\mathbf{v}_1, \ldots, \mathbf{v}_m$ for V. Now put

$$\hat{\mathbf{x}} = \sum_{i=1}^{m} (\mathbf{x} \cdot \mathbf{v}_i)\mathbf{v}_i.$$

Evidently $\hat{\mathbf{x}} \in V$. I claim that $\mathbf{x} - \hat{\mathbf{x}} \in V^\perp$. To prove this, it is enough (by Lemma C4.11) to prove that $(\mathbf{x} - \hat{\mathbf{x}}) \cdot \mathbf{v}_j = 0$ for each $j = 1, \ldots, m$. And indeed,

$$\begin{aligned}
(\mathbf{x} - \hat{\mathbf{x}}) \cdot \mathbf{v}_j &= \mathbf{x} \cdot \mathbf{v}_j - \hat{\mathbf{x}} \cdot \mathbf{v}_j \\
&= \mathbf{x} \cdot \mathbf{v}_j - \sum_{i=1}^{m} (\mathbf{x} \cdot \mathbf{v}_i)\mathbf{v}_i \cdot \mathbf{v}_j \\
&= \mathbf{x} \cdot \mathbf{v}_j - \mathbf{x} \cdot \mathbf{v}_j = 0,
\end{aligned}$$

proving the claim. Now $\mathbf{x} = \hat{\mathbf{x}} + (\mathbf{x} - \hat{\mathbf{x}})$ with $\hat{\mathbf{x}} \in V$ and $\mathbf{x} - \hat{\mathbf{x}} \in V^\perp$, proving (ii).

Finally, for (iii), take bases $\mathbf{v}_1, \ldots, \mathbf{v}_m$ for V and $\mathbf{w}_1, \ldots, \mathbf{w}_k$ for $V^\perp$. I claim that $\mathbf{v}_1, \ldots, \mathbf{v}_m, \mathbf{w}_1, \ldots, \mathbf{w}_k$ is a basis for $\mathbb{R}^n$. To prove linear independence, suppose that

$$c_1\mathbf{v}_1 + \cdots + c_m\mathbf{v}_m + d_1\mathbf{w}_1 + \cdots + d_k\mathbf{w}_k = 0$$

for some scalars c_i, d_j. Then $\sum_{i=1}^m c_i\mathbf{v}_i = \sum_{j=1}^k (-d_j)\mathbf{w}_j$. The left-hand side belongs to V and the right-hand side to $V^\perp$, hence both sides belong to $V \cap V^\perp$. It follows from part (i) that both sides are $\mathbf{0}$. So $\sum_{i=1}^m c_i\mathbf{v}_i = \mathbf{0}$, which by linear independence of $\mathbf{v}_1, \ldots, \mathbf{v}_m$ implies that $c_1 = \cdots = c_m = 0$. For similar reasons, $d_1 = \cdots = d_k = 0$. This proves linear independence.

To prove that $\mathbf{v}_1, \ldots, \mathbf{v}_m, \mathbf{w}_1, \ldots, \mathbf{w}_k$ span $\mathbb{R}^n$, let $\mathbf{x} \in \mathbb{R}^n$. By part (ii), there exist $\mathbf{v} \in V$ and $\mathbf{w} \in V^\perp$ such that $\mathbf{x} = \mathbf{v} + \mathbf{w}$. But $\mathbf{v}$ is a linear combination of $\mathbf{v}_1, \ldots, \mathbf{v}_m$ and $\mathbf{w}$ is a linear combination of $\mathbf{w}_1, \ldots, \mathbf{w}_k$, so $\mathbf{x}$ is a linear combination of $\mathbf{v}_1, \ldots, \mathbf{v}_m, \mathbf{w}_1, \ldots, \mathbf{w}_k$.

We have proved that $\mathbf{v}_1, \ldots, \mathbf{v}_m, \mathbf{w}_1, \ldots, \mathbf{w}_k$ is a basis for $\mathbb{R}^n$, where $m = \dim V$ and $k = \dim V^\perp$. Since all bases of $\mathbb{R}^n$ have the same number of elements, $m + k = n$. □

Start with a plane P through the origin in $\mathbb{R}^3$. Take the line L through the origin orthogonal to P. Now take the plane P' through the origin orthogonal to L. That's just P again, right? Right:

Corollary C4.13 *Let V be a linear subspace of $\mathbb{R}^n$. Then $(V^\perp)^\perp = V$.*

Proof First we show that $V \subseteq (V^\perp)^\perp$. Let $\mathbf{v} \in V$. To show that $\mathbf{v} \in (V^\perp)^\perp$, we have to prove that $\mathbf{v} \cdot \mathbf{x} = 0$ for all $\mathbf{x} \in V^\perp$. This is immediate from the definition of $V^\perp$.

By Proposition C4.12(iii) applied to V, we have $\dim V + \dim V^\perp = n$. But we can also apply Proposition C4.12(iii) to $V^\perp$, and that gives $\dim V^\perp + \dim(V^\perp)^\perp = n$. Hence $\dim V = \dim(V^\perp)^\perp$.

So V and $(V^\perp)^\perp$ are two linear subspaces of $\mathbb{R}^n$ of the same dimension, with $V \subseteq (V^\perp)^\perp$. It follows from Lemma C2.18 (the 'with equality if and only if' part) that $V = (V^\perp)^\perp$. □

C5 A second look at the rank theorem

For the lecture of Monday, 12 October 2015; part five of five

The theorems have been coming thick and fast. But now we get the payoff, easily deducing some of the big results of the course.

Theorem C5.1 (Rank theorem, second version) *For any matrix A,*

$$\textit{row-rank}(A) + \textit{nullity}(A) = \textit{number of columns of } A.$$

Proof Let A be an $m \times n$ matrix.

First we show that $\mathrm{row}(A)^\perp = \ker(A)$. Write the rows of A as $\mathbf{v}_1, \ldots, \mathbf{v}_m \in \mathbb{R}^n$. (Again, we're blurring the distinction between row and column vectors here, since officially $\mathbf{v}_i$ is a row vector and the elements of $\mathbb{R}^n$ are column vectors; but this will do no harm.) By definition, $\mathrm{row}(A)$ is spanned by $\mathbf{v}_1, \ldots, \mathbf{v}_m$. So by Lemma C4.11,

$$\mathrm{row}(A)^\perp = \{\mathbf{x} \in \mathbb{R}^n : \mathbf{v}_1 \cdot \mathbf{x} = \cdots = \mathbf{v}_m \cdot \mathbf{x} = 0\}.$$

But $\mathbf{v}_1 \cdot \mathbf{x}, \ldots, \mathbf{v}_m \cdot \mathbf{x}$ are precisely the m entries of $A\mathbf{x} \in \mathbb{R}^m$ (by definition of matrix multiplication), so

$$\mathrm{row}(A)^\perp = \{\mathbf{x} \in \mathbb{R}^n : A\mathbf{x} = 0\} = \ker(A),$$

as required.

On the other hand, $\dim(\mathrm{row}(A)) + \dim(\mathrm{row}(A)^\perp) = n$ by Proposition C4.12. Hence $\dim(\mathrm{row}(A)) + \dim(\ker(A)) = n$, which is exactly what the theorem states. $\square$

Theorem C5.2 *The row rank of a matrix is equal to its column rank.*

Proof This follows immediately from the two versions of the rank theorem (Theorem C3.2 and Theorem C5.1). $\square$

We can now define the **rank** of a matrix A, written as $\mathrm{rank}(A)$, to be either the row rank or the column rank of A: they're the same! So both versions of the rank theorem say

$$\text{rank} + \text{nullity} = \text{number of columns}.$$

But we needed to prove both versions in order to deduce that the two kinds of rank were the same.

Armed with all this theory, we're now ready to go back to simultaneous equations. We will find that we can now say something new.

Chapter D

Simultaneous linear equations, revisited

Chapter C contained a lot of new theory. In this chapter, we reap the rewards.

First, we use the theory to give us lots of different ways of telling whether a matrix is invertible. Several of these have to do with linear systems; for example, we will show that a square matrix A is invertible if and only if the homogeneous linear system $A\mathbf{x} = \mathbf{0}$ has no solutions except for the trivial one, $\mathbf{x} = \mathbf{0}$.

We then re-interpret the rank theorem in terms of linear systems. This is a follow-up to the discussion at the end of Section B1. There, we made a slightly vague guess about the dimension of the set of solutions of a linear system. We're now able to make that guess precise, and prove that it's correct.

The last chapter talked a lot about bases, but in theoretical terms only: we said very little about how to actually *compute* a basis for a given subspace. Section D4 gives practical methods for computing bases in several situations.

Finally, Section D5 introduces the only big new definition of this chapter: determinants. As we'll see, these are useful in linear algebra, and they are also an essential tool for computing multi-variable integrals.

D1 Invertible matrices

For the lecture of Monday, 26 October 2015; part one of five

Back in Section A3, we defined an $m \times n$ matrix A to be 'invertible' if there exists an $n \times m$ matrix B such that $AB = I_m$ and $BA = I_n$. In Proposition A3.3, we asserted two non-obvious facts: first, that if A is invertible then $m = n$, and second, that for $n \times n$ matrices A and B, if $AB = I_n$ then $BA = I_n$.

Back then, we were in no position to prove those claims. But we can prove them now, by using the theory we have developed.

Proposition D1.1 *Invertible matrices are square.*

Proof Let A be an $m \times n$ invertible matrix. We must prove that $m = n$.

The kernel of A is trivial, since if $\mathbf{x} \in \mathbb{R}^n$ with $A\mathbf{x} = \mathbf{0}$ then $A^{-1}A\mathbf{x} = A^{-1}\mathbf{0}$, so $\mathbf{x} = \mathbf{0}$. Hence A has nullity 0. The rank theorem (Theorem C3.2) then implies that the (column) rank of A is n. So $\dim \mathrm{col}(A) = n$. But $\mathrm{col}(A)$ is a subspace of $\mathbb{R}^m$, so has dimension at most m (by Lemma C2.18). Hence $n \leq m$.

We have just shown that the number of columns in an invertible matrix is less than or equal to the number of rows. Applying this to the $n \times m$ invertible matrix A^{-1} tells us that $m \leq n$. Hence $m = n$. □

A square matrix that is not invertible is said to be **singular**.

As we will see, there are many conditions on a square matrix that are equivalent to invertibility. The following three conditions will turn out to be equivalent to invertibility, but for now we just show that they are equivalent to each other:

Lemma D1.2 *Let A be an $n \times n$ matrix. The following are equivalent:*

i. $\ker(A) = \{\mathbf{0}\}$*;*

ii. the homogeneous linear system $A\mathbf{x} = \mathbf{0}$ has only the trivial solution $\mathbf{x} = \mathbf{0}$;

iii. $\mathrm{nullity}(A) = 0$.

Proof Conditions (i) and (ii) are equivalent by definition of kernel. Conditions (i) and (iii) are equivalent because $\{\mathbf{0}\}$ is the unique 0-dimensional subspace of $\mathbb{R}^n$. □

Again, the next lemma lists some conditions on an $n \times n$ matrix that are equivalent to each other, and will soon be shown to be equivalent to invertibility.

Lemma D1.3 *Let A be an $n \times n$ matrix. The following are equivalent:*

i. the columns of A are linearly independent;

ii. the columns of A span $\mathbb{R}^n$;

iii. the columns of A are a basis of $\mathbb{R}^n$;

iv. $\mathrm{rank}(A) = n$.

Proof The equivalence of conditions (i)–(iii) follows from Lemma C2.17. Also, (ii) is equivalent to (iv) because $\mathbb{R}^n$ is the unique n-dimensional subspace of $\mathbb{R}^n$. □

Now we can show that all these conditions, and more besides, are equivalent to invertibility.

Theorem D1.4 (Fundamental theorem of invertible matrices, part 1) *Let A be an $n \times n$ matrix. The following are equivalent:*

i. A is invertible;

ii. there exists an $n \times n$ matrix A' such that $A'A = I_n$;

iii. $\ker(A) = \{\mathbf{0}\}$*;*

iv. the homogeneous linear system $A\mathbf{x} = \mathbf{0}$ has only the trivial solution $\mathbf{x} = \mathbf{0}$;

v. $\mathrm{nullity}(A) = 0$*;*

vi. the columns of A are linearly independent;

vii. *the columns of A span $\mathbb{R}^n$;*

viii. *the columns of A are a basis of $\mathbb{R}^n$;*

ix. rank$(A) = n$*;*

x. *for all $\mathbf{b} \in \mathbb{R}^n$, the non-homogeneous linear system $A\mathbf{x} = \mathbf{b}$ has exactly one solution;*

xi. *for all integers $p \geq 0$ and $n \times p$ matrices B, there is exactly one $n \times p$ matrix X such that $AX = B$.*

Proof We already know that (iii)–(v) are equivalent and that (vi)–(ix) are equivalent, so it suffices to prove that (i)$\Longrightarrow$(ii)$\Longrightarrow$(iv)$\Longrightarrow$(vi) and (viii)$\Longrightarrow$(x)$\Longrightarrow$(xi)$\Longrightarrow$(i). (Suggestion: draw a diagram showing all the implications.)

(i)$\Longrightarrow$(ii) is immediate from the definition of invertibility.

(ii)$\Longrightarrow$(iv): take some A' such that $A'A = I_n$, and let $\mathbf{x} \in \mathbb{R}^n$ with $A\mathbf{x} = \mathbf{0}$. Then $A'(A\mathbf{x}) = A'\mathbf{0} = \mathbf{0}$. But $A'(A\mathbf{x}) = (A'A)\mathbf{x} = \mathbf{x}$, so $\mathbf{x} = \mathbf{0}$.

(iv)$\Longrightarrow$(vi): write the columns of A as $\mathbf{v}_1, \ldots, \mathbf{v}_n$. As observed in the proof of Lemma C1.9 (and as you will show in Assignment 4, q.2), we have

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

for any $\mathbf{x} \in \mathbb{R}^n$. So if $x_1, \ldots, x_n$ are scalars such that $\sum_i x_i\mathbf{v}_i = \mathbf{0}$ then $A\mathbf{x} = \mathbf{0}$, so $\mathbf{x} = \mathbf{0}$ by (iv), so $x_1 = \cdots = x_n = 0$. Hence $\mathbf{v}_1, \ldots, \mathbf{v}_n$ are linearly independent.

(viii)$\Longrightarrow$(x): again, write the columns of A as $\mathbf{v}_1, \ldots, \mathbf{v}_n$. Let $\mathbf{b} \in \mathbb{R}^n$. We must prove that there is exactly one $\mathbf{x} \in \mathbb{R}^n$ such that

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

But $\mathbf{v}_1, \ldots, \mathbf{v}_n$ is a basis for $\mathbb{R}^n$, so as remarked after the definition of basis (Definition C2.3), there are unique scalars $x_1, \ldots, x_n$ making this equation hold. This proves (x).

(x)$\Longrightarrow$(xi): assume (x), and let B be an $n \times p$ matrix. Write the columns of B as $\mathbf{b}_1, \ldots, \mathbf{b}_p$. By (x), there are unique $\mathbf{x}_1, \ldots, \mathbf{x}_p$ such that

$$A\mathbf{x}_1 = \mathbf{b}_1, \ \ldots, \ A\mathbf{x}_p = \mathbf{b}_p.$$

But for any $n \times p$ matrix X, the kth column of AX is A times the kth column of X. Hence the matrix X with columns $\mathbf{x}_1, \ldots, \mathbf{x}_p$ is the unique solution to $AX = B$.

(xi)$\Longrightarrow$(i): assume (xi). Taking $B = I_n$, there is a unique matrix A' such that $AA' = I_n$. Observe now that $A(A'A) = (AA')A = I_nA = A$ and $AI_n = A$. But taking $B = A$ in (xi) tells us that there is only one matrix X such that $AX = A$, and both $X = A'A$ and $X = I_n$ satisfy this, so $A'A = I_n$. Hence A is invertible. $\square$

Further equivalent conditions for invertibility can be obtained by 'swapping the roles of the rows and columns'. Probably the most efficient way to make this idea precise is to use the notion of transpose, as in the following lemma and theorem.

Lemma D1.5 *The transpose of an invertible matrix is invertible.*

Proof Let A be an invertible $m \times n$ matrix. Taking transposes on both sides of the equation $A^{-1}A = I_n$ gives $A^T(A^{-1})^T = I_n$ (using the fact that $(BA)^T = A^T B^T$). Similarly, taking transposes in $AA^{-1} = I_m$ gives $(A^{-1})^T A^T = I_m$. So A^T is invertible with inverse $(A^{-1})^T$. □

Theorem D1.6 (Fundamental theorem of invertible matrices, part 2) *Let A be an $n \times n$ matrix. The following are equivalent:*

i. A is invertible;

ii. there exists an $n \times n$ matrix A' such that $AA' = I_n$;

iii. the rows of A are linearly independent;

iv. the rows of A span $\mathbb{R}^n$;

v. the rows of A are a basis of $\mathbb{R}^n$.

Proof We apply Theorem D1.4 to the matrix A^T.

Condition (i) of the present theorem states that A is invertible, which by Lemma D1.5 is equivalent to A^T being invertible. This is condition (i) of Theorem D1.4 applied to A^T.

Condition (ii) of the present theorem holds if and only if there is some A' satisfying $(AA')^T = I_n$, if and only if there is some A' satisfying $(A')^T A^T = I_n$, if and only if there is some A'' satisfying $A''A^T = I_n$. This is condition (ii) of Theorem D1.4 applied to A^T.

The rows of A are the columns of A^T, so condition (iii) of the present theorem is equivalent to condition (vi) of Theorem D1.4 applied to A^T. Similarly, conditions (iv) and (v) of the present theorem are equivalent to conditions (vii) and (viii) of Theorem D1.4 applied to A^T.

So each of the five conditions in the present theorem is equivalent to one of the conditions of Theorem D1.4 applied to A^T. Since all the conditions of that theorem are equivalent, so too are the five conditions above. □

Corollary D1.7 *Let A and B be $n \times n$ matrices. Then $AB = I_n \iff BA = I_n$.*

Proof Suppose that $AB = I_n$. Then A is invertible by Theorem D1.6, so $A^{-1}(AB) = A^{-1}I_n$, so $B = A^{-1}$, so $BA = A^{-1}A = I_n$. The converse is similar. □

We now know a great deal about which matrices are invertible—at least in theory. But we know little about two practical questions: how to decide *whether* a given matrix is invertible, and if it is, *how* to find its inverse. These deficiencies are repaired in the next section.

D2 Elementary row operations, revisited

For the lecture of Monday, 26 October 2015; part two of five

Elementary row operations were introduced in Section B2 as a way of solving linear systems. Here we look at them more carefully.

We begin by showing that for every elementary row operation, there is a certain special matrix E with the property that multiplication on the left by E has the effect of performing that operation. For example, consider the elementary row operation 'add 3 times the second row to the first row'. Then there is a certain matrix E with the property that for any matrix A, the product EA is equal to the result of applying $R_1 \to R_1 + 3R_2$ to A.

If this is true for *all* matrices A, then it must be true when A is the identity matrix I. So, E must be the result of applying $R_1 \to R_1 + 3R_2$ to I. Such matrices E have a name:

Definition D2.1 An $m \times m$ matrix E is said to be **elementary** if it is equal to the result of applying a single elementary row operation to I_m.

Since there are three types of elementary row operation, there are three types of elementary matrix. I will use the following notation:

- $E^{i,j}_{\text{swap}}$ is the result of interchanging rows i and j of I_m (where $i, j \in \{1, \ldots, m\}$ with $i \neq j$);
- $E^{i;c}_{\text{mult}}$ is the result of multiplying row i of I_m by c (where $i \in \{1, \ldots, m\}$ and $0 \neq c \in \mathbb{R}$);
- $E^{i,j;c}_{\text{add}}$ is the result of adding c times row j to row i of I_m (where $i, j \in \{1, \ldots, m\}$ with $i \neq j$, and $c \in \mathbb{R}$).

(Warning: I have just made up this notation. Don't expect anyone outside this class to understand it!)

Example D2.2 When $m = 4$,

$$E^{1,2}_{\text{swap}} = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \quad E^{1;c}_{\text{mult}} = \begin{pmatrix} c & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \quad E^{1,2;c}_{\text{add}} = \begin{pmatrix} 1 & c & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

We now prove the claim made earlier:

Proposition D2.3 *Let E be an $m \times m$ elementary matrix and let A be any $m \times n$ matrix. Then EA is the matrix obtained from A by applying the elementary row operation corresponding to E.*

In other words, $E^{i,j}_{\text{swap}} A$ is the result of applying the elementary row operation $R_i \leftrightarrow R_j$ to A, and similarly for the other two types of row operation.

Proof We prove this for $E = E^{i,j;c}_{\text{add}}$, where $i, j \in \{1, \ldots, m\}$ with $i \neq j$ and $c \in \mathbb{R}$. The other two types are no harder and are left as exercises.

We can assume without loss of generality that $i = 1$ and $j = 2$. Thus,

$$E = \begin{pmatrix} 1 & c & 0 & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \end{pmatrix}.$$

Writing the (p, q)-entry of A as a_{pq}, it follows that

$$EA = \begin{pmatrix} a_{11} + ca_{21} & a_{12} + ca_{22} & a_{13} + ca_{23} & \cdots & a_{1n} + ca_{2n} \\ a_{21} & a_{22} & a_{23} & \cdots & a_{2n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & a_{m3} & \cdots & a_{mn} \end{pmatrix}.$$

This is exactly the result of applying $R_1 \to R_1 + cR_2$ to A. □

Any elementary row operation can be undone by another elementary row operation. Swapping rows i and j is undone by doing the same swap again; multiplying row i by $c \neq 0$ is undone by multiplying row i by $1/c$; and adding c times row j to row i is undone by subtracting c times row j from row i.

Lemma D2.4 *Every elementary matrix is invertible, with elementary inverse.*

Proof I claim that

$$\left(E^{i,j}_{\text{swap}}\right)^{-1} = E^{i,j}_{\text{swap}}, \qquad \left(E^{i;c}_{\text{mult}}\right)^{-1} = E^{i;1/c}_{\text{mult}}, \qquad \left(E^{i,j;c}_{\text{add}}\right)^{-1} = E^{i,j;-c}_{\text{add}}.$$

There are at least two ways to prove these claims. I will do the proofs for $E^{i;c}_{\text{mult}}$, but similar arguments apply to the other types of elementary matrix.

First, we can simply compute the matrix products, checking that $E^{i;c}_{\text{mult}} E^{i;1/c}_{\text{mult}} = I$. The claim then follows from Theorem D1.6(ii).

Alternatively, we can argue as follows (which has the advantage of not requiring any calculation). By Proposition D2.3, $E^{i;c}_{\text{mult}} E^{i;1/c}_{\text{mult}} I$ is the result of taking I, applying the row operation $R_i \to (1/c)R_i$, then applying the row operation $R_i \to cR_i$. These two row operations are inverse to one another, so

$$E^{i;c}_{\text{mult}} E^{i;1/c}_{\text{mult}} I = I.$$

The claim then follows from Theorem D1.6(ii). □

Lemma D2.5 *Let A be an $m \times n$ matrix, and let R be another $m \times n$ matrix that has been obtained from A by applying a finite sequence of elementary row operations. Then:*

i. $R = E_k \cdots E_2 E_1 A$ for some $k \geq 0$ and elementary matrices $E_1, E_2, \ldots, E_k$; and

ii. $R = EA$ for some $m \times m$ invertible matrix E.

Proof To prove (i), suppose that R has been obtained from A by a sequence of k elementary row operations. Write E_1 for the elementary matrix corresponding to the first operation, and so on. Then by Proposition D2.3, $R = E_k \cdots E_2 E_1 A$.

For (ii), put $E = E_k \cdots E_2 E_1$; then $R = EA$. Each of $E_1, \ldots, E_k$ is invertible by Lemma D2.4, and any product of invertible matrices is invertible (by Lemma A3.5 and induction), so E is invertible. □

Remark D2.6 Back in Section B2, we solved linear systems by using elementary row operations on augmented matrices: see Example B2.1, for instance. Starting with a system $A\mathbf{x} = \mathbf{b}$, we applied the same elementary row operations to A and $\mathbf{b}$ until A was in reduced row echelon form. Writing $E_1, \ldots, E_k$ for the elementary matrices corresponding to those operations, the reduced system is therefore

$$E_k \cdots E_2 E_1 A\mathbf{x} = E_k \cdots E_2 E_1 \mathbf{b}.$$

Since $E_1, \ldots, E_k$ are invertible, a vector $\mathbf{x}$ satisfies this equation if and only if it satisfies $A\mathbf{x} = \mathbf{b}$. In other words, *the reduced system has exactly the same solutions as the original system.* At the end of Example B2.1, I wrote that it was 'maybe not completely clear what justifies' the principle that the reduced and original systems have the same solutions. This is the justification.

In the last section, we found lots of conditions on a square matrix equivalent to it being invertible. We are about to write down two more, and for this, we will need the following observation about matrices in RREF.

Lemma D2.7 *The only $n \times n$ invertible matrix in reduced row echelon form is I_n.*

Proof Let R be an invertible matrix in RREF. Theorem D1.4 implies that since R is invertible, the only column vector $\mathbf{x}$ satisfying $R\mathbf{x} = \mathbf{0}$ is $\mathbf{x} = \mathbf{0}$. If the last row of R were zero then we would have

$$R \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix} = \mathbf{0},$$

a contradiction. So the last row of R is not zero. Since R is in row echelon form, R has no zero rows. Also because R is in REF, the leading entry in each row must be on the diagonal (top-left to bottom-right) of the matrix. And because R is in *reduced* REF, those leading entries are all 1 and all the other entries in the columns containing them are 0. Hence $R = I_n$. □

Theorem D2.8 (Fundamental theorem of invertible matrices, part 3) *Let A be an $n \times n$ matrix. The following are equivalent:*

i. A is invertible;

ii. the reduced row echelon form of A is I_n;

iii. A can be expressed as a product $E_1 E_2 \cdots E_k$ of elementary matrices.

Proof (i)$\Longrightarrow$(ii): suppose that A is invertible, and write R for its reduced row echelon form. By Lemma D2.5(ii), $R = EA$ for some invertible matrix E. Since both E and A are invertible, R is invertible too. So by Lemma D2.7, $R = I_n$.

(ii)$\Longrightarrow$(iii): suppose that the RREF of A is I_n. Then by Lemma D2.5(i), $I_n = (E_k \cdots E_2 E_1)A$ for some elementary matrices $E_1, \ldots, E_k$. By Lemma D2.4, each E_i is invertible with elementary inverse, so A is the product $E_1^{-1} E_2^{-1} \cdots E_k^{-1}$ of elementary matrices.

(iii)$\Longrightarrow$(i): elementary matrices are invertible (by Lemma D2.4), and any product of invertible matrices is invertible (by Lemma A3.5 and induction), so any product of elementary matrices is invertible. □

So we now have a practical way of testing *whether* a matrix A is invertible:

- put A into reduced row echelon form;
- if the RREF is the identity then A is invertible;
- if the RREF is not the identity, then A is not invertible.

We'll see some examples in a moment. But first, we answer a closely related question: if A is invertible, *how* do we find its inverse? The next proposition tells us:

Proposition D2.9 *Let A be an invertible $n \times n$ matrix. If a sequence of elementary row operations turns A into I_n, then the same sequence turns I_n into A^{-1}.*

Proof Take elementary row operations that turn A into I_n, and write $E_1, \ldots, E_k$ for the corresponding elementary matrices. Then $I_n = E_k \cdots E_1 A$. Hence

$$A^{-1} = E_k \cdots E_1 = E_k \cdots E_1 I_n.$$

But $E_k \cdots E_1 I_n$ is the matrix obtained from I_n by applying those same elementary row operations. $\square$

Example D2.10 Is the matrix

$$A = \begin{pmatrix} 1 & 0 & 2 \\ 0 & 3 & 0 \\ 4 & 0 & 5 \end{pmatrix}$$

invertible? If so, what is its inverse?

Place the identity matrix next to A:

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

Using elementary row operations on the whole 3×6 matrix, put the left-hand half into reduced row echelon form:

$$\begin{aligned}
\left(\begin{array}{ccc|ccc} 1 & 0 & 2 & 1 & 0 & 0 \\ 0 & 3 & 0 & 0 & 1 & 0 \\ 4 & 0 & 5 & 0 & 0 & 1 \end{array}\right)
&\xrightarrow[R_3 \to R_3 - 4R_1]{} \left(\begin{array}{ccc|ccc} 1 & 0 & 2 & 1 & 0 & 0 \\ 0 & 3 & 0 & 0 & 1 & 0 \\ 0 & 0 & -3 & -4 & 0 & 1 \end{array}\right) \\
&\xrightarrow[R_2 \to (1/3)R_2,\ R_3 \to (-1/3)R_3]{} \left(\begin{array}{ccc|ccc} 1 & 0 & 2 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1/3 & 0 \\ 0 & 0 & 1 & 4/3 & 0 & -1/3 \end{array}\right) \\
&\xrightarrow[R_1 \to R_1 - 2R_3]{} \left(\begin{array}{ccc|ccc} 1 & 0 & 0 & -5/3 & 0 & 2/3 \\ 0 & 1 & 0 & 0 & 1/3 & 0 \\ 0 & 0 & 1 & 4/3 & 0 & -1/3 \end{array}\right).
\end{aligned}$$

The RREF of A is I_3, so by Theorem D2.8(ii), A is invertible. Then by Proposition D2.9, A^{-1} is the right-hand half; that is,

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

Example D2.11 Let's try another. Is the matrix

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

invertible? If so, what is its inverse?

Apply the same method:

$$\left(\begin{array}{ccc|ccc} 9 & 8 & 7 & 1 & 0 & 0 \\ 6 & 5 & 4 & 0 & 1 & 0 \\ 3 & 2 & 1 & 0 & 0 & 1 \end{array}\right) \xrightarrow[R_1 \to (1/9)R_1]{} \left(\begin{array}{ccc|ccc} 1 & 8/9 & 7/9 & 1/9 & 0 & 0 \\ 6 & 5 & 4 & 0 & 1 & 0 \\ 3 & 2 & 1 & 0 & 0 & 1 \end{array}\right)$$

$$\xrightarrow[R_2 \to R_2 - 6R_1,\ R_3 \to R_3 - 3R_1]{} \left(\begin{array}{ccc|ccc} 1 & 8/9 & 7/9 & 1/9 & 0 & 0 \\ 0 & -1/3 & -2/3 & -2/3 & 1 & 0 \\ 0 & -2/3 & -4/3 & -1/3 & 0 & 1 \end{array}\right)$$

$$\xrightarrow[R_3 \to R_3 - 2R_2]{} \left(\begin{array}{ccc|ccc} 1 & 8/9 & 7/9 & 1/9 & 0 & 0 \\ 0 & -1/3 & -2/3 & -2/3 & 1 & 0 \\ 0 & 0 & 0 & 1 & -2 & 1 \end{array}\right).$$

We haven't yet reduced the left-hand half to RREF, but it already has a zero row, so the RREF will have a zero row too. Hence A is not invertible, by Theorem D2.8(ii).

(The right-hand half plays no part this time; it only would have been useful if A had turned out to be invertible.)

D3 A third look at the rank theorem

For the lecture of Monday, 26 October 2015; part three of five

We first met the rank theorem at the end of Section B1, where we guessed that for homogeneous systems of linear equations,

$$\begin{aligned}&\text{dimension of the set of solutions}\\ &\quad= \text{number of variables} - \text{number of independent equations}.\end{aligned} \tag{D:1}$$

The trouble was, we had no precise definition of 'dimension' or 'number of independent equations'—let alone a *proof* of this guess.

But we can now do everything properly. Consider a homogeneous linear system

$$\begin{aligned}a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n &= 0\\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n &= 0\\ &\vdots\\ a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n &= 0.\end{aligned}$$

As usual, write A for the $m \times n$ matrix (a_{ij}); then the system is equivalent to $A\mathbf{x} = \mathbf{0}$. We think of A as known and $\mathbf{x} \in \mathbb{R}^n$ is unknown.

Let's examine the three phrases used in equation (D:1).

First, the set of solutions $\mathbf{x}$ is $\ker(A)$ (by definition of kernel). It is a linear subspace of $\mathbb{R}^n$ (by Lemma C1.4). So, it makes sense to talk about the 'dimension of the set of solutions'. This is $\dim(\ker(A))$, or in other words, the nullity of A.

Second, the 'number of variables' is simply n, the number of columns of A.

Third and finally, each equation in the linear system corresponds to a row of A. So, the slightly vague phrase 'number of independent equations' means the 'number of independent rows of A', which can sensibly be interpreted as the dimension of the row space of A. In other words, it's the rank of A.

So, a sensible interpretation of (D:1) is: for an $m \times n$ matrix A,

$$\text{nullity}(A) = n - \text{rank}(A).$$

And that's true, because it's exactly the rank theorem, Theorem C5.1!

Here is one immediate and important consequence:

Proposition D3.1 *A homogeneous linear system with more variables than equations has at least one nontrivial solution.*

Such systems are said to be **underdetermined**.

Proof Let n be the number of variables and m the number of equations; then $m < n$. Write A for the matrix of coefficients. Then A is an $m \times n$ matrix, so $\text{rank}(A) \leq m$. Hence $\text{rank}(A) < n$, and so $\text{nullity}(A) \geq 1$ by the rank theorem. But $\text{nullity}(A)$ is the dimension of the set of solutions to the system, so $\mathbf{0}$ is not the only solution. □

What about non-homogeneous systems? These need not have any solution at all, even if they have more variables than equations. For instance, the system

$$\begin{aligned} 2x_1 + 3x_2 + 4x_3 &= 1 \\ 20x_1 + 30x_2 + 40x_3 &= 2 \end{aligned}$$

has no solutions. And even if the system does have a solution, the solutions do not form a linear subspace, since $\mathbf{0}$ is never a solution for a non-homogeneous system. (For if $\mathbf{0}$ were a solution then all the right-hand sides would be 0, so the system would be homogeneous.)

However, something can be said. Suppose that our non-homogeneous system $A\mathbf{x} = \mathbf{b}$ does have at least one solution: $\mathbf{u}$, say. Then by Lemma B1.5, the set of all solutions consists of the vectors $\mathbf{u} + \mathbf{w}$ where $\mathbf{w}$ is a solution of the *homogeneous* system $A\mathbf{x} = \mathbf{0}$. So, the solutions to the non-homogeneous system correspond one-to-one with the solutions to the homogeneous system, by adding or subtracting $\mathbf{u}$.

For instance, suppose that our non-homogeneous solution $A\mathbf{x} = \mathbf{b}$ has at least one solution and that the solutions to the homogeneous system $A\mathbf{x} = \mathbf{0}$ form a 2-dimensional subspace of $\mathbb{R}^n$—that is, a plane through the origin. Then the set of all solutions to the non-homogeneous system is also a plane, although not one that passes through the origin. Put another way, the general solution to the non-homogeneous system has two free variables.

D4 Calculating bases

For the lecture of Monday, 26 October 2015; part four of five

Given a specific matrix, how can you calculate a basis for its row space? What about its column space, or its kernel? And how can you compute the rank and nullity of the matrix?

Given a subspace of $\mathbb{R}^n$, how can you find a basis for its orthogonal complement?

Given a list of vectors in $\mathbb{R}^n$, how do you know whether they're linearly independent? How can you find a basis for the subspace that they span?

Background to the methods

Here we'll discover practical answers to all these questions. We'll use the theory we've developed so far, plus a few more results that we prove now:

Lemma D4.1 *Let E be an $m \times m$ invertible matrix and let A be any $m \times n$ matrix. Then*

$$\ker(EA) = \ker(A), \quad \mathrm{row}(EA) = \mathrm{row}(A), \quad \mathrm{rank}(EA) = \mathrm{rank}(A).$$

Proof For the first equation, let $\mathbf{x} \in \mathbb{R}^n$. If $EA\mathbf{x} = \mathbf{0}$ then multiplying each side by E^{-1} on the left gives $A\mathbf{x} = \mathbf{0}$; conversely, if $A\mathbf{x} = \mathbf{0}$ then multiplying each side by E on the left gives $EA\mathbf{x} = \mathbf{0}$.

For the second, we showed in the proof of Theorem C5.1 that $\mathrm{row}(M)^\perp = \ker(M)$ for all matrices M. Taking orthogonal complements on both sides gives $(\mathrm{row}(M)^\perp)^\perp = \ker(M)^\perp$, or equivalently $\mathrm{row}(M) = \ker(M)^\perp$ (by Corollary C4.13). Hence

$$\mathrm{row}(EA) = \ker(EA)^\perp = \ker(A)^\perp = \mathrm{row}(A).$$

Now $\mathrm{rank}(EA) = \dim(\mathrm{row}(EA)) = \dim(\mathrm{row}(A)) = \mathrm{rank}(A)$. □

Lemma D4.2 *Let R be a matrix in row echelon form. Then the nonzero rows of R are a basis for* $\mathrm{row}(R)$.

Proof By definition, the rows of R span $\mathrm{row}(R)$, and omitting the zero rows does not alter the span, so the nonzero rows of R also span $\mathrm{row}(R)$. It remains to show that the nonzero rows are linearly independent.

Suppose that the matrix R is $m \times n$, with k nonzero rows. (They must be the first k.) For $i = 1, \ldots, k$, write the ith row as $\mathbf{v}_i \in \mathbb{R}^n$, write the leading entry in the ith row as ℓ_i, and let us say that this leading entry is in the p_ith column. By definition of row echelon form,

$$1 \leq p_1 < p_2 < \cdots < p_k \leq n.$$

Now let $c_1, \ldots, c_k$ be scalars such that

$$c_1\mathbf{v}_1 + c_2\mathbf{v}_2 + \cdots + c_k\mathbf{v}_k = \mathbf{0}. \tag{D:2}$$

We must prove that $c_1 = \cdots = c_k = 0$.

Apart from the first row, there are no nonzero entries in the p_1th column. So comparing the p_1th entries on each side of equation (D:2) gives $c_1\ell_1 = 0$. But ℓ_1 is a leading entry, so is not zero, so $c_1 = 0$. Hence (D:2) now gives

$$c_2\mathbf{v}_2 + \cdots + c_k\mathbf{v}_k = \mathbf{0}.$$

If we delete the first row from A then what remains is still in REF, so we can repeat the same argument to get $c_2 = 0$. Continuing in this way gives $c_i = 0$ for all $i = 1, 2, \ldots, k$, as required. □

Putting together the last two lemmas gives:

Proposition D4.3 *Let A be a matrix and R any row echelon form of A. Then:*

i. A and R have the same kernel and the same row space;

ii. $\operatorname{rank}(A)$ *is the number of nonzero rows of R.*

Proof By Lemma D2.5(ii), $R = EA$ for some invertible matrix A. Lemma D4.1 then implies part (i) and that $\operatorname{rank}(A) = \operatorname{rank}(R)$. On the other hand, $\operatorname{rank}(R)$ is the number of nonzero rows of R (by Lemma D4.2), proving (ii). □

(Poole *defines* the rank of a matrix to be the number of nonzero rows in any row echelon form, showing that this does not depend on which row echelon form is chosen.)

Warning D4.4 A matrix and any of its row echelon forms have the same row space, but *not* usually the same column space. For instance, $A = \left(\begin{smallmatrix} 1 & 0 \\ 1 & 0 \end{smallmatrix}\right)$ has RREF $R = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}\right)$, but $\operatorname{col}(A) = \operatorname{span}\{\left(\begin{smallmatrix} 1 \\ 1 \end{smallmatrix}\right)\}$ while $\operatorname{col}(R) = \operatorname{span}\{\left(\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right)\}$.

There is also a notion of *column* echelon form, and a matrix has the same column space as any of its *column* echelon forms.

The methods

We can now answer all the questions posed at the start of this section.

Example D4.5 Given a matrix, how can we calculate a basis for its row space? Take, for instance,

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

After a sequence of elementary row operations, we find that the RREF of A is

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

By Lemma D4.2, the nonzero rows of R form a basis for $\operatorname{row}(R)$, which by Proposition D4.3(i) is equal to $\operatorname{row}(A)$. So

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

is a basis for $\operatorname{row}(A)$.

(We calculated the *reduced* row echelon form of A, but any other row echelon form would also have worked, for the same reasons.)

Example D4.6 Given a list of vectors, how can we calculate a basis for their span? For instance, take

$$\mathbf{v}_1 = \begin{pmatrix} 1 \\ 1 \\ 3 \\ 1 \\ 6 \end{pmatrix}, \quad \mathbf{v}_2 = \begin{pmatrix} 2 \\ -1 \\ 0 \\ 1 \\ -1 \end{pmatrix}, \quad \mathbf{v}_3 = \begin{pmatrix} -3 \\ 2 \\ 1 \\ -2 \\ 1 \end{pmatrix}, \quad \mathbf{v}_4 = \begin{pmatrix} 4 \\ 1 \\ 6 \\ 1 \\ 3 \end{pmatrix}.$$

Turn these into row vectors (i.e. take transposes) and put them together as the rows of a matrix. In this example, this gives the matrix A of Example D4.5. Then $\operatorname{span}\{\mathbf{v}_1^T, \mathbf{v}_2^T, \mathbf{v}_3^T, \mathbf{v}_4^T\} = \operatorname{row}(A)$, and we have already found a basis for $\operatorname{row}(A)$. Taking transposes again, we conclude that

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

is a basis for $\operatorname{span}\{\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3, \mathbf{v}_4\}$.

Example D4.7 By Proposition D4.3(ii), we can calculate the rank of a matrix by computing a row echelon form and then counting its nonzero rows. So for the matrix A of Example D4.5, we have $\operatorname{rank}(A) = 3$. And by the rank theorem,

$$\operatorname{nullity}(A) = (\text{number of columns of } A) - \operatorname{rank}(A) = 5 - 3 = 2.$$

Example D4.8 Given a list of vectors, how do we determine whether they are linearly independent?

Vectors $\mathbf{v}_1, \ldots, \mathbf{v}_m \in \mathbb{R}^n$ are linearly independent if and only if the subspace $\operatorname{span}\{\mathbf{v}_1, \ldots, \mathbf{v}_m\}$ has dimension m. (For if they are linearly independent then they form an m-element basis for their span. Conversely, if their span has dimension m then they are linearly independent by the ever-useful Lemma C2.17.)

The dimension of $\operatorname{span}\{\mathbf{v}_1, \ldots, \mathbf{v}_m\}$ is the (row) rank of the matrix A with rows $\mathbf{v}_1, \ldots, \mathbf{v}_m$; and we already know how to calculate the rank of a matrix. Since A is an $m \times n$ matrix, it has rank m if and only if a row echelon form of A has no zero rows.

In summary: to decide whether $\mathbf{v}_1, \ldots, \mathbf{v}_m$ are linearly independent, we form the matrix A with $\mathbf{v}_1, \ldots, \mathbf{v}_m$ as rows and compute a row echelon form R of A. If R has a zero row then $\mathbf{v}_1, \ldots, \mathbf{v}_m$ are linearly dependent; otherwise, they are independent. In the example above of $\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3, \mathbf{v}_4 \in \mathbb{R}^5$, the last row of the reduced row echelon form is zero, so they are linearly dependent.

Example D4.9 To calculate a basis for the column space of a matrix, we do just the same as for the row space in Example D4.5, but calculating a column echelon form instead.

Example D4.10 Given a matrix A, how do we calculate a basis for $\ker(A)$?

By definition, $\ker(A)$ is the set of solutions $\mathbf{x}$ of the homogeneous linear system $A\mathbf{x} = \mathbf{0}$. We already saw how to solve linear systems in Chapter B:

put A into reduced row echelon form, then simply read off the solutions. For instance, take the matrix A of Example D4.5, whose RREF is

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

By Proposition D4.3(i), $\ker(A) = \ker(R)$. Now $\ker(R)$ consists of all vectors $\mathbf{x} \in \mathbb{R}^n$ such that $R\mathbf{x} = \mathbf{0}$, or equivalently

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

The leading entries of R are in columns 1, 2 and 4. Each of the equations above contains exactly one of x_1, x_2 and x_4 (with a coefficient of 1) together with some of the remaining variables, x_3 and x_5. Moving the remaining variables to the right-hand sides, we find that $\mathbf{x} \in \ker(R) = \ker(A)$ if and only if

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

So, writing $s = x_3$ and $t = x_5$ for the free variables,

$$\ker(A) = \left\{ \begin{pmatrix} -s+t \\ -2s-3t \\ s \\ -4t \\ t \end{pmatrix} : s, t \in \mathbb{R} \right\}.$$

So $\ker(A)$ has dimension 2 (as we already calculated in Example D4.7). It has a basis given by taking $\left(\begin{smallmatrix} s \\ t \end{smallmatrix}\right)$ to be either $\left(\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right)$ or $\left(\begin{smallmatrix} 0 \\ 1 \end{smallmatrix}\right)$. In other words,

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

is a basis for $\ker(A)$.

Example D4.11 Finally, suppose we have a subspace V of $\mathbb{R}^n$, defined as the span of vectors $\mathbf{v}_1, \ldots, \mathbf{v}_m$. How can we find a basis for its orthogonal complement $V^\perp$?

Once more, let A be the $m \times n$ matrix with rows $\mathbf{v}_1, \ldots, \mathbf{v}_m$. Then $V = \mathrm{row}(A)$. In the proof of Theorem C5.1, we saw that $\mathrm{row}(A)^\perp = \ker(A)$. So, $V^\perp = \ker(A)$. Finding a basis for $V^\perp$ is, therefore, the same as finding a basis for $\ker(A)$, which we just saw how to do in Example D4.10.

D5 Determinants

For the lecture of Monday, 26 October 2015; part five of five

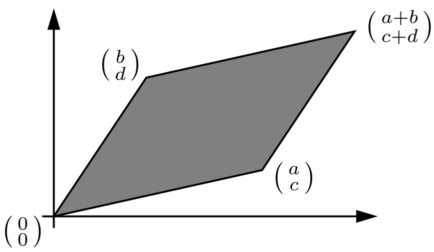
In this section, we meet the concept of the determinant of a square matrix. You've already seen it for 2×2 and maybe 3×3 matrices, but here we'll do it for arbitrary $n \times n$ matrices.

What's the point of determinants? First, they'll give us yet another condition for the invertibility of a matrix, and another method for finding the inverse. Second, they turn out to be essential for changing variables in several-variable integrals. (We won't cover that here, but the word to watch out for in other courses is *Jacobian*.) Third, and related to the first two, the algebraic concept of determinant has a lot to do with the geometric concept of volume, as we're about to see.

Intuitive background

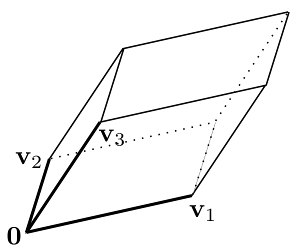
Let us begin with 2×2 matrices $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$. As you know from Example A3.4(ii) or elsewhere, the determinant of A is defined as $\det(A) = ad - bc$. But what does $ad - bc$ *mean*?

Consider the two columns of our matrix, $\left(\begin{smallmatrix} a \\ c \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} b \\ d \end{smallmatrix}\right)$. Draw the parallelogram whose edges are these two vectors:



It's not too hard to see that the area of this parallelogram is $ad - bc$ (exercise!). So, the determinant of A is the area of the parallelogram whose edge-vectors are the columns of A.

We can try something similar in dimension three. Let A be a 3×3 matrix. The three columns $\mathbf{v}_1$, $\mathbf{v}_2$ and $\mathbf{v}_3$ of A are vectors in $\mathbb{R}^3$, and we can think about the volume of the 'squashed cube' whose edges are those three vectors:



A 'squashed cube' is called a **parallelepiped**. So to continue the pattern that we observed in two dimensions, we'd like to define the determinant of a 3×3 matrix A to be the volume of the parallepiped whose edge-vectors are the columns of A.

Below, we give an algebraic definition of the determinant of an $n \times n$ matrix. It can be shown that in the 3×3 case, the determinant really is equal to the volume of our parallelepiped. And once suitable definitions of 'higher-dimensional volume' and 'higher-dimensional parallelepiped' have been made, it can be shown that the same pattern continues in all dimensions.

There is a subtlety concerning signs. Determinants can sometimes be negative, whereas areas and volumes cannot. For example, $\det\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right) = -1$, and yet the parallelogram with edge-vectors $\left(\begin{smallmatrix} 0 \\ 1 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right)$ is the unit square, which has area $+1$. Actually, the area of the parallelogram (in the two-dimensional case) or volume of the parallelepiped (in the three-dimensional case) is *the absolute value of* the determinant of the matrix. Whether the determinant is positive or negative depends on the order in which the edge-vectors are listed.

Definition and examples

We define the determinant $\det(A)$ of an $n \times n$ matrix A by induction on n.

The **determinant** of a 1×1 matrix (a) is a.

Now let $n \geq 2$, and suppose that determinant is defined for $(n-1) \times (n-1)$ matrices. Let $A = (A_{ij})_{1 \leq i \leq n,\, 1 \leq j \leq n}$ be an $n \times n$ matrix. Whenever $i, j \in \{1, \ldots, n\}$, write $A[i, j]$ for the $(n-1) \times (n-1)$ matrix obtained from A by deleting the ith row and jth column. The **determinant** of A is

$$\det(A) = \sum_{j=1}^{n} (-1)^{1+j} A_{1j} \det(A[1, j]).$$

Examples D5.1 i. Let $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$. Then $A[1,1] = (d)$ and $A[1,2] = (c)$, so

$$\det(A) = (-1)^{1+1} a \det((d)) + (-1)^{1+2} b \det((c)) = ad - bc.$$

So, our new definition agrees with the definition in Example A3.4(ii).

ii. Let

$$A = \begin{pmatrix} A_{11} & A_{12} & A_{13} \\ A_{21} & A_{22} & A_{23} \\ A_{31} & A_{32} & A_{33} \end{pmatrix}$$

be a 3×3 matrix. Then

$$\det(A) = A_{11} \det \begin{pmatrix} A_{22} & A_{23} \\ A_{32} & A_{33} \end{pmatrix} - A_{12} \det \begin{pmatrix} A_{21} & A_{23} \\ A_{31} & A_{33} \end{pmatrix} + A_{13} \det \begin{pmatrix} A_{21} & A_{22} \\ A_{31} & A_{32} \end{pmatrix}$$

and each of the individual 2×2 determinants can be worked out using the formula in the previous example.

iii. Similar calculations can be performed for larger matrices. For instance, if A is a 4×4 matrix then

$$\det(A) = A_{11} \det(A[1,1]) - A_{12} \det(A[1,2]) + A_{13} \det(A[1,3]) - A_{14} \det(A[1,4]),$$

and $A[1,1]$, $A[1,2]$, $A[1,3]$ and $A[1,4]$ are 3×3 matrices, so their determinants can be computed as in the previous example.

iv. An easy proof by induction shows that $\det(I_n) = 1$ for all n.

The definition of determinant appears to give a special status to the first row. The next result says that this is an illusion: the same kind of expansion can be done along any row, or even any column.

Proposition D5.2 *Let A be an $n \times n$ matrix. Then for any $i \in \{1, \ldots, n\}$,*

$$\det(A) = \sum_{j=1}^{n} (-1)^{i+j} A_{ij} \det(A[i,j]).$$

Also, for any $j \in \{1, \ldots, n\}$,

$$\det(A) = \sum_{i=1}^{n} (-1)^{i+j} A_{ij} \det(A[i,j]).$$

Proof Omitted. $\square$

We can use this result to speed up calculations of determinants, as in the next example. To handle the signs $(-1)^{i+j}$, it is useful to observe that they form a chess board pattern:

$$\begin{pmatrix} + & - & + & - & \cdots \\ - & + & - & + & \cdots \\ + & - & + & - & \cdots \\ - & + & - & + & \cdots \\ \vdots & \vdots & \vdots & \vdots & \ddots \end{pmatrix}$$

Example D5.3 Suppose we want to compute the determinant of

$$A = \begin{pmatrix} 3 & 1 & 0 & 2 \\ 10 & 4 & 3 & -9 \\ 4 & -1 & 0 & 4 \\ -7 & 2 & 0 & 0 \end{pmatrix}.$$

If we simply use the definition of determinant then we will have three summands to deal with, one for each nonzero entry in the top row. However, Proposition D5.2 allows us to expand along any other row or column. We will make the calculation easier if we expand down the third column, giving:

$$\det(A) = -3 \det \begin{pmatrix} 3 & 1 & 2 \\ 4 & -1 & 4 \\ -7 & 2 & 0 \end{pmatrix}.$$

(The minus sign on the right-hand side is because $(-1)^{2+3} = -1$, as in the chess board pattern.) To compute the determinant of this 3×3 matrix, it will make life easier if we expand along its third row (or column). This gives

$$\begin{aligned} \det(A) &= -3 \left[-7 \det \begin{pmatrix} 1 & 2 \\ -1 & 4 \end{pmatrix} - 2 \det \begin{pmatrix} 3 & 2 \\ 4 & 4 \end{pmatrix} \right] \\ &= -3\big[-7(1 \times 4 + 2 \times 1) - 2(3 \times 4 - 2 \times 4)\big] \\ &= -3[-7 \times 6 - 2 \times 4] = 150. \end{aligned}$$

Properties of determinants

Here are some properties of determinants, stated without proof.

Proposition D5.4 *Let A be an $n \times n$ matrix, with rows $\mathbf{v}_1, \dots, \mathbf{v}_n$.*

i. *Let B be the matrix obtained from A by swapping rows i and j (where $i \neq j$). Then* $\det(B) = -\det(A)$.

ii. *Let B be the matrix obtained from A by multiplying the ith row by a scalar c. Then* $\det(B) = c \det(A)$.

iii. *If some row $\mathbf{v}_i$ is $\mathbf{0}$ then* $\det(A) = 0$.

iv. *Let $\mathbf{v}'_i \in \mathbb{R}^n$ be a row vector, let A' be the matrix with rows*

$$\mathbf{v}_1, \dots, \mathbf{v}_{i-1}, \mathbf{v}'_i, \mathbf{v}_{i+1}, \dots, \mathbf{v}_n,$$

and let B be the matrix with rows

$$\mathbf{v}_1, \dots, \mathbf{v}_{i-1}, \mathbf{v}_i + \mathbf{v}'_i, \mathbf{v}_{i+1}, \dots, \mathbf{v}_n.$$

Then $\det(B) = \det(A) + \det(A')$.

v. $\det(A^T) = \det(A)$.

vi. $\det(AB) = \det(A)\det(B)$ *for any $n \times n$ matrix B.*

Proof Omitted. □

Corollary D5.5 *Let A be an $n \times n$ matrix. If two rows of A are identical, or two columns of A are identical, then* $\det(A) = 0$.

Proof Suppose that rows i and j are identical. Then $\det(A) = -\det(A)$ by Proposition D5.4(i), so $\det(A) = 0$.

If two columns of A are identical then two rows of A^T are identical, so $\det(A^T) = 0$, so $\det(A) = 0$ by Proposition D5.4(v). □

Corollary D5.6 *Any invertible matrix has nonzero determinant.*

Proof Let A be an invertible matrix. Then $AA^{-1} = I$, so $\det(A)\det(A^{-1}) = \det(I) = 1$ by Proposition D5.4(vi) and Example D5.1(iv). Hence $\det(A) \neq 0$. □

We will also prove the converse of this corollary, but first, we need some terminology. The (i, j)-**cofactor** of A is $C_{ij} = (-1)^{i+j} \det(A[i, j])$. So by Proposition D5.2,

$$\det(A) = \sum_{j=1}^{n} A_{ij} C_{ij}$$

for any $i \in \{1, \dots, n\}$.

The **adjugate** of A is the $n \times n$ matrix $\operatorname{adj} A$ whose (i, j)-entry is C_{ji}. Note the reversal of the indices. (The adjugate is sometimes called the **classical adjoint**, or just the **adjoint**, but this terminology is problematic as the word 'adjoint' is also used in linear algebra for something different.)

Example D5.7 The adjugate of a 2×2 matrix $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ is

$$\operatorname{adj}(A) = \begin{pmatrix} C_{11} & C_{21} \\ C_{12} & C_{22} \end{pmatrix} = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}.$$

Notice that $A \operatorname{adj}(A) = (ad - bc)I = \det(A)I$. We will now show that this is actually true for all square matrices, not just 2×2.

Proposition D5.8 *$A(\operatorname{adj} A) = \det(A)I_n$ for all $n \times n$ matrices A.*

Proof Let us use the convention that the (i, j)-entry of a matrix M is written as M_{ij}. Let $i, k \in \{1, \ldots, n\}$. We must show that $(A(\operatorname{adj} A))_{ik}$ is equal to $\det(A)$ if $i = k$, or 0 if $i \neq k$. We have

$$(A(\operatorname{adj} A))_{ik} = \sum_{j=1}^{n} A_{ij} C_{kj} = \sum_{j=1}^{n} (-1)^{k+j} A_{ij} \det(A[k, j]).$$

If $i = k$ then this sum is equal to $\det(A)$, by Proposition D5.2.

Now suppose that $i \neq k$. Let A' be the $n \times n$ matrix obtained from A by replacing the kth row with the ith row (and leaving all the other rows alone, including the ith). The rows of A' and A are the same apart from the kth, so $A'[k, j] = A[k, j]$ for all j. Also, $A'_{kj} = A_{ij}$ for all j. Hence

$$(A(\operatorname{adj} A))_{ik} = \sum_{j=1}^{n} (-1)^{k+j} A'_{kj} \det(A'[k, j]),$$

which is equal to $\det(A')$ by Proposition D5.2. But two rows of A' are equal, so $\det(A') = 0$ by Corollary D5.5. Hence $(A(\operatorname{adj} A))_{ik} = 0$, as required. □

Theorem D5.9 *Let A be an $n \times n$ matrix. Then A is invertible if and only if $\det A \neq 0$. If A is invertible, then $A^{-1} = \frac{1}{\det A} \operatorname{adj} A$.*

Proof 'Only if' is Corollary D5.6, and 'if' follows from Proposition D5.8. □

Examples D5.10

i. A 2×2 matrix $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ is invertible if and only if $ad \neq bc$, and in that case,

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

ii. Theorem D5.9 can be used to test for invertibility of any square matrix, and in the case that it is invertible, to find the inverse. However, it is very labour-intensive. Using the elementary row operation method (as in Example D2.10) is much more efficient, especially for large matrices.

Let us finish by seeing how Theorem D5.9 fits with the volume-based understanding of determinants. We introduced determinants for 3×3 matrices by saying that $\det(A)$ is the volume of the parallelepiped whose edge-vectors are the columns $\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3$ of A. According to the theorem we just proved, A is invertible exactly when that volume is nonzero. Does that make sense?

The volume of the parallelepiped is zero if and only if $\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3$ all lie on some plane. This happens if and only if $\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3$ are linearly dependent. But we know that they are linearly dependent if and only if A is not invertible (by Theorem D1.4. So, the volume of the parallelepiped is *non*zero if and only if A *is* invertible. Since the volume is $\det(A)$, that fits exactly with Theorem D5.9.

Chapter E

Introduction to linear transformations

E1 Definition and examples

For the lecture of Monday, 9 November 2015; part one of six

Often we are interested in ways of transforming vectors in $\mathbb{R}^n$, such as by rotating or reflecting or stretching them. These are all methods for taking one vector in $\mathbb{R}^n$ and producing another. More generally, we will be interested in ways of taking a vector in $\mathbb{R}^n$ and producing a vector in $\mathbb{R}^m$, where perhaps $m \neq n$. (We'll meet some examples soon.) In other words, we are interested in functions from $\mathbb{R}^n$ to $\mathbb{R}^m$.

Since we're doing *linear* algebra, we're primarily interested in those functions that 'respect the linear structure', or 'get along well with addition and scalar multiplication'. What this means, exactly, is the following.

Definition E1.1 Let $n, m \geq 0$. A **linear transformation** (or **linear map**, or **linear mapping**) from $\mathbb{R}^n$ to $\mathbb{R}^m$ is a function $T\colon \mathbb{R}^n \to \mathbb{R}^m$ with the following properties:

i. $T(\mathbf{0}) = \mathbf{0}$;

ii. $T(\mathbf{v} + \mathbf{w}) = T(\mathbf{v}) + T(\mathbf{w})$ for all $\mathbf{v}, \mathbf{w} \in \mathbb{R}^n$;

iii. $T(c\mathbf{v}) = cT(\mathbf{v})$ for all $c \in \mathbb{R}$ and $\mathbf{v} \in \mathbb{R}^n$.

These might remind you of the three conditions in the definition of subspace (Definition C1.1).

In condition (i), the $\mathbf{0}$ on the left-hand side is the zero vector of $\mathbb{R}^n$, whereas the $\mathbf{0}$ on the right-hand side is the zero vector of $\mathbb{R}^m$. (This is the only possible interpretation if the equation is to make sense.)

Examples E1.2 i. There is a linear transformation $T\colon \mathbb{R}^2 \to \mathbb{R}^3$ defined by

$$T\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 3x + 2y \\ y - 4x \\ -y \end{pmatrix}$$

$(x, y \in \mathbb{R})$. (On the left-hand side, we should strictly speaking have written $T\big(\binom{x}{y}\big)$, but we usually drop one set of brackets.) Let's check the three conditions:

- $T(\mathbf{0}) = T\binom{0}{0} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix} = \mathbf{0}$;
- for $\mathbf{v} = \binom{v_1}{v_2}$ and $\mathbf{w} = \binom{w_1}{w_2}$ in $\mathbb{R}^2$, we have

$$\begin{aligned} T(\mathbf{v} + \mathbf{w}) &= T\binom{v_1+w_1}{v_2+w_2} \\ &= \begin{pmatrix} 3(v_1+w_1)+2(v_2+w_2) \\ (v_2+w_2)-4(v_1+w_1) \\ -(v_2+w_2) \end{pmatrix} \\ &= \begin{pmatrix} 3v_1+2v_2 \\ v_2-4v_1 \\ -v_2 \end{pmatrix} + \begin{pmatrix} 3w_1+2w_2 \\ w_2-4w_1 \\ -w_2 \end{pmatrix} \\ &= T(\mathbf{v}) + T(\mathbf{w}); \end{aligned}$$

- for $c \in \mathbb{R}$ and $\mathbf{v} \in \mathbb{R}^2$, we have

$$T(c\mathbf{v}) = T\binom{cv_1}{cv_2} = \begin{pmatrix} 3cv_1+2cv_2 \\ cv_2-4cv_1 \\ -cv_2 \end{pmatrix} = c\begin{pmatrix} 3v_1+2v_2 \\ v_2-4v_1 \\ -v_2 \end{pmatrix} = cT(\mathbf{v}).$$

Later, we'll find a *much* faster way of performing these checks.

ii. Similarly, you can check that the function $T\colon \mathbb{R}^2 \to \mathbb{R}^1 = \mathbb{R}$ defined by

$$T\binom{x}{y} = 3x - 2y$$

$(x, y \in \mathbb{R})$ is a linear transformation.

iii. Neither of the functions $S, T\colon \mathbb{R}^2 \to \mathbb{R}^2$ defined by

$$S\binom{x}{y} = \binom{1}{x}, \qquad T\binom{x}{y} = \binom{x^2}{y}$$

$(x, y \in \mathbb{R})$ is a linear transformation. To see that S is not, note that $S(\mathbf{0}) \neq \mathbf{0}$. To see that T is not, note that

$$T\big(2\tbinom{1}{0}\big) = T\binom{2}{0} = \binom{4}{0}$$

whereas

$$2T\binom{1}{0} = 2\binom{1}{0} = \binom{2}{0}$$

and so $T\big(2\binom{1}{0}\big) \neq 2T\binom{1}{0}$.

iv. There are linear transformations $S, T\colon \mathbb{R}^3 \to \mathbb{R}^2$ defined by

$$S\begin{pmatrix} x \\ y \\ z \end{pmatrix} = \binom{x}{y}, \qquad T\begin{pmatrix} x \\ y \\ z \end{pmatrix} = \binom{x}{z}$$

$(x, y, z \in \mathbb{R})$, and there is a linear transformation $U\colon \mathbb{R}^3 \to \mathbb{R}$ defined by

$$U\begin{pmatrix} x \\ y \\ z \end{pmatrix} = y.$$

Transformations like this are called **projections**. We will return to them later.

v. In the opposite direction, there are linear transformations $S^*, T^* \colon \mathbb{R}^2 \to \mathbb{R}^3$ defined by

$$S^*\left(\begin{smallmatrix} x \\ y \end{smallmatrix}\right) = \left(\begin{smallmatrix} x \\ y \\ 0 \end{smallmatrix}\right), \qquad T^*\left(\begin{smallmatrix} x \\ y \end{smallmatrix}\right) = \left(\begin{smallmatrix} x \\ 0 \\ y \end{smallmatrix}\right)$$

$(x, y \in \mathbb{R})$, and there is a linear transformation $U^* \colon \mathbb{R} \to \mathbb{R}^3$ defined by

$$U^*(y) = \left(\begin{smallmatrix} 0 \\ y \\ 0 \end{smallmatrix}\right).$$

It's often useful to know that the three conditions in Definition E1.1 can, in fact, be reduced to one:

Lemma E1.3 *Let $n, m \geq 0$, and let $T \colon \mathbb{R}^n \to \mathbb{R}^m$ be a function. Then T is a linear transformation if and only if*

$$T(a\mathbf{v} + b\mathbf{w}) = aT(\mathbf{v}) + bT(\mathbf{w})$$

for all $a, b \in \mathbb{R}$ and $\mathbf{v}, \mathbf{w} \in \mathbb{R}^n$.

Proof First suppose that T is a linear transformation. Then for all $a, b \in \mathbb{R}$ and $\mathbf{v}, \mathbf{w} \in \mathbb{R}^n$, we have

$$T(a\mathbf{v} + b\mathbf{w}) = T(a\mathbf{v}) + T(b\mathbf{w}) = aT(\mathbf{v}) + bT(\mathbf{w})$$

where the first equality follows from condition (ii) of Definition E1.1 and the second follows from condition (iii).

Conversely, suppose that $T(a\mathbf{v} + b\mathbf{w}) = aT(\mathbf{v}) + bT(\mathbf{w})$ for all $a, b \in \mathbb{R}$ and $\mathbf{v}, \mathbf{w} \in \mathbb{R}^n$. We show that the three conditions of Definition E1.1 hold.

i. We have $T(1\cdot\mathbf{0} + 1\cdot\mathbf{0}) = 1T(\mathbf{0}) + 1T(\mathbf{0})$, or equivalently $T(\mathbf{0}) = T(\mathbf{0}) + T(\mathbf{0})$. Subtracting $T(\mathbf{0})$ from each side gives $\mathbf{0} = T(\mathbf{0})$.

ii. Let $\mathbf{v}, \mathbf{w} \in \mathbb{R}^n$. Then $T(1\mathbf{v} + 1\mathbf{w}) = 1T(\mathbf{v}) + 1T(\mathbf{w})$, or equivalently $T(\mathbf{v} + \mathbf{w}) = T(\mathbf{v}) + T(\mathbf{w})$, as required.

iii. Let $c \in \mathbb{R}$ and $\mathbf{v} \in \mathbb{R}^n$. Then $T(c\mathbf{v} + 0\mathbf{v}) = cT(\mathbf{v}) + 0T(\mathbf{v})$, or equivalently $T(c\mathbf{v}) = cT(\mathbf{v})$, as required. □

In Examples E1.2, we met various different kinds of linear transformation. Are there lots of linear transformations $\mathbb{R}^n \to \mathbb{R}^m$, or only a few? How much freedom do we have to make up new ones? Is there an easy way to describe them all? In the rest of this section, we'll answer all these questions, constructing even more examples of linear transformations along the way.

First, we prove a result describing how much freedom we have when we try to write down a linear transformation $T \colon \mathbb{R}^n \to \mathbb{R}^m$. Each of the standard basis vectors $\mathbf{e}_1, \ldots, \mathbf{e}_n$ of $\mathbb{R}^n$ (defined in Example C2.4(i)) has to be mapped by T to some point in $\mathbb{R}^m$. It turns out that we can choose freely where in $\mathbb{R}^m$ each $\mathbf{e}_j$ is mapped to, but once we've made those choices, everything else about T is completely determined.

And in fact, the same holds whatever basis of $\mathbb{R}^n$ we work with; it's not only true for the *standard* basis. This is the content of the following result.

Proposition E1.4 *Let $n, m \geq 0$, let $\mathbf{v}_1, \ldots, \mathbf{v}_n$ be a basis for $\mathbb{R}^n$, and let $\mathbf{u}_1, \ldots, \mathbf{u}_n$ be any vectors in $\mathbb{R}^m$. Then there is exactly one linear transformation $T \colon \mathbb{R}^n \to \mathbb{R}^m$ such that*

$$T(\mathbf{v}_1) = \mathbf{u}_1, \ T(\mathbf{v}_2) = \mathbf{u}_2, \ \ldots, \ T(\mathbf{v}_n) = \mathbf{u}_n.$$

Proof We must show that there *exists* a linear transformation T with this property (that is, there is *at least* one), and that it is *unique* with this property (that is, there is *at most* one). We perform these two tasks in the opposite order.

Uniqueness Let $S, T \colon \mathbb{R}^n \to \mathbb{R}^m$ be linear transformations such that $S(\mathbf{v}_j) = \mathbf{u}_j$ and $T(\mathbf{v}_j) = \mathbf{u}_j$ for all $j \in \{1, \ldots, n\}$. We must show that $S = T$.

Since S and T are functions $\mathbb{R}^n \to \mathbb{R}^m$, this means showing that $S(\mathbf{x}) = T(\mathbf{x})$ for all $\mathbf{x} \in \mathbb{R}^n$. Let $\mathbf{x} \in \mathbb{R}^n$. Since $\mathbf{v}_1, \ldots, \mathbf{v}_n$ span $\mathbb{R}^n$, we can write

$$\mathbf{x} = x_1\mathbf{v}_1 + x_2\mathbf{v}_2 + \cdots + x_n\mathbf{v}_n$$

for some $x_1, \ldots, x_n \in \mathbb{R}$. So by Lemma E1.3 and induction,

$$S(\mathbf{x}) = x_1 S(\mathbf{v}_1) + x_2 S(\mathbf{v}_2) + \cdots + x_n S(\mathbf{v}_n).$$

But we assumed that $S(\mathbf{v}_j) = \mathbf{u}_j$ for each j, so

$$S(\mathbf{x}) = x_1\mathbf{u}_1 + x_2\mathbf{u}_2 + \cdots + x_n\mathbf{u}_n.$$

The same argument applied to T gives

$$T(\mathbf{x}) = x_1\mathbf{u}_1 + x_2\mathbf{u}_2 + \cdots + x_n\mathbf{u}_n.$$

Hence $S(\mathbf{x}) = T(\mathbf{x})$, as required.

Existence We must prove that there exists a linear transformation $T \colon \mathbb{R}^n \to \mathbb{R}^m$ such that $T(\mathbf{v}_j) = \mathbf{u}_j$ for all $j \in \{1, \ldots, n\}$. Since $\mathbf{v}_1, \ldots, \mathbf{v}_n$ is a basis of $\mathbb{R}^n$, each $\mathbf{x} \in \mathbb{R}^n$ can be written as

$$\mathbf{x} = x_1\mathbf{v}_1 + x_2\mathbf{v}_2 + \cdots + x_n\mathbf{v}_n$$

for unique $x_1, \ldots, x_n \in \mathbb{R}$. Define

$$T(\mathbf{x}) = x_1\mathbf{u}_1 + x_2\mathbf{u}_2 + \cdots + x_n\mathbf{u}_n \in \mathbb{R}^m.$$

(The inspiration for that step was what we discovered in the uniqueness part.)

This defines a function $T \colon \mathbb{R}^n \to \mathbb{R}^m$. To show that it is linear, we use Lemma E1.3. Let $a, b \in \mathbb{R}$ and $\mathbf{x}, \mathbf{y} \in \mathbb{R}^n$. Write $\mathbf{x} = \sum_{j=1}^n x_j\mathbf{v}_j$ and $\mathbf{y} = \sum y_j\mathbf{v}_j$; then

$$a\mathbf{x} + b\mathbf{y} = \sum_{j=1}^n (ax_j + by_j)\mathbf{v}_j.$$

Now

$$T(\mathbf{x}) = \sum_{j=1}^n x_j\mathbf{u}_j, \qquad T(\mathbf{y}) = \sum_{j=1}^n y_j\mathbf{u}_j,$$

and

$$\begin{aligned}
T(a\mathbf{x}+b\mathbf{y}) &= \sum_{j=1}^{n}(ax_j+by_j)\mathbf{u}_j \\
&= \sum_{j=1}^{n}(ax_j\mathbf{u}_j+by_j\mathbf{u}_j) \\
&= a\sum_{j=1}^{n}x_j\mathbf{u}_j+b\sum_{j=1}^{n}y_j\mathbf{u}_j \\
&= aT(\mathbf{x})+bT(\mathbf{y}),
\end{aligned}$$

as required. □

An informal way of putting Proposition E1.4 is this: if you have a basis of $\mathbb{R}^n$, then knowing what a linear transformation $T\colon \mathbb{R}^n \to \mathbb{R}^m$ does to every basis element tells you what it does to *every* point of $\mathbb{R}^n$. The proof tells you how. Applied to the standard basis $\mathbf{e}_1,\dots,\mathbf{e}_n$ of $\mathbb{R}^n$, it gives the formula

$$T\begin{pmatrix}x_1\\x_2\\\vdots\\x_n\end{pmatrix} = x_1T(\mathbf{e}_1)+x_2T(\mathbf{e}_2)+\cdots+x_nT(\mathbf{e}_n). \qquad \text{(E:1)}$$

This can be very useful when working out specific linear transformations. For instance:

Example E1.5 Suppose you are told that rotation anticlockwise by an angle θ, centred on the origin, defines a linear transformation $R_\theta\colon \mathbb{R}^2 \to \mathbb{R}^2$. How do you find an explicit formula for R_θ?

One strategy is as follows. Rotation anticlockwise by θ sends $\binom{1}{0}$ to $\binom{\cos\theta}{\sin\theta}$ and $\binom{0}{1}$ to $\binom{-\sin\theta}{\cos\theta}$. (Draw a picture!) Since we are told that R_θ is linear, equation (E:1) gives

$$R_\theta\begin{pmatrix}x\\y\end{pmatrix} = x\begin{pmatrix}\cos\theta\\\sin\theta\end{pmatrix}+y\begin{pmatrix}-\sin\theta\\\cos\theta\end{pmatrix} = \begin{pmatrix}x\cos\theta-y\sin\theta\\x\sin\theta+y\cos\theta\end{pmatrix}.$$

You can now check that this really does have the effect of rotating anticlockwise by θ. Indeed, if $\begin{pmatrix}x\\y\end{pmatrix}$ has polar coordinates (r,α) then

$$\begin{pmatrix}x\cos\theta-y\sin\theta\\x\sin\theta+y\cos\theta\end{pmatrix} = \begin{pmatrix}r\cos\alpha\cos\theta-r\sin\alpha\sin\theta\\r\cos\alpha\sin\theta+r\sin\alpha\cos\theta\end{pmatrix} = \begin{pmatrix}r\cos(\alpha+\theta)\\r\sin(\alpha+\theta)\end{pmatrix},$$

which is the point with polar coordinates $(r,\alpha+\theta)$.

Example E1.6 Reflection in any line through the origin also defines a linear transformation $T\colon \mathbb{R}^2 \to \mathbb{R}^2$. For instance, reflection in the line $y=x$ maps $\binom{1}{0}$ to $\binom{0}{1}$ and $\binom{0}{1}$ to $\binom{1}{0}$ (again, draw a picture!), so T is given in general by

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

E2 The standard matrix of a linear transformation

For the lecture of Monday, 9 November 2015; part two of six

Here is a very general way of constructing linear transformations.

Example E2.1 Let A be an $m \times n$ matrix. Then there is a linear transformation $T_A \colon \mathbb{R}^n \to \mathbb{R}^m$ defined by

$$T_A(\mathbf{x}) = A\mathbf{x}$$

($\mathbf{x} \in \mathbb{R}^n$). Let us check that this makes sense: A is an $m \times n$ matrix and $\mathbf{x}$ is an $n \times 1$ matrix, so $A\mathbf{x}$ is an $m \times 1$ matrix, that is, an element of $\mathbb{R}^m$, as required. And let us check that T_A is linear, using Lemma E1.3: for all $a, b \in \mathbb{R}$ and $\mathbf{x}, \mathbf{y} \in \mathbb{R}^n$, we have

$$T_A(a\mathbf{x} + b\mathbf{y}) = A(a\mathbf{x} + b\mathbf{y}) = aA\mathbf{x} + bA\mathbf{y} = aT_A(\mathbf{x}) + bT_A(\mathbf{y}),$$

as required.

In fact, *every* linear transformation $T \colon \mathbb{R}^n \to \mathbb{R}^m$ is equal to T_A for some matrix A. Better still, there is *exactly one* A such that $T = T_A$. We prove this in a moment, after recording two useful lemmas.

Lemma E2.2 *Let A be an $m \times n$ matrix, with columns $\mathbf{v}_1, \ldots, \mathbf{v}_n \in \mathbb{R}^m$. Let $\mathbf{x} \in \mathbb{R}^n$ be a column vector. Then*

$$A\mathbf{x} = x_1\mathbf{v}_1 + \cdots + x_n\mathbf{v}_n.$$

Proof Assignment 4, q.2. $\square$

Lemma E2.3 *Let A be an $m \times n$ matrix and $1 \leq j \leq n$. Write $\mathbf{e}_j$ for the jth standard basis vector of $\mathbb{R}^n$. Then $A\mathbf{e}_j$ is the jth column of A.*

Proof This is the special case $\mathbf{x} = \mathbf{e}_j$ of Lemma E2.2. $\square$

Now we fulfil our earlier promise:

Proposition E2.4 *Let $T \colon \mathbb{R}^n \to \mathbb{R}^m$ be a linear transformation. Then there is exactly one $m \times n$ matrix A such that $T = T_A$.*

Proof Write $\mathbf{e}_1, \ldots, \mathbf{e}_n$ for the standard basis of $\mathbb{R}^n$.

Uniqueness Suppose that A is an $m \times n$ matrix satisfying $T = T_A$. Then $A\mathbf{e}_j = T_A(\mathbf{e}_j) = T(\mathbf{e}_j)$ for each $j \in \{1, \ldots, n\}$, so by Lemma E2.3, A is the matrix with columns $T(\mathbf{e}_1), T(\mathbf{e}_2), \ldots, T(\mathbf{e}_n)$. This determines A uniquely.

Existence Let A be the $m \times n$ matrix with columns $T(\mathbf{e}_1), T(\mathbf{e}_2), \ldots, T(\mathbf{e}_n)$. We will show that $T = T_A$. Since both T and T_A are functions $\mathbb{R}^n \to \mathbb{R}^m$, this means showing that $T(\mathbf{x}) = T_A(\mathbf{x})$ for all $\mathbf{x} \in \mathbb{R}^n$.

Let $\mathbf{x} \in \mathbb{R}^n$. By Lemma E2.2,

$$A\mathbf{x} = x_1T(\mathbf{e}_1) + x_2T(\mathbf{e}_2) + \cdots + x_nT(\mathbf{e}_n)$$

But the left-hand side is $T_A(\mathbf{x})$ by definition of T_A, and the right-hand side is $T(\mathbf{x})$ by equation (E:1) (page 67), so $T_A(\mathbf{x}) = T(\mathbf{x})$, as required. $\square$

Remark E2.5 The moral of this proposition is that linear transformations $\mathbb{R}^n \to \mathbb{R}^m$ are essentially the same thing as $m \times n$ matrices, at least once we have chosen bases for $\mathbb{R}^m$ and $\mathbb{R}^n$. (We will see the significance of the choice of bases in Section E4.)

As the proof shows, if you are given a linear transformation T and want to find the unique matrix A such that $T_A = T$, you take A to be the matrix whose 1st column is $T(\mathbf{e}_1)$, whose 2nd column is $T(\mathbf{e}_2)$, and so on. We call A the **standard matrix** of T, and write it as $[T]$. So for a given linear transformation $T\colon \mathbb{R}^n \to \mathbb{R}^m$, the standard matrix of T is the unique $m \times n$ matrix $[T]$ such that

$$T(\mathbf{x}) = [T]\mathbf{x}$$

for all $\mathbf{x} \in \mathbb{R}^n$.

We now know how to go back and forth between matrices and linear transformations. An $m \times n$ matrix A gives rise to the linear transformation $T_A\colon \mathbb{R}^n \to \mathbb{R}^m$, defined by

$$T_A(\mathbf{x}) = A\mathbf{x}$$

for all $\mathbf{x} \in \mathbb{R}^n$. In the other direction, we have just seen that a linear transformation $T\colon \mathbb{R}^n \to \mathbb{R}^m$ gives rise to the $m \times n$ matrix $[T]$. These two back-and-forth processes are inverse to one another: for instance, if we start with a matrix A, take the linear transformation T_A, and then take its standard matrix $[T_A]$, then we get back to where we started ($[T_A] = A$).

Example E2.6 Proposition E2.4 implies that all the examples of linear transformations mentioned so far can be expressed as multiplication by a matrix. For instance, the transformation $T\colon \mathbb{R}^2 \to \mathbb{R}^3$ of Example E1.2(i) is equal to T_A where

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

(In other words, $T(\mathbf{x}) = A\mathbf{x}$ for all $\mathbf{x} \in \mathbb{R}^2$.) We know that T_A is always a linear transformation for any matrix A, so it follows immediately that the T of Example E1.2(i) is linear. So, there is no need to do any of the checks we did in that example.

Similarly, the rotation map R_θ defined in Example E1.5 has standard matrix

$$[R_\theta] = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}.$$

This is the matrix whose two columns are $T(\mathbf{e}_1) = T\left(\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right)$ and is $T(\mathbf{e}_2) = T\left(\begin{smallmatrix} 0 \\ 1 \end{smallmatrix}\right)$.

Examples E2.7 We now consider scalings of various kinds.

i. For any $c \in \mathbb{R}$, there is a linear transformation $\mathbb{R}^n \to \mathbb{R}^n$ defined by $\mathbf{x} \mapsto c\mathbf{x}$. This scales by a factor of c in all directions. Its standard matrix is

$$\begin{pmatrix} c & 0 & \cdots & 0 \\ 0 & c & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & c \end{pmatrix}.$$

ii. More generally, we can scale by different factors in the directions of the different coordinate axes. Scaling by a factor of c_1 in the $\mathbf{e}_1$ direction, c_2 in the $\mathbf{e}_2$ direction, and so on, gives a linear transformation $\mathbb{R}^n \to \mathbb{R}^n$ with standard matrix

$$\begin{pmatrix} c_1 & 0 & \cdots & 0 \\ 0 & c_2 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & c_n \end{pmatrix}.$$

iii. More generally still, we can do the same thing with respect to any orthogonal basis $\mathbf{v}_1, \ldots, \mathbf{v}_n$ of $\mathbb{R}^n$, scaling by a factor of c_j in the $\mathbf{v}_j$ direction. (Suggestion: draw a picture in $\mathbb{R}^2$.) This does define a linear transformation, but it is not so simple to write down its standard matrix (a point to which we return in Section E4). However, Proposition E1.4 guarantees that there is one and only one linear transformation $T \colon \mathbb{R}^n \to \mathbb{R}^n$ with the desired property that $T(\mathbf{v}_j) = c_j \mathbf{v}_j$ for each $j \in \{1, \ldots, n\}$.

iv. *Even* more generally still, we can do the same thing with respect to *any* basis of $\mathbb{R}^n$, not necessarily orthogonal. The effect is harder to visualize, but can still be thought of as scaling in different (non-orthogonal) directions.

E3 Composing and inverting linear transformations

For the lecture of Monday, 9 November 2015; part three of six

If doing a linear transformation is in any way interesting or useful, then doing two in a row is also likely to be interesting or useful. For instance, reflecting in any line through the origin defines a linear transformation $\mathbb{R}^2 \to \mathbb{R}^2$, so we might ask: what is the combined effect of reflecting in one line and then another? (I'll leave this particular question for you to think about.)

In this section, we answer the general questions about composing linear transformations. Then we look at similar questions involving the inverses of linear transformations: when they exist, and what they are.

First we need to recall some set theory. Let X, Y and Z be sets. Any pair of functions $f\colon X \to Y$ and $g\colon Y \to Z$ give rise to a new function $g \circ f\colon X \to Z$, defined by

$$(g \circ f)(x) = g(f(x))$$

($x \in X$). This function $g \circ f$ is called the **composite** of f and g, and is sometimes written as just gf. Also, for every set Y, there is an **identity** function $1_Y : Y \to Y$ (sometimes written as id_Y), defined by

$$1_Y(y) = y$$

($y \in Y$). It has the properties that $1_Y \circ f = f$ for any function $f\colon X \to Y$, and similarly $g \circ 1_Y = g$ for any $g\colon Y \to Z$.

Lemma E3.1 i. *Let $p, n, m \geq 0$, and let $U\colon \mathbb{R}^p \to \mathbb{R}^n$ and $T\colon \mathbb{R}^n \to \mathbb{R}^m$ be linear transformations. Then the composite $T \circ U\colon \mathbb{R}^p \to \mathbb{R}^m$ is also a linear transformation.*

ii. *Let $n \geq 0$. Then the identity function $1_{\mathbb{R}^n} : \mathbb{R}^n \to \mathbb{R}^n$ is a linear transformation.*

Proof We use Lemma E1.3. For (i), let $a, b \in \mathbb{R}$ and $\mathbf{x}, \mathbf{y} \in \mathbb{R}^p$. Then

$$\begin{aligned}
(T \circ U)(a\mathbf{x} + b\mathbf{y}) &= T(U(a\mathbf{x} + b\mathbf{y})) && \text{(by definition of } T \circ U\text{)}\\
&= T(aU(\mathbf{x}) + bU(\mathbf{y})) && \text{(by linearity of } U\text{)}\\
&= aT(U(\mathbf{x})) + bT(U(\mathbf{y})) && \text{(by linearity of } T\text{)}\\
&= a(T \circ U)(\mathbf{x}) + b(T \circ U)(\mathbf{y}) && \text{(by definition of } T \circ U\text{),}
\end{aligned}$$

as required. For (ii), let $a, b \in \mathbb{R}$ and $\mathbf{x}, \mathbf{y} \in \mathbb{R}^n$. Then

$$1_{\mathbb{R}^n}(a\mathbf{x} + b\mathbf{y}) = a\mathbf{x} + b\mathbf{y} = a1_{\mathbb{R}^n}(\mathbf{x}) + b1_{\mathbb{R}^n}(\mathbf{y}). \qquad \square$$

What is the standard matrix of the composite of two linear transformations? It is the product of their standard matrices. What is the standard matrix of the identity transformation? It is the identity matrix:

Lemma E3.2 i. *Let $n, m, p \geq 0$, and let $U\colon \mathbb{R}^p \to \mathbb{R}^n$ and $T\colon \mathbb{R}^n \to \mathbb{R}^m$ be linear transformations. Then $[T \circ U] = [T][U]$.*

ii. Let $n \geq 0$. Then $[1_{\mathbb{R}^n}] = I_n$.

Proof For (i), first note that the matrix product $[T][U]$ does make sense, since $[T]$ is an $m \times n$ matrix and $[U]$ is an $n \times p$ matrix. Both $[T \circ U]$ and $[T][U]$ are $m \times p$ matrices. We could show that they are equal by calculating their entries, but we can do it more efficiently using Proposition E2.4, as follows.

The proposition implies that $[T \circ U]$ is the *unique* matrix A such that $A\mathbf{x} = (T \circ U)(\mathbf{x})$ for all $\mathbf{x} \in \mathbb{R}^p$. However, for all $\mathbf{x} \in \mathbb{R}^p$ we have

$$[T][U]\mathbf{x} = [T]U(\mathbf{x}) = T(U(\mathbf{x})) = (T \circ U)(\mathbf{x}).$$

Hence $A = [T][U]$ also has the property above. It follows from the statement on uniqueness that $[T \circ U] = [T][U]$.

For (ii), simply note that $1_{\mathbb{R}^n}(\mathbf{x}) = \mathbf{x} = I_n\mathbf{x}$ for all $\mathbf{x} \in \mathbb{R}^n$. □

Example E3.3 Is there a 2×2 matrix A such that $A \neq I$ but $A^{13} = I$? Lemma E3.2 makes this easy to answer. Put $A = [R_{2\pi/13}]$, where the linear transformation $R_{2\pi/13} : \mathbb{R}^2 \to \mathbb{R}^2$ is as defined in Example E1.5. We have $R_{2\pi/13} \neq 1_{\mathbb{R}^2}$, and different linear transformations have different standard matrices, so $A \neq I$. But

$$A^{13} = [R_{2\pi/13}]^{13} = [R^{13}_{2\pi/13}] = [1_{\mathbb{R}^2}] = I$$

(where $R^{13}_{2\pi/13}$ means the 13-fold composite $R_{2\pi/13} \circ R_{2\pi/13} \circ \cdots \circ R_{2\pi/13}$), by Lemma E3.2 and induction. So A has the properties required.

Now we turn to inverses. Again, let us begin by recalling the situation for functions between sets.

Remark E3.4 Let X and Y be sets. A function $f \colon X \to Y$ is:

- **injective** (or **one-to-one**) if for each $y \in Y$, there is *at most one* $x \in X$ such that $f(x) = y$;
- **surjective** (or **onto**) if for each $y \in Y$, there is *at least one* $x \in X$ such that $f(x) = y$;
- **bijective** if for each $y \in Y$, there is *exactly one* $x \in X$ such that $f(x) = y$, or equivalently if f is both injective and surjective.

If f is bijective then there is a unique function $f^{-1} \colon Y \to X$ such that $f^{-1} \circ f = 1_X$ and $f \circ f^{-1} = 1_Y$; this is called the **inverse** of f. Conversely, if f has an inverse then f is bijective.

Lemma E3.5 *Let $n, m \geq 0$. Let $T \colon \mathbb{R}^n \to \mathbb{R}^m$ be a bijective linear transformation. Then the inverse function $T^{-1} \colon \mathbb{R}^m \to \mathbb{R}^n$ is also a linear transformation.*

Proof We use Lemma E1.3. Let $a, b \in \mathbb{R}$ and $\mathbf{v}, \mathbf{w} \in \mathbb{R}^m$. By linearity of T,

$$T\big(aT^{-1}(\mathbf{v}) + bT^{-1}(\mathbf{w})\big) = aT(T^{-1}(\mathbf{v})) + bT(T^{-1}(\mathbf{w})) = a\mathbf{v} + b\mathbf{w}.$$

So $T\big(aT^{-1}(\mathbf{v}) + bT^{-1}(\mathbf{w})\big) = a\mathbf{v} + b\mathbf{w}$. Applying T^{-1} to both sides gives $aT^{-1}(\mathbf{v}) + bT^{-1}(\mathbf{w}) = T^{-1}(a\mathbf{v} + b\mathbf{w})$, as required. □

A linear transformation is said to be **invertible** if it is bijective, or equivalently (by Lemma E3.5) if it has an inverse linear transformation. For an invertible linear transformation T, we can ask: what is the standard matrix of T^{-1} in terms of that of T?

Lemma E3.6 *A linear transformation T is invertible if and only if its standard matrix is invertible. In that case, $[T^{-1}] = [T]^{-1}$.*

Proof Let $T\colon \mathbb{R}^n \to \mathbb{R}^m$ be a linear transformation.

First suppose that T is invertible. We have $T^{-1} \circ T = 1_{\mathbb{R}^n}$, so by Lemma E3.2, taking the standard matrix of each side gives $[T^{-1}][T] = I_n$. Similarly, $[T][T^{-1}] = I_m$. It follows that $[T]$ is invertible with inverse $[T^{-1}]$.

Conversely, suppose that the matrix $[T]$ is invertible. Write $A = [T]$. Then A is an $m \times n$ matrix, so A^{-1} is an $n \times m$ matrix. (We know that invertible matrices are square, so in fact $m = n$, but that observation isn't actually needed here.) Hence we have the linear transformation $T_{A^{-1}}\colon \mathbb{R}^m \to \mathbb{R}^n$. Claim: this is inverse to T. Proof: for all $x \in \mathbb{R}^n$,

$$(T_{A^{-1}} \circ T)(\mathbf{x}) = T_{A^{-1}}(T(\mathbf{x})) = A^{-1}A\mathbf{x} = \mathbf{x},$$

so $T_{A^{-1}} \circ T = 1_{\mathbb{R}^n}$. By a similar argument, $T \circ T_{A^{-1}} = 1_{\mathbb{R}^m}$. This proves the claim. Hence T is invertible. $\square$

We already proved that any invertible matrix has the same number of rows and columns. This implies that the domain and codomain of an invertible linear transformation have the same dimension:

Proposition E3.7 *Let $n, m \geq 0$. If there exists an invertible linear transformation from $\mathbb{R}^n$ to $\mathbb{R}^m$, then $n = m$.*

Proof If such a linear transformation exists then by Lemma E3.6, there is an $m \times n$ invertible matrix, which by Proposition D1.1 implies that $m = n$. $\square$

E4 Change of basis

For the lecture of Monday, 9 November 2015; part four of six

Recall that given any basis $\mathbf{v}_1, \ldots, \mathbf{v}_n$ of $\mathbb{R}^n$, every element $\mathbf{x}$ of $\mathbb{R}^n$ can be expressed as

$$\mathbf{x} = x_1\mathbf{v}_1 + \cdots + x_n\mathbf{v}_n \tag{E:2}$$

for *unique* scalars $x_1, \ldots, x_n$. (This was noted after Definition C2.3.) Most of the time, we use the standard basis $\mathbf{e}_1, \ldots, \mathbf{e}_n$ of $\mathbb{R}^n$. In that case, the scalars $x_1, \ldots, x_n$ in (E:2) are simply the coordinates of $\mathbf{x}$, and (E:2) simply states that

$$\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = x_1\mathbf{e}_1 + \cdots + x_n\mathbf{e}_n.$$

But sometimes, it is useful to use different bases of $\mathbb{R}^n$. This section explains how linear transformations look from the point of view of bases other than the standard one, and how to relate these different viewpoints.

Example E4.1 Take any basis $\mathbf{v}_1, \mathbf{v}_2$ of $\mathbb{R}^2$, and any basis $\mathbf{u}_1, \mathbf{u}_2, \mathbf{u}_3$ of $\mathbb{R}^3$. Then there is a linear transformation $T\colon \mathbb{R}^2 \to \mathbb{R}^3$ defined by

$$T(x_1\mathbf{v}_1 + x_2\mathbf{v}_2) = (3x_1 + 2x_2)\mathbf{u}_1 + (x_2 - 4x_1)\mathbf{u}_2 - x_2\mathbf{u}_3$$

($x_1, x_2 \in \mathbb{R}$). You can check directly that this really is a linear transformation, just as we did in Example E1.2(i).

If $\mathbf{v}_1, \mathbf{v}_2$ is the standard basis of $\mathbb{R}^2$ and $\mathbf{u}_1, \mathbf{u}_2, \mathbf{u}_3$ is the standard basis of $\mathbb{R}^3$ then T is, in fact, equal to the linear transformation of Example E1.2(i). But in general, it is different.

We can encode the coefficients in a matrix. We say that the 'matrix of T with respect to the bases $\mathbf{v}_1, \mathbf{v}_2$ and $\mathbf{u}_1, \mathbf{u}_2, \mathbf{u}_3$' is

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

Here is the general terminology.

Definition E4.2 Let $T\colon \mathbb{R}^n \to \mathbb{R}^m$ be a linear transformation, let $\mathbf{v}_1, \ldots, \mathbf{v}_n$ be a basis of $\mathbb{R}^n$, and let $\mathbf{u}_1, \ldots, \mathbf{u}_m$ be a basis of $\mathbb{R}^m$. Then the **matrix of T with respect to the bases $\mathbf{v}_1, \ldots, \mathbf{v}_n$ and $\mathbf{u}_1, \ldots, \mathbf{u}_m$** is the $m \times n$ matrix $B = (B_{ij})$ defined by

$$T(\mathbf{v}_j) = \sum_{i=1}^{m} B_{ij}\mathbf{u}_i$$

for all $j \in \{1, \ldots, n\}$.

Example E4.3 Suppose that $\mathbf{v}_1, \ldots, \mathbf{v}_n$ is the standard basis $\mathbf{e}_1^n, \ldots, \mathbf{e}_n^n$ of $\mathbb{R}^n$ and that $\mathbf{u}_1, \ldots, \mathbf{u}_m$ is the standard basis $\mathbf{e}_1^m, \ldots, \mathbf{e}_m^m$ of $\mathbb{R}^m$. (The superscripts n and m are to distinguish between the standard basis of $\mathbb{R}^n$ and the standard basis of $\mathbb{R}^m$.) Then the matrix of T with respect to the standard bases is the $m \times n$ matrix B defined by

$$T(\mathbf{e}_j^n) = \sum_{i=1}^{m} B_{ij} \mathbf{e}_i^m$$

$(1 \leq j \leq n)$, or equivalently

$$T(\mathbf{e}_j^n) = \begin{pmatrix} B_{1j} \\ \vdots \\ B_{m_j} \end{pmatrix}$$

for all j. In other words, B is the matrix whose jth column is $T(\mathbf{e}_j^n)$. But as we saw in Section E2, this says precisely that B is the standard matrix of T. So, the matrix of T with respect to the standard bases on $\mathbb{R}^n$ and $\mathbb{R}^m$ is exactly the standard matrix of T—as the terminology might lead us to hope!

Sometimes it is more convenient to use one basis than another. We already saw this in Examples E2.7(iii) and (iv). Here is a specific example.

Example E4.4 The vectors $\binom{2}{1}$ and $\binom{-1}{2}$ form a basis (in fact, an orthogonal basis) for $\mathbb{R}^2$. We can therefore define a linear transformation $T\colon \mathbb{R}^2 \to \mathbb{R}^2$ by

$$x_1 \begin{pmatrix} 2 \\ 1 \end{pmatrix} + x_2 \begin{pmatrix} -1 \\ 2 \end{pmatrix} \;\mapsto\; 2x_1 \begin{pmatrix} 2 \\ 1 \end{pmatrix} + 3x_2 \begin{pmatrix} -1 \\ 2 \end{pmatrix}$$

$(x_1, x_2 \in \mathbb{R})$. This scales by a factor of 2 in the $\binom{2}{1}$ direction and a factor of 3 in the $\binom{-1}{2}$ direction. (Suggestion: draw a picture.)

The matrix of T with respect to the basis $\binom{2}{1}, \binom{-1}{2}$ (as the chosen basis on both the domain *and* the codomain) is $\left(\begin{smallmatrix} 2 & 0 \\ 0 & 3 \end{smallmatrix}\right)$, since

$$T \begin{pmatrix} 2 \\ 1 \end{pmatrix} = 2 \begin{pmatrix} 2 \\ 1 \end{pmatrix}, \qquad T \begin{pmatrix} -1 \\ 2 \end{pmatrix} = 3 \begin{pmatrix} -1 \\ 2 \end{pmatrix}.$$

Suppose we have a linear transformation like the one in this example, where we know its matrix with respect to some chosen bases. How can we find its *standard* matrix? The next result tells us. Notation: given m-dimensional column vectors $\mathbf{w}_1, \ldots, \mathbf{w}_n$, we write $(\mathbf{w}_1|\mathbf{w}_2|\cdots|\mathbf{w}_n)$ for the $m \times n$ matrix with columns $\mathbf{w}_1, \ldots, \mathbf{w}_n$.

Theorem E4.5 *Let $T\colon \mathbb{R}^n \to \mathbb{R}^m$ be a linear transformation, let $\mathbf{v}_1, \ldots, \mathbf{v}_n$ be a basis for $\mathbb{R}^n$, and let $\mathbf{u}_1, \ldots, \mathbf{u}_m$ be a basis for $\mathbb{R}^m$. Write*

$$P = (\mathbf{v}_1|\mathbf{v}_2|\cdots|\mathbf{v}_n), \qquad Q = (\mathbf{u}_1|\mathbf{u}_2|\cdots|\mathbf{u}_m).$$

Write A for the standard matrix of T, and B for the matrix of T with respect to the bases $\mathbf{v}_1, \ldots, \mathbf{v}_n$ and $\mathbf{u}_1, \ldots, \mathbf{u}_m$.

Then P and Q are invertible, and the matrices A and B are related by the equations

$$A = QBP^{-1}, \qquad B = Q^{-1}AP.$$

Proof The columns of the $n \times n$ matrix P form a basis of $\mathbb{R}^n$, so by Theorem D1.4, P is invertible. Similarly, the $m \times m$ matrix Q is invertible.

First, let us write down what we know. Since A is the matrix of T with respect to the standard bases,

$$T(\mathbf{e}_j^n) = \sum_{i=1}^{m} A_{ij}\mathbf{e}_i^m \tag{E:3}$$

for each $j \in \{1, \ldots, n\}$. (Here we are using the convention that the (k, ℓ)-entry of a matrix M is written as $M_{k\ell}$.) Since B is the matrix of T with respect to the bases $\mathbf{v}_1, \ldots, \mathbf{v}_n$ and $\mathbf{u}_1, \ldots, \mathbf{u}_m$,

$$T(\mathbf{v}_j) = \sum_{i=1}^{m} B_{ij}\mathbf{u}_i \tag{E:4}$$

for each $j \in \{1, \ldots, n\}$. By definition of P,

$$\mathbf{v}_j = \sum_{j'=1}^{n} P_{j'j}\mathbf{e}_{j'}^n \tag{E:5}$$

for each $j \in \{1, \ldots, n\}$. And by definition of Q,

$$\mathbf{u}_i = \sum_{i'=1}^{m} Q_{i'i}\mathbf{e}_{i'}^m \tag{E:6}$$

for each $i \in \{1, \ldots, m\}$.

Now substitute (E:6) into (E:4):

$$\begin{aligned} T(\mathbf{v}_j) &= \sum_{i=1}^{m} B_{ij} \sum_{i'=1}^{m} Q_{i'i}\mathbf{e}_{i'}^m = \sum_{i'=1}^{m} \left(\sum_{i=1}^{m} Q_{i'i}B_{ij} \right) \mathbf{e}_{i'}^m \\ &= \sum_{i'=1}^{m} (QB)_{i'j}\mathbf{e}_{i'}^m = \sum_{i=1}^{m} (QB)_{ij}\mathbf{e}_i^m \end{aligned}$$

for each $j \in \{1, \ldots, n\}$. On the other hand, we can apply T to both sides of (E:5), use linearity, and then substitute in (E:3) to get

$$\begin{aligned} T(\mathbf{v}_j) &= \sum_{j'=1}^{n} P_{j'j}T(\mathbf{e}_{j'}^n) = \sum_{j'=1}^{n} P_{j'j} \sum_{i=1}^{m} A_{ij'}\mathbf{e}_i^m \\ &= \sum_{i=1}^{m} \left(\sum_{j'=1}^{n} A_{ij'}P_{j'j} \right) \mathbf{e}_i^m = \sum_{i=1}^{m} (AP)_{ij}\mathbf{e}_i^m \end{aligned}$$

for each $j \in \{1, \ldots, n\}$. Comparing these two expressions for $T(\mathbf{v}_j)$ gives

$$\sum_{i=1}^{m} (QB)_{ij}\mathbf{e}_i^m = \sum_{i=1}^{m} (AP)_{ij}\mathbf{e}_i^m$$

for each j. But $\mathbf{e}_1^m, \ldots, \mathbf{e}_m^m$ is a basis, so this implies that $(QB)_{ij} = (AP)_{ij}$ for each j and i. In other words, $QB = AP$. The result follows. $\square$

This result covers the general case of a linear transformation $T\colon \mathbb{R}^n \to \mathbb{R}^m$, where m need not be equal to n. But often, we are most interested in the case where $m = n$: thus, T is a linear transformation $\mathbb{R}^n \to \mathbb{R}^n$. In principle, we could use one basis $\mathbf{v}_1, \ldots, \mathbf{v}_n$ for the domain and another basis $\mathbf{u}_1, \ldots, \mathbf{u}_n$ for the codomain, and ask for the matrix of T with respect to those two bases. But in practice, when $m = n$, we typically use the same basis on both domain and codomain.

For the rest of this section, we will consider only this situation. Thus, we have a linear transformation $T\colon \mathbb{R}^n \to \mathbb{R}^n$ and a basis $\mathbf{v}_1, \ldots, \mathbf{v}_n$ of $\mathbb{R}^n$. By the **matrix of T with respect to the basis** $\mathbf{v}_1, \ldots, \mathbf{v}_n$, we mean the matrix of T with respect to that basis on both domain and codomain. So, as in Definition E4.2, this is the $n \times n$ matrix B defined by

$$T(\mathbf{v}_j) = \sum_{i=1}^{n} B_{ij} \mathbf{v}_i$$

for each $j \in \{1, \ldots, n\}$.

In this case, Theorem E4.5 says the following:

Corollary E4.6 *Let $T\colon \mathbb{R}^n \to \mathbb{R}^n$ be a linear transformation and let $\mathbf{v}_1, \ldots, \mathbf{v}_n$ be a basis for $\mathbb{R}^n$. Write*

$$P = (\mathbf{v}_1 | \mathbf{v}_2 | \cdots | \mathbf{v}_n).$$

Write A for the standard matrix of T, and B for the matrix of T with respect to the basis $\mathbf{v}_1, \ldots, \mathbf{v}_n$. Then P is invertible, and the matrices A and B are related by the equations

$$A = PBP^{-1}, \qquad B = P^{-1}AP.$$

Proof This is just the special case of Theorem E4.5 in which $m = n$ and $\mathbf{u}_1 = \mathbf{v}_1, \ldots, \mathbf{u}_n = \mathbf{v}_n$. □

For example, we can use Corollary E4.6 to answer a question posed earlier:

Example E4.7 What is the standard matrix of the linear transformation defined in Example E4.4?

There, we had the basis $\left(\begin{smallmatrix} 2 \\ 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} -1 \\ 2 \end{smallmatrix}\right)$ and the linear transformation $T : \mathbb{R}^2 \to \mathbb{R}^2$ whose matrix with respect to that basis is $\left(\begin{smallmatrix} 2 & 0 \\ 0 & 3 \end{smallmatrix}\right)$. In the notation of Corollary E4.6, $P = \left(\begin{smallmatrix} 2 & -1 \\ 1 & 2 \end{smallmatrix}\right)$, so the standard matrix A of T is given by

$$A = \begin{pmatrix} 2 & -1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} 2 & 0 \\ 0 & 3 \end{pmatrix} \begin{pmatrix} 2 & -1 \\ 1 & 2 \end{pmatrix}^{-1} = \frac{1}{5} \begin{pmatrix} 11 & -2 \\ -2 & 14 \end{pmatrix}.$$

You can check that this is correct: we have

$$\frac{1}{5} \begin{pmatrix} 11 & -2 \\ -2 & 14 \end{pmatrix} \begin{pmatrix} 2 \\ 1 \end{pmatrix} = 2 \begin{pmatrix} 2 \\ 1 \end{pmatrix}, \qquad \frac{1}{5} \begin{pmatrix} 11 & -2 \\ -2 & 14 \end{pmatrix} \begin{pmatrix} -1 \\ 2 \end{pmatrix} = 3 \begin{pmatrix} -1 \\ 2 \end{pmatrix},$$

which agrees with the fact that $T\left(\begin{smallmatrix} 2 \\ 1 \end{smallmatrix}\right) = 2\left(\begin{smallmatrix} 2 \\ 1 \end{smallmatrix}\right)$ and $T\left(\begin{smallmatrix} -1 \\ 2 \end{smallmatrix}\right) = 3\left(\begin{smallmatrix} -1 \\ 2 \end{smallmatrix}\right)$.

Corollary E4.6 tells us that matrices of the same linear transformation $\mathbb{R}^n \to \mathbb{R}^n$ with respect to different bases are related in a certain way. It is useful to have some terminology for this.

Definition E4.8 Let A and B be $n \times n$ matrices. We say that A is **similar** to B (or 'A and B are similar'), and write $A \sim B$, if there exists an invertible $n \times n$ matrix P such that $A = PBP^{-1}$.

The next lemma says that the word 'similar' behaves in a sensible way: if A is similar to B then B is similar to A, and so on.

Lemma E4.9 *i. Let A be an $n \times n$ matrix. Then $A \sim A$.*

ii. Let A and B be $n \times n$ matrices. If $A \sim B$ then $B \sim A$.

iii. Let A, B and C be $n \times n$ matrices. If $A \sim B$ and $B \sim C$, then $A \sim C$.

(In the jargon that you probably either met recently or will meet soon in PPS, these three conditions say that similarity is an **equivalence relation** on the set of all $n \times n$ matrices.)

Proof For (i), we have $A = I_n A I_n^{-1}$, so $A \sim A$.

For (ii), suppose that $A \sim B$; then we can choose an invertible matrix P such that $A = PBP^{-1}$. Put $Q = P^{-1}$. Then Q is invertible and $B = P^{-1}AP = QAQ^{-1}$, so $B \sim A$.

For (iii), suppose that $A \sim B$ and $B \sim C$. Then we can choose invertible matrices P and Q such that $A = PBP^{-1}$ and $B = QCQ^{-1}$. By Lemma A3.5, PQ is invertible with inverse $Q^{-1}P^{-1}$, giving

$$A = P(QCQ^{-1})P^{-1} = (PQ)C(PQ)^{-1}.$$

Hence $A \sim C$. □

Proposition E4.10 *Let $T\colon \mathbb{R}^n \to \mathbb{R}^n$ be a linear transformation. Let $\mathbf{v}_1, \ldots, \mathbf{v}_n$ and $\mathbf{v}'_1, \ldots, \mathbf{v}'_n$ be bases of $\mathbb{R}^n$. Then the matrix of T with respect to $\mathbf{v}_1, \ldots, \mathbf{v}_n$ is similar to the matrix of T with respect to $\mathbf{v}'_1, \ldots, \mathbf{v}'_n$.*

Proof Write B for the matrix of T with respect to $\mathbf{v}_1, \ldots, \mathbf{v}_n$, and B' for the matrix of T with respect to $\mathbf{v}'_1, \ldots, \mathbf{v}'_n$. Write A for the standard matrix of T. Corollary E4.6 implies that $A \sim B$, and that $A \sim B'$. Then $B \sim A$ by Lemma E4.9(ii), so $B \sim B'$ by Lemma E4.9(iii). □

Looking at matrices of the same linear transformation with respect to different bases is something like looking at a sculpture from different angles. It's the same sculpture, but you see different aspects of it from different angles, and understanding what you're seeing may be easier from some angles than others. In the same way, the linear transformation T of Examples E4.4 and E4.7 is much easier to understand (and has a much simpler matrix) from the point of view of the non-standard basis $\left(\begin{smallmatrix} 2 \\ 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} -1 \\ 2 \end{smallmatrix}\right)$ than from the point of view of the standard basis.

E5 Determinants, revisited

For the lecture of Monday, 9 November 2015; part five of six

Similar matrices represent different points of view on the same linear transformation, so it's not surprising that they share many properties. For instance:

Lemma E5.1 *Similar matrices have the same determinant.*

Proof Let A and B be similar matrices. Then $A = PBP^{-1}$ for some invertible matrix P. Recall from Proposition D5.4(vi) that $\det(XY) = \det(X)\det(Y)$ for any $n \times n$ matrices X and Y, and from the proof of Corollary D5.6 that if X is an invertible matrix then $\det(X^{-1}) = 1/\det X$. It follows that

$$\det(A) = \det(P)\det(B)\det(P^{-1}) = \det(P)\det(B)/\det(P) = \det(B). \qquad \square$$

By this lemma and Proposition E4.10, given a linear transformation $T: \mathbb{R}^n \to \mathbb{R}^n$, the matrix of T with respect to *any* basis always has the same determinant, no matter which basis is chosen. We can therefore define the **determinant** $\det(T)$ to be the determinant of any of these matrices.

Example E5.2 Consider again the linear transformation $T: \mathbb{R}^2 \to \mathbb{R}^2$ of Examples E4.4 and E4.7. The matrix of T with respect to one basis is $\left(\begin{smallmatrix} 2 & 0 \\ 0 & 3 \end{smallmatrix}\right)$, and with respect to another is $\frac{1}{5}\left(\begin{smallmatrix} 11 & -2 \\ -2 & 14 \end{smallmatrix}\right)$. Our general results guarantee (and you can check directly) that these two matrices have the same determinant, namely, 6. So by definition, $\det(T) = 6$.

We can use the concept of linear transformation to get some more intuition about determinants. Determinants were introduced in terms of area and volume (Section D5). There, we said that for a matrix $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$, the determinant is the area of the parallelogram whose edges are the vectors $\left(\begin{smallmatrix} a \\ c \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} b \\ d \end{smallmatrix}\right)$. Now, that parallelogram L is given by

$$L = \left\{ x\left(\begin{smallmatrix} a \\ c \end{smallmatrix}\right) + y\left(\begin{smallmatrix} b \\ d \end{smallmatrix}\right) : 0 \le x \le 1,\ 0 \le y \le 1 \right\}.$$

On the other hand, the unit square K is given by

$$K = \left\{ \left(\begin{smallmatrix} x \\ y \end{smallmatrix}\right) : 0 \le x \le 1,\ 0 \le y \le 1 \right\} = \{x\mathbf{e}_1 + y\mathbf{e}_2 : 0 \le x \le 1,\ 0 \le y \le 1\}.$$

It follows that the linear transformation $T_A: \mathbb{R}^2 \to \mathbb{R}^2$ maps the unit square K onto the parallelogram L: for

$$\begin{aligned} \{T_A(\mathbf{x}) : \mathbf{x} \in K\} &= \{A(x\mathbf{e}_1 + y\mathbf{e}_2) : 0 \le x \le 1,\ 0 \le y \le 1\} \\ &= \{x(A\mathbf{e}_1) + y(A\mathbf{e}_2) : 0 \le x \le 1,\ 0 \le y \le 1\} \\ &= L \end{aligned}$$

where in the last step we used the fact that the columns of A are $A\mathbf{e}_1$ and $A\mathbf{e}_2$.

Now, the unit square K has area 1, and the parallelogram L has area $\det(A)$, which is equal to $\det(T_A)$ (by definition of the latter). So applying T_A to K multiplied its area by a factor of $\det(T_A)$.

In fact, it can be shown that for *any* sensible subset H of $\mathbb{R}^2$, and for any linear transformation $T: \mathbb{R}^2 \to \mathbb{R}^2$, the area of $\{T(\mathbf{x}) : \mathbf{x} \in H\}$ is the area of H

multiplied by $\det(T)$. ('Sensible' just means that it is possible to measure the area of H.) And similar results hold in $\mathbb{R}^3$ for volume instead of area—and even in higher dimensions, once suitable higher-dimensional versions of volume have been defined. This principle is crucial to computing multi-dimensional integrals, as you may already have discovered in SVCDE.

In a slogan:

Determinant is volume scale factor.

In other words, applying a linear transformation T to a shape multiplies its volume by $\det(T)$.

Finally, a linear transformation $\mathbb{R}^n \to \mathbb{R}^n$ is invertible unless its volume scale factor is zero:

Lemma E5.3 *Let $T\colon \mathbb{R}^n \to \mathbb{R}^n$ be a linear transformation. Then T is invertible if and only if $\det(T) \neq 0$.*

Proof T is invertible if and only if its standard matrix $[T]$ is invertible (by Lemma E3.6), if and only if $\det([T]) \neq 0$ (by Theorem D5.9). But $\det(T) = \det([T])$ by definition. $\square$

E6 A fourth look at the rank theorem

For the lecture of Monday, 9 November 2015; part six of six

It is often beneficial to think about linear transformations as objects in their own right, rather than in terms of the matrices that represent them with respect to any particular bases. We have already seen how to define the determinant of a linear transformation $\mathbb{R}^n \to \mathbb{R}^n$. Here, we will see how to define the kernel, rank and nullity of a linear transformation $\mathbb{R}^n \to \mathbb{R}^m$ (where perhaps $m \neq n$), and we will see how these concepts relate to the same concepts for matrices.

Definition E6.1 Let $T\colon \mathbb{R}^n \to \mathbb{R}^m$ be a linear transformation. The **kernel** of T is

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

The **image** (or **range**) of T is

$$\operatorname{im}(T) = \{\mathbf{y} \in \mathbb{R}^m : T(\mathbf{x}) = \mathbf{y} \text{ for at least one } \mathbf{x} \in \mathbb{R}^n\}.$$

(There are also some people who use 'range' to mean codomain rather than image, so it is less ambiguous to avoid the word 'range' entirely.)

You've already met both these concepts, in light disguise. The kernel of T is precisely the kernel of its standard matrix $[T]$. (This is immediate from the definitions.) In other words, it's the set of solutions $\mathbf{x}$ to the homogeneous linear system $[T]\mathbf{x} = \mathbf{0}$.

The image of T can be written as

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

By Lemma C1.9, this is exactly the column-space of $[T]$.

So $\ker(T)$ is a linear subspace of $\mathbb{R}^n$ and $\operatorname{im}(T)$ is a linear subspace of $\mathbb{R}^m$. We define the **nullity** of T to be $\dim(\ker(T))$ and the **rank** of T to be $\dim(\operatorname{im}(T))$. These are, therefore, the same as the nullity and (column) rank of $[T]$.

To summarize what we have found so far:

Lemma E6.2 *Let $T\colon \mathbb{R}^n \to \mathbb{R}^m$ be a linear transformation. Then*

$$\ker(T) = \ker([T]), \qquad \operatorname{im}(T) = \operatorname{col}([T]),$$
$$\operatorname{nullity}(T) = \operatorname{nullity}([T]), \qquad \operatorname{rank}(T) = \operatorname{rank}([T]). \qquad \square$$

So you've already seen plenty of examples of the kernel, image, nullity and rank of a linear transformation—they're just the same as the kernel, column space, nullity and rank of its standard matrix.

(In case you're wondering about the *row* space: we showed in the proof of Lemma D4.1 that $\operatorname{row}(M) = \ker(M)^\perp$ for any M, so $\operatorname{row}([T]) = \ker(T)^\perp$.)

Theorem E6.3 (Rank theorem, third version) *Let $T\colon \mathbb{R}^n \to \mathbb{R}^m$ be a linear transformation. Then*

$$\operatorname{rank}(T) + \operatorname{nullity}(T) = n.$$

Proof This follows from the first version of the rank theorem (Theorem C3.2) and Lemma E6.2. $\square$

In Section D1, we found many conditions on a matrix equivalent to it being invertible. Using the version of the rank theorem that we just proved, we can do something similar for linear transformations.

First, we look at some conditions on a linear transformation that are equivalent to it being injective (one-to-one), and some conditions equivalent to it being surjective (onto).

Lemma E6.4 *Let $T\colon \mathbb{R}^n \to \mathbb{R}^m$ be a linear transformation. Then:*

i. T is injective $\iff \ker(T) = \{\mathbf{0}\} \iff \operatorname{nullity}(T) = 0$.

ii. T is surjective $\iff \operatorname{im}(T) = \mathbb{R}^m \iff \operatorname{rank}(T) = m$.

Proof For (i): suppose that T is injective. Certainly $\mathbf{0} \in \ker(T)$. On the other hand, if $\mathbf{x} \in \ker(T)$ then $T(\mathbf{x}) = \mathbf{0} = T(\mathbf{0})$, so by injectivity, $\mathbf{x} = \mathbf{0}$. Hence $\ker(T) = \{\mathbf{0}\}$.

Conversely, suppose that $\ker(T) = \{\mathbf{0}\}$. To prove that T is injective, let $\mathbf{x}, \mathbf{x}' \in \mathbb{R}^n$ with $T(\mathbf{x}) = T(\mathbf{x}')$; we must show that $\mathbf{x} = \mathbf{x}'$. By linearity,

$$T(\mathbf{x} - \mathbf{x}') = T(\mathbf{x}) - T(\mathbf{x}') = \mathbf{0},$$

so $\mathbf{x} - \mathbf{x}' \in \ker(T)$. But $\ker(T) = \{\mathbf{0}\}$, so $\mathbf{x} - \mathbf{x}' = \mathbf{0}$, so $\mathbf{x} = \mathbf{x}'$, as required.

The only 0-dimensional linear subspace of $\mathbb{R}^n$ is $\{\mathbf{0}\}$, so $\ker(T) = \{\mathbf{0}\} \iff \operatorname{nullity}(T) = 0$. This completes the proof of (i).

For (ii), it is immediate from the definitions that T is surjective if and only if $\operatorname{im}(T) = \mathbb{R}^m$. Since $\mathbb{R}^m$ is the only m-dimensional subspace of $\mathbb{R}^m$, this in turn is equivalent to the condition that $\operatorname{rank}(T) = m$. □

In the special case $m = n$, we can deduce an important result about linear transformations from $\mathbb{R}^n$ to itself.

Theorem E6.5 *Let $T\colon \mathbb{R}^n \to \mathbb{R}^n$ be a linear transformation. Then*

$$T \text{ is injective} \iff T \text{ is bijective} \iff T \text{ is surjective.}$$

Proof By Lemma E6.4 and the rank theorem for linear transformations (Theorem E6.3),

$$T \text{ is injective} \iff \operatorname{nullity}(T) = 0 \iff \operatorname{rank}(T) = n \iff T \text{ is surjective.}$$

So if T is either injective or surjective then it is both, that is, bijective. Conversely, if it is bijective then by definition it is both injective and surjective. □

Warning E6.6 This is only true for linear transformations whose domain and codomain have the same dimension! For transformations $\mathbb{R}^n \to \mathbb{R}^m$ with $m \neq n$, it is certainly possible to be surjective but not injective (as in Example E1.2(iv)) or surjective but not injective (as in Example E1.2(v)).

It is enlightening to compare Theorem E6.5 to the following fact: for any finite set X and function $f\colon X \to X$,

$$f \text{ is injective} \iff f \text{ is bijective} \iff f \text{ is surjective.}$$

I'll leave the proof to you; it's closely related to the so-called 'pigeonhole principle'.

Chapter F

Linear operators on $\mathbb{R}^n$

The previous chapter was about linear transformations $T\colon \mathbb{R}^n \to \mathbb{R}^m$, where the domain $\mathbb{R}^n$ and codomain $\mathbb{R}^m$ may have different dimensions. But it turns out that there are especially interesting things to say about the case where the domain and codomain are the same: $T\colon \mathbb{R}^n \to \mathbb{R}^n$.

A linear transformation $\mathbb{R}^n \to \mathbb{R}^n$ is called a **linear operator** on $\mathbb{R}^n$. Here are some of the things you can do with a linear operator that you can't do with a linear transformation in general:

- Iterate it; that is, do it repeatedly. If T is a linear operator on $\mathbb{R}^n$ then the composites $T^2 = T \circ T$ ('do T twice'), $T^3 = T \circ T \circ T$, etc., all make sense, and they too are linear operators on $\mathbb{R}^n$ (by Lemma E3.1). These composites only exist because T has the same domain and codomain.
- Look for an inverse. (When $n \neq m$, we *can* ask whether a linear transformation $\mathbb{R}^n \to \mathbb{R}^m$ has an inverse, but Proposition E3.7 says that the answer is always 'no'.)
- Take its determinant (as defined in Section E5).
- Ask which points $\mathbf{x}$ of $\mathbb{R}^n$ are 'fixed' by T, in the sense that $T(\mathbf{x}) = \mathbf{x}$.
- Look for eigenvalues and eigenvectors (defined below).
- Ask whether it is 'diagonalizable'—that is, whether its matrix with respect to some basis of $\mathbb{R}^n$ is diagonal. We investigate this in Sections F3 and F6.

F1 Eigenvalues and eigenvectors

For the lecture of Monday, 23 November 2015; part one of six

Consider reflection of the plane in the x-axis, which is a linear operator T on $\mathbb{R}^2$. Of course, the x-axis plays a special role for T: it is the axis of reflection! But we can say this a bit more precisely by observing that the x-axis is exactly the set of vectors $\mathbf{x}$ such that $T(\mathbf{x}) = \mathbf{x}$ (or '$\mathbf{x}$ is fixed by T').

The y-axis also plays a special role for T, since it has the special property that when it is reflected in the x-axis, it is mapped onto itself—but flipped around. We can make this precise by observing that the y-axis is exactly the set of vectors $\mathbf{y}$ such that $T(\mathbf{y}) = -\mathbf{y}$.

Generally, for any linear operator T on $\mathbb{R}^n$, we can look for the points $\mathbf{x}$ such that $T(\mathbf{x}) = \mathbf{x}$. (For instance, if T is a rotation of $\mathbb{R}^2$ then there are no such fixed points apart from $\mathbf{0}$, unless the rotation is by an angle of 0 or π.) And we have repeatedly seen the importance of the *kernel* of T, which is the set of vectors $\mathbf{x}$ satisfying $T(\mathbf{x}) = \mathbf{0}$.

All of these are examples of 'eigenvectors', defined as follows.

Definition F1.1 Let T be a linear operator on $\mathbb{R}^n$. An **eigenvalue** of T is a real number λ such that $T(\mathbf{x}) = \lambda\mathbf{x}$ for some vector $\mathbf{x} \neq \mathbf{0}$ in $\mathbb{R}^n$. We then say that $\mathbf{x}$ is an **eigenvector** of T with eigenvalue λ.

In other words, an eigenvector of T is a nonzero vector $\mathbf{x}$ such that $T(\mathbf{x})$ is a scalar multiple of $\mathbf{x}$.

Warning F1.2

i. By definition, the eigenvalues of a linear operator on $\mathbb{R}^n$ are *real* numbers, and the eigenvectors are *real* vectors. It makes no sense to say '$1 + 2i$ is an eigenvalue of T' or '$\binom{2i}{7}$ is an eigenvector of T'.

ii. By definition, eigenvectors are nonzero. The zero vector $\mathbf{0}$ is not counted as an eigenvector. Why? Because by definition of linearity, $T(\mathbf{0}) = \lambda\mathbf{0}$ for all real λ. If we allowed $\mathbf{0}$ as an eigenvector, then it would be an eigenvector with all eigenvalues. But as it is, each eigenvector has only one eigenvalue: if $T(\mathbf{x}) = \lambda\mathbf{x}$ and $T(\mathbf{x}) = \mu\mathbf{x}$ with $\mathbf{x} \neq \mathbf{0}$, then $\lambda = \mu$.

Examples F1.3

i. Let $T\colon \mathbb{R}^2 \to \mathbb{R}^2$ be reflection in the x-axis. Then $T\binom{x}{0} = \binom{x}{0}$ for all $x \in \mathbb{R}$. Hence 1 is an eigenvalue of T, and $\binom{x}{0}$ is an eigenvector of T with eigenvalue 1 for all real $x \neq 0$.

   Also, $T\binom{0}{y} = -\binom{0}{y}$ for all $x \in \mathbb{R}$. Hence -1 is also an eigenvalue of T, and $\binom{0}{y}$ is an eigenvector of T with eigenvalue -1 for all real $x \neq 0$.

   In fact, ± 1 are the *only* eigenvalues of T. Later, we'll prove a general result that allows us to conclude this immediately. For now, you should be able to see that if $\mathbf{x}$ is a vector such that $T(\mathbf{x})$ is a scalar multiple of $\mathbf{x}$ then $\mathbf{x}$ is on either the x-axis or the y-axis.

ii. Similarly, let Π be any 2-dimensional subspace of $\mathbb{R}^3$ (a plane through $\mathbf{0}$), and let $T\colon \mathbb{R}^3 \to \mathbb{R}^3$ be reflection in Π. Then every nonzero point on the plane is an eigenvector with eigenvalue 1, and every nonzero point on the line through the origin perpendicular to Π is an eigenvector with eigenvalue -1. These are the only two eigenvalues of T.

iii. Consider the linear operator $R_{\pi/3}$ on $\mathbb{R}^2$ (rotation by $\pi/3$ around $\mathbf{0}$). There are *no* vectors $\mathbf{x} \in \mathbb{R}^2$ such that $T(\mathbf{x})$ is a scalar multiple of $\mathbf{x}$, apart from $\mathbf{0}$. Hence $R_{\pi/3}$ has no eigenvalues or eigenvectors at all.

   The same is true of R_θ for any other value of θ, apart from integer multiples of π. (Exercise: why do we have to exclude these?)

iv. Define a linear operator T on $\mathbb{R}^n$ by $T(\mathbf{x}) = -7\mathbf{x}$ for all $\mathbf{x} \in \mathbb{R}^n$. Then every nonzero vector is an eigenvector with eigenvalue -7.

v. Eigen*vectors* are not allowed to be zero, but eigen*values* can be. In fact, eigenvectors with eigenvalue 0 are very useful: for a linear operator T on $\mathbb{R}^n$, the eigenvectors of T with eigenvalue 0 are exactly the nonzero vectors in the kernel of T. This is because $T(\mathbf{x}) = 0\mathbf{x} \iff T(\mathbf{x}) = \mathbf{0}$.

A major theme of the last chapter was that we can translate back and forth between linear transformations and matrices. For linear operators, this means the following. In one direction, every linear operator T on $\mathbb{R}^n$ has a standard matrix $[T]$ (an $n \times n$ matrix). In the other direction, every $n \times n$ matrix A gives rise to a linear operator T_A on $\mathbb{R}^n$, defined by $T_A(\mathbf{x}) = A\mathbf{x}$.

We can take the definition of eigenvalues/vectors for linear operators and translate it into the language of matrices:

Definition F1.4 Let A be an $n \times n$ real matrix. An **eigenvalue** of A is a real number λ such that $A\mathbf{x} = \lambda\mathbf{x}$ for some vector $\mathbf{x} \neq \mathbf{0}$ in $\mathbb{R}^n$. We then say that $\mathbf{x}$ is an **eigenvector** of A with eigenvalue λ.

Examples F1.5 i. The eigenvalues and eigenvectors of a linear operator are exactly the eigenvalues and eigenvectors of its standard matrix. For instance, reflection of $\mathbb{R}^2$ in the x-axis has standard matrix $\left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$, so by Example F1.3(i), its eigenvalues are 1 and -1.

ii. Let A be a **diagonal** matrix, that is, one of the form

$$A = \begin{pmatrix} c_1 & 0 & \cdots & 0 \\ 0 & c_2 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & c_n \end{pmatrix}$$

where $c_1, \ldots, c_n \in \mathbb{R}$. Then $A\mathbf{e}_j = c_j\mathbf{e}_j$ for each $j \in \{1, \ldots, n\}$ (since $A\mathbf{e}_j$ is the jth column of A). Hence $\mathbf{e}_j$ is an eigenvector of A, with eigenvalue c_j, for each j.

If $\mathbf{x}$ is an eigenvector for an operator T, with eigenvalue λ, then so is every nonzero scalar multiple $c\mathbf{x}$ of $\mathbf{x}$: for

$$T(c\mathbf{x}) = cT(\mathbf{x}) = c\lambda\mathbf{x} = \lambda(c\mathbf{x}).$$

So T maps the line $\operatorname{span}\{\mathbf{x}\}$ into itself, scaling it by a factor of λ. Roughly speaking, then, eigenvectors correspond to 'lines that are mapped into themselves'.

These thoughts lead us to consider the set of all eigenvectors having a particular eigenvalue.

Definition F1.6 Let A be an $n \times n$ real matrix, and let $\lambda \in \mathbb{R}$. The **λ-eigenspace** of A is

$$E_\lambda(A) = \{\mathbf{x} \in \mathbb{R}^n : A\mathbf{x} = \lambda\mathbf{x}\}.$$

Similarly, if T is a linear operator on $\mathbb{R}^n$, the **λ-eigenspace** of T is

$$E_\lambda(T) = \{\mathbf{x} \in \mathbb{R}^n : T(\mathbf{x}) = \lambda\mathbf{x}\}.$$

The definitions for matrices and operators are really the same, in the sense that the λ-eigenspace of an operator is equal to the λ-eigenspace of its standard matrix. The next few results could equally well be presented in terms of matrices or linear operators. We will mostly present them in the language of matrices.

First, eigenspaces are closely related to kernels:

Lemma F1.7 *Let A be an $n \times n$ matrix, and let λ be a scalar. Then $E_\lambda(A) = \ker(A - \lambda I)$.*

Proof For $\mathbf{x} \in \mathbf{R}^n$, we have

$$\begin{aligned} \mathbf{x} \in E_\lambda(T) &\iff A\mathbf{x} - \lambda\mathbf{x} = \mathbf{0} \\ &\iff (A - \lambda I)\mathbf{x} = \mathbf{0} \\ &\iff \mathbf{x} \in \ker(A - \lambda I). \end{aligned} \qquad \square$$

We noted above that if $\mathbf{x}$ is an eigenvector with eigenvalue λ then so is every nonzero scalar multiple of $\mathbf{x}$. It follows that every eigenspace is closed under scalar multiplication. (A small thought here: $\mathbf{0}$ belongs to every eigenspace, even though it is not an eigenvector.)

Lemma F1.8 *Every eigenspace of an $n \times n$ square matrix, or of a linear operator on $\mathbb{R}^n$, is a linear subspace of $\mathbb{R}^n$.*

Proof Let A be an $n \times n$ matrix and $\lambda \in \mathbb{R}$. Then $E_\lambda(A) = \ker(A - \lambda I)$, which by Lemma C1.4 is a linear subspace of $\mathbb{R}^n$. This proves the result on matrices.

Now let T be a linear operator on $\mathbb{R}^n$. We have $E_\lambda(T) = E_\lambda([T])$, so this is also a subspace. $\square$

Example F1.9 Let Π be a plane through $\mathbf{0}$ in $\mathbb{R}^3$ and let $T\colon \mathbb{R}^3 \to \mathbb{R}^3$ be reflection in Π, as in Example F1.3(ii). Then the 1-eigenspace of T is Π, and the (-1)-eigenspace of T is the line through the origin perpendicular to Π. For $\lambda \neq \pm 1$, the λ-eigenspace of T is $\{\mathbf{0}\}$.

We defined the λ-eigenspace for *all* scalars λ, even if λ is not an eigenvalue. If λ is not an eigenvalue then $E_\lambda(A)$ is the trivial subspace $\{\mathbf{0}\}$. The eigenvalues of A are exactly those scalars λ such that $E_\lambda(A)$ is nontrivial.

Proposition F1.10 *Let A be an $n \times n$ square matrix and $\lambda \in \mathbb{R}$. The following are equivalent:*

i. *λ is an eigenvalue of A;*

ii. *the λ-eigenspace $E_\lambda(A)$ is nontrivial (that is, not equal to $\{\mathbf{0}\}$);*

iii. *$A - \lambda I$ is not invertible;*

iv. $\det(A - \lambda I) = 0$.

Proof By definition of eigenvalue, λ is an eigenvalue of A if and only if $E_\lambda(A)$ contains some nonzero vector, or in other words, is nontrivial. But $E_\lambda(A) = \ker(A - \lambda I)$, so this is equivalent to $\ker(A - \lambda I)$ being nontrivial. By the fundamental theorem of invertible matrices (Theorem D1.4), this is equivalent to $A - \lambda I$ not being invertible, which in turn is equivalent to its determinant being zero (Theorem D5.9). $\square$

Example F1.11 Let A be an $n \times n$ matrix. Putting $\lambda = 0$ in Proposition F1.10 tells us that 0 is an eigenvalue of A if and only if A is singular (non-invertible).

F2 The characteristic polynomial

For the lecture of Monday, 23 November 2015; part two of six

Suppose we are handed a square matrix. How can we find its eigenvalues and eigenvectors? If we don't have a convenient geometric description of the linear operator corresponding to the matrix, do we have to just guess?

This section provides a practical method for computing eigenvalues and eigenvectors. In Proposition F1.10, we saw that λ is an eigenvalue for a square matrix A if and only if $\det(A-\lambda I) = 0$. It is not too hard to see that $\det(A-\lambda I)$ is, in fact, a polynomial in λ. It has a name:

Definition F2.1 Let A be a square matrix. The **characteristic polynomial** χ_A of A is defined by $\chi_A(\lambda) = \det(A - \lambda I)$. (Here λ is the variable of the polynomial.)

Proposition F1.10 immediately implies:

Proposition F2.2 *Let A be a square matrix. Then the eigenvalues of A are exactly the roots of its characteristic polynomial χ_A.* $\square$

Examples F2.3 i. Consider reflection in the x-axis, which is a linear operator on $\mathbb{R}^2$. Its standard matrix A is $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$, and

$$\chi_A(\lambda) = \det \begin{pmatrix} 1-\lambda & 0 \\ 0 & -1-\lambda \end{pmatrix} = (1-\lambda)(-1-\lambda) = (\lambda-1)(\lambda+1).$$

So the roots of χ_A are ± 1. By Proposition F2.2, these are exactly the eigenvalues of A. This confirms what we already found in Example F1.3(i).

We can also confirm our previous statements about the eigenspaces of A. The 1-eigenspace is

$$E_1(A) = \ker(A - 1I) = \ker \begin{pmatrix} 0 & 0 \\ 0 & -2 \end{pmatrix} = \left\{ \begin{pmatrix} x \\ 0 \end{pmatrix} : x \in \mathbb{R} \right\}.$$

So as expected, the 1-eigenspace is exactly the x-axis, and the eigenvectors with eigenvalue 1 are all the points $\begin{pmatrix} x \\ 0 \end{pmatrix}$ except $\mathbf{0}$. A similar calculation tells us that $E_{-1}(A)$ is exactly the y-axis.

ii. In (i), it was easy to calculate the λ-eigenspace $E_\lambda(A) = \ker(A - \lambda I)$. In more complicated examples, we would find the eigenspaces $\ker(A - \lambda I)$ by the usual row reduction method for calculating kernels (as in Example D4.10), for each eigenvalue λ in turn.

iii. Let

$$A = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix}.$$

Then

$$\chi_A(\lambda) = \det \begin{pmatrix} 1-\lambda & 2 & 3 \\ 4 & 5-\lambda & 6 \\ 7 & 8 & 9-\lambda \end{pmatrix},$$

which after some calculation gives

$$\chi_A(\lambda) = -\lambda^3 + 15\lambda^2 + 18\lambda.$$

The roots of this polynomial are 0 and $(15 \pm \sqrt{297})/2$, so these are the eigenvalues of A. Since 0 is an eigenvalue, A is not invertible, by Example F1.11.

iv. In Example F1.3(iii), we argued geometrically that the operator $R_{\pi/3}$ on $\mathbb{R}^2$ (rotation by $\pi/3$) has no eigenvalues. Here is algebraic confirmation. The standard matrix of $R_{\pi/3}$ is

$$\begin{pmatrix} \cos\pi/3 & -\sin\pi/3 \\ \sin\pi/3 & \cos\pi/3 \end{pmatrix} = \begin{pmatrix} 1/2 & -\sqrt{3}/2 \\ \sqrt{3}/2 & 1/2 \end{pmatrix}$$

(by Example E2.6). This has characteristic polynomial

$$(1/2 - \lambda)(1/2 - \lambda) + (\sqrt{3}/2)^2 = \lambda^2 - \lambda + 1.$$

This quadratic has discriminant $(-1)^2 - 4 \times 1 \times 1 = -3 < 0$, so it has no real roots. Hence $R_{\pi/3}$ has no eigenvalues.

v. The characteristic polynomial of the diagonal matrix

$$A = \begin{pmatrix} c_1 & 0 & \cdots & 0 \\ 0 & c_2 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & c_n \end{pmatrix}$$

is

$$\chi_A(\lambda) = (c_1 - \lambda)(c_2 - \lambda) \cdots (c_n - \lambda).$$

In Example F1.5(ii), we found that $c_1, c_2, \ldots, c_n$ are eigenvalues of A. We now know that they are the *only* eigenvalues of A, since they are the only roots of χ_A.

As these examples show, the characteristic polynomial of an $n \times n$ matrix is a polynomial of degree n, with leading coefficient $(-1)^n$.

Corollary F2.4 *An $n \times n$ square matrix (or a linear operator on $\mathbb{R}^n$) has at most n eigenvalues. In particular, it has only finitely many eigenvalues.*

Proof Any polynomial of degree n has at most n roots, so this follows from Proposition F2.2. □

The fact that a matrix or operator has only finitely many eigenvalues was not obvious from the definition of eigenvalue!

But perhaps it should not be surprising. Fix a square matrix A. For each scalar λ, we obtain another square matrix $A - \lambda I$. Now, in question 1 of the Workshop 5 activity, you discovered that a matrix 'chosen at random' is 'usually' invertible. So, as λ varies, we would expect most of these matrices $A - \lambda I$ to be invertible, and only exceptionally non-invertible. In other words, we would expect λ to be an eigenvalue for only a special few values of λ. Corollary F2.4 makes this rough statement precise.

In any case, every square matrix or linear operator has attached to it a finite set of scalars: its set of eigenvalues, which is called the **spectrum** of the matrix or operator. This is related to usages of the word *spectrum* in the physical sciences. When you hear people talk about mass spectroscopy or the emission spectrum of hydrogen, there is a connection with eigenvalues.

Remark F2.5 In some contexts, it is useful to consider eigenvalues and eigenvectors for *differential* operators. This course is not the place to give the definitions, but it is easy to see the resemblance between differential equations such as

$$f' = \lambda f$$

and the equation

$$T(\mathbf{x}) = \lambda \mathbf{x}$$

in the definition of eigenvalue. If we write f' as $D(f)$ then the first equation becomes $D(f) = \lambda f$; indeed, D is linear in the sense that $D(af + bg) = (af + bg)' = af' + bg' = aD(f) + bD(g)$. The right way to make the connection precise is to use the language of vector spaces, but that is not an examinable part of this course.

The characteristic polynomial of a matrix or operator tells us *what the eigenvalues are*. But it also gives us information about *how big the eigenspaces are*. It is only partial information, as we will see; but it is useful information all the same.

Definition F2.6 Let A be an $n \times n$ matrix and let λ be an eigenvalue of A. The **geometric multiplicity** of λ is $\dim(E_\lambda(A))$, the dimension of the λ-eigenspace.

Examples F2.7 i. Let

$$A = \begin{pmatrix} 3 & 0 & 0 \\ 0 & 3 & 0 \\ 0 & 0 & 5 \end{pmatrix}.$$

The eigenvalues are 3 and 5, and

$$E_3(A) = \ker(A - 3I) = \left\{ \left(\begin{smallmatrix} x \\ y \\ 0 \end{smallmatrix}\right) : x, y \in \mathbb{R} \right\},$$
$$E_5(A) = \ker(A - 5I) = \left\{ \left(\begin{smallmatrix} 0 \\ 0 \\ z \end{smallmatrix}\right) : z \in \mathbb{R} \right\}.$$

Hence 3 and 5 have geometric multiplicities 2 and 1, respectively.

ii. Let

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

Then $\chi_A(\lambda) = \lambda^2$, so 0 is the only eigenvalue for A. We have

$$E_0(A) = \ker(A) = \left\{ \left(\begin{smallmatrix} x \\ 0 \end{smallmatrix}\right) : x \in \mathbb{R} \right\},$$

so 0 has geometric multiplicity 1.

When λ_0 is an eigenvalue of a matrix A, the characteristic polynomial $\chi_A(\lambda)$ has $(\lambda - \lambda_0)$ as a factor. When $\chi_A(\lambda)$ is written in fully factorized form, it may contain as a factor not just $(\lambda - \lambda_0)$ but a higher power, say $(\lambda - \lambda_0)^k$. This number k is called the **algebraic multiplicity** of λ_0.

Example F2.8 Let

$$A = \begin{pmatrix} -3 & 0 & 0 & 0 & 0 \\ 0 & -3 & 0 & 0 & 0 \\ 0 & 0 & 8 & 0 & 0 \\ 0 & 0 & 0 & 0 & -1 \\ 0 & 0 & 0 & 1 & 0 \end{pmatrix}.$$

Then

$$\chi_A(\lambda) = -(\lambda + 3)^2(\lambda - 8)(\lambda^2 + 1).$$

Since $\lambda^2 + 1$ has no real roots, $\chi_A(\lambda)$ factorizes no further (over $\mathbb{R}$), so the only eigenvalues of A are -3 and 8. The algebraic multiplicity of -3 is 2, and the algebraic multiplicity of 8 is 1.

Now the crucial fact is:

Theorem F2.9 *Let A be a square matrix and let λ be an eigenvalue of A. Then the geometric multiplicity of λ is less than or equal to its algebraic multiplicity.*

Proof Omitted. □

This theorem tells us that once we have calculated the characteristic polynomial, we immediately have an upper bound on the dimension of every eigenspace.

Examples F2.10

i. The diagonal matrix of Example F2.7(i) has characteristic polynomial $-(\lambda - 3)^2(\lambda - 5)$, so the algebraic multiplicities of the eigenvalues 3 and 5 are 2 and 1, respectively. These are equal to their geometric multiplicities.

ii. On the other hand, in the 2×2 matrix A of Example F2.7(ii), the unique eigenvalue 0 has algebraic multiplicity 2 (since $\chi_A(\lambda) = (\lambda - 0)^2$) but geometric multiplicity only 1.

We have been telling the story of the characteristic polynomial in terms of matrices, but it can also be told for linear operators, as follows.

Lemma F2.11 *Similar matrices have the same characteristic polynomial (and therefore the same eigenvalues).*

Proof Let A and B be similar $n \times n$ matrices. Then $A = PBP^{-1}$ for some invertible matrix P. Hence

$$\chi_A(\lambda) = \det(PBP^{-1} - \lambda I) = \det(P(B - \lambda I)P^{-1}) = \det(B - \lambda I) = \chi_B(\lambda),$$

where the third equality holds because similar matrices have the same determinant (Lemma E5.1). □

Given a linear operator T on $\mathbb{R}^n$, we define its **characteristic polynomial** χ_T to be the characteristic polynomial of T with respect to any basis of $\mathbb{R}^n$; it makes no difference which we choose, by Lemma F2.11.

F3 Diagonalizable matrices

For the lecture of Monday, 23 November 2015; part three of six

Diagonal matrices are fantastically easy to work with. Take a diagonal matrix

$$A = \begin{pmatrix} c_1 & 0 & \cdots & 0 \\ 0 & c_2 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & c_n \end{pmatrix},$$

which for convenience, I will write as

$$\mathrm{diag}(c_1, c_2, \ldots, c_n).$$

Then it is very easy to calculate all the powers of A: simply,

$$A^r = (c_1^r, c_2^r, \ldots, c_n^r)$$

for any integer $r \geq 0$. It is very easy to tell whether A is invertible: it is if every c_i is nonzero, and it is not otherwise. If it *is* invertible then

$$A^{-1} = (1/c_1, 1/c_2, \ldots, 1/c_n)$$

(which in fact is just the formula for A^r with $r = -1$). It is very easy to calculate the determinant:

$$\det(A) = c_1 c_2 \cdots c_n.$$

Also very easy are the rank and nullity: the rank is the number of values of i for which $c_i \neq 0$, and the nullity is the number of values of i for which $c_i = 0$. Everything about diagonal matrices is easy.

So, life would be a breeze if every matrix was diagonal. Of course, that's not true! Most matrices aren't diagonal. And similarly, given a linear operator T on $\mathbb{R}^n$, the standard matrix of T is usually not diagonal. But many linear operators do have the property that their matrix is diagonal *if you choose the right basis.* Another way to say this: many square matrices are *similar* to a diagonal matrix.

The purpose of this section is to explain what all this means.

Definition F3.1 A square matrix is **diagonalizable** if it is similar to some diagonal matrix.

In other words, an $n \times n$ matrix A is diagonalizable if and only if there exists an invertible $n \times n$ matrix P such that $P^{-1}AP$ is diagonal.

Example F3.2 Certainly every diagonal matrix is diagonalizable. But some non-diagonal matrices are diagonalizable. For instance, we showed in Example E4.7 that $\frac{1}{5}\left(\begin{smallmatrix} 11 & -2 \\ -2 & 14 \end{smallmatrix}\right)$ is similar to the diagonal matrix $\mathrm{diag}(2, 3)$, so it is diagonalizable.

Since we are interested in matrices similar to diagonal matrices, we are interested in the equation $P^{-1}AP = D$, where P is invertible and D is diagonal. Here is what this means explicitly:

Lemma F3.3 *Let A, P and D be $n \times n$ matrices. Suppose that P is invertible, and write its columns as $\mathbf{v}_1, \ldots, \mathbf{v}_n$. Suppose that $D = \operatorname{diag}(\lambda_1, \ldots, \lambda_n)$ is diagonal. Then*

$$P^{-1}AP = D \iff A\mathbf{v}_1 = \lambda_1\mathbf{v}_1,\ A\mathbf{v}_2 = \lambda_2\mathbf{v}_2,\ \ldots,\ A\mathbf{v}_n = \lambda_n\mathbf{v}_n.$$

Proof We have $P^{-1}AP = D$ if and only if $AP = PD$. For $i \in \{1, \ldots, n\}$, the ith column of AP is $A\mathbf{v}_i$ and the ith column of PD is $\lambda_i\mathbf{v}_i$. Hence $AP = PD$ if and only if $A\mathbf{v}_i = \lambda_i\mathbf{v}_i$ for all i. $\square$

Here is what diagonalizability means in terms of linear operators.

Lemma F3.4 *Let T be a linear operator on $\mathbb{R}^n$. The following are equivalent:*

i. the standard matrix of T is diagonalizable;

ii. there is a basis of $\mathbb{R}^n$ consisting of eigenvectors of T;

iii. the matrix of T with respect to some basis of $\mathbb{R}^n$ is diagonal.

Proof (i)⇒(ii): assume (i). Then $P^{-1}[T]P = \operatorname{diag}(\lambda_1, \ldots, \lambda_n)$ for some invertible P and scalars λ_i. Since P is invertible, its columns $\mathbf{v}_1, \ldots, \mathbf{v}_n$ are a basis of $\mathbb{R}^n$. By Lemma F3.3, $[T]\mathbf{v}_i = \lambda_i\mathbf{v}_i$ for all $i \in \{1, \ldots, n\}$. On the other hand, the fundamental property of the standard matrix (Section E2) is that $T(\mathbf{x}) = [T]\mathbf{x}$ for all $\mathbf{x} \in \mathbb{R}^n$. So for each i, we have $T(\mathbf{v}_i) = \lambda_i\mathbf{v}_i$ (with $\mathbf{v}_i \neq \mathbf{0}$, since $\mathbf{v}_1, \ldots, \mathbf{v_n}$ are linearly independent). Hence $\mathbf{v}_1, \ldots, \mathbf{v}_n$ are eigenvectors.

(ii)⇒(iii): if $\mathbf{v}_1, \ldots, \mathbf{v}_n$ is a basis of eigenvectors, with respective eigenvalues $\lambda_1, \ldots, \lambda_n$, then the matrix of T with respect to $\mathbf{v}_1, \ldots, \mathbf{v}_n$ is $\operatorname{diag}(\lambda_1, \ldots, \lambda_n)$.

(iii)⇒(i) follows from Corollary E4.6. $\square$

Translating from linear operators into square matrices, this tells us:

Lemma F3.5 *Let A be an $n \times n$ matrix. Then A is diagonalizable if and only if there is a basis of $\mathbb{R}^n$ consisting of eigenvectors of A.*

Proof Put $T = T_A$ (defined as in Example E2.1). Then $[T] = A$, so Lemma F3.4(i) states that A is diagonalizable. On the other hand, the eigenvectors of T are exactly the eigenvectors of A, so Lemma F3.4(ii) states that there is a basis of $\mathbb{R}^n$ consisting of eigenvectors of A. $\square$

Proposition F3.6 *Let A be a square matrix. Let $\mathbf{v}_1, \ldots, \mathbf{v}_m$ be eigenvectors of A, with eigenvalues $\lambda_1, \ldots, \lambda_m$ respectively. If $\lambda_1, \ldots, \lambda_m$ are pairwise distinct (that is, $\lambda_i \neq \lambda_j$ for all $i \neq j$) then $\mathbf{v}_1, \ldots, \mathbf{v}_m$ are linearly independent.*

Briefly put: eigenvectors with distinct eigenvalues are linearly independent.

Proof We prove this by induction on m. If $m = 1$ then the result is trivially true, since any nonzero vector on its own is linearly independent, and eigenvectors are nonzero. Suppose that $m \geq 2$, assume the result for $m - 1$, and let $c_1, \ldots, c_m$ be scalars such that

$$c_1\mathbf{v}_1 + c_2\mathbf{v}_2 + \cdots + c_m\mathbf{v}_m = \mathbf{0}. \tag{F:1}$$

We have to prove that $c_1 = c_2 = \cdots = c_m = 0$.

For all $i \in \{1, \ldots, m\}$, we have

$$(A - \lambda_m I)\mathbf{v}_i = A\mathbf{v}_i - \lambda_m \mathbf{v}_i = (\lambda_i - \lambda_m)\mathbf{v}_i,$$

so multiplying each side of (F:1) on the left by $A - \lambda_m I$ gives

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

By inductive hypothesis, $\mathbf{v}_1, \ldots, \mathbf{v}_{m-1}$ are linearly independent, so

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

But $\lambda_1, \ldots, \lambda_m$ are pairwise distinct, so $c_1 = c_2 = \cdots = c_{m-1} = 0$. Now (F:1) gives $c_m \mathbf{v}_m = \mathbf{0}$, and since the eigenvector $\mathbf{v}_m$ is by definition nonzero, $c_m = 0$ too. So $\mathbf{v}_1, \ldots, \mathbf{v}_m$ are linearly independent, completing the induction. □

Theorem F3.7 *Let A be an $n \times n$ matrix with n distinct eigenvalues. Then A is diagonalizable.*

Proof By hypothesis, we can choose n eigenvectors $\mathbf{v}_1, \ldots, \mathbf{v}_n$ with pairwise distinct eigenvalues. By Proposition F3.6, $\mathbf{v}_1, \ldots, \mathbf{v}_n$ are linearly independent. By Lemma C2.17, any n linearly independent vectors in $\mathbb{R}^n$ form a basis of $\mathbb{R}^n$. Hence there is a basis of $\mathbb{R}^n$ consisting of eigenvectors of A, which by Lemma F3.5 means that A is diagonalizable. □

The converse fails: e.g. the 2×2 identity matrix is certainly diagonalizable (it's diagonal!) but its only eigenvalue is 1.

Example F3.8 Let

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

Then

$$\chi_A(\lambda) = \det \begin{pmatrix} 5-\lambda & -1 & -2 \\ 0 & -6-\lambda & 3 \\ 0 & 0 & 3-\lambda \end{pmatrix} = (5-\lambda)(-6-\lambda)(3-\lambda).$$

(This determinant is most efficiently calculated by first expanding down the first column of A, then expanding down the second column of the remaining 2×2 matrix, as in Proposition D5.2 and Example D5.3.) So A has eigenvalues 5, -6 and 3. Since A is a 3×3 matrix with 3 distinct eigenvalues, it is diagonalizable.

Suppose we now wish to find an invertible matrix P and a diagonal matrix D such that $P^{-1}AP = D$. Lemma F3.3 tells us how: the diagonal matrix D has the eigenvalues down the diagonal, and the columns of P are any eigenvectors with those eigenvalues. In this example, we calculate that

$$\begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} \in \ker(A - 5I), \qquad \begin{pmatrix} 1 \\ 11 \\ 0 \end{pmatrix} \in \ker(A + 6I), \qquad \begin{pmatrix} 7 \\ 2 \\ 6 \end{pmatrix} \in \ker(A - 3I)$$

(by the usual methods for solving linear systems). Hence $P^{-1}AP = D$ where

$$P = \begin{pmatrix} 1 & 1 & 7 \\ 0 & 11 & 2 \\ 0 & 0 & 6 \end{pmatrix}, \quad D = \begin{pmatrix} 5 & 0 & 0 \\ 0 & -6 & 0 \\ 0 & 0 & 3 \end{pmatrix}.$$

For all we know so far, *every* square matrix could be diagonalizable. This is not, in fact, true. The following result is useful in showing that a given matrix is not diagonalizable.

Proposition F3.9 *Let A be a square matrix. Then A is diagonalizable if and only if the following conditions both hold:*

i. The characteristic polynomial of A can be factorized as

$$\chi_A(\lambda) = (\lambda - \lambda_1)^{k_1}(\lambda - \lambda_2)^{k_2} \cdots (\lambda - \lambda_r)^{k_r}$$

for some distinct scalars $\lambda_1, \ldots, \lambda_r$ and some integers $k_1, \ldots, k_r$.

ii. For every eigenvalue of A, the geometric multiplicity is equal to the algebraic multiplicity (that is, $\dim(E_{\lambda_i}(A)) = k_i$ for all i).

Proof Omitted. □

Examples F3.10 i. The matrix A of Example F2.8 has characteristic polynomial $-(\lambda+3)^2(\lambda-8)(\lambda^2+1)$, which does not factorize any further over $\mathbb{R}$, since λ^2+1 has no real roots. So A fails condition (i) of Proposition F3.9, and is therefore not diagonalizable.

This can also be shown directly (giving a clue to how the proposition is proved). The eigenvalues of A are -3 and 8. Since -3 has algebraic multiplicity 2, it has geometric multiplicity at most 2 (by Theorem F2.9). Since 8 has algebraic multiplicity 1, it has geometric multiplicity exactly 1 (by Theorem F2.9, and because the geometric multiplicity of an eigenvalue is always ≥ 1). Now every eigenvector of A belongs to either the (-3)-eigenspace or the 8-eigenspace, so any linearly independent list of eigenvectors of A has at most $2 + 1 = 3$ elements. Hence there is no basis of $\mathbb{R}^5$ consisting of eigenvectors of A.

ii. Let $A = \left(\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right)$, as in Examples F2.7(ii) and F2.10(ii). Then the eigenvalue 0 has algebraic multiplicity 2 but geometric multiplicity only 1, so it fails condition (ii) of Proposition F3.9. Hence A is not diagonalizable.

Again, this can also be shown directly. We found previously that 0 is the only eigenvalue. Since it has geometric multiplicity 1, it is not possible to find two linearly independent eigenvectors of A. Hence there is no basis of $\mathbb{R}^2$ consisting of eigenvectors of A.

F4 Orthogonal matrices

For the lecture of Monday, 23 November 2015; part four of six

In general, applying a linear operator to $\mathbb{R}^n$ distorts the geometry: both lengths and angles can change. For instance, let $A = \left(\begin{smallmatrix} 2 & 0 \\ 0 & 2 \end{smallmatrix}\right)$; then $\mathbf{e}_1 = \left(\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right)$ has length 1, but $T_A(\mathbf{e}_1) = \left(\begin{smallmatrix} 2 \\ 0 \end{smallmatrix}\right)$ has length 2. Or let $A = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$; then the angle between $\mathbf{e}_1$ and $\mathbf{e}_2$ is $\pi/2$, but the angle between $T_A(\mathbf{e}_1) = \left(\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right)$ and $T_A(\mathbf{e}_2) = \left(\begin{smallmatrix} 1 \\ 1 \end{smallmatrix}\right)$ is $\pi/4$.

From a geometric point of view, it is natural to pay special attention to those operators that *do* preserve lengths and angles. Those operators (or their standard matrices) are called 'orthogonal'.

Definition F4.1 A real square matrix A is **orthogonal** if A is invertible and $A^{-1} = A^T$.

So, A is orthogonal if and only if $A^T A = I$ and $AA^T = I$. In fact, either one of $A^T A = I$ and $AA^T = I$ implies the other (for *square* matrices A), by Corollary D1.7.

This doesn't appear to have anything to do with preservation of length and angle! But we will eventually show that it really does.

Example F4.2 We saw in Example E2.6 that rotation by an angle of θ, as a linear operator R_θ on $\mathbb{R}^2$, has standard matrix

$$[R_\theta] = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}.$$

This matrix is orthogonal, since

$$[R_\theta][R_\theta]^T = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} \begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Lemma F4.3 *Let A be a real square matrix. Then A is orthogonal if and only if A^T is orthogonal.*

Proof A is orthogonal if and only if $A^T A = I = AA^T$, whereas A^T is orthogonal if and only if $(A^T)^T A^T = I = A^T (A^T)^T$. But $(A^T)^T = A$, so these are equivalent. □

Proposition F4.4 *Let A be a real square matrix. The following are equivalent:*

i. A is orthogonal;

ii. the columns of A are orthonormal;

iii. the rows of A are orthonormal.

Proof We prove that (i)⇔(ii). Since the rows of A are the columns of A^T, the equivalence (i)⇔(iii) will then follow from Lemma F4.3.

We use the convention that the (p, q)-entry of a matrix M is written as M_{pq}. Suppose that A is an $n \times n$ matrix, and write $\mathbf{v}_1, \ldots, \mathbf{v}_n$ for the columns of A. For $i, k \in \{1, \ldots, n\}$, we have

$$(A^T A)_{ik} = \sum_{j=1}^{n} (A^T)_{ij} A_{jk} = \sum_{j=1}^{n} A_{ji} A_{jk} = \mathbf{v}_i \cdot \mathbf{v}_k.$$

If A is orthogonal then $A^T A = I$, so for all $i, k \in \{1, \ldots, n\}$,

$$\mathbf{v}_i \cdot \mathbf{v}_k = (A^T A)_{ik} = \begin{cases} 1 & \text{if } i = k, \\ 0 & \text{if } i \neq k, \end{cases}$$

which means that $\mathbf{v}_1, \ldots, \mathbf{v}_n$ are orthonormal. The same argument reversed shows that if $\mathbf{v}_1, \ldots, \mathbf{v}_n$ are orthonormal then $A^T A = I$ and so (by Corollary D1.7) A is orthogonal. □

In the light of this proposition, orthogonal matrices should really be called *orthonormal* matrices. But unfortunately, they're not.

Remark F4.5 Proposition F4.4 implies that if the rows of a square matrix are orthonormal then so are the columns. Proving this from scratch is really quite hard. Even for 2×2 matrices, it's not obvious. If you think it is, try it!

Example F4.6 In the rotation matrix of Example F4.2, both columns have length 1 (because $\cos^2\theta + \sin^2\theta = 1$) and the dot product of the two columns is 0. Hence the columns are orthonormal. This gives a slightly easier proof that this matrix is orthogonal.

The next few results fulfil the promise made at the start of this section: that the orthogonal matrices are those that preserve angle and length.

Proposition F4.7 *Let A be a real square matrix. Then A is orthogonal if and only if*

$$(A\mathbf{x}) \cdot (A\mathbf{y}) = \mathbf{x} \cdot \mathbf{y}$$

for all $\mathbf{x}, \mathbf{y} \in \mathbb{R}^n$.

Proof Recall that for column vectors $\mathbf{u}$ and $\mathbf{v}$ of the same dimension, $\mathbf{u} \cdot \mathbf{v} = \mathbf{u}^T\mathbf{v}$.

Suppose that A is orthogonal. Then for all $\mathbf{x}, \mathbf{y} \in \mathbb{R}^n$,

$$(A\mathbf{x}) \cdot (A\mathbf{y}) = (A\mathbf{x})^T(A\mathbf{y}) = \mathbf{x}^T A^T A\mathbf{y} = \mathbf{x}^T\mathbf{y} = \mathbf{x} \cdot \mathbf{y}.$$

Conversely, suppose that $(A\mathbf{x}) \cdot (A\mathbf{y}) = \mathbf{x} \cdot \mathbf{y}$ for all $\mathbf{x}, \mathbf{y} \in \mathbb{R}^n$. Let $i, j \in \{1, \ldots, n\}$. Then

$$(A\mathbf{e}_i) \cdot (A\mathbf{e}_j) = \mathbf{e}_i \cdot \mathbf{e}_j = \begin{cases} 1 & \text{if } i = j, \\ 0 & \text{if } i \neq j. \end{cases}$$

But $A\mathbf{e}_i$ is the ith column of A (Lemma E2.3), so the columns of A are orthonormal. Hence by Proposition F4.4, A is orthogonal. □

The formula '$\mathbf{x} \cdot \mathbf{y} = \|\mathbf{x}\| \, \|\mathbf{y}\| \cos\theta$' for the dot product of vectors $\mathbf{x}$ and $\mathbf{y}$ (where θ is the angle between them) demonstrates that the dot product combines aspects of length and angle. Length can be expressed in terms of the dot product, by the formula $\|\mathbf{x}\| = \sqrt{\mathbf{x} \cdot \mathbf{x}}$. Less obvious is the converse, that the dot product can be expressed in terms of lengths. This is the main content of the next lemma. It is something like the fact that the lengths of the sides of a triangle determine the angles.

Lemma F4.8 (Polarization identity) *Let* $\mathbf{x}, \mathbf{y} \in \mathbb{R}^n$. *Then*

$$\mathbf{x} \cdot \mathbf{y} = \frac{1}{4}\Big(\|\mathbf{x}+\mathbf{y}\|^2 - \|\mathbf{x}-\mathbf{y}\|^2\Big).$$

Proof We have

$$\begin{aligned}
\|\mathbf{x}+\mathbf{y}\|^2 - \|\mathbf{x}-\mathbf{y}\|^2 &= (\mathbf{x}+\mathbf{y}) \cdot (\mathbf{x}+\mathbf{y}) - (\mathbf{x}-\mathbf{y}) \cdot (\mathbf{x}-\mathbf{y}) \\
&= (\mathbf{x} \cdot \mathbf{x} + 2\mathbf{x} \cdot \mathbf{y} + \mathbf{y} \cdot \mathbf{y}) - (\mathbf{x} \cdot \mathbf{x} - 2\mathbf{x} \cdot \mathbf{y} + \mathbf{y} \cdot \mathbf{y}) \\
&= 4\mathbf{x} \cdot \mathbf{y}.
\end{aligned}$$

□

We can now show that the orthogonal matrices are exactly those that preserve length, in the following sense:

Proposition F4.9 *Let A be a real square matrix. Then A is orthogonal if and only if*

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

for all $\mathbf{x} \in \mathbb{R}^n$.

Proof Suppose that A is orthogonal. Then by Proposition F4.7,

$$\|A\mathbf{x}\| = \sqrt{(A\mathbf{x}) \cdot (A\mathbf{x})} = \sqrt{\mathbf{x} \cdot \mathbf{x}} = \|\mathbf{x}\|$$

for all $\mathbf{x} \in \mathbb{R}^n$.

Conversely, suppose that $\|A\mathbf{x}\| = \|\mathbf{x}\|$ for all $\mathbf{x} \in \mathbb{R}^n$. We show that $(A\mathbf{x}) \cdot (A\mathbf{y}) = \mathbf{x} \cdot \mathbf{y}$ for all $\mathbf{x}, \mathbf{y} \in \mathbb{R}^n$; then Proposition F4.7 will imply that A is orthogonal. Let $\mathbf{x}, \mathbf{y} \in \mathbb{R}^n$. Then

$$\begin{aligned}
(A\mathbf{x}) \cdot (A\mathbf{y}) &= \frac{1}{4}\Big(\|A\mathbf{x} + A\mathbf{y}\|^2 - \|A\mathbf{x} - A\mathbf{y}\|^2\Big) \\
&= \frac{1}{4}\Big(\|A(\mathbf{x}+\mathbf{y})\|^2 - \|A(\mathbf{x}-\mathbf{y})\|^2\Big) \\
&= \frac{1}{4}\Big(\|\mathbf{x}+\mathbf{y}\|^2 - \|\mathbf{x}-\mathbf{y}\|^2\Big) \\
&= \mathbf{x} \cdot \mathbf{y}
\end{aligned}$$

(using the polarization identity twice), as required. □

Examples F4.10 i. For which linear operators T on $\mathbb{R}^2$ is the standard matrix $[T]$ orthogonal? We have already seen that $[T]$ is orthogonal when T is rotation of $\mathbb{R}^2$ by any angle. The same is true for reflection of $\mathbb{R}^2$ in any line through the origin. Indeed, as you discovered in Workshop 8, if F_θ denotes reflection in the line through $\mathbf{0}$ at angle θ from the positive x-axis then

$$[F_\theta] = \begin{pmatrix} \cos 2\theta & \sin 2\theta \\ \sin 2\theta & -\cos 2\theta \end{pmatrix}.$$

It is easy to see that the columns are orthonormal, so this matrix is indeed orthogonal.

These results confirm our geometric intuition that rotation and reflection preserve length. In fact, rotations and reflections are the *only* 2×2 orthogonal matrices. Proving this is a pleasant exercise.

ii. The 3×3 orthogonal matrices can also be completely classified. They are the standard matrices of the following linear operators:

- rotation by any angle around any axis through the origin;
- reflection in any plane through the origin;
- 'reflection in the origin', that is, $\mathbf{x} \mapsto -\mathbf{x}$.

An important difference between rotations and reflections is that rotations have determinant 1 and reflections have determinant -1. There are no other possibilities for the determinant, because of the following result:

Lemma F4.11 *Any orthogonal matrix has determinant* ± 1.

Proof Let A be an orthogonal matrix. Then

$$1 = \det I = \det(AA^T) = (\det A)(\det A^T) = (\det A)^2$$

by parts (vi) and (v) of Proposition D5.4. Hence $\det A = \pm 1$. □

We finish this section with a lemma that we will need later:

Lemma F4.12 *Let A and B be $n \times n$ orthogonal matrices. Then AB is orthogonal.*

Proof We have $(AB)^T(AB) = B^T A^T AB = B^T IB = B^T B = I$. □

F5 A little linear algebra over $\mathbb{C}$

For the lecture of Monday, 23 November 2015; part five of six

There are some facts purely about *real* numbers that are most easily proved by using the *complex* numbers. We are about to meet one of them.

First, let's review some general facts about the complex numbers. For every complex number z, there are unique real numbers x and y such that $z = x + iy$. The **complex conjugate** of z is $\overline{z} = x - iy$. Graphically, complex conjugation is reflection in the real axis. A complex number z is real if and only if $z = \overline{z}$.

As you can check (and *should* check if you've never done so before!), complex conjugation preserves addition and multiplication:

$$\overline{z + w} = \overline{z} + \overline{w}, \qquad \overline{z \cdot w} = \overline{z} \cdot \overline{w} \tag{F:2}$$

for all $z, w \in \mathbb{C}$. Also, the modulus $|z| = \sqrt{x^2 + y^2}$ of a complex number $z = x + iy$ can be expressed in terms of conjugates:

$$|z| = \sqrt{z\overline{z}}$$

The modulus has the property that $|z| \geq 0$ for all z, with equality if and only if $z = 0$.

Now a miracle happens! We deliberately constructed $\mathbb{C}$ in such a way that it contains a square root of -1. In other words, by defining $\mathbb{C}$ as the set of all expressions $x + iy$ ($x, y \in \mathbb{R}$) where i is a square root of -1, we made sure that $\mathbb{C}$ contains a solution to the equation $z^2 + 1 = 0$. That equation has no solution in $\mathbb{R}$. But there are lots of *other* polynomial equations that have no solution in $\mathbb{R}$, like $z^6 + 1 = 0$ and $2z^4 + z + 1 = 0$, and we have no right to expect that *these* have any solution in $\mathbb{C}$. Nevertheless, they do!

This result is so amazing and important that it bears a grand name:

Theorem F5.1 (Fundamental theorem of algebra) *Every non-constant polynomial over $\mathbb{C}$ has at least one root in $\mathbb{C}$.*

Proof (sketch; non-examinable) There are many known proofs of this theorem, but none is very simple as far as I know. Here is an outline of my favourite. If you want to know how to make it precise, you should take the 4th year course Algebraic Topology.

Write $p(z) = a_n z^n + a_{n-1} z^{n-1} + \cdots + a_1 z + a_0$, with $a_n \neq 0$ and $n \geq 1$. Suppose for a contradiction that p has no root.

For $r \geq 0$, write C_r for the circle in the complex plane with centre 0 and radius r. As z moves one revolution around C_r, $p(z)$ traces out a loop L_r in $\mathbb{C}$. It cannot pass *through* 0, since p has no root, but we can ask whether L_r *winds around* 0.

(Picture a pole sticking up at 0 and the loop L_r as made of string. The question is whether the string is wound around the pole.)

When $r = 0$, the loop L_r is constant at $p(0)$, so it does not wind around 0. When r is small, the whole loop L_r lies close to $p(0)$, so again it does not wind around 0. As r increases, L_r changes continuously, and so it does not wind around 0 for any value of r. (It takes some work to make that step precise, but the intuitive idea is that if L_r does not wind around 0 and $L_{r+\varepsilon}$ does, then $L_{r+\delta}$ must actually pass *through* 0 for some δ between 0 and ε, which is impossible.)

However, when r is large, $p(z)$ behaves roughly like its leading term $a_n z^n$, so the loop L_r winds n times round 0. Since $n \geq 1$, this is a contradiction. □

Corollary F5.2 *Let $p(z) = a_n z^n + a_{n-1} z^{n-1} + \cdots + a_1 z + a_0$ be a polynomial over $\mathbb{C}$. Then*

$$p(z) = a_n(z - \lambda_1)(z - \lambda_2) \cdots (z - \lambda_n)$$

for some $\lambda_1, \lambda_2, \ldots, \lambda_n \in \mathbb{C}$.

Proof (sketch; non-examinable) This follows by induction from Theorem F5.1. □

Now let us try to do some linear algebra over $\mathbb{C}$. How much of what we have done in this course still works if we replace $\mathbb{R}$ by $\mathbb{C}$?

Most of it. In particular, given an $n \times n$ complex matrix A, and $\lambda \in \mathbb{C}$, we can (and do) define an **eigenvector** for A, with **eigenvalue** λ, to be a nonzero vector $\mathbf{x} \in \mathbb{C}^n$ such that $A\mathbf{x} = \lambda\mathbf{x}$. We can also define determinants and characteristic polynomials, just as for $\mathbb{R}$. And just as for $\mathbb{R}$ (Proposition F2.2), a scalar $\lambda \in \mathbb{C}$ is an eigenvalue for a square matrix over $\mathbb{C}$ if and only if it is a root of its characteristic polynomial.

Warning F5.3 The terminology concerning real and complex eigenvalues is slightly delicate.

For a linear transformation $T\colon \mathbb{R}^n \to \mathbb{R}^n$, the eigenvalues are by definition *real* numbers, and the eigenvectors are by definition in $\mathbb{R}^n$. (See Warning F1.2.)

For a linear transformation $T\colon \mathbb{C}^n \to \mathbb{C}^n$, the eigenvalues are complex numbers (which may or may not be real), and the eigenvectors are in $\mathbb{C}^n$.

For complex matrices, the eigenvalues are again complex numbers (real or not), and the eigenvectors are again in $\mathbb{C}^n$.

But for *real matrices*, the situation is less clear-cut. For example, what does it mean to say 'an eigenvalue of $\left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$'? If we are treating it as a *real* matrix, then it has no eigenvalues. But if we are treating it as a *complex* matrix, it has eigenvalues $\pm i$.

So in the context of real matrices, it is helpful to speak of 'real eigenvalues' and 'complex eigenvalues', for clarity. For example, the matrix $\left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ has complex eigenvalues $\pm i$, but no real eigenvalues at all.

We've seen that there are real matrices with no real eigenvalues. A crucial advantage of $\mathbb{C}$ over $\mathbb{R}$ is that *every complex square matrix has an eigenvalue:*

Theorem F5.4 *Let $n \geq 1$, and let A be an $n \times n$ complex matrix. Then A has at least one eigenvalue.*

Proof The characteristic polynomial χ_A is a polynomial over $\mathbb{C}$ of degree $n \geq 1$, so by Theorem F5.1, has at least one root in $\mathbb{C}$. As stated above, any such root is an eigenvalue of A. □

Soon, we will use this result about complex matrices to prove a result about real matrices; but first we need to consider complex conjugates of matrices.

Any $m \times n$ matrix $X = (X_{ij})$ with entries in $\mathbb{C}$ has a **complex conjugate** $\overline{X}$, which is also an $m \times n$ matrix with entries in $\mathbb{C}$; its (i,j)-entry is $\overline{X_{ij}}$. In particular, this applies in the case when X is a vector. Complex conjugation of matrices preserves addition and multiplication, just as in (F:2):

Lemma F5.5 *Let X and Y be $m \times n$ matrices over $\mathbb{C}$, and let Z be an $n \times p$ matrix over $\mathbb{C}$. Then*

$$\overline{X+Y} = \overline{X} + \overline{Y}, \qquad \overline{YZ} = \overline{Y}\,\overline{Z}.$$

Proof We prove just the second; the first is no harder, and is left as an exercise. We use the convention that the (p,q)-entry of a matrix M is written as M_{pq}.

First, both $\overline{YZ}$ and $\overline{Y}\,\overline{Z}$ are $m \times p$ matrices. Now let $1 \leq i \leq m$ and $1 \leq k \leq p$. We have

$$\begin{aligned}
(\overline{YZ})_{ik} &= \overline{(YZ)_{ik}} && \text{(by definition of } \overline{YZ}\text{)}\\
&= \overline{\sum_{j=1}^{n} Y_{ij} Z_{jk}} && \text{(by definition of matrix multiplication)}\\
&= \sum_{j=1}^{n} \overline{Y_{ij}}\,\overline{Z_{jk}} && \text{(by (F:2))}\\
&= \sum_{j=1}^{n} \overline{Y}_{ij}\,\overline{Z}_{jk} && \text{(by definition of } \overline{Y} \text{ and } \overline{Z}\text{)}\\
&= (\overline{Y}\,\overline{Z})_{ik} && \text{(by definition of matrix multiplication).} \quad \square
\end{aligned}$$

For real vectors $\mathbf{x} \in \mathbb{R}^n$, we have $\mathbf{x}^T\mathbf{x} = \mathbf{x}\cdot\mathbf{x} = \sum x_i^2$ (as noted in Chapter A). It follows that $\mathbf{x}^T\mathbf{x} = 0$ if and only if $\mathbf{x} = \mathbf{0}$. Something similar holds for complex vectors, as long as we insert a complex conjugate into the formula:

Lemma F5.6 *Let $\mathbf{z} \in \mathbb{C}^n$. Then $\overline{\mathbf{z}}^T\mathbf{z} = \sum_{i=1}^{n} |z_i|^2$.*

Proof First, $\overline{\mathbf{z}}^T$ is a $1 \times n$ matrix over $\mathbb{C}$, and $\mathbf{z}$ is an $n \times 1$ matrix over $\mathbb{C}$, so $\overline{\mathbf{z}}^T\mathbf{z}$ is a 1×1 matrix over $\mathbb{C}$, that is, a complex number. Now,

$$\overline{\mathbf{z}}^T\mathbf{z} = \sum_{i=1}^{n} \overline{z_i} z_i = \sum_{i=1}^{n} |z_i|^2.$$

$\square$

For real matrices A, we are often interested in the condition that A is symmetric: $A^T = A$. For complex matrices A, symmetry turns out to be less interesting than the condition that $\overline{A}^T = A$. (Such matrices are called 'Hermitian'.) Our next result concerns such matrices.

Proposition F5.7 *Let A be an $n \times n$ complex matrix such that $\overline{A}^T = A$. Then every eigenvalue of A is real.*

Proof Let A be such a matrix and let $\lambda \in \mathbb{C}$ be an eigenvalue. Take an eigenvector $\mathbf{z} \in \mathbb{C}^n$ with eigenvalue λ.

We will evaluate $\overline{\mathbf{z}}^T A\mathbf{z}$ in two ways. Note that it is a 1×1 matrix over $\mathbb{C}$, that is, a complex number.

On the one hand,

$$\overline{\mathbf{z}}^T A\mathbf{z} = \overline{\mathbf{z}}^T \lambda\mathbf{z} = \lambda\overline{\mathbf{z}}^T\mathbf{z} = \lambda \sum_{i=1}^{n} |z_i|^2$$

where the last step is by Lemma F5.6. On the other hand,

$$\begin{aligned}
\overline{\mathbf{z}}^T A\mathbf{z} &= \overline{\mathbf{z}}^T \overline{A}^T \mathbf{z} && \text{(by hypothesis)} \\
&= (\overline{A}\,\overline{\mathbf{z}})^T \mathbf{z} && \text{(by Lemma A3.2(iii))} \\
&= (\overline{A\mathbf{z}})^T \mathbf{z} && \text{(by Lemma F5.5)} \\
&= (\overline{\lambda\mathbf{z}})^T \mathbf{z} && \\
&= \overline{\lambda}\,\overline{\mathbf{z}}^T \mathbf{z} && \text{(directly from the definitions)} \\
&= \overline{\lambda}\sum_{i=1}^{n} |z_i|^2. && \text{(by Lemma F5.6).}
\end{aligned}$$

Putting together the two expressions for $\overline{\mathbf{z}}^T A\mathbf{z}$ gives

$$\lambda\sum_{i=1}^{n} |z_i|^2 = \overline{\lambda}\sum_{i=1}^{n} |z_i|^2.$$

But $\mathbf{z} \neq \mathbf{0}$ by definition of eigenvector, so $\sum |z_i|^2 \neq 0$, so $\lambda = \overline{\lambda}$, so λ is real. □

We now use what we know about complex matrices to prove a result that is purely about real matrices.

Theorem F5.8 *Every real symmetric matrix has at least one real eigenvalue.*

Proof Let A be a real symmetric $n \times n$ matrix (where $n \geq 1$). By Theorem F5.4, A has at least one complex eigenvalue λ. Now $A = \overline{A} = \overline{A}^T$ since A is real and symmetric, so λ is real by Proposition F5.7. □

The significance of this result will be revealed in the next section.

F6 Symmetric matrices

For the lecture of Monday, 23 November 2015; part six of six

The main result of this section is that every symmetric matrix is diagonalizable. Better still, it is *orthogonally* diagonalizable, in the following sense:

Definition F6.1 A real square matrix A is **orthogonally diagonalizable** if there exists an orthogonal matrix P such that $P^{-1}AP$ is diagonal.

(Since the inverse of an orthogonal matrix is the same as its transpose, we could equivalently replace '$P^{-1}AP$' by 'P^TAP' here.)

Why would we care about *orthogonal* diagonalizability? It is because orthonormal bases are the most convenient ones; they share many of the properties of the standard basis, which is the one we are most familiar with. And just as ordinary diagonalizability is equivalent to the existence of a basis of eigenvectors, *orthogonal* diagonalizability is equivalent to the existence of an *orthonormal* basis of eigenvectors:

Lemma F6.2 *Let A be an $n \times n$ matrix. Then A is orthogonally diagonalizable if and only if there is an orthonormal basis of $\mathbb{R}^n$ consisting of eigenvectors of A.*

Proof By Lemma F3.3, A is orthogonally diagonalizable if and only if there exists an orthogonal matrix $P = (\mathbf{v}_1|\mathbf{v}_2|\cdots|\mathbf{v}_n)$ such that $\mathbf{v}_1, \ldots, \mathbf{v}_n$ are eigenvectors for A. But since the orthogonal matrices are exactly the square matrices whose columns are orthonormal, such a P exists if and only if there exist n orthonormal eigenvectors of A, or equivalently an orthonormal basis of $\mathbb{R}^n$ consisting of eigenvectors of A. $\square$

As for the case of ordinary diagonalizability, if $P^{-1}AP = D$ with P orthogonal and D diagonal, then the columns of P form an orthonormal basis of eigenvectors of A and the diagonal entries of D are the corresponding eigenvalues.

Example F6.3 Let $A = \left(\begin{smallmatrix} 5 & -1 \\ -1 & 5 \end{smallmatrix}\right)$. Then $\chi_A(\lambda) = (\lambda-4)(\lambda-6)$, an eigenvector with eigenvalue 4 is $\left(\begin{smallmatrix} 1 \\ 1 \end{smallmatrix}\right)$, and an eigenvector with eigenvalue 6 is $\left(\begin{smallmatrix} -1 \\ 1 \end{smallmatrix}\right)$. These eigenvectors are orthogonal but not orthonormal. We scale them to make them orthonormal, and define P to be the matrix with these orthonormal eigenvectors as its columns:

$$P = \begin{pmatrix} 1/\sqrt{2} & -1/\sqrt{2} \\ 1/\sqrt{2} & 1/\sqrt{2} \end{pmatrix}.$$

Then P is orthogonal, $P^TAP = \operatorname{diag}(4, 6)$, and A is orthogonally diagonalizable.

It is no coincidence that in this example, the orthogonally diagonalizable matrix A happened to be symmetric. In fact:

Lemma F6.4 *Every orthogonally diagonalizable matrix is symmetric.*

Proof Let A be an orthogonally diagonalizable matrix. Then $P^TAP = D$ for some orthogonal matrix P and diagonal matrix D. We have $A = PDP^T$ (since $P^T = P^{-1}$), and D is symmetric, so

$$A^T = (PDP^T)^T = (P^T)^T D^T P^T = PDP^T = A. \qquad \square$$

We now prove the converse, which is much harder.

Theorem F6.5 *A real square matrix is orthogonally diagonalizable if and only if it is symmetric.*

Proof We have just proved 'only if'. For 'if', we use induction on the size of the matrix. It is clear for 1×1 matrices. Now let $n \geq 2$, let A be an $n \times n$ symmetric matrix, and suppose inductively that $(n-1) \times (n-1)$ symmetric matrices are orthogonally diagonalizable.

By Theorem F5.8, A has at least one real eigenvalue. Thus, $A\mathbf{w}_1 = \lambda_1 \mathbf{w}_1$ for some $\lambda_1 \in \mathbb{R}$ and vector $\mathbf{w}_1 \neq \mathbf{0}$. Extend $\mathbf{w}_1$ to a basis $\mathbf{w}_1, \mathbf{w}_2, \ldots, \mathbf{w}_n$ of $\mathbb{R}^n$ (which is possible by Lemma C2.11). By the Gram–Schmidt process (Theorem C4.6), we can then find an orthonormal basis $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n$ of $\mathbb{R}^n$ such that $\text{span}\{\mathbf{v}_1\} = \text{span}\{\mathbf{w}_1\}$. Then $\mathbf{v}_1$ is a scalar multiple of $\mathbf{w}_1$, so $A\mathbf{v}_1 = \lambda_1 \mathbf{v}_1$.

(We now forget $\mathbf{w}_1, \ldots, \mathbf{w}_n$, remembering only that we have an orthonormal basis $\mathbf{v}_1, \ldots, \mathbf{v}_n$ of $\mathbb{R}^n$ whose first element is an eigenvector of A.)

Let $Q = (\mathbf{v}_1 | \mathbf{v}_2 | \cdots | \mathbf{v}_n)$. Then Q has orthonormal columns, so it is orthogonal. Now consider the matrix $Q^T A Q = Q^{-1} A Q$. By Lemma E2.3, $Q\mathbf{e}_1 = \mathbf{v}_1$ and the first column of $Q^T A Q$ is

$$Q^T A Q \mathbf{e}_1 = Q^T A \mathbf{v}_1 = Q^T \lambda_1 \mathbf{v}_1 = \lambda_1 Q^{-1} \mathbf{v}_1 = \lambda_1 \mathbf{e}_1 = \begin{pmatrix} \lambda_1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}.$$

Moreover, $Q^T A Q$ is symmetric, since

$$(Q^T A Q)^T = Q^T A^T (Q^T)^T = Q^T A Q$$

(using the symmetry of A). So the first row of $Q^T A Q$ is $(\lambda_1 \ 0 \ \cdots \ 0)$. Hence

$$Q^T A Q = \begin{pmatrix} \lambda_1 & 0 & \cdots & 0 \\ 0 & a'_{11} & \cdots & a'_{1,n-1} \\ \vdots & \vdots & & \vdots \\ 0 & a'_{n-1,1} & \cdots & a'_{n-1,n-1} \end{pmatrix} \qquad \text{(F:3)}$$

for some real numbers a'_{ij}. Since $Q^T A Q$ is symmetric, the matrix

$$A' = \begin{pmatrix} a'_{11} & \cdots & a'_{1,n-1} \\ \vdots & & \vdots \\ a'_{n-1,1} & \cdots & a'_{n-1,n-1} \end{pmatrix}$$

is symmetric too. By inductive hypothesis, A' is orthogonally diagonalizable, so $Q'^T A' Q' = \text{diag}(\lambda_2, \ldots, \lambda_n)$ for some $(n-1) \times (n-1)$ orthogonal matrix Q' and $\lambda_2, \ldots, \lambda_n \in \mathbb{R}$.

For convenience, let us write equation (F:3) as

$$Q^T A Q = \left(\begin{array}{c|ccc} \lambda_1 & 0 & \cdots & 0 \\ \hline 0 & & & \\ \vdots & & A' & \\ 0 & & & \end{array}\right).$$

Define an $n \times n$ matrix R by

$$R = \left(\begin{array}{c|ccc} 1 & 0 & \cdots & 0 \\ \hline 0 & & & \\ \vdots & & Q' & \\ 0 & & & \end{array}\right).$$

Then

$$\begin{aligned} R^T(Q^TAQ)R &= \left(\begin{array}{c|ccc} 1 & 0 & \cdots & 0 \\ \hline 0 & & & \\ \vdots & & Q' & \\ 0 & & & \end{array}\right)^T \left(\begin{array}{c|ccc} \lambda_1 & 0 & \cdots & 0 \\ \hline 0 & & & \\ \vdots & & A' & \\ 0 & & & \end{array}\right) \left(\begin{array}{c|ccc} 1 & 0 & \cdots & 0 \\ \hline 0 & & & \\ \vdots & & Q' & \\ 0 & & & \end{array}\right) \\ &= \left(\begin{array}{c|ccc} \lambda_1 & 0 & \cdots & 0 \\ \hline 0 & & & \\ \vdots & & Q'^TA'Q' & \\ 0 & & & \end{array}\right) \\ &= \mathrm{diag}(\lambda_1, \lambda_2, \ldots, \lambda_n). \end{aligned}$$

Put $P = QR$. We have just shown that P^TAP is diagonal.

It remains to prove that P is orthogonal. Indeed, Q is orthogonal (as noted above), and R is orthogonal since

$$R^TR = \left(\begin{array}{c|ccc} 1 & 0 & \cdots & 0 \\ \hline 0 & & & \\ \vdots & & Q' & \\ 0 & & & \end{array}\right)^T \left(\begin{array}{c|ccc} 1 & 0 & \cdots & 0 \\ \hline 0 & & & \\ \vdots & & Q' & \\ 0 & & & \end{array}\right) = \left(\begin{array}{c|ccc} 1 & 0 & \cdots & 0 \\ \hline 0 & & & \\ \vdots & & Q'^TQ' & \\ 0 & & & \end{array}\right) = I_n.$$

So P is the product of two orthogonal matrices, and therefore orthogonal by Lemma F4.12. This completes the induction. □

We'll finish with an example that looks very hard, but which the theory we've developed makes easy.

Example F6.6 Let

$$A = \begin{pmatrix} 14 & -14 & -16 \\ -14 & 23 & -2 \\ -16 & -2 & 8 \end{pmatrix}.$$

What is A^{99}?

We observed at the beginning of Section F3 that powers of diagonal matrices are very easy to calculate. Our matrix A is not diagonal, but it is symmetric, so it must be orthogonally diagonalizable.

We calculate that A has characteristic polynomial

$$\chi_A(\lambda) = -(\lambda + 9)(\lambda - 36)(\lambda - 18),$$

so its eigenvalues are -9, 36 and 18. Using row reduction, we find a nonzero solution $\mathbf{x}$ to $(A + 9I)\mathbf{x} = \mathbf{0}$ (that is, an eigenvector with eigenvalue -9); one such is $\begin{pmatrix} 2 \\ 1 \\ 2 \end{pmatrix}$. Normalizing so that it has length 1 gives the eigenvector $\begin{pmatrix} 2/3 \\ 1/3 \\ 2/3 \end{pmatrix}$. Similarly, we find unit-length eigenvectors $\begin{pmatrix} -2/3 \\ 2/3 \\ 1/3 \end{pmatrix}$ and $\begin{pmatrix} 1/3 \\ 2/3 \\ -2/3 \end{pmatrix}$ with eigenvalues 36 and 18, respectively. The theory tells us that these last three vectors are orthonormal (and one can check this directly). Put

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

Then P is orthogonal and $P^T AP = D$, where $D = \operatorname{diag}(-9, 36, 18)$.

It follows that $A = PDP^T = PDP^{-1}$. Hence

$$\begin{aligned} A^{99} &= (PDP^{-1})(PDP^{-1}) \cdots (PDP^{-1}) = PD^{99}P^{-1} \\ &= \begin{pmatrix} 2/3 & -2/3 & 1/3 \\ 1/3 & 2/3 & 2/3 \\ 2/3 & 1/3 & -2/3 \end{pmatrix} \begin{pmatrix} (-9)^{99} & 0 & 0 \\ 0 & 36^{99} & 0 \\ 0 & 0 & 18^{99} \end{pmatrix} \begin{pmatrix} 2/3 & 1/3 & 2/3 \\ -2/3 & 2/3 & 1/3 \\ 1/3 & 2/3 & -2/3 \end{pmatrix} \end{aligned}$$

by cancelling and using the fact that $P^{-1} = P^T$. Multiplying this out, we conclude that A^{99} is equal to

$$\frac{1}{9} \begin{pmatrix} 4 \cdot (-9)^{99} + 4 \cdot 36^{99} + 18^{99} & 2 \cdot (-9)^{99} - 4 \cdot 36^{99} + 2 \cdot 18^{99} & 4 \cdot (-9)^{99} - 2 \cdot 36^{99} - 2 \cdot 18^{99} \\ 2 \cdot (-9)^{99} - 4 \cdot 36^{99} + 2 \cdot 18^{99} & (-9)^{99} + 4 \cdot 36^{99} + 4 \cdot 18^{99} & 2 \cdot (-9)^{99} + 2 \cdot 36^{99} - 4 \cdot 18^{99} \\ 4 \cdot (-9)^{99} - 2 \cdot 36^{99} - 2 \cdot 18^{99} & 2 \cdot (-9)^{99} + 2 \cdot 36^{99} - 4 \cdot 18^{99} & 4 \cdot (-9)^{99} + 36^{99} + 4 \cdot 18^{99} \end{pmatrix}.$$

Of course, what we've really just done is found a formula for A^n for all positive integers n.

We can use the same technique to find the powers of any diagonalizable matrix. In this example, our matrix was *orthogonally* diagonalizable (that is, symmetric), which made it very easy to find the inverse of P: it's just the transpose. But we already have an algorithm for calculating inverses (as in Section D2), so we could have found P^{-1} anyway, even if P hadn't been orthogonal.

* * *