Common Notation

Symbol	Meaning	Reference
$\mathbb{R}$	the set of real numbers	1
$\in$	is an element of	1.1
$\mathbb{Q}$	the set of rational numbers	1.1
$\mathbb{Z}$	the set of integers	1.1
$\mathbb{N}$	the set of natural numbers	1.1
$\mathbb{Z}/n\mathbb{Z}$	the set of integers modulo n	1.1
$\mathbb{F}_p$	the finite field of order p	1.1
$\mathbb{C}$	the set of complex numbers	1.2
$\overline{z}$	complex conjugation	1.2
$\lvert z\rvert$	complex modulus or absolute value	1.2
$\overrightarrow{AB}$	vector from A to B	2.1
O	Origin	2.1
$\mathbb{R}^2$	The Cartesian plane	2.1
$\mathbb{R}^3$	Euclidean Threespace	2.1
$\mathbb{R}^n$	Real n-dimensional space	2.2
$\mathbb{F}^n$	The space of n-dimensional vectors over $\mathbb{F}$	2.2
V	a vector space	2.3
$\mathbf{0}$	The zero vector	2.3
$\mathbf{v}, \mathbf{w}$	vectors	2.3

Contents

1 Fields

From calculus we should be used to working with the real numbers, which we denote $\mathbb{R}$. We're used enough to them that we don't really think about them a lot, honestly. But the real numbers aren't the only kind of numbers out there, and we want flexibility to consider other kinds as well. So we want to describe the important properties of the real numbers that we use frequently, and then see what else has those properties.

1.1 Introduction to Fields

Definition 1.1. Suppose $\mathbb{F}$ is a set with two binary operations, $+$ and $\times$. We say $\mathbb{F}$ is a *field* if it satisfies the following axioms:

(a) (Closure) If $x, y \in \mathbb{F}$ then $x + y, xy \in \mathbb{F}$.

(b) (Commutativity) $x + y = y + x$ and $xy = yx$ for all $x, y \in \mathbb{F}$.

(c) (Associativity) $(x + y) + z = x + (y + z)$ and $(xy)z = x(yz)$ for all $x, y, z \in \mathbb{F}$.

(d) (Identities) There is an element $0 \in \mathbb{F}$ such that $x + 0 = x$ for all $x \in \mathbb{F}$. There is an element $1 \in \mathbb{F}$ such that $1x = x$ for all $x \in \mathbb{F}$.

(e) (Inverses) For every $x \in \mathbb{F}$ there is a $-x \in \mathbb{F}$ such that $x + (-x) = 0$. For every non-zero $x \in \mathbb{F}$ there is an element $x^{-1} \in \mathbb{F}$ such that $xx^{-1} = 1$.

(f) (Distributivity) $x(y + z) = xy + xz$ for all $x, y, z \in \mathbb{F}$.

Remark 1.2. The real numbers, of course, have more properties than this—barely. The real numbers are the unique *complete ordered* field. "Ordered" means that if we have two distinct real numbers, we can say which one is bigger. "Complete" means that it's good for doing calculus. Neither of those properties will be important in this course very often, so we will be able to do almost everything over "fields" in general.

Example 1.3. The set $\mathbb{Q}$ of rational numbers is a field. The sets $\mathbb{R}$ and $\mathbb{C}$ of real and complex numbers are fields.

The set $\mathbb{Z}$ of integers is not a field, because it does not have multiplicative inverses. (We call this set a *ring*).

The set $\mathbb{N}$ of natural numbers is not a field. It does not have multiplicative or additive inverses.

The set $\mathbb{Z}/n\mathbb{Z}$ of integers modulo n is is a field if n is prime, and is not a field if n is composite. We sometimes call these the *finite fields* $\mathbb{Z}/p\mathbb{Z}$ or $\mathbb{F}_p$. These may come up from time to time in this course.

Example 1.4. Consider specifically the set $\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z} = \{0, 1\}$, the integers mod 2. We have the operations

$$\begin{array}{lll} 0+0=0 & 0+1=1+0=1 & 1+1=0 \\ 0\times 0=0 & 0\times 1=1\times 0=0 & 1\times 1=1. \end{array}$$

We can check the field axioms and see this is a field.

Proposition 1.5. *Let $\mathbb{F}$ be a field. For all $a, b, c \in \mathbb{F}$, we have*

(a) (Cancellation of addition) If $a + b = a + c$, then $b = c$.

(b) (Cancellation of multiplication) If $a \cdot b = a \cdot c$ and $a \neq 0$, then $b = c$.

(c) $a \cdot 0 = 0$.

(d) $(-a) \cdot b = a \cdot (-b) = -(a \cdot b)$.

(e) $(-a) \cdot (-b) = a \cdot b$.

But the two main examples we will see in this course are the *real numbers* and the *complex numbers*. We'll assume you're familiar with the real numbers from calculus, so we won't talk to much more about their specific properties. But we do need to do a quick overview of the complex numbers.

1.2 The complex numbers

Definition 1.6. A *complex number* is a number $z = a + bi$ where $a, b \in \mathbb{R}$. We say that $a = \Re(z)$ is the *real part* and $b = \Im(z)$ is the *imaginary part*. The set of all complex numbers is $\mathbb{C} = \{a + bi : a, bin\mathbb{R}\}$.

We can add complex numbers in the obvious way. We can also multiply them, once we take the rule that $i^2 = -1$.

$$\begin{aligned}(a+bi)+(c+di) &= (a+c)+(b+d)i \\ (a+bi)(c+di) &= ac+adi+bci+bdi^2 \\ &= ac+adi+bci+bd(-1) \\ &= (ac-bd)+(ad+bc)i\end{aligned}$$

Example 1.7. Let $z = 3 - i$ and $w = \pi + 4i$. Then $z + w = 3 + pi + 3i$, and

$$zw = (3-i)(\pi+4i) = 3\pi + 4 + (12-\pi)i.$$

We want to check that $\mathbb{C}$ is also a field, which means we need to check the six properties in definition 1.1. We just showed that addition and multiplication are closed; most of the properties are very easy to check, given that we know that the *real numbers* have those properties.

Proposition 1.8 (Commutativity of complex numbers)**.** *If $z, w \in \mathbb{C}$, then $z + w = w + z$ and $zw = wz$.*

Proof. Let $z = a + bi$ and $w = c + di$. Then

$$\begin{aligned}z+w &= (a+bi)+(c+di) = (a+c)+(b+d)i \\ w+z &= (c+di)+(a+bi) = (c+a)+(d+b)i \\ &= (a+c)+(b+d)i && \text{by additive commutatitivity}\end{aligned}$$

Similarly,

$$\begin{aligned}zw &= (a+bi)(c+di) = (ac-bd)+(ad+bc)i \\ wz &= (c+di)(a+bi) = (ca-db)+(cb+da)i \\ &= (ac-bd)+(bc+ad)i && \text{by multiplicative commutativity} \\ &= (ac-bd)+(ad+bc)i && \text{by additive commutativity.}\end{aligned}$$

□

The important thing to notice about this proof, as a matter of proof technique, is that we don't need to do anything weird and fancy, or special to the complex numbers, to check these properties. We're just using the fact that the complex numbers are made up of real numbers, and we know the real numbers are a field. We'll use this approach constantly throughout the semester.

But there's one property that isn't trivial: multiplicative inverses. How do we *divide* by a complex number? We can start by defining a useful operation:

Definition 1.9. Let $z = a + bi$. Then the *complex conjugate* of z is the complex number $\overline{z} = a - bi$.

This complex conjugate has a number of useful properties, but the one we're interested in here is that

$$z\overline{z} = (a + bi)(a - bi) = a^2 + b^2 + (ab - ab)i = a^2 + b^2,$$

which is a real number. And we know how to divide by real numbers!

So if $z = a + bi \in \mathbb{C}$ is not zero, then we can define a new number

$$w = \frac{\overline{z}}{z\overline{z}} = \frac{a - bi}{a^2 + b^2} = \frac{a}{a^2 + b^2} - \frac{b}{a^2 + b^2}i.$$

This is a complex number since $\frac{a}{a^2+b^2}, \frac{-b}{a^2+b^2} \in \mathbb{R}$, and we can check that

$$\begin{aligned} zw &= (a + bi)\left(\frac{a}{a^2 + b^2} - \frac{b}{a^2 + b^2}i\right) \\ &= \left(\frac{a^2}{a^2 + b^2} + \frac{b^2}{a^2 + b^2}\right) + \left(\frac{ab}{a^2 + b^2} - \frac{ab}{a^2 + b^2}\right)i \\ &= \frac{a^2 + b^2}{a^2 + b^2} + 0i = 1 + 0i. \end{aligned}$$

Example 1.10. We'll still take $z = 3 - i$ and $w = \pi + 4i$. Then $\overline{z} = 3 + i$, and

$$z^{-1} = \frac{\overline{z}}{z\overline{z}} = \frac{3 + i}{3^2 + 1^1} = \frac{3}{10} + \frac{i}{10}.$$

So we can compute

$$\begin{aligned} \frac{w}{z} &= (\pi + 4i)\left(\frac{3}{10} + \frac{i}{10}\right) \\ &= \frac{3\pi}{10} - \frac{4}{10} + \left(\frac{12}{10} + \frac{\pi}{10}\right)i \\ &= \frac{3\pi - 4}{10} + \frac{12 - \pi}{10}i. \end{aligned}$$

Proposition 1.11 (Properties of the complex conjugate)**.** *Let $z, w \in \mathbb{C}$. Then:*

(a) $\overline{\overline{z}} = z$.

(b) $\overline{z + w} = \overline{z} + \overline{w}$.

(c) $\overline{zw} = \overline{z} \cdot \overline{w}$.

(d) $\overline{\left(\frac{z}{w}\right)} = \frac{\overline{z}}{\overline{w}}$ *if* $w \neq 0$.

(e) z *is a real number if and only if* $\overline{z} = z$.

Proof. The proofs of (b) and (c) are in the book, so we'll prove the other parts.

(a) Let $z = a + bi$. Then $\overline{z} = a - bi$ and so $\overline{\overline{z}} = a - (-b)i = a + bi = z$.

(d) Let $z = a + bi$ and $w = c + di$ where $w \neq 0$. Then we can compute

$$\begin{aligned}\overline{\left(\frac{z}{w}\right)} &= \overline{\left(\frac{a+bi}{c+di}\right)} = \overline{\left(\frac{(a+bi)(c-di)}{c^2+d^2}\right)} \\ &= \overline{\left(\frac{ac+bd}{c^2+d^2} + \frac{-ad+bc}{c^2+d^2}i\right)} \\ &= \frac{ac+bd}{c^2+d^2} + \frac{ad-bc}{c^2+d^2}i.\end{aligned}$$

But we can also compute out the other side, and see

$$\begin{aligned}\frac{\overline{z}}{\overline{w}} = \frac{a-bi}{c-di} &= \frac{(a-bi)(c+di)}{c^2+d^2} \\ &= \frac{(ac+bd)+(ad-bc)i}{c^2+d^2}.\end{aligned}$$

and so $\overline{\left(\frac{z}{w}\right)} = \frac{\overline{z}}{\overline{w}}$.

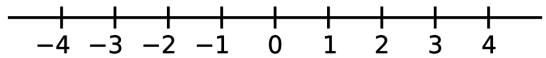
(e) If z is real, then $z = a + 0i$ for some $c \in \mathbb{R}$. Then $\overline{z} = a - 0i = a + 0i = z$.

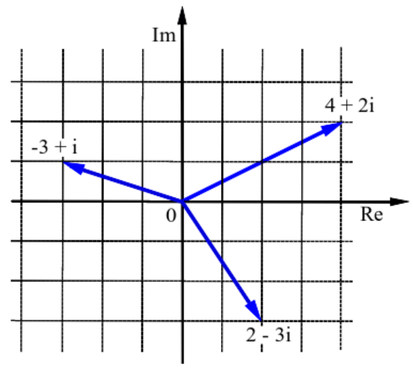
Conversely, suppose $z = a + bi$ and $z = \overline{z}$. We know that $\overline{z} = a - bi$, so we have $a + bi = a - bi$. This implies that $bi = -bi$ and thus that $b = -b$, so $b = 0$. Thus $z = a + 0i \in \mathbb{R}$.

□

One of the lenses this course will keep returning to is the idea of geometry, and a little of that can help us right now. If we have a pair of real numbers, we can graph it on a plane, using the first number for the horizontal coordinate and the second number for the vertical coordinate. But a complex number $z = a + bi$ is a pair of real numbers. And that means that, just like we can think of the real numbers as forming a line:

we can think of the complex numbers as forming a plane:





We'll return to this geometric picture soon, but for right now I want to think about distance. You can see each complex number implies a right triangle, so we can find the distance from the origin $0 + 0i$ with the Pythagorean Theorem. If $z = a + bi$ the lengths of these sides are just a and b, so we have

Definition 1.12. Let $z = a + bi$ where $a, b \in \mathbb{R}$. The *absolute value* or *modulus* of z is

$$|z| = \sqrt{a^2 + b^2}.$$

Conveniently we can compute this in terms of more fundamental operations, because we saw that $z \cdot \overline{z} = a^2 + b^2$. Thus $|z| = \sqrt{z\overline{z}}$.

We can derive the following properties for the complex absolute value:

Proposition 1.13. *Let $z, w \in \mathbb{C}$. Then*

(a) $|zw| = |z| \cdot |w|$.

(b) $\left|\frac{z}{w}\right| = \frac{|z|}{|w|}$ *if* $w \neq 0$.

(c) $|z + w| \leq |z| + |w|$ *(Triangle Inequality).*

(d) $|z| - |w| \leq |z + w|$ *(Reverse Triangle Inequality).*

2 Vector Spaces

In this course we want to study "high-dimensional spaces" and "vectors". That's not very specific, though, until we explain exactly what we mean by those things.

An important idea of this course is that it is helpful to study the same things from more than one perspective; sometimes a question that is difficult from one perspective is easy from another, so the ability to have multiple viewpoints and translate between them is extremely useful.

In this course we will take three different perspectives, which I am calling "geometric", "algebraic", and "formal". The first involves spatial reasoning and pictures; the second involves arithmetic and algebraic computations; the third involves formal definitions and properties.

A common definition of a vector is "something that has size and direction." This is a *geometric* viewpoint, since it calls to mind a picture. We can also view it from an *algebraic* point of view by giving it a set of coordinates. For instance, we can specify a two-dimensional vector by giving a pair of real numbers (x, y), which tells us where the vector points from the origin at $(0, 0)$.

The formal perspective is the most abstract and sometimes the most confusing, but often the most fruitful. This is the approach we took in section 1.1 when we defined a field: there, we took the properties the real numbers satisfy, and looked for other types of numbers that work the same way. Here we're going to start with the "ordinary" types of vectors we see in physics or in multivariable calculus, and abstract out their properties.

In the table below I have several concepts, and ways of thinking about them in each perspective. It's fine if you don't know what some of these things mean, especially in the "formal" column; if you knew all of this already you wouldn't need to take this course.

Geometric	Algebraic	Formal
size and direction	n-tuples	vectors
consecutive motion	pointwise addition	vector addition
stretching, rotations, reflections	matrices	linear functions
number of independent directions	number of coordinates	dimension
plane	system of linear equations	subspace
angle	dot product	inner product
Length	magnitude	norm

2.1 Motivation: Geometric Vectors

You should be familiar with the *Cartesian plane* from high school geometry. (It is named after the French mathematician René Descartes, who is credited with inventing the idea of putting numbered cordinates on the plane.)

As probably looks familiar from high school geometry, given two points A and B in the plane, we can write $\overrightarrow{AB}$ for the vector with *initial point* A and *terminal point* B.

Since a vector is just a length and a direction, the vector is "the same" if both the initial and terminal points are shifted by the same amount. If we fix an *origin* point O, then any point A gives us a vector $\overrightarrow{OA}$. Any vector can be shifted until its initial point is O, so each vector corresponds to exactly one point. We call this *standard position*.

We represent points algebraically with pairs of real numbers, since points in the plane are determined by two coordinates. We use $\mathbb{R}^2 = \{(x, y) : x, y \in \mathbb{R}\}$ to denote the set of all ordered pairs of real numbers; thus $\mathbb{R}^2$ is an algebraic description of the Cartesian plane. (We use $\mathbb{R}$ to denote the set of real numbers, and the superscript ^{2} tells us that we need two of them). We define the origin O to be the "zero" point $(0, 0)$.

Definition 2.1. If $A = (x, y)$ is a point in $\mathbb{R}^2$, then we denote the vector $\overrightarrow{OA}$ by $\begin{bmatrix} x \\ y \end{bmatrix}$.

We can do something very similar with threespace.

Definition 2.2. We define *Euclidean threespace* to be the three-dimensional space described by three real coordinates. We notate it $\mathbb{R}^3$. The point $(0, 0, 0)$ is called the *origin* and often notated O.

If $A = (x, y, z)$ is a point, then the vector $\overrightarrow{OA}$ is denoted $\begin{bmatrix} x \\ y \\ z \end{bmatrix}$.

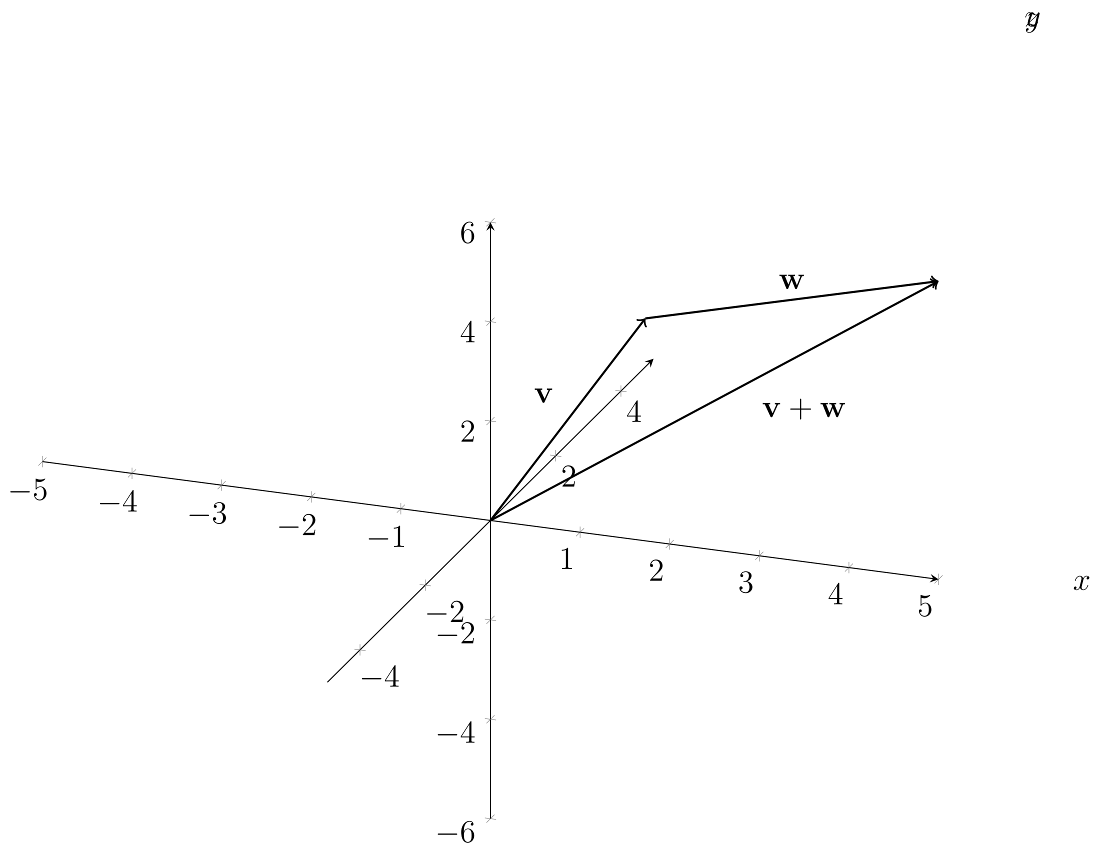
There are two operations we can do on these vectors:

(a) We can *add* two vectors together. Geometrically, this corresponds to following one vector and then the other; you can picture this as laying them tip-to-tail. Algebraically, we just add the coordinates.

(b) We can *multiply* a vector by a *scalar*. Geometrically corresponds to stretching a vector by some factor. Algebraically we just multiply each coordinate by the scalar.

Example 2.3. Let $\mathbf{v} = \begin{bmatrix} 1 \\ 2 \\ 3 \end{bmatrix}$ and $w = \begin{bmatrix} 4 \\ -2 \\ 3 \end{bmatrix}$. Then

$$\mathbf{v} + \mathbf{w} = \begin{bmatrix} 5 \\ 0 \\ 6 \end{bmatrix}, \quad 3 \cdot \mathbf{v} = \begin{bmatrix} 3 \\ 6 \\ 9 \end{bmatrix}, \text{ and } \quad (-2) \cdot \mathbf{w} = \begin{bmatrix} -8 \\ 4 \\ -6 \end{bmatrix}.$$



2.2 An Algebraic Generalization

There are two straightforward ways we can generalize our Cartesian space $\mathbb{R}^3$. The most obvious is just to replace the 3 with a 4, or a 5, or a 6. If $\mathbb{R}^2$ is ordered pairs of real numbers, and $\mathbb{R}^3$ is ordered triples, then $\mathbb{R}^n$ is ordered n-tuples.

Definition 2.4. We define *real n-dimensional space* to be the set of n-tuples of real numbers, $\mathbb{R}^n = \{(x_1, x_2, \ldots, x_n) : x_i \in \mathbb{R}\}$.

By "abuse of notation" we will also use $\mathbb{R}^n$ to refer to the set of vectors in $\mathbb{R}^n$. We define scalar multiplication and vector addition by

$$r \cdot \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix} = \begin{bmatrix} rx_1 \\ rx_2 \\ \vdots \\ rx_n \end{bmatrix} \qquad \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix} + \begin{bmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{bmatrix} = \begin{bmatrix} x_1 + y_1 \\ x_2 + y_2 \\ \vdots \\ x_n + y_n \end{bmatrix}.$$

Example 2.5. Let $\mathbf{v} = \begin{bmatrix} 1 \\ 3 \\ 2 \\ 4 \end{bmatrix}$ and $\mathbf{w} = \begin{bmatrix} 5 \\ -1 \\ 2 \\ 8 \end{bmatrix}$ be vectors in $\mathbb{R}^4$. Then

$$\mathbf{v} + \mathbf{w} = \begin{bmatrix} 1 \\ 3 \\ 2 \\ 4 \end{bmatrix} + \begin{bmatrix} 5 \\ -1 \\ 2 \\ 8 \end{bmatrix} = \begin{bmatrix} 6 \\ 2 \\ 4 \\ 12 \end{bmatrix}, \quad -3 \cdot \mathbf{v} = \begin{bmatrix} -3 \\ -9 \\ -6 \\ -12 \end{bmatrix}.$$

The other way we can generalize this is to not work over the real numbers. The real numbers are a good model for every-day geometry, so we started there. But *algebraically* we could do all of these same operations with any other field.

Definition 2.6. Let $\mathbb{F}$ be any field. Then $\mathbb{F}^n = \{(x_1, x_2, \ldots, x_n) : x_i \in \mathbb{F}\}$ is the set of ordered n-ples over $\mathbb{F}$. We then define scalar multiplication and vector addition by

$$r \cdot \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix} = \begin{bmatrix} rx_1 \\ rx_2 \\ \vdots \\ rx_n \end{bmatrix} \qquad \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix} + \begin{bmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{bmatrix} = \begin{bmatrix} x_1 + y_1 \\ x_2 + y_2 \\ \vdots \\ x_n + y_n \end{bmatrix}.$$

Notice that definition 2.6is *exactly* the same as definition 2.4, except we don't specify what the field is.

Example 2.7. Let $\mathbf{v} = (3 + i, 1, 2i)$ and $\mathbf{w} = (2, 5i, 4 - 2i)$ be vectors in $\mathbb{C}^3$. Then

$$\mathbf{v} + \mathbf{w} = (5 + i, 1 + 5i, 4)$$
$$(2 - i)\mathbf{v} = (7 - i, 2 - i, 2 + 4i).$$

Notice that the scalar is a complex number, because we're working over $\mathbb{C}$.

Example 2.8. Let $\mathbf{v} = (1, 2, 3)$ and $\mathbf{w} = (3, 4, 1)$ be vectors in $\mathbb{F}_5$. Then

$$\begin{aligned} \mathbf{v} + \mathbf{w} &= (4, 1, 4) \\ 2\mathbf{v} &= (2, 4, 1). \end{aligned}$$

Our scalar is indeed an element of $\mathbb{F}_5$, and all the arithmetic is being done mod 5.

2.3 Defining Vector Spaces

We want to figure out what properties we're actually using to work with these sets of vectors. Obviously, we have a set of vectors, and a set of scalars; and we have two operations, addition and scalar multiplication. These operations also behave "nicely", following all of the rules in this long and tedious definition:

Definition 2.9. Let $\mathbb{F}$ be a field, and V be a set, together with two operations:

- A *vector addition* which allows you to add two elements of V and get a new element of V. If $\mathbf{v}, \mathbf{w} \in V$ then the sum is denoted $\mathbf{v} + \mathbf{w}$ and must also be an element of V.
- A *scalar multiplication* which allows you to multiply an element of V by a "scalar" element of $\mathbb{F}$ and get a new element of V. If $a \in \mathbb{F}$ and $\mathbf{v} \in V$ then the scalar multiple is denoted $a \cdot \mathbf{v}$ and must also be an element of V.

Further, suppose the following axioms hold for any $\mathbf{u}, \mathbf{v}, \mathbf{w} \in V$, and any $a, b \in \mathbb{F}$:

(a) (Closure under addition) $\mathbf{u} + \mathbf{v} \in V$

(b) (Closure under scalar multiplication) $a\mathbf{u} \in V$

(c) (Additive commutativity) $\mathbf{u} + \mathbf{v} = \mathbf{v} + \mathbf{u}$

(d) (Additive associativity) $(\mathbf{u} + \mathbf{v}) + \mathbf{w} = \mathbf{u} + (\mathbf{v} + \mathbf{w})$

(e) (Additive identity) There is an element $\mathbf{0} \in V$ called the "zero vector", such that $\mathbf{u} + \mathbf{0} = \mathbf{u}$ for every $\mathbf{u}$.

(f) (Additive inverses) For each $\mathbf{u} \in V$ there is another element $-\mathbf{u} \in V$ such that $\mathbf{u} + (-\mathbf{u}) = \mathbf{0}$.

(g) (Distributivity) $a(\mathbf{u} + \mathbf{v}) = a\mathbf{u} + a\mathbf{v}$

(h) (Distributivity) $(a + b)\mathbf{u} = a\mathbf{u} + b\mathbf{u}$

(i) (Multiplicative associativity) $a(b\mathbf{u}) = (ab)\mathbf{u}$

(j) (Multiplicative Identity) $1\mathbf{u} = \mathbf{u}$.

Then we say V is a *Vector Space* over $\mathbb{F}$, and we call its elements *vectors*.

Remark 2.10. Technically, those first two axioms are superfluous; if you can add two elements, you can add two elements and also get something. But they still need to be true: if adding two vectors doesn't give you another vector, you don't have a vector space. And we have to check them to make sure our vector space definition makes sense.

Example 2.11. $\mathbb{F}^n$ is a vector space, with the previously defined vector addition and scalar multiplication. We check:

Let $\mathbf{u} = (u_1, \dots, u_n).\mathbf{v} = (v_1, \dots, v_n), \mathbf{w} = (w_1, \dots, w_n) \in \mathbb{F}^n, \quad r, s \in \mathbb{F}$. Then, knowing the usual rules of commutativity and associativity of basic arithmetic, we can compute:

(a) $\mathbf{u} + \mathbf{v} = (u_1, \dots, u_n) + (v_1, \dots, v_n) = (u_1 + v_1, \dots, u_n + v_n) \in \mathbb{F}^n$.

(b)
$$r\mathbf{u} = r(u_1, \dots, u_n) = (ru_1, \dots, ru_n) \in \mathbb{F}.$$

(c)
$$\begin{aligned}\mathbf{u} + \mathbf{v} &= (u_1, \dots, u_n) + (v_1, \dots, v_n) = (u_1 + v_1, \dots, u_n + v_n) \\ &= (v_1 + u_1, \dots, v_n + u_n) = (v_1, \dots, v_n) + (u_1, \dots, u_n) = \mathbf{v} + \mathbf{u}\end{aligned}$$

(d)
$$\begin{aligned}(\mathbf{u} + \mathbf{v}) + \mathbf{w} &= (u_1 + v_1, \dots, u_n + v_n) + (w_1, \dots, w_n) = (v_1 + u_1 + w_1, \dots, v_n + u_n + w_n) \\ &= (v_1, \dots, v_n) + (u_1 + w_1, \dots, u_n + w_n) = \mathbf{v} + (\mathbf{u} + \mathbf{w})\end{aligned}$$

(e) We have $\mathbf{0} = (0, \dots, 0)$. Then
$$\mathbf{0} + \mathbf{v} = (0 + v_1, \dots, 0 + v_n) = (v_1, \dots, v_n) = \mathbf{v}.$$

(f) Set $-\mathbf{u} = (-u_1, \dots, -u_n)$. Then
$$\mathbf{u} + (-\mathbf{u}) = (u_1 + (-u_1), \dots, u_n + (-u_n)) = (0, \dots, 0) = \mathbf{0}.$$

(g)

$$\begin{aligned} r(\mathbf{u}+\mathbf{v}) &= r(u_1+v_1,\dots,u_n+v_n) = (r(u_1+v_1),\dots,r(u_n+v_n)) \\ &= (ru_1+rv_1,\dots,ru_n+rv_n) = (ru_1,\dots,ru_n)+(rv_1,\dots,rv_n) = r\mathbf{u}+r\mathbf{v}. \end{aligned}$$

(h)

$$\begin{aligned} (r+s)\mathbf{u} &= (r+s)(u_1,\dots,u_n) = ((r+s)u_1,\dots,(r+s)u_n) \\ &= (ru_1+su_1,\dots,ru_n+su_n) = (ru_1,\dots,ru_n)+(su_1,\dots,su_n) = r\mathbf{u}+s\mathbf{u}. \end{aligned}$$

(i)

$$r(s\mathbf{u}) = r(su_1,\dots,su_n) = (rsu_1,\dots,rsu_n) = rs(u_1,\dots,u_n).$$

(j)

$$1\mathbf{u} = 1(u_1,\dots,u_n) = (1\cdot u_1,\dots,1\cdot u_n) = (u_1,\dots,u_n) = \mathbf{u}.$$

So what else is a vector space and "looks like $\mathbb{R}^n$"? The most important example in this course will be *matrices*.

Definition 2.12. A *matrix over a field* $\mathbb{F}$ is a rectangular array of elements of $\mathbb{F}$. A matrix with m rows and n columns is *a $m \times n$ matrix*, and we notate the set of all such matrices by $M_{m\times n}(\mathbb{F})$, or just $M_{m\times n}$ if the field is clear from context. .

A $m \times n$ matrix is *square* if $m = n$, that is, it has the same number of rows as columns. We will sometimes represent the set of $n \times n$ square matrices by M_n.

We will generally describe the elements of a matrix with the notation

$$(a_{ij}) = \begin{bmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{bmatrix}.$$

We can define operations on these matrices:

- If $A = (a_{ij})$ is an $m \times n$ matrix over a field $\mathbb{F}$, and $r \in \mathbb{F}$, then we can multiply each entry of the matrix A by the r. This is called *scalar multiplication* and we say that r is a *scalar*.

$$rA = (ra_{ij}) = \begin{bmatrix} ra_{11} & ra_{12} & \dots & ra_{1n} \\ ra_{21} & ra_{22} & \dots & ra_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ ra_{m1} & ra_{m2} & \dots & ra_{mn} \end{bmatrix}.$$

- If $A = (a_{ij})$ and $B = (b_{ij})$ are two $m \times n$ matrices over a field $\mathbb{F}$, we can add the two matrices by adding each individual pair of coordinates together.

$$A + B = (a_{ij} + b_{ij}) = \begin{bmatrix} a_{11} + b_{11} & a_{12} + b_{12} & \dots & a_{1n} + b_{1n} \\ a_{21} + b_{21} & a_{22} + b_{22} & \dots & a_{2n} + b_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} + b_{m1} & a_{m2} + b_{m2} & \dots & a_{mn} + b_{mn} \end{bmatrix}.$$

Example 2.13. The set $M_{m \times n}(\mathbb{F})$ of $m \times n$ matrices is a vector space under the addition and scalar multiplication defined above, with zero vector given by

$$\mathbf{0} = (0) = \begin{bmatrix} 0 & 0 & \dots & 0 \\ 0 & 0 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 0 \end{bmatrix}.$$

I'm not going to prove this, but you can see that it should be true for the same reason FR^{mn} is a vector space: they're both just lists of numbers, but one is arranged in a column and the other in a rectangle. The operations are the same.

Example 2.14. Pick a field $\mathbb{F}$, and let $\mathcal{P}_{\mathbb{F}}(x) = \{a_0 + a_1 x + \dots + a_n x^n : n \in \mathbb{N}, a_i \in \mathbb{F}\}$ be the set of polynomials with coefficients in $\mathbb{F}$. Define addition by

$$(a_0 + a_1 x + \dots + a_n x^n) + (b_0 + b_1 x + \dots + b_n x^n) = (a_0 + b_0) + (a_1 + b_1)x + \dots + (a_n + b_n)x^n$$

and define scalar multiplication by

$$r(a_0 + a_1 x + \dots + a_n x^n) = ra_0 + ra_1 x + \dots + ra_n x^n.$$

Then $\mathcal{P}_{\mathbb{F}}(x)$ is a vector space.

Example 2.15. Fix a field $\mathbb{F}$, and let S be the space of all doubly infinite sequences $\{y_k\} = \{\dots, y_{-2}, y_{-1}, y_0, y_1, y_2, \dots : y_i \in \mathbb{F}\}$. We call this the space of (discrete) *signals*: it represents a sequence of measurements taken at regular time intervals. These sorts of regular measurements are common in engineering and digital information applications (such as digital music).

We define addition and scalar multiplication on the space of signals componentwise, so that

$$\{\dots, x_{-1}, x_0, x_1, \dots\} + \{\dots, y_{-1}, y_0, y_1, \dots\} = \{\dots x_{-1} + y_{-1}, x_0 + y_0, x_1 + y_1, \dots\}$$

and

$$r\{\dots, y_{-1}, y_0, y_1, \dots\} = \{\dots, ry_{-1}, ry_0, ry_1, \dots\}.$$

(In essence, S is composed of vectors that are infinitely long in both directions). Then S is a vector space.

Example 2.16. Let $\mathcal{F}(\mathbb{R}, \mathbb{R}) = \mathcal{F}$ be the set of functions from $\mathbb{R}$ to $\mathbb{R}$—that is, functions that take in a real number and return a real number, the vanilla functions of single-variable calculus. Define addition by $(f + g)(x) = f(x) + g(x)$ and define scalar multiplication by $(rf)(x) = r \cdot f(x)$. Then $\mathcal{F}$ is a vector space. You will prove this is a vector space in your homework.

Example 2.17. The integers $\mathbb{Z}$ are *not* a vector space (under the usual definitions of addition and multiplication). For instance, $1 \in \mathbb{Z}$ but $.5 \cdot 1 = .5 \not\in \mathbb{Z}$.

(We only need to find one axiom that doesn't hold to show that a set is not a vector space, since a vector space must satisfy all the axioms).

Example 2.18. The closed interval $[0, 5]$ is not a vector space (under the usual operations) , since $3, 4 \in [0, 5]$ but $3 + 4 = 7 \not\in [0, 5]$.

Example 2.19. Let $V = \mathbb{R}$ with scalar multiplication given by $r \cdot x = rx$ and addition given by $x \oplus y = 2x + y$. Then V is not a vector space, since $x \oplus y = 2x + y \neq 2y + x = y \oplus x$; in particular, we see that $3 \oplus 5 = 11$ but $5 \oplus 3 = 13$.

There are many more examples of vector spaces, but as you can see it's fairly tedious to prove that any particular thing is a vector space. In section 2.4 we'll develop a *much* easier way to establish that something is a vector space, so we won't develop any more examples now.

2.3.1 Properties of Vector Spaces

The great thing about the formal approach is that we can show that anything that satisfies the axioms of a vector space must aso follow some other rules. We'll establish a few of those rules here, though of course, there's a sense in which the entire rest of this course will be spent establishing those rules.

As before, you shouldn't think of these rules as new facts; all of them are "obvious". The point is that if we get the list of properties from definition 2.9, then all of these other things still have to occur. It's a guarantee that vector spaces behave how we expect—that they all do behave like $\mathbb{F}^n$, or indeed like $\mathbb{R}^3$, in all the ways we will expect.

Proposition 2.20 (Cancellation)**.** *Let V be a vector space and suppose $\mathbf{u}, \mathbf{v}, \mathbf{w} \in V$ are vectors. If $\mathbf{u} + \mathbf{w} = \mathbf{v} + \mathbf{w}$, then $\mathbf{u} = \mathbf{v}$.*

Remark 2.21*.* We stated this law for *fields* earlier; now we're also claiming it holds for *vector spaces*. But the proof is essentially the same in both cases. (This is the shadow of something called "universal algebra"; there are many other algebraic structures we could define, which will all have this same cancellation law for the same reason.)

Proof. By axiom we know that $\mathbf{w}$ has an additive inverse $-\mathbf{w}$. Then we have

$$\begin{aligned}
\mathbf{u} + \mathbf{w} &= \mathbf{v} + \mathbf{w} \\
(\mathbf{u} + \mathbf{w}) + (-\mathbf{w}) &= (\mathbf{v} + \mathbf{w}) + (-\mathbf{w}) \\
\mathbf{u} + (\mathbf{w} + (-\mathbf{w})) &= \mathbf{v} + (\mathbf{w} + (-\mathbf{w})) && \text{Additive associativity} \\
\mathbf{u} + \mathbf{0} &= \mathbf{v} + \mathbf{0} && \text{Additive inverses} \\
\mathbf{u} &= \mathbf{v} && \text{Additive identity.}
\end{aligned}$$

□

Proposition 2.22. *The additive inverse $-\mathbf{v}$ of a vector $\mathbf{v}$ is unique. That is, if $\mathbf{v} + \mathbf{u} = \mathbf{0}$, then $\mathbf{u} = -\mathbf{v}$.*

Proof. Suppose $\mathbf{v} + \mathbf{u} = \mathbf{0}$. By the additive inverses property we know that $\mathbf{v} + (-\mathbf{v}) = \mathbf{0}$, and thus $\mathbf{v} + \mathbf{u} = \mathbf{v} + (-\mathbf{v})$. By cancellation we have $\mathbf{u} = -\mathbf{v}$. □

Remark 2.23*.* In our axioms we asserted that every vector *has* an inverse, but didn't require that there be only one.

Proposition 2.24. *Suppose V is a vector space with $\mathbf{u} \in V$ a vector and $r \in \mathbb{R}$ a scalar. Then:*

(a) $0\mathbf{u} = \mathbf{0}$

(b) $r\mathbf{0} = \mathbf{0}$

(c) $(-1)\mathbf{u} = -\mathbf{u}$.

Remark 2.25*.* We would actually be pretty sad if any of those statements were false, since it would make our notation look very strange. (Especially the last statement). The fact that these statements *are* true justifies us using the notation we use.

Proof. (a)

$$\begin{aligned} \mathbf{u} = 1 \cdot \mathbf{u} &= (0+1)\mathbf{u} && \text{Multiplicative identity} \\ &= 0\mathbf{u} + 1\mathbf{u} && \text{Distributivity} \\ &= 0\mathbf{u} + \mathbf{u} && \text{Multiplicative identity} \\ \mathbf{0} + \mathbf{u} &= 0\mathbf{u} + \mathbf{u} && \text{Additive identity} \\ \mathbf{0} &= 0\mathbf{u} && \text{Cancellation} \end{aligned}$$

(b) We know that $\mathbf{0} = \mathbf{0}+\mathbf{0}$ by additive identity, so $r\mathbf{0} = r(\mathbf{0}+\mathbf{0}) = r\mathbf{0}+r\mathbf{0}$ by distributivity. Then we have

$$\begin{aligned} \mathbf{0} + r\mathbf{0} &= r\mathbf{0} + r\mathbf{0} && \text{additive identity} \\ \mathbf{0} &= r\mathbf{0} && \text{cancellation.} \end{aligned}$$

(c) We have

$$\begin{aligned} \mathbf{v} + (-1)\mathbf{v} &= 1\mathbf{1} + (-1)\mathbf{v} && \text{multiplicative inverses} \\ &= (1 + (-1))\mathbf{v} && \text{distributivity} \\ &= 0\mathbf{v} = \mathbf{0}. \end{aligned}$$

Then by uniqueness of additive inverses, we have $(-1)\mathbf{v} = -\mathbf{v}$.

□

Example 2.26. We'll give one last example of a vector space, which is both important and silly.

We define the *zero vector space* to be the set $\{\mathbf{0}\}$ with addition given by $\mathbf{0}+\mathbf{0} = \mathbf{0}$ and scalar multiplication given by $r \cdot \mathbf{0} = \mathbf{0}$. It's easy to check that this is in fact a vector space.

Notice that we didn't ask what "kind" of object this is; we just said it has the zero vector and nothing else. As such, this could be the zero vector of any vector space at all. In section 2.4 we will talk about vector spaces that fit inside other vector spaces, like this one.

2.4 Vector Space Subspaces

Our very first two examples of a vector space were the Cartesian plane and Euclidean three-space. But we see that while we can think of them as totally distinct vector spaces, the plane sits *inside* threespace, as a subset. In fact it sits inside it in a number of different ways; we can start by taking the xy plane, the xz plane, or the yz plane.

Definition 2.27. Let V be a vector space. A subset $W \subseteq V$ is a *subspace* of V if W is also a vector space with the same operations as V.

Example 2.28. The Cartesian plane $\mathbb{R}^2$ is a subset of threespace $\mathbb{R}^3$. Similarly the line $\mathbb{R}^1$ is a subset of the plane $\mathbb{R}^2$. (And we can stack this up as high as we want; $\mathbb{R}^7 \subseteq \mathbb{R}^8$.

In general, if $n < m$ then $\mathbb{F}^n$ is a subspace of $\mathbb{F}^m$.

Example 2.29.

Example 2.30. Let $V = \mathbb{R}^3$ and let $W = \{(x, y, x+y) \in \mathbb{R}^3\}$. Geometrically, this is a plane (given by $z = x + y$). We could in fact write $W = \{(x, y, z) : z = x + y\}$; this is a more useful way to write it for multivariable calculus, but less useful for lienar algebra. W is certainly a subset of V, so we just need to figure out if W is a subspace.

We could do this by checking all ten axioms, but that would take a very long time; we want a better tool. And it seems like we should be able to avoid a lot of that work since we *already* know many of the axioms hold in $\mathbb{R}^3$.

In fact, one major reason to care about subspaces is that it allows us to avoid a lot of work. If $W \subseteq V$, it seems like most of the vector space axioms should hold *automatically*. After all, if elements of V add commutatively, and elements of W are in V, then the elements of W must add commutatively. And in fact there's very little we have to check.

Proposition 2.31. *Let V be a vector space over a field $\mathbb{F}$ and $W \subseteq V$. Then W is a subspace of V if and only if the following three "subspace" conditions hold:*

(a) $\mathbf{0} \in W$ *(zero vector);*

(b) Whenever $\mathbf{u}, \mathbf{v} \in W$ *then* $\mathbf{u} + \mathbf{v} \in W$ *(Closed under addition); and*

(c) Whenever $r \in \mathbb{F}$ *and* $\mathbf{u} \in W$ *then* $r\mathbf{u} \in W$ *(Closed under scalar multiplication).*

Proof. Suppose W is a subspace of V. Then W is a vector space, so it contains a zero vector and is closed under addition and multiplication by the definition of vector spaces.

Conversely, suppose $W \subseteq V$ and the three subspace conditions hold. We need to check the ten axioms of a vector space. But most of these properties are inherited from the fact that any element of W is also an element of V, and W has the same operations as V. The only really non-trivial one is that the additive inverse exists.

Let $\mathbf{u}, \mathbf{v}, \mathbf{w} \in W$ (and thus $\mathbf{u}, \mathbf{v}, \mathbf{w} \in V$), and $r, s \in \mathbb{F}$.

(a) W is closed under addition by hypothesis.

(b) W is closed under scalar multiplication by hypothesis.

(c) $\mathbf{u} + \mathbf{v} = \mathbf{v} + \mathbf{u}$ since V is a vector space.

(d) $(\mathbf{u} + \mathbf{v}) + \mathbf{w} = \mathbf{u} + (\mathbf{v} + \mathbf{w})$ since V is a vector space.

(e) $\mathbf{0} \in W$ by hypothesis, and $\mathbf{u} + \mathbf{0} = \mathbf{u}$ since V is a vector space.

(f) $-\mathbf{u} = (-1)\mathbf{u} \in W$ by closure under scalar multiplication.

(g) $r(\mathbf{u} + \mathbf{v}) = r\mathbf{u} + r\mathbf{v}$ since V is a vector space.

(h) $(r + s)\mathbf{u} = r\mathbf{u} + s\mathbf{u}$ since V is a vector space.

(i) $(rs)\mathbf{u} = r(s\mathbf{u})$ since V is a vector space.

(j) $1\mathbf{u} = \mathbf{u}$ since V is a vector space.

Thus W satisfies the axioms of a vector space, and is itself a vector space. □

Example 2.32 (Continued)**.** Let's continute to take $V = \mathbb{R}^3$ and $W = \{(x, y, x + y) \in \mathbb{R}^3\}$. To show that W is a subspace of V we only need to check three things.

If $(x_1, y_1, x_1 + y_1), (x_2, y_2, x_2 + y_2) \in W$ then

$$\begin{bmatrix} x_1 \\ y_1 \\ x_1 + y_1 \end{bmatrix} + \begin{bmatrix} x_2 \\ y_2 \\ x_2 + y_2 \end{bmatrix} = \begin{bmatrix} x_1 + x_2 \\ y_1 + y_2 \\ (x_1 + x_2) + (y_1 + y_2) \end{bmatrix} \in W.$$

If $r \in \mathbb{R}$, then

$$r \begin{bmatrix} x \\ y \\ x + y \end{bmatrix} = \begin{bmatrix} rx \\ ry \\ (rx) + (ry) \end{bmatrix} \in W.$$

And the zero vector is

$$\begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 + 0 \end{bmatrix} \in W.$$

Thus W is a subspace of V.

Example 2.33. If V is a vector space, then 0 and V are both subspaces of V. We don't actually need to check anything here, since both are clearly subsets of V, and both are already known to be vector spaces.

(When we want to ignore this possibility we will refer to "proper" or "nontrivial" subspaces, which are neither the trivial space nor the entire space).

Example 2.34. Let $V = \mathbb{R}^2$ and let $W = \{(x, x^2)\} = \{(x, y) : y = x^2\} \subseteq V$. Then W is *not* a subspace.

W does in fact contain the zero vector $(0, 0) = (0, 0^2)$. But we see that $(1, 1) \in W$, and $(1, 1) + (1, 1) = (2, 2) \notin W$. Thus W is not a subspace.

Example 2.35. Let $V = \mathbb{F}_3^2$ and let $W = \{(0, 0), (1, 2), (2, 1)\} \subset V$. Is W a subspace?

It's easy to see that $\mathbf{0} = (0, 0) \in W$. We just need to check it's closed under addition and scalar multiplication.

It's a little hard to check this without just testing elements. But we compute:

$$\begin{aligned} (0,0) + (0,0) &= (0,0) \in W & (0,0) + (1,2) &= (1,2) \in W \\ (0,0) + (2,1) &= (2,1) \in W & (1,2) + (1,2) &= (2,1) \in W \\ (1,2) + (2,1) &= (0,0) \in W & (2,1) + (2,1) &= (1,2) \in W. \end{aligned}$$

And similarly

$$\begin{aligned} 0 \cdot (0,0) &= (0,0) \in W & 0 \cdot (1,2) &= (0,0) \in W & 0 \cdot (2,1) &= (0,0) \in W \\ 1 \cdot (0,0) &= (0,0) \in W & 1 \cdot (1,2) &= (1,2) \in W & 1 \cdot (2,1) &= (2,1) \in W \\ 2 \cdot (0,0) &= (0,0) \in W & 2 \cdot (1,2) &= (2,1) \in W & 2 \cdot (2,1) &= (1,2) \in W \end{aligned}$$

So W is closed under addition and scalar multiplication, so it's a subspace.

Example 2.36. Let $V = \mathcal{P}(x)$ and let $W = \{a_1 x + \cdots + a_n x^n\} = x\mathcal{P}(x)$ be the set of polynomials with zero constant term. Is W a subspace of V?

(a) The zero polynomial $0 + 0x + \cdots + 0x^n = 0$ certainly has zero constant term, so is in W.

(b) If $a_1 x + \cdots + a_n x^n$ and $b_1 x + \cdots + b_n x^n \in W$, then

$$(a_1 x + \cdots + a_n x^n) + (b_1 x + \cdots + b_n x^n) = (a_1 + b_1)x + \cdots + (a_n + b_n)x^n \in W.$$

Alternatively, we can say that if we add two polynomials with zero constant term, their sum will have zero constant term.

(c) If $r \in \mathbb{R}$ and $a_1 x + \cdots + a_n x^n \in W$, then

$$r\left(a_1 x + \cdots + a_n x^n\right) = (ra_1)x + \cdots + (ra_n)x^n$$

has zero constant term and is in W.

Thus W is a subspace of V.

Example 2.37. Let $V = \mathcal{P}(x)$ and let $W = \{a_0 + a_1 x\}$ be the space of linear polynomials. Then W is a subspace of V.

(a) The zero polynomial $0 + 0x \in W$.

(b) If $a_0 + a_1 x, b_0 + b_1 x \in W$, then $(a_0 + a_1 x) + (b_0 + b_1 x) = (a_0 + b_0) + (a_1 + b_1)x \in W$.

(c) If $r \in \mathbb{R}$ and $a_0 + a_1 x \in W$, then $r(a_0 + a_1 x) = ra_0 + (ra_1)x \in W$.

Example 2.38. Let $V = \mathcal{P}(x)$ and let $W = \{1 + ax\}$ be the space of linear polynomials with constant term 1. Is W a subspace of V?

No, because $0 = 0 + 0x \notin W$.

Exercise 2.39. *Fix a natural number $n \geq 0$. Let $V = \mathcal{P}(x)$ and let $W = \mathcal{P}_n(x) = \{a_0 + a_1 x + \cdots + a_n x^n\}$ be the set of polynomials with degree at most n. Then $\mathcal{P}_n(x)$ is a subspace of $\mathcal{P}(x)$.*

Example 2.40. Let $V = \mathcal{F}(\mathbb{R}, \mathbb{R})$ be the space of functions of one real variable, and let $W = \mathcal{D}(\mathbb{R}, \mathbb{R})$ be the space of differentiable functions from $\mathbb{R}$ to $\mathbb{R}$. Is W a subspace of V?

(a) The zero function is differentiable, so the zero vector is in W.

(b) From calculus we know that the derivative of the sums is the sum of the derivatives; thus the sum of differentiable functions is differentiable. That is, $(f+g)'(x) = f'(x) + g'(x)$.

So if $f, g \in W$, then f and g are differentiable, and thus $f + g$ is differentiable and thus in W.

(c) Again we know that $(rf)'(x) = rf'(x)$. If f is in W, then f is differentiable. Thus rf is differentiable and therefore in W.

Example 2.41. Let $V = \mathcal{F}(\mathbb{R}, \mathbb{R})$ and let $W = \mathcal{F}([a, b], \mathbb{R})$ be the space of functions from the closed interval $[a, b]$ to $\mathbb{R}$. We can view W as a subset of V by, say, looking at all the functions that are zero outside of $[a, b]$. Is W a subspace of V?

(a) The zero function is in W.

(b) If f and g are functions from $[a, b] \to \mathbb{R}$, then $(f + g)$ is as well.

(c) If f is a function from $[a, b] \to \mathbb{R}$, then rf is as well.

Example 2.42. Let $V = \mathcal{F}(\mathbb{R}, R)$. Then $\mathcal{C}(\mathbb{R}, \mathbb{R})$ the space of *continuous* real-valued functions is a subspace of V. So iare $\mathcal{D}(\mathbb{R}, \mathbb{R})$ the space of differentiable functions and $\mathcal{C}^\infty(\mathbb{R}, \mathbb{R})$ the space of infinitely differentiable functions.

Example 2.43. Let $V = \mathcal{F}(\mathbb{R}, R)$ and let $W = \{f : f(x) = f(-x) \forall x \in \mathbb{R}\}$ be the set of *even* real-valued functions, the functions that are symmetric around 0. Then W is a subspace of V.

Example 2.44. Let $V = \mathcal{F}(\mathbb{R}, \mathbb{R})$ and let $W = \mathcal{F}(\mathbb{R}, [a, b])$ be the space of functions from $\mathbb{R}$ to the closed interval $[a, b]$. Is W a subspace of V?

No! The simplest condition to check is scalar multiplication. Let $f(x) = b$ be a function in V. Let $r = (b + 1)/b$. Then $(rf)(x) = fb = b + 1$ and thus $rf \notin W$.

Example 2.45. Let $V = S$ be the space of signals, and let W be the space of signals that are eventually zero. That is, $W = \{\{y_k\} : \exists n \text{ such that } y_m = 0 \, \forall \, m > n\}$. Then W is a subspace of V.

The space $\{\{y_k\} : y_0 = 0\}$ is a subspace of V. But the space $\{\{y_k\} : y_0 = 1\}$ is not.

Theorem 2.46. *Any intersection of subspaces of a vector space V is a subspace of V.*

Proof. Let $\mathcal{C}$ be any collection of subspaces of V (there might be two, or three, or infinitely many subspaces in $\mathcal{C}$). Let W be the intersection of all subspaces in $\mathcal{C}$.

Since every subspace contains $\mathbf{0}$, therefore, $\mathbf{z}ero \in W$. Now let $a \in \mathbb{F}$ and $x, y \in W$. Since x and y are in the intersection of every subspace of $\mathcal{C}$, they are contained in each subspace in $\mathcal{C}$. Because each subspace is closed under addition, therefore $x + y$ is contained in each subspace in $\mathcal{C}$ and so $x + y \in W$.

Similarly, each subspace in $\mathcal{C}$ is closed under scalar multiplication, so each subspace contains ax. Hence $ax \in W$. Since W contains $\mathbf{z}ero$ and is closed under addition and scalar multiplication, by our subspace theorem, W is a subspace of V. □

2.5 Linear Combinations and Linear Equations

We have defined many vector spaces, but we started by looking at $\mathbb{R}^n$, which is much easier to think about. One of the nicest and most helpful things about $\mathbb{R}^n$ is the existence of *coordinates*. Rather than, say, just drawing a point on a graph, or perhaps giving an angle and a distance, we can specify a point in $\mathbb{R}^3$ by giving its x-coordinate, its y-coordinate, and its z-coordinate. And similarly, we can specify a point in $\mathbb{R}^7$ by specifying seven real-number coordinates.

In contrast, it's not really clear what it means to talk about coordinates for $\mathcal{F}(\mathbb{R},\mathbb{R})$. But if we had coordinates there, it would make our life much easier. (In particular, physicists often want to talk about subspaces of $\mathcal{F}(\mathbb{R},\mathbb{R})$ and then put coordinates on them and treat them like $\mathbb{R}^n$). So we would like to find a way to put coordinates on any vector space V.

There are a few ideas that will mix in here, but the first one is that coordinate let us express a vector as a sum of simple vectors. If I have a vector $(1,3,2)$, one way I can think of this is

$$\begin{bmatrix}1\\3\\2\end{bmatrix} = 1\cdot\begin{bmatrix}1\\0\\0\end{bmatrix} + 3\cdot\begin{bmatrix}0\\1\\0\end{bmatrix} + \begin{bmatrix}0\\0\\1\end{bmatrix}.$$

Definition 2.47. If V is a vector space $S = \{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n\}$ is a list of vectors in V, then a *linear combination* of of the vectors in S is a vector of the form

$$\sum_{i=1}^{n} a_i\mathbf{v}_i = a_1\mathbf{v}_1 + a_2\mathbf{v}_2 + \cdots + a_n\mathbf{v}_n$$

where $a_i \in \mathbb{R}$ are (real number) scalars.

A linear combination of vectors in V will always itself be an element of V, since V is closed under scalar multiplication and under vector addition.

Geometrically, a linear combination of vectors represents some destination you can reach only going in the directions of your chosen vectors (for any distance. So if I can go north or west, any distance"northwest" will be a linear combination of those vectors. And "southeast" will as well, since we can always go in the "opposite" direction. But "up" will not be.

Remark 2.48. This is a "linear" combination because it combines the vectors in the same way a line or plane does—adding all the vectors together, but with some coefficient. We will revisit this terminology in the next section when we discuss linear functions.

It's totally possible to have a linear combination of infinitely many vectors. But studying these requires some sense of convergence, and thus calculus/analysis. So we won't talk about it in *this* class, except for the occasional aside.

Example 2.49. Here is a table of the number of grams of protein, fats, and carbohydrates in 10g portions of certain foods (rounded to give us easier numbers):[1]

Food (10g)	Protein (g)	Fats (g)	Carbs (g)
ground beef	4	4	0
lentils	2	1	3
rice (brown)	1	0	5
cauliflower	1	0	1

We could record each different food as a vector in $\mathbb{R}^3$. So we have

$$g = \begin{bmatrix} 4 \\ 4 \\ 0 \end{bmatrix}, \quad \ell = \begin{bmatrix} 2 \\ 1 \\ 3 \end{bmatrix}, \quad r = \begin{bmatrix} 1 \\ 0 \\ 5 \end{bmatrix}, \quad c = \begin{bmatrix} 1 \\ 0 \\ 1 \end{bmatrix}.$$

Then if we prepare a meal consisting of 100g of ground beef, 150g of rice, and 200g of cauliflower, the macronutrient content is the linear combination

$$10g + 15r + 20c = 10 \begin{bmatrix} 4 \\ 4 \\ 0 \end{bmatrix} + 15 \begin{bmatrix} 1 \\ 0 \\ 5 \end{bmatrix} + 20 \begin{bmatrix} 1 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 75 \\ 40 \\ 95 \end{bmatrix}.$$

A very reasonable question to ask here is: if we have a fixed vector $\mathbf{b}$, and a set of vectors $\mathbf{u}_1, \mathbf{u}_2, \dots, \mathbf{u}_n$, can we express $\mathbf{b}$ as a linear combination of the other vectors?

Example 2.50. Can we write $(1, 3, 2)$ as a linear combination of $(1, 0, 0)$ and $(1, 1, 1)$?

In this case it's pretty easy to see that we can't, because any linear combination of these two vectors would have the same second and third coordinate. In other words, if we had

$$\begin{aligned} \begin{bmatrix} 1 \\ 3 \\ 2 \end{bmatrix} &= a \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix} + b \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix} \\ &= \begin{bmatrix} a+b \\ b \\ b \end{bmatrix} \end{aligned}$$

which implies $3 = b = 2$.

Example 2.51. Is it possible to prepare a meal using the four ingredients if we want to get exactly 70g of protein, 30g of fat, and 40g of carbs? This is asking if the vector $(70, 30, 40)$ is a linear combination of the vectors g, ℓ, r, c.

In other words, we must determine if there are scalars a_1, a_2, a_3, a_4 such that

$$\begin{aligned} \begin{bmatrix} 70 \\ 30 \\ 40 \end{bmatrix} &= a_1 \begin{bmatrix} 4 \\ 4 \\ 0 \end{bmatrix} + a_2 \begin{bmatrix} 2 \\ 1 \\ 3 \end{bmatrix} + a_3 \begin{bmatrix} 1 \\ 0 \\ 5 \end{bmatrix} + a_4 \begin{bmatrix} 1 \\ 0 \\ 1 \end{bmatrix} \\ &= \begin{bmatrix} 4a_1 + 2a_2 + a_3 + a_4 \\ 4a_1 + a_2 \\ 3a_2 + 5a_3 + a_4 \end{bmatrix} \end{aligned}$$

And that means we need to solve the following *system of linear equations*:

$$\begin{aligned} 4a_1 + 2a_2 + \ \ a_3 + a_4 &= 70 \\ 4a_1 + \ \ a_2 \qquad\qquad &= 30 \\ 3a_2 + 5a_3 + a_4 &= 40. \end{aligned}$$

Definition 2.52. A *system of linear equations* is a system of the form

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

with the a_{ij} and b_is all real numbers. We say this is a system of m equations in n unknowns.

Importantly, these equations are restricted to be relatively simple. In each equation we multiply each variable by some constant real number, add them together, and set that equal to some constant real number. We aren't allowed to multiply variables together, or do anything else fancy with them. This means the equations can't get too complicated, and are relatively easy to work with.

Thus our question about vectors became a question about linear equations. (Or maybe originally our question about linear equations became a question about vectors; they're two ways of seeing the same thing. As the course develops we'll see a few other ways we can think of the same questions.)

There are a few ways to approach solving systems of equations like this. One is by substitution: solve for one variable in terms of the other variables, and substitute into another equation. But this gets quite cumbersome. A better way is to add copies of one equation to another.

Example 2.53 (Continued)**.** We have the system of equations

$$\begin{aligned} 4a_1 + 2a_2 + \ \ a_3 + a_4 &= 70 \\ 4a_1 + \ \ a_2 \qquad\qquad &= 30 \\ 3a_2 + 5a_3 + a_4 &= 40. \end{aligned}$$

We can eliminate the a_1 terms from all but the first equation by subtracting the first equation from the second, giving:

$$\begin{aligned} 4a_1 + 2a_2 + \ \ a_3 + a_4 &= 70 \\ - \ \ a_2 - \ \ a_3 - a_4 &= -40 \\ 3a_2 + 5a_3 + a_4 &= 40. \end{aligned}$$

We might flip the second equation to make it easier to look at:

$$\begin{aligned} 4a_1 + 2a_2 + \ \ a_3 + a_4 &= 70 \\ a_2 + \ \ a_3 + a_4 &= 40 \\ 3a_2 + 5a_3 + a_4 &= 40. \end{aligned}$$

Now we can get rid of most of the a_2 terms. We subtract 2 times the second equation from the first and 3 times the second equation from the third to obtain

$$\begin{aligned} 4a_1 \qquad - \ \ a_3 - \ \ a_4 &= -10 \\ a_2 + \ \ a_3 + \ \ a_4 &= 40 \\ 2a_3 - 2a_4 &= -80. \end{aligned}$$

Divide the third equation by 2 (or multiply by 1/2) to get

$$\begin{aligned} 3a_1 \qquad - a_3 - a_4 &= -10 \\ a_2 + a_3 + a_4 &= 40 \\ a_3 - a_4 &= -40. \end{aligned}$$

Then add it to the first equation and subtract it from the second equation to yield

$$\begin{aligned} 4a_1 \qquad\qquad - 2a_4 &= -50 \\ a_2 \qquad + 2a_4 &= 80 \\ a_3 - \ \ a_4 &= -40. \end{aligned}$$

And now we still have a system of three equations in four unknowns. But it should be clear now that if we pick *any* real number for a_4, that will give us exactly one solution to the whole system:

$$\left(\frac{-50 + 2a_4}{4}, 80 - 2a_4, -40 + a_4, a_4\right) = \left(\frac{-25 + a_4}{2}, 80 - 2a_4, -40 + a_4, a_4\right).$$

We want a general approach to solving these equations. We say that two systems of equations are *equivalent* if they have the same set of solutions. Thus the process of solving a system of equations is mostly the process of converting a system into an equivalent system that is simpler.

There are three basic operations we can perform on a system of equations to get an equivalent system:

(a) We can write the equations in a different order.

(b) We can multiply any equation by a nonzero scalar.

(c) We can add a multiple of one equation to another.

All three of these operations are guaranteed not to change the solution set; proving this is a reasonable exercise. Our goal now is to find an efficient way to use these rules to get a useful solution to our system.

But, it's possible for us to be lazy about this by encoding our system in a matrix.

Right now, we will just use this as a convenient notational shortcut; we will see later on in the course that this has a number of theoretical and practical advantages.

Definition 2.54. The *coefficient matrix* of a system of linear equations given by

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

is the matrix

$$\begin{bmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{bmatrix}$$

and the *augmented coefficient matrix* is

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

Example 2.55. Suppose we have a system

$$4x + 2y + 2z = 8$$
$$3x + 2y + z = 6.$$

Then the coefficient matrix is

$$\begin{bmatrix} 4 & 2 & 2 \\ 3 & 2 & 1 \end{bmatrix}$$

and the augmented coefficient matrix is

$$\left[\begin{array}{ccc|c} 4 & 2 & 2 & 8 \\ 3 & 2 & 1 & 6. \end{array}\right]$$

Earlier we listed three operations we can perform on a system of equations without changing the solution set: we can reorder the equations, multiply an equation by a nonzero scalar, or add a multiple of one equation to another. We can do analogous things to the coefficient matrix.

Definition 2.56. The three *elementary row operations* on a matrix are

I Interchange two rows.

II Multiply a row by a nonzero real number.

III Replace a row by its sum with a multiple of another row.

Example 2.57. What can we do with our previous matrix? We can

$$\begin{bmatrix} 4 & 2 & 2 \\ 3 & 2 & 1 \end{bmatrix} \overset{I}{\to} \begin{bmatrix} 3 & 2 & 1 \\ 4 & 2 & 2 \end{bmatrix} \overset{II}{\to} \begin{bmatrix} 3 & 2 & 1 \\ 2 & 1 & 1 \end{bmatrix} \overset{III}{\to} \begin{bmatrix} 1 & 1 & 0 \\ 2 & 1 & 1 \end{bmatrix}.$$

So how do we use this to solve a system of equations? The basic idea is to remove variables from successive equations until we get one equation that contains only one variable—at which point we can substitute for that variable, and then the others. To do that with this matrix, we have

$$\left[\begin{array}{ccc|c} 4 & 2 & 2 & 8 \\ 3 & 2 & 1 & 6 \end{array}\right] \overset{III}{\to} \left[\begin{array}{ccc|c} 1 & 0 & 1 & 2 \\ 3 & 2 & 1 & 6 \end{array}\right] \overset{III}{\to} \left[\begin{array}{ccc|c} 1 & 0 & 1 & 2 \\ 0 & 2 & -2 & 0 \end{array}\right] \overset{II}{\to} \left[\begin{array}{ccc|c} 1 & 0 & 1 & 2 \\ 0 & 1 & -1 & 0 \end{array}\right].$$

What does this tell us? That our system of equations is equivalent to the system

$$x + z = 2$$
$$y - z = 0.$$

This gives us the answer: $z = 2 - x$ and $y = z = 2 - x$. So the set of solutions is the set of triples $\{(x, 2 - x, 2 - x)\}$.

Example 2.58. In $\mathcal{P}_3(\mathcal{R})$, we claim that the polynomial

$$f = 2x^3 - 2x^2 + 12x - 6$$

is a linear combination of the polynomials

$$g_1 = x^3 - 2x^2 - 5x - 3 \quad \text{and} \quad g_2 = 3x^3 - 5x^2 - 4x - 9$$

but that the polynomial

$$h = 3x^3 - 2x^2 + 7x + 8$$

is not.

To show that f is a linear combination of g_1 and g_2, we need to find scalars $a_1, a_2 \in \mathbb{R}$ such that $f = a_1 g_1 + a_2 g_2$, that is

$$\begin{aligned} 2x^3 - 2x^2 + 12x - 6 &= a_1(x^3 - 2x^2 - 5x - 3) + a_2(3x^3 - 5x^2 - 4x - 9) \\ &= (a_1 + 3a_2)x^3 + (-2a_1 - 5a_2)x^2 + (-5a_1 - 4a_2)x + (-3a_1 - 9a_2). \end{aligned}$$

Therefore, we want to solve the following system of linear equations for a_1 and a_2:

$$\begin{aligned} a_1 + 3a_2 &= 2 \\ -2a_1 - 5a_2 &= -2 \\ -5a_1 - 4a_2 &= 12 \\ -3a_1 - 9a_2 &= -6. \end{aligned}$$

We write this as a matrix:

$$\left[\begin{array}{cc|c} 1 & 3 & 2 \\ -2 & -5 & -2 \\ -5 & -4 & 12 \\ -3 & -9 & -6 \end{array}\right] \to \left[\begin{array}{cc|c} 1 & 3 & 2 \\ 0 & 1 & 2 \\ 0 & 11 & 22 \\ 0 & 0 & 0 \end{array}\right] \to \left[\begin{array}{cc|c} 1 & 0 & -4 \\ 0 & 1 & 2 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{array}\right]$$

which corresponds to the system

$$\begin{aligned} a_1 \qquad\quad &= -4 \\ a_2 \quad &= 2 \\ 0 &= 0 \\ 0 &= 0 \end{aligned}$$

and thus we have a single solution. And indeed we can verify that $f = -4g_1 + 2g_2$.

Now let's show that h is not a linear combination of g_1 and g_2? If it were, then there would be scalars $a_1, a_2 \in \mathbb{R}$ such that

$$\begin{aligned} 3x^3 - 2x^2 + 7x + 8 &= a_1(x^3 - 2x^2 - 5x - 3) + a_2(3x^3 - 5x^2 - 4x - 9) \\ &= (a_1 + 3a_2)x^3 + (-2a_1 - 5a_2)x^2 + (-5a_1 - 4a_2)x + (-3a_1 - 9a_2). \end{aligned}$$

In other words, there would be a solution to the following system:

$$\begin{aligned} a_1 + 3a_2 &= 3 \\ -2a_1 - 5a_2 &= -2 \\ -5a_1 - 4a_2 &= 7 \\ -3a_1 - 9a_2 &= 8. \end{aligned}$$

This becomes the matrix

$$\left[\begin{array}{cc|c} 1 & 3 & 3 \\ -2 & -5 & -2 \\ -5 & -4 & 7 \\ -3 & -9 & 8 \end{array}\right] \to \left[\begin{array}{cc|c} 1 & 3 & 3 \\ 0 & 1 & 4 \\ 0 & 11 & 22 \\ 0 & 0 & 17 \end{array}\right]$$

and we can already see this system will have no solutions, because the fourth line gives us $0 = 17$, which is false.

Definition 2.59. A matrix is in *row echelon form* if

- Every row containing nonzero elements is above every row containing only zeroes; and
- The first (leftmost) nonzero entry of each row is to the right of the first nonzero entry of the above row.

Remark 2.60. Some people require the first nonzero entry in each nonzero row to be 1. This is really a matter of taste and doesn't matter much, but you should do it to be safe; it's an easy extra step to take by simply dividing each row by its leading coefficient.

Example 2.61. The following matrices are all in Row Echelon Form:

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

The following matrices are not in Row Echelon Form:

$$\begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \end{bmatrix} \quad \begin{bmatrix} 3 & 2 & 5 & 1 \\ 0 & 0 & 1 & 3 \\ 0 & 5 & 1 & 2 \end{bmatrix} \quad \begin{bmatrix} 1 & 3 & 5 \\ 0 & 1 & 2 \\ 0 & 0 & 3 \\ 0 & 0 & 1 \end{bmatrix}.$$

A system of equations sometimes has a solution, but does not always. We say a system is *inconsistent* if there is no solution; we say a system is *consistent* if there is at least one solution.

Definition 2.62. A matrix is in *reduced row echelon form* if it is in row echelon form, and the first nonzero entry in each row is the only entry in its column.

This means that we will have some number of columns that each have a bunch of zeroes and one 1. Other than that we may or may not have more columns, which can contain basically anything; we've used up all our degrees of freedom to fix those columns that contain the leading term of some row.

Note that the columns we have fixed are not necessarily the first columns, as the next example shows.

Example 2.63. The following matrices are all in reduced Row Echelon Form:

$$\begin{bmatrix} 1 & 0 & 0 & 5 \\ 0 & 1 & 0 & 4 \\ 0 & 0 & 1 & 3 \end{bmatrix} \quad \begin{bmatrix} 1 & 17 & 0 & 2 & 8 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix} \quad \begin{bmatrix} 1 & 0 & 5 \\ 0 & 1 & 3 \\ 0 & 0 & 0 \end{bmatrix}.$$

The following matrices are not in reduced Row Echelon Form:

$$\begin{bmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 \end{bmatrix} \quad \begin{bmatrix} 3 & 0 & 0 & 1 \\ 0 & 3 & 0 & 3 \\ 0 & 0 & 2 & 2 \end{bmatrix} \quad \begin{bmatrix} 1 & 0 & 15 & 3 \\ 0 & 0 & 1 & 2 \\ 0 & 0 & 0 & 1 \end{bmatrix}.$$

2.6 Spanning and Linear Independence

Recall we want to put a set of "coordinates" on our vector spaces. Any "coordinate system" will need to have two basic properties: first, we want it to represent any vector in our vector space; second, we want it to represent each vector only once. So we first want to talk about the vectors that can be represented by a given collection of vectors.

Definition 2.64. Let V be a vector space $S = \{\mathbf{v}_1, \dots, \mathbf{v}_n\}$ be a set of vectors in V. We say the *span* of S is the set of all linear combinations of vectors in S, and write it $\operatorname{span}(S)$ or $\operatorname{span}(\mathbf{v}_1, \dots, \mathbf{v}_n)$.

For notational consistency, we define the span of the empty set $\operatorname{span}(\{\})$ to be the trivial vector space $\mathbf{0} = \{\mathbf{0}\}$.

Example 2.65. As before, take $V = \mathbb{R}^3$ and $S = \{(1,0,0),(0,1,0)\}$. Then

$$\operatorname{span}(S) = \{a(1,0,0) + b(0,1,0)\} = \{(a,b,0)\}.$$

Now let $T = \{(3,2,0),(13,7,0)\}$. Then

$$\operatorname{span}(T) = \{a(3,2,0) + b(13,7,0)\} = \{(3a+13b, 2a+7b, 0)\}.$$

Spans are really convenient to work with because the span of any set will always be a subspace.

Proposition 2.66. *If V is a vector space over a field $\mathbb{F}$ and $S = \{\mathbf{u}_1, \mathbf{u}_2, \dots, \mathbf{u}_n\} \subset V$, then $\operatorname{span}(S)$ is a subspace of V.*

Proof. If $S = \varnothing$ then $\operatorname{span}(S) = \{\mathbf{0}\}$ by definition, so it is the trivial subspace of V.

So now suppose S is non-empty. We know that $S \subset V$, and since any linear combination of vectors in V is itself a vector in V, we know that $\operatorname{span}(S) \subset V$. So we just need to check the three subspace conditions.

(a) Because $S \neq \varnothing$, there is some vector $\mathbf{v} \in S$, and then $0 \cdot \mathbf{v} = \mathbf{0}$. This is a linear combination of vectors in S, so it is in $\operatorname{span}(S)$.

(b) Suppose $\mathbf{v}_1, \mathbf{v}_2 \in \operatorname{span}(S)$. This implies that we can write

$$\mathbf{v}_1 = a_1\mathbf{u}_1 + \dots + a_n\mathbf{v}_n \qquad \mathbf{v}_2 = b_1\mathbf{w}_1 + \dots + b_m\mathbf{w}_m$$

for some $a_i, b_j \in \mathbb{F}$, and some $\mathbf{v}_i, \mathbf{w}_j \in S$. Thus

$$\begin{aligned} \mathbf{v} + \mathbf{v}_2 &= \big(a_1\mathbf{u}_1 + \dots + a_n\mathbf{v}_n\big) + \big(b_1\mathbf{w}_1 + \dots + b_m\mathbf{w}_m\big) \\ &= a_1\mathbf{u}_1 + \dots + a_n\mathbf{v}_n + b_1\mathbf{w}_1 + \dots + b_m\mathbf{w}_m \end{aligned}$$

is a linear combination of vectors in S, and thus an element of $\operatorname{span}(S)$.

(c) Suppose $r \in \mathbb{F}$ and $\mathbf{v} \in \operatorname{span}(S)$. Then we can write

$$\mathbf{v} = a_1\mathbf{u}_1 + \cdots + a_n\mathbf{u}_n$$

for some $a_i \in \mathbb{F}$. Then

$$r\mathbf{v} = r\left(a_1\mathbf{u}_1 + \cdots + a_n\mathbf{v}_n\right) = (ra_1)\mathbf{u}_1 + \cdots + (ra_n)\mathbf{u}_n \in \operatorname{span}(S).$$

Thus we see that $\operatorname{span}(S)$ is a subspace of V. □

Corollary 2.67. *Let V be a vector space over $\mathbb{F}$, let W be a subspace of V, and let $S \subset V$. If W contains V then W contains* $\operatorname{span}(S)$.

Proof. We know that W is a vector space containing S, so $\operatorname{span}(S)$ must be a subspace of W. □

Corollary 2.68. *If V is a vector space and $S \subseteq V$, then* $\operatorname{span}(S)$ *is the smallest subspace of V containing S.*

Proof. We just showed in proposition 2.66 that $\operatorname{span}(S)$ is a subspace of V, and of course it contains S. So we just need to show that there's no smaller subspace. In particular, I'll prove that if W is a subspace of V, and $S \subseteq W$, then $\operatorname{span}(S) \subseteq W$.

So suppose W is a subspace of V and $S \subseteq W$. Let $\mathbf{v} \in \operatorname{span}(S)$. The $\mathbf{v}$ is a linear combination of vectors in S. But $S \subseteq W$, so $\mathbf{v}$ is a linear combination of vectors in W, and thus an element of W since W is a vector space. Thus any element of $\operatorname{span}(S)$ is an element of W, so $\operatorname{span}(S) \subseteq W$. □

Definition 2.69. Let V be a vector space and $S \subset V$. If $\operatorname{span}(S) = V$ then we say S *spans* V, or *generates* V, or is a *spanning set* for V.

If S spans V, then we can express any element of V purely in terms of elements of S. But this expression might not be unique! Thus we need to introduce a second concept.

Definition 2.70. Let V be a vector space over F, and $S \subset V$. We say S is *linearly independent* if, for any finite collection of vectors $\mathbf{v}_1, \ldots, \mathbf{v}_n \in S$, the only scalars solving the equation

$$a_1\mathbf{v}_1 + \cdots + a_n\mathbf{v}_n = \mathbf{0}$$

are $a_1 = \cdots = a_n = 0$.

If a set of vectors is not linearly independent, we call it *linearly dependent* and there is a *linear dependence* relationship among the vectors.

Remark 2.71. This is one of the more subtle definitions in this course, and often gives people a lot of trouble when they first start working with it. In particular, it features a problem with *nested conditionals*: a set of vectors is linearly independent if, *if* there is a linear combination equal to zero, then all of the coefficients must be zero. I didn't use that phrasing in the formal definition because it's incredibly awkward to have to instances of the word "if" in a row, but that does highlight the problem.

In particular, to prove a set is linearly independent, you shouldn't try to prove that any linear combination is equal to zero. And you shouldn't try to prove that a particular set of coefficients is zero. Instead you should start out with the *hypothesis* that a finite linear combination of vectors produces zero, and then prove that all of the coefficients must have been zero.

(In practice this will almost always involve solving a system of linear equations, and thus row reducing a matrix.)

Example 2.72. (a) The set $S = \{(1,0,0),(0,1,0),(0,0,1)\}$ is linearly independent: suppose

$$\begin{bmatrix}0\\0\\0\end{bmatrix} = a\begin{bmatrix}1\\0\\0\end{bmatrix} + b\begin{bmatrix}0\\1\\0\end{bmatrix} + c\begin{bmatrix}0\\0\\1\end{bmatrix} = \begin{bmatrix}a\\b\\c\end{bmatrix}.$$

Then we have the system of equations $a = 0, b = 0, c = 0$ and thus all the scalars are zero.

(b) The set $S = \{(1,0,0),(0,1,0)\}$ is linearly independent. Suppose

$$\begin{bmatrix}0\\0\\0\end{bmatrix} = a\begin{bmatrix}1\\0\\0\end{bmatrix} + b\begin{bmatrix}0\\1\\0\end{bmatrix} = \begin{bmatrix}a\\b\\0\end{bmatrix}.$$

Then we have the system of equations $a = 0, b = 0$ and thus all the scalars are zero.

(c) The set $\mathrm{S} = \{(1,0,0),(0,1,0),(1,1,0)\}$ is not linearly independent, since

$$1\begin{bmatrix}1\\0\\0\end{bmatrix} + 1\begin{bmatrix}0\\1\\0\end{bmatrix} + (-1)\begin{bmatrix}1\\1\\0\end{bmatrix} = \begin{bmatrix}0\\0\\0\end{bmatrix} = \mathbf{0}.$$

(d) Any set containing the zero vector is linearly dependent, since $1 \cdot \mathbf{0} = \mathbf{0}$ but $1 \neq 0$.

Example 2.73. The set $S = \{1, x, x^2, x^3\}$ is linearly independent in $\mathcal{P}_3(x)$. So is the set $T = \{1 + x + x^2 + x^3, 1 + x + x^2, 1 + x, 1\}$.

Theorem 2.74. *Let V be a vector space and let $S_1 \subseteq S_2 \subseteq V$. If S_1 is linearly dependent, then S_2 is linearly dependent.*

Proof. If S_1 is linearly dependent, then there are vectors $u_1, \ldots, u_n \in S_1$ and scalars not all zero $a_1, \ldots, a_n \in \mathbb{F}$ such that

$$a_1\mathbf{u}_1 + \cdots + a_n\mathbf{u}_n = \mathbf{0}.$$

But since $S_1 \subseteq S_2$, therefore each $\mathbf{u}_i \in S_2$. So the previous equation shows that S_2 is linearly dependent by definition. □

Corollary 2.75. *Let V be a vector space and let $S_1 \subseteq S_2 \subseteq V$. If S_2 is linearly independent, then S_1 is linearly independent.*

Proof. This is just the contrapositive of the previous theorem. □

From an intuitive standpoint, these two results make sense. If S_1 is linearly dependent, then has some sort of redundancy. But since $S_1 \subseteq S_2$, therefore S_2 also contains redundant vectors. Adding more vectors to a redundant set cannot make the set less redundant. So S_2 must be linearly dependent.

Similarly, if S_2 is linearly independent, then the vectors in S_2 point in "genuinely different directions". Taking a subset, those vectors will still point in "genuinely different directions".

Recall that earlier we saw that the set $\{(1, 0, 0), (0, 1, 0), (1, 1, 0)\}$ was linearly dependent. But we might notice that we can remove a vector and get a linearly independent set with the same span—we can just get rid of the redundancy. Conversely, we can start with the linearly independent set $\{(1, 0, 0), (0, 1, 0)\}$ and try to add a vector. If that vector is in the span, then it will be redundant, and we get a linearly dependent set. But if it's *not* in the span, it's not redundant, and we get an independent set.

Theorem 2.76. *Let S be a linearly independent subset of a vector space V, and let $\mathbf{v} \in V$. Then $S \cup \{\mathbf{v}\}$ is linearly dependent if and only if $\mathbf{v} \in \operatorname{span}(S)$.*

Proof. Suppose S is a linearly independent subset of a vector space V and let $v \in V$.

[⇒]. Suppose that $S \cup \{\mathbf{v}\}$ is linearly dependent. Then there are distinct vectors $\mathbf{u}_1, \ldots, \mathbf{u}_n \in S$ and scalars $a_1, \ldots, a_n, b \in \mathbb{F}$ not all zero such that

$$a_1\mathbf{u}_1 + \cdots + a_n\mathbf{u}_n + bv = \mathbf{0}.$$

Now we claim that $b \neq 0$, since if it were 0, then we could delete it from the above equation to get a nontrivial linear combination of the $\mathbf{u}_i$'s to equal $\mathbf{0}$, which is not possible since S itself is linearly independent.

Since $b \neq 0$, it has a multiplicative inverse, so we can write

$$\mathbf{v} = b^{-1}(-a_1\mathbf{u}_1 - a_2\mathbf{u}_2 - \cdots - a_n\mathbf{u}_n).$$

This shows that $\mathbf{v} \in \operatorname{span}(S)$.

[$\Leftarrow$]. Conversely, suppose $\mathbf{v} \in \operatorname{span}(S)$. Then there exist vectors $\mathbf{v}_1, \dots, \mathbf{v}_m \in S$ and scalars $b_1, \dots, b_m \in \mathbb{F}$ such that

$$\mathbf{v} = b_1\mathbf{v}_1 + \cdots + b_m\mathbf{v}_m.$$

Hence,

$$b_1\mathbf{v}_1 + \cdots + b_m\mathbf{v}_m - v = \mathbf{0}.$$

Note that $\mathbf{v} \neq \mathbf{v}_i$ for any i, since we are assuming $\mathbf{v} \notin S$. Hence, this is a nontrivial linear combination of the vectors in $S \cup \{\mathbf{v}\}$ which equals $\mathbf{0}$ (it is nontrivial since the coefficient on $\mathbf{v}$ is -1). Thus, $S \cup \{\mathbf{v}\}$ is linearly dependent. □

2.7 Bases and Dimension

Now we're ready to introduce our idea of coordinates. Recall we wanted a set S such that we could write any vector in V as a sum of vectors in S, but only one way. With our new notation, we can define:

Definition 2.77. If V is a vector space and S is a spanning set for V that is also linearly independent, we say that S is a *basis* for V.

Example 2.78. The set $\{(1,0,0), (0,1,0), (0,0,1)\}$ is a basis for $\mathbb{R}^3$, as we have seen before. We call this set the *standard basis* for $\mathbb{R}^3$, and we write the three elements $\mathbf{e}_1, \mathbf{e}_2, \mathbf{e}_3$.

We can generalize this to $\mathbb{R}^n$. We define the *standard basis vectors* for $\mathbb{R}^n$ by

$$\mathbf{e}_1 = \begin{bmatrix} 1 \\ 0 \\ 0 \\ \vdots \\ 0 \\ 0 \end{bmatrix} \quad \mathbf{e}_2 = \begin{bmatrix} 0 \\ 1 \\ 0 \\ \vdots \\ 0 \\ 0 \end{bmatrix} \quad \dots \quad \mathbf{e}_n = \begin{bmatrix} 0 \\ 0 \\ 0 \\ \vdots \\ 0 \\ 1 \end{bmatrix}$$

and the set of standard basis vectors is the *standard basis*. You can check that the standard basis is in fact a basis.

Example 2.79. Every (non-trivial) vector space has more than one basis. The set $S = \{(1,0,0),(1,1,0),(1,1,1)\}$ is a basis for $\mathbb{R}^3$:

First we show that it is a spanning set. Let $(a,b,c) \in \mathbb{R}^3$. Then we want to solve

$$\begin{bmatrix} a \\ b \\ c \end{bmatrix} = \alpha_1 \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix} + \alpha_2 \begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix} + \alpha_3 \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix}$$

which gives the augmented matrix

$$\left[\begin{array}{ccc|c} 1 & 1 & 1 & a \\ 0 & 1 & 1 & b \\ 0 & 0 & 1 & c \end{array}\right] \to \left[\begin{array}{ccc|c} 1 & 0 & 0 & a-b \\ 0 & 1 & 0 & b-c \\ 0 & 0 & 1 & c \end{array}\right]$$

which tells us that $\alpha_3 = c, \alpha_2 = b-c, \alpha_1 = a-b$. Thus there is a solution for any $(a,b,c) \in \mathbb{R}^3$, and the set spans.

We also need to prove linear indepencence. So suppose

$$\mathbf{0} = \alpha_1 \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix} + \alpha_2 \begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix} + \alpha_3 \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix}.$$

This gives us a system of linear equations corresponding to the homogeneous system

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

so the only solution here is $\alpha_1 = \alpha_2 = \alpha_3 = 0$.

Thus S is linear independent, and since it also spans, it is a basis.

Example 2.80. The set $S = \{(1,0,0),(0,1,0)\}$ is not a basis for $\mathbb{R}^3$. It is linearly independent (since it is a subset of the standard basis, which is linear independent), but it is not a spanning set, since $(0,0,1)$ is not in the span of S.

Example 2.81. The set $S = \{(2,3),(3,4),(4,4)\}$ is a spanning set for $\mathbb{R}^2$ but not a basis. To see that it's a spanning set we solve

$$\begin{bmatrix} a \\ b \end{bmatrix} = \alpha_1 \begin{bmatrix} 2 \\ 3 \end{bmatrix} + \alpha_2 \begin{bmatrix} 3 \\ 4 \end{bmatrix} + \alpha_3 \begin{bmatrix} 4 \\ 4 \end{bmatrix} = \begin{bmatrix} 2\alpha_1 + 3\alpha_2 + 4\alpha_3 \\ 3\alpha_1 + 4\alpha_2 + 4\alpha_3 \end{bmatrix}$$

giving the system of equations

$$a = 2\alpha_1 + 3\alpha_2 + 4\alpha_3 \qquad\qquad b = 3\alpha_1 + 4\alpha_2 + 4\alpha_3$$

and the augmented matrix

$$\left[\begin{array}{ccc|c} 2 & 3 & 4 & a \\ 3 & 4 & 4 & b \end{array}\right] \to \left[\begin{array}{ccc|c} 1 & 1 & 0 & b-a \\ 2 & 3 & 4 & a \end{array}\right] \to \left[\begin{array}{ccc|c} 1 & 1 & 0 & b-a \\ 0 & 1 & 4 & 3a-2b \end{array}\right] \to \left[\begin{array}{ccc|c} 1 & 0 & -4 & 3b-4a \\ 0 & 1 & 4 & 3a-2b \end{array}\right].$$

Thus for any $(a, b) \in \mathbb{R}^2$, at least one solution exists; in fact we can pick α_3 to be any real number and we get a corresponding solution $(3b - 4a + 4\alpha_3, 3a - 2b - 4\alpha_3, \alpha_3)$. Thus the set spans.

But S is not linearly independent. We can see this in a few ways. Most easily we can observe that $(2, 3) + (1/4)(4, 4) = (3, 4)$. If we can't see that on our own, we can do a couple things. We can find the nullspace:

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

and we see the nullspace $\{(4\alpha, -4\alpha, \alpha)\}$ is non-trivial, so the set is not linearly independent.

But if these row operations seem familiar, that's because we did exactly the same thing to check spanning! So we can look at our spanning equations and try to find all the solutions when we take $a = b = 0$. We see that there's more than one solution there, so the vectors aren't linearly independent.

Determining whether a set is a basis is sometimes annoying, but doesn't involve anything we haven't already done: a basis is just a set that both spans and is linearly independent, and we can check both properties individually. But we'd like to make things a little simpler.

Further, we want to talk about how "big" a space is, and this should plausibly be determined by how many elements there are in the basis. But since every space has more than one basis, talking about the size of "the" basis is potentially problematic. Fortunately, this is not an actual problem, as we shall see.

Lemma 2.82. *If $S = \{\mathbf{v}_1, \dots, \mathbf{v}_n\}$ spans a vector space V, and $T = \{\mathbf{u}_1, \dots, \mathbf{u}_m\}$ is a collection of vectors in V with $m > n$, then T is linearly dependent.*

Proof. There are two possible ways to prove this. One involves simply writing out a bunch of linear equations and solving them; this works, but is more tedious than informative. We'll use a more formal and abstract approach to proving this instead, which, hopefully, will actually explain some of *why* this is true.

We will start with the set S, and one by one we will trade out vectors in S for vectors in T, and show that we always still have a spanning set. We will suppose T is linearly independent, and show that $m \leq n$.

Since S is a spanning set, we know that $\mathbf{u}_1 \in \operatorname{span}(S)$, and thus $\{\mathbf{v}_1, \dots, \mathbf{v}_n, \mathbf{u}_1\}$ is linearly dependent.. Then we can rewrite our linear dependence equation to express $\mathbf{v}_1$ (without loss of generality) as a linear combination of $\{\mathbf{u}_1, \mathbf{v}_2, \dots, \mathbf{v}_n\} = S_1$, and thus

$$\operatorname{span}(S) = \operatorname{span}(\{\mathbf{v}_1, \dots, \mathbf{v}_n, \mathbf{u}_1\}) = \operatorname{span}(S_1).$$

We can repeat this process: at every step we add the next vector from T to get the set $\{\mathbf{u}_1, \dots, \mathbf{u}_k, \mathbf{v}_k, \dots, \mathbf{v}_n\}$. Since S_{k-1} is a spanning set, this set is linearly dependent; since the $\mathbf{u}_i$ are linearly independent by hypothesis, we can remove one of the $\mathbf{v}_i$, and without loss of generality we can remove $\mathbf{v}_k$, to obtain the set $S_k = \{\mathbf{u}_1, \dots, \mathbf{u}_k, \mathbf{v}_{k+1}, \dots, \mathbf{v}_n\}$.

If $m > n$, we can continue until we have replaced every $\mathbf{v}_i$. Then we have $S_n = \{\mathbf{u}_1, \dots, \mathbf{u}_n\}$ is a spanning set, and thus $\mathbf{u}_{n+1} \in \operatorname{span}(S_n)$ and so T is linearly dependent, which contradicts our assumption.

Thus if T is linearly independent, we must have $m \leq n$. Conversely, if $m > n$ then T is linearly dependent, as we stated. ☐

Corollary 2.83. *$S = \{\mathbf{v}_1, \dots, \mathbf{v}_n\}$ and $T = \{\mathbf{u}_1, \dots, \mathbf{u}_m\}$ are two bases for a space V, then they are the same size, i.e. $m = n$.*

Proof. S is a spanning set and T is linearly independent, so we can't have $m > n$ by lemma 2.82. But T is a spanning set and S is linearly independent, so we can't have $n > m$ by lemma 2.82. Thus $n = m$. ☐

Definition 2.84. Let V be a vector space. If V has a basis consisting of n vectors, we say that V has *dimension* n and write $\dim V = n$. The trivial vector space $\{\mathbf{0}\}$ has dimension 0.

We say that V is *finite–dimensional* if there is a finite set of vectors that spans V. (Thus if V is n-dimensional it is finite-dimensional). Otherwise, we say that V is *infinite–dimensional.*

In this course we will primarily discuss finite dimensional vector spaces; but there are many important infinite-dimensional examples.

Example 2.85. The set of standard basis vectors $\{\mathbf{e}_1, \dots, \mathbf{e}_n\}$ is a basis for $\mathbb{R}^n$, so $\mathbb{R}^n$ is n-dimensional.

The set $\{1, x, \dots, x^n\}$ is a basis for $\mathcal{P}_n(x)$. This set has $n+1$ vectors, so $\dim \mathcal{P}_n(x) = n+1$.

$\mathcal{P}(x)$ does not have a finite basis. We can see this since the set $S = \{1, x, \dots, x^n\}$ is linearly independent for any n; but every spanning set is at least as big as any linearly independent set, so we can never have a finite spanning set. However, if we allow infinite bases, then $\{1, x, \dots, x^n, \dots\}$ is a basis for $\mathcal{P}(x)$.

Remark 2.86. $\mathcal{C}([a,b],\mathbb{R})$ is infinite–dimensional, but if we allow infinite sums and make convergence arguments it is possible to think of the set $\{1, x, \dots, x^n, \dots\}$ as a sort of ("separable") basis. But this requires analysis and is outside the scope of this course. We can also build a (separable) basis out of the functions $\sin(nx)$ and $\cos(nx)$ for $n \in \mathbb{N}$; this is the foundation of Fourier analysis and Fourier series.

The set $\mathcal{F}(\mathbb{R},\mathbb{R})$ is absurdly huge, and does not have a countable basis. If you believe the axiom of choice it has a basis, as all sets do, but you can't possibly write it down. You can think of it has having "coordinates" given by functions like

$$f_r(x) = \begin{cases} 1 & x = r \\ 0 & x \neq r \end{cases}$$

but this isn't a basis because it would require uncountable sums, which you can't really define.

How do we find bases? There are two basic ways we can build them.

Lemma 2.87 (Basis Reduction)**.** *Suppose $S = \{\mathbf{v}_1, \dots, \mathbf{v}_n\}$ is a spanning set for V. Then S can be reduced to a basis for V. That is, there is a subset $B \subseteq S$ that is a basis for V.*

Proof. If S is linearly independent, then it is a basis and we're done.

So suppose S is linearly dependent. Then we know at least one vector is redundant, so without loss of generality we can reorder the set so that we can write $\mathbf{v}_n$ as a linear combination of the other vectors in S.

But then $\operatorname{span}(S) = \operatorname{span}(\{\mathbf{v}_1, \dots, \mathbf{v}_{n-1}\})$, and $S_1 = \{\mathbf{v}_1, \dots, \mathbf{v}_{n-1}\}$ is a spanning set for V and a proper subset of S. If S_1 is linearly independent, then it is a basis; if not, we can repeat this process until we reach a linearly independent set, which is our basis B. □

Remark 2.88. This proof assumes that S is finite. The result is still (mostly) true if S is infinite, but if the space is finite-dimensional this isn't interesting, and if the space is infinite-dimensional things get very complicated and we don't want to worry about them here.

Example 2.89. Let $S = \{(1,1,0), (1,1,1), (0,0,1), (2,7,0)\}$ be a spanning set for $\mathbb{R}^3$. Find a basis $B \subseteq S$ for $\mathbb{R}^3$.

We'll take as given that this is a spanning set, which is not difficult to check. We see that we can write $(1,1,1) = (1,1,0) + (0,0,1)$, so we can remove $(1,1,1)$ without changing the span, and we have $B = \{(1,1,0), (0,0,1), (2,7,0)\} \subseteq S$ is a basis for $\mathbb{R}^3$.

Lemma 2.90 (Basis Padding). *Suppose $S = \{\mathbf{v}_1, \ldots, \mathbf{v}_n\}$ is linearly independent in V. Then if V has any finite spanning set $T = \{\mathbf{u}_1, \ldots, \mathbf{u}_m\}$, we can obtain a basis by padding S. That is, there is a basis B for V with $S \subseteq B$.*

Proof. If $T \subset \operatorname{span}(S)$, then $\operatorname{span}(T) \subset \operatorname{span}(S)$, so S is a spanning set for V and thus a basis, so we're done.

So suppose without loss of generality that $\mathbf{u}_1 \notin \operatorname{span}(S)$. Then $S_1 = \{\mathbf{v}_1, \ldots, \mathbf{v}_n, \mathbf{u}_1\}$ is linearly independent since we can't write any element as a linear combination of the others.

If S_1 spans V, then it is a basis and we're done. If not, there is some other $\mathbf{u}_i \notin \operatorname{span}(S_1)$, so we can repeat the process, and after at most m steps this process will terminate (since we run out of elements in T). When we reach a spanning set, this is our basis.

□

Example 2.91. Let $S = \{1 + x, x^2 - 3\} \subset \mathcal{P}_2(x)$. Can we find a basis B for $\mathcal{P}_2(x)$ that contains T?

We need to find a vector (or quadratic polynomial) that isn't in S. There are lots of choices here, but it looks to me like 1 is not in the span of S. Then we check: suppose $a(1 + x) + b(x^2 - 3) = 1$. Then we have

$$(a - 3b) + ax + bx^2 = 1$$

which gives the system

$$\left[\begin{array}{cc|c} 1 & -3 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{array}\right] \to \left[\begin{array}{cc|c} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{array}\right]$$

which has no solution. Thus indeed $1 \notin \operatorname{span}(S)$, so $\{1, 1 + x, x^2 - 3\}$ is a basis for $\mathcal{P}_3(x)$.

Corollary 2.92. *Let V be a finite-dimensional vector space over a field $\mathbb{F}$, and let W be a subspace of V. Then W is finite-dimensional, and* $\dim(W) \leq \dim(V)$.

Further, if $\dim(W) = \dim(V)$, *then* $W = V$.

Proof. Suppose $\dim(V) = n$. If $W = \{\mathbf{0}\}$, then $\dim(W) = 0 \leq n$ so we are done.

Otherwise, W contains a nonzero vector, say $\mathbf{v}_1 \in W$. Since $\mathbf{v}_1 \neq \mathbf{0}$, the set $\{\mathbf{v}_1\}$ is linearly independent. By basis padding, we can add choose vectors $\mathbf{v}_2, \ldots, \mathbf{v}_k$ in W such that $S = \{\mathbf{v}_1, \ldots, \mathbf{v}_k\}$ is a basis for W, and $\dim(W) = k$.

But S is a linearly independent subset of V, and thus S can't have more than n vectors. Thus $k \leq n$ and so $\dim(W) \leq \dim V$.

If $\dim(W) = n$, S is a linearly independent subset of V containing n vectors. By basis padding, it is a subset of some basis for V. But any basis for V must have exactly n elements, and thus S is a basis for V. Since S spans V and $W = \operatorname{span}(S)$, we conclude that $W = V$.

□

3 Linear Transformations

Now that we understand vector spaces a bit more, we want to see how functions between vector spaces work. There are of course lots of functions that that take in vectors and output other vectors; almost any multivariable function technically qualifies. But we actually want to care about functions that in some sense are compatible with the actual vector space structure.

3.1 Definition and examples

Definition 3.1. Let U and V be vector spaces over a field $\mathbb{F}$, and let $L : U \to V$ be a function with domain U and codomain V. We say L is a *linear transformation* if:

(a) Whenever $\mathbf{u}_1, \mathbf{u}_2 \in U$, then $L(\mathbf{u}_1 + \mathbf{u}_2) = L(\mathbf{u}_1) + L(\mathbf{u}_2)$.

(b) Whenever $\mathbf{u} \in U$ and $r \in \mathbb{F}$, then $L(r\mathbf{u}) = rL(\mathbf{u})$.

Geometrically, a linear transformation can stretch, rotate, and reflect, but it cannot bend or shift.

Example 3.2. Consider the function from $\mathbb{R}^2$ to $\mathbb{R}^2$ given by a rotation of ninety degrees counterclockwise. We can see by drawing pictures that the sum of two rotated vectors is the rotation of the sum of the vectors, and that the rotation of a streched vector is the same as the strech of a rotated vector. So this is a linear transformation.

Example 3.3. A *translation* is a function defined by $f(\mathbf{x}) = \mathbf{x} + \mathbf{u}$ for some fixed vector $\mathbf{u}$. (Geometrically, it corresponds to sliding or translating your input in the direction and distance of the vector $\mathbf{u}$).

This is *not* a linear transformation. For instance, $f(r\mathbf{x}) = r\mathbf{x} + \mathbf{u} \neq r(\mathbf{x} + \mathbf{u}) = rf(\mathbf{x})$ unless $\mathbf{u} = \mathbf{0}$.

Example 3.4. The function $f(x) = x^2$ is not a linear transformation from $\mathbb{R}$ to $\mathbb{R}$, since $f(2x) = (2x)^2 = 4x^2 \neq 2x^2 = 2f(x)$.

Example 3.5. Define a function $L : \mathbb{R}^3 \to \mathbb{R}^2$ by $L(x, y, z) = (x + y, 2z - x)$. We check:

$$\begin{aligned} L((x_1, y_1, z_1) + (x_2, y_2, z_2)) &= L(x_1 + x_2, y_1 + y_2, z_1 + z_2) \\ &= (x_1 + x_2 + y_1 + y_2, 2z_1 + 2z_2 - x_1 - x_2) \\ &= (x_1 + y_1, 2z_1 - x_1) + (x_2 + y_2, 2z_2 - x_2) \\ &= L(x_1, y_1, z_1) + L(x_2, y_2, z_2). \\ L(r(x, y, z)) &= L(rx, ry, rz) = (rx + ry, 2rz - rx) = \\ &= r(x + y, 2z - x) = rL(x, y, z). \end{aligned}$$

Thus L is a linear transformation by definition.

Example 3.6. Define $T : M_{m\times n}(\mathbb{F}) \to M_{n\times m}(\mathbb{F})$ by $T(A) = A^t$, where A^t is the transpose of A. On your problem set, you proved that for $A, B \in M_{m\times n}(\mathbb{F})$, $(A + B)^t = A^t + B^t$. In other words, you proved that $T(A + B) = T(A) + T(B)$.

You could similarly prove that $T(cA) = cT(A)$ or $(cA)^t = cA^t$. This shows that T is a linear transformation.

Example 3.7. Let $V = \mathcal{P}(\mathbb{R})$. Define $D : V \to V$ by $D(f) = f'$, the derivative of f. You learned in calculus that $(f + g)' = f' + g'$ and $(cf)' = cf'$ for all $c \in \mathbb{R}$. In other words, $D(f + g) = D(f) + D(g)$ and $D(cf) = cD(f)$ so D is linear.

Similarly, we can define $I : V \to V$ by $I(f) = \int_0^x f(t)\,dt$, the integral of f. Then we know $\int_0^x f(t) + g(t)\,dt = \int_0^x f(t)\,dt + \int_0^x g(t)\,dt$ and $\int_0^x cf(t)\,dt = c\int_0^x f(t)\,dt$, so I is linear.

Question: why can't I just take the linear operator $f \mapsto \int f(x)\,dx$?

3.2 Kernel, Image, and the Rank-Nullity Theorem

There are some important properties we can attach to any linear transformation we study. In particular, any linear transformation implies the existence of a couple of special sets of vectors.

Definition 3.8. Let $L : U \to V$ be a linear transformation. If $\mathbf{u} \in U$ is a vector, we say the element $L(\mathbf{u}) \in V$ is the *image* of $\mathbf{u}$.

If $S \subset U$ then we define the image of S to be the set $L(S) = \{L(\mathbf{u}) : \mathbf{u} \in S\}$ to be the set of images of elements of S. We say the image of the entire set U is the *image* (or sometimes *range*) of the function L.

The *kernel* (or sometimes *nullspace*) of L is the set $\ker(L) = \{\mathbf{u} \in U : L(\mathbf{u}) = \mathbf{0}\}$ of elements of U whose image is the zero vector.

Another way of thinking about linear transformations is that they send lines to lines. In particular, the image of a subspace under a linear transformation is always a subspace—thus the image of a line will be either a point or a line.

Proposition 3.9. *Let $L : U \to V$ be a linear transformation, and let $S \subseteq U$ be a subspace of U. Then:*

(a) $\ker(L)$ *is a subspace of U.*

(b) The image $L(S)$ of S is a subspace of V.

Proof. (a) See homework 4.

(b) We use the subspace theorem:

(a) We wish to show that $\mathbf{0} \in L(S)$. We claim in particular that $L(\mathbf{0}) = \mathbf{0}$: that is, the image of the zero vector in U must be the zero vector in V. Recall that $0 \cdot \mathbf{v} = \mathbf{0}$ for any $\mathbf{v} \in V$, so we have

$$L(\mathbf{0}) = L(0 \cdot \mathbf{0}) = 0L(\mathbf{0}) = \mathbf{0}.$$

Thus since S is a subspace we have $\mathbf{0} \in S$ and thus $\mathbf{0} \in L(S)$.

(b) Suppose $\mathbf{v} \in L(S)$ and $r \in \mathbb{R}$. Then there is some $\mathbf{u} \in S$ with $L(\mathbf{u}) = \mathbf{v}$, and since S is a subspace we know that $r\mathbf{u} \in S$. Thus

$$r\mathbf{v} = rL(\mathbf{u}) = L(r\mathbf{u}) \in L(S).$$

(c) Suppose $\mathbf{v}_1, \mathbf{v}_2 \in L(S)$. Then there exist $\mathbf{u}_1, \mathbf{u}_2 \in S$ such that $L(\mathbf{u}_1) = \mathbf{v}_1$ and $L(\mathbf{u}_2) = \mathbf{v}_2$. Since S is a subspace we know that $\mathbf{u}_1 + \mathbf{u}_2 \in S$. Then

$$\mathbf{v}_1 + \mathbf{v}_2 = L(\mathbf{u}_1) + L(\mathbf{u}_2) = L(\mathbf{u}_1 + \mathbf{u}_2) \in L(S).$$

□

Corollary 3.10. *If $L : U \to V$ is a linear transformation, then the image of L is a subspace of V.*

Let's think about some of the transformations we've already studied.

Example 3.11. In our geometric example of a ninety degree counterclockwise rotation, the kernel is just the origin—nothing gets mapped to the origin except the origin. The image is the entire plane.

Example 3.12. Let $V = \mathcal{P}(\mathbb{R})$ be the space of real polynomials, and consider again our functions D the derivative and I the integral. We can see that $\ker(D)$ is the set of constant polynomials, $\ker(D) = \{a : a \in \mathbb{R}\}$. The image is all polynomials.

Conversely, the kernel of I is $\ker(I) = \{0\}$, since no polynomial will have a zero integral except the zero polynomial. But the image is polynomials with zero constant term, $\operatorname{Im}(I) = \{a_1 x + a_2 x^2 + \cdots + a_n x^n\}$.

Example 3.13. Let $\mathcal{D}([a,b],\mathbb{R})$ be the space of continuously differentiable functions from the closed interval $[a,b]$ to the real line. Define the derivative operator $D : \mathcal{D}([a,b],\mathbb{R}) \to \mathcal{C}([a,b],\mathbb{R})$ by $D(f) = f'$. First we claim that D is a linear operator: we have that $D(f+g) = (f+g)' = f' + g' = D(f) + D(g)$, and $D(rf) = (rf)' + rf' = rD(f)$.

The kernel of D is the space of constant functions, which is a one-dimensional subspace. The image of D is actually a little hard to see, but it's actually the set of all continuous functions on $[a,b]$.

In other contexts we might write $\frac{d}{dx}$ instead of D for this linear transformation.

Example 3.14. Let $\mathcal{C}([a,b],\mathbb{R})$ be the set of all continuous functions on the closed interval $[a,b]$. The (indefinite) integral isn't quite a linear transformation, since there's an ambiguity in choice of constant. (This is what we mean when we say something is "not well defined": if I tell you to give me the integral of x^2, you can't give me a specific function back so my question is not precise enough).

But the function $I(f) = \int_a^x f(t)\,dt$ is a linear transformation, since $\int_a^x (f+g)(t)\,dt = \int_a^x f(t)\,dt + \int_a^x g(t)\,dt$ and $\int_a^x rf(t)\,dt = r\int_a^x f(t)\,dt$. In this case the choice of a as the basepoint resolves the earlier ambiguity.

The kernel of I is the trivial vector space containing only the zero function. The image is again a bit hard to see, but works out to be the space of differentiable functions with the property that $F(a) = 0$.

This last example shows an important principle: our derivative and integral linear transformations (almost) undo each other. This is a very important property and we will look at it on its own in a bit.

Theorem 3.15. *Let $T : V \to W$ be a linear transformation. If $\beta = \{\mathbf{v}_1, \dots, \mathbf{v}_n\}$ is a basis for V, then*

$$R(T) = \operatorname{span}(T(\beta)) = \operatorname{span}(T(v_1), \dots, T(v_n)).$$

Proof. We need to show both inclusions.

[$\supseteq$]. By definition, it is clear that $\{T(v_1), \dots, T(v_n)\} \subseteq R(T)$. Then by proposition 2.66 we know that $\text{span}(T(v_1), \dots, T(V_n)) \subseteq R(T)$, which shows one of the inclusions.

[$\subseteq$]. Now suppose that $x \in R(T)$. This means that there exists $v \in V$ such that $T(v) = x$. Since $v \in V$ and β is a basis for V, there exist scalars $c_1, \dots, c_n \in \mathbb{F}$ such that

$$v = c_1 v_1 + \cdots + c_n v_n.$$

Then

$$\begin{aligned} x = T(v) &= T(c_1 v_1 + \cdots + c_n v_n) \\ &= T(c_1 v_1) + \cdots + T(c_n v_n) \\ &= c_1 T(v_1) + \cdots + c_n T(v_n) \end{aligned}$$

and so x is a linear combination of the vectors $T(v_1), \dots, T(v_n)$, in other words, $x \in \text{span}(T(v_1), \dots, T(v_n)$, and so we have the other inclusion. $\square$

Since we have two nice subspaces, we have new vector spaces and can talk about their properties. The most important property of vector spaces that we've discussed is the dimension. (Bases are more important but aren't really a "property".)

Definition 3.16. Let $L : V \to W$ be a linear transformation. If $\ker(L)$ is finite-dimensional, we define the *nullity* of L to be $\text{null}(L) = \dim(\ker(L))$. If $\text{Im}(L)$ is finite-dimensional, we define the *rank* of L to be $\text{rk}(L) = \dim(\text{Im}(L))$.

The kernel is all the vectors that get sent to zero; we can think of it as all the image that L destroys or discards. The image is all the vectors that get output, and thus we can think of it as the image that gets preserved, or sent onwards, by L. And this implies a relationship: all the information can be either destroyed, or preserved, but not both.

More algebraically, if the kernel is large, that means a lot of vectors are being sent to $\mathbf{0}$. And that means that relatively few vectors can be sent to non-zero vectors, so the image must be small.

Formalizing this relationship leads to

Theorem 3.17 (Rank-Nullity)**.** *Let V, W be vector spaces over $\mathbb{F}$, and let $T : V \to W$ be linear. If V is finite-dimensional, then*

$$\text{null}(L) + \text{rk}(L) = \dim(V).$$

Proof. Suppose that $\dim(V) = n$ and $\dim(\ker(T)) = k$. We can then take a basis $\{v_1, \dots, v_k\}$ of $\ker(T)$. By the basis padding theorem, we may extend this linearly independent set to a basis of V, say $\beta = \{v_1, \dots, v_n\}$.

We claim that $S = \{T(v_{k+1}), \dots, T(v_n)\}$ is a basis for $\operatorname{Im}(T)$. First, we prove that S generates $\operatorname{Im}(T)$. Note that we have that

$$\begin{aligned} \operatorname{Im}(T) &= \operatorname{span}(T(v_1), \dots, T(v_k), T(v_{k+1}), \dots T(v_n)) \\ &= \operatorname{span}(\mathbf{0}, \dots, \mathbf{0}, T(v_{k+1}), \dots T(v_n)) \\ &= \operatorname{span}(T(v_{k+1}), \dots T(v_n)) = \operatorname{span}(S). \end{aligned}$$

Hence, S generates $R(T)$.

Next, we must show that S is linearly independent. To this end, suppose we have scalars $c_{k+1}, \dots, c_n \in \mathcal{F}$ such that

$$\sum_{i=k+1}^{n} c_i T(v_i) = \mathbf{0}.$$

Using the fact that T is linear, we have

$$\sum_{i=k+1}^{n} c_i T(v_i) = T\left(\sum_{i=k+1}^{n} c_i v_i\right) = \mathbf{0}$$

which shows that

$$\sum_{i=k+1}^{n} c_i v_i \in \ker(T).$$

Since $v_1, \dots, v_k$ is a basis of $\ker(T)$, there exist scalars $c_1, \dots, c_k$, such that

$$\sum_{i=1}^{k} c_i v_i = \sum_{i=k+1}^{n} c_i v_i$$

and so

$$\sum_{i=1}^{k} c_i v_i + \sum_{i=k+1}^{n} (-c_i) v_i = \mathbf{0}.$$

But now since β is a basis for V, the set $v_1, \dots, v_n$ is linearly independent, which forces all of the $c_i = 0$. But this shows that $T(v_{k+1}), \dots, T(v_n)$ is linearly independent.

This shows that

$$\operatorname{rk}(T) = \dim \operatorname{Im}(T) = n - k = \dim(V) - \operatorname{null}(T),$$

from which the theorem follows.

□

This theorem gives us a major constraint on what linear functions can possibly look like. We have more to say about this structure, but first we want to understand how to compute with linear functions a little more easily. Fortunately, we have an extremely powerful tool for doing so.

3.3 The Matrix of a Linear Transformation

We've seen some examples of linear transformations, but they're fundamentally awkward to compute with. But we can use matrices to make all our computations simpler—and turn almost every computation into a row reduction.

We want to start by looking at the situation just in $\mathbb{R}^n$ or $\mathbb{F}^n$. We want to study linear functions in those spaces, and it turns out they can all be represented by matrices. First we need some facts about matrices.

Definition 3.18. If $A \in M_{\ell\times m}$ and $B \in M_{m\times n}$, then there is a matrix $AB \in M_{\ell\times n}$ whose ij element is

$$c_{ij} = \sum_{k=1}^{m} a_{ik}b_{kj}.$$

If you're familiar with the dot product, you can think that the ij element of AB is the dot product of the ith row of A with the jth column of b.

Note that A and B don't have to have the same dimension! Instead, A has the same number of columns that B has rows. The new matrix will have the same number of rows as A and the same number of columns as B.

Matrix multiplication is *associative*, by which we mean that $(AB)C = A(BC)$.

Matrix multiplication is not commutative: in general, it's not even the case that AB and BA both make sense. If $A \in M_{3\times 4}$ and $B \in M_{4\times 2}$ then AB is a 3×2 matrix, but BA isn't a thing we can compute. But even if AB and BA are both well-defined, they are not equal.

Example 3.19.

$$\begin{bmatrix} 3 & 5 & 1 \\ -2 & 0 & 2 \end{bmatrix} \begin{bmatrix} 2 & 1 \\ 1 & 3 \\ 4 & 1 \end{bmatrix} = \begin{bmatrix} 3\cdot 2 + 5\cdot 1 + 1\cdot 4 & 3\cdot 1 + 5\cdot 3 + 1\cdot 1 \\ -2\cdot 2 + 0\cdot 1 + 2\cdot 4 & -2\cdot 1 + 0\cdot 3 + 2\cdot 1 \end{bmatrix} = \begin{bmatrix} 15 & 19 \\ 4 & 0 \end{bmatrix}$$

$$\begin{bmatrix} 2 & 1 \\ 1 & 3 \\ 4 & 1 \end{bmatrix} \begin{bmatrix} 3 & 5 & 1 \\ -2 & 0 & 2 \end{bmatrix} = \begin{bmatrix} 2\cdot 3 + 1\cdot(-2) & 2\cdot 5 + 1\cdot 0 & 2\cdot 1 + 1\cdot 2 \\ 1\cdot 3 + 3\cdot(-2) & 1\cdot 5 + 3\cdot 0 & 1\cdot 1 + 3\cdot 2 \\ 4\cdot 3 + 1\cdot(-2) & 4\cdot 5 + 1\cdot 0 & 4\cdot 1 + 1\cdot 2 \end{bmatrix} = \begin{bmatrix} 4 & 10 & 4 \\ -3 & 5 & 7 \\ 10 & 20 & 6 \end{bmatrix}.$$

Particularly nice things happen when our matrices are square. Any time we have two $n \times n$ matrices we can multiply them by each other in either order (though we will still get different things each way!).

Example 3.20.

$$\begin{bmatrix} 4 & 1 \\ -3 & 5 \end{bmatrix} \begin{bmatrix} -1 & 1 \\ 1 & -2 \end{bmatrix} = \begin{bmatrix} -3 & 2 \\ 8 & -13 \end{bmatrix}$$
$$\begin{bmatrix} -1 & 1 \\ 1 & -2 \end{bmatrix} \begin{bmatrix} 4 & 1 \\ -3 & 5 \end{bmatrix} = \begin{bmatrix} -7 & 4 \\ 10 & -9 \end{bmatrix}.$$

However, matrix multiplication does satisfy the *distributive* and *associative* properties.

Fact 3.21. *If $A \in M_{\ell \times m}$ and $B, C \in M_{m \times n}$ then $A(B+C) = AB + AC$.*

If $A \in M_{\ell \times m}, B \in M_{m \times n}, C \in M_{n \times p}$ then $(AB)C = A(BC)$.

Example 3.22.

$$\begin{bmatrix} 1 & 3 \\ 2 & 4 \end{bmatrix} \begin{bmatrix} 5 & -1 \\ 3 & 2 \end{bmatrix} = \begin{bmatrix} 1 \cdot 5 + 3 \cdot 3 & 1 \cdot (-1) + 3 \cdot 2 \\ 2 \cdot 5 + 4 \cdot 3 & 2 \cdot (-1) + 4 \cdot 2 \end{bmatrix} = \begin{bmatrix} 14 & 5 \\ 22 & 6 \end{bmatrix}$$
$$\begin{bmatrix} 4 & 6 \\ 2 & 1 \end{bmatrix} \begin{bmatrix} 3 & 1 & 5 \\ 4 & 1 & 6 \end{bmatrix} = \begin{bmatrix} 4 \cdot 3 + 6 \cdot 4 & 4 \cdot 1 + 6 \cdot 1 & 4 \cdot 5 + 6 \cdot 6 \\ 2 \cdot 3 + 1 \cdot 4 & 2 \cdot 1 + 1 \cdot 1 & 2 \cdot 5 + 1 \cdot 6 \end{bmatrix} = \begin{bmatrix} 36 & 10 & 56 \\ 10 & 3 & 16 \end{bmatrix}.$$

So how does this give us a linear function? If we have a vector in $\mathbb{F}^n$, we can view it as a $n \times 1$ matrix. And then multiplying by a $m \times n$ matrix will give us a $m \times 1$ matrix—which is a vector in $\mathbb{F}^m$!

Example 3.23. Let $A = \begin{bmatrix} 3 & 5 & 1 \\ 2 & -1 & 3 \end{bmatrix}$ be a matrix, and $\mathbf{u} = \begin{bmatrix} 5 \\ -2 \\ 1 \end{bmatrix}$. Then we can compute

$$\begin{aligned} A\mathbf{u} &= \begin{bmatrix} 3 & 5 & 1 \\ 2 & -1 & 3 \end{bmatrix} \begin{bmatrix} 5 \\ -2 \\ 1 \end{bmatrix} \\ &= \begin{bmatrix} 6 \\ 15 \end{bmatrix}. \end{aligned}$$

Now let's see what happens to each element of the standard basis for $\mathbb{R}^3$.

$$A\mathbf{e}_1 = \begin{bmatrix} 3 & 5 & 1 \\ 2 & -1 & 3 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} 3 \\ 2 \end{bmatrix}$$

$$A\mathbf{e}_1 = \begin{bmatrix} 3 & 5 & 1 \\ 2 & -1 & 3 \end{bmatrix} \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 5 \\ -1 \end{bmatrix}$$

$$A\mathbf{e}_1 = \begin{bmatrix} 3 & 5 & 1 \\ 2 & -1 & 3 \end{bmatrix} \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 3 \end{bmatrix}.$$

We notice that the image of the standard basis elements are just the columns of the matrix! This isn't a coincidence; the columns of our matrix are telling us exactly where our basis vectors go. And we'll see that this is enough to tell us about our entire function—as long as it's linear.

But remember we said that $A(B + C) = AB + AC$. That implies that $A(\mathbf{u} + \mathbf{v}) = A\mathbf{u} + a\mathbf{v}$. It also shouldn't be too hard to convince yourself that scalar multiplication commutes: $A(rB) = r(AB)$, and thus $A(r\mathbf{u}) = r(A\mathbf{u})$. So multiplication by a matrix is always a linear function.

It's less obvious, but it turns out that any linear function $\mathbb{F}^n \to \mathbb{F}^m$ can be described by a matrix. But we'll wait and prove this along with the proof for all vector spaces.

So now we want to figure out how to apply this logic to vector spaces that aren't $\mathbb{F}^n$. And that requires us to use our discussion of bases to get *coordinates* on our space.

Definition 3.24. If V is a vector space over $\mathbb{F}$, we define an *ordered basis* for V to be a basis for V with a specific fixed order.

Let $\beta = \{\mathbf{v}_1, \dots, \mathbf{v}_n\}$ be an ordered basis for V. Then if $\mathbf{v} \in V$, we can uniquely write

$$\mathbf{v} = a_1\mathbf{v}_1 + \cdots + a_n\mathbf{v}_n$$

for $a_i \in \mathbb{F}$. We define the *coordinate vector of* $\mathbf{v}$ *with respect to* β to be

$$[\mathbf{u}]_\beta = \begin{bmatrix} a_1 \\ \vdots \\ a_n \end{bmatrix} \in \mathbb{F}^n.$$

We call the a_i the *coordinates* of $\mathbf{v}$ with respect to β.

This is one more layer of precision to our idea that any finite-dimensional vector space "looks like" $\mathbb{F}^n$.

Example 3.25. Let $U = \mathcal{P}_3(x)$. Then $E = \{1, x, x^2, x^3\}$ is a basis for U. Also, $F = \{1, 1+x, 1+x^2, 1+x^3\}$ is a basis for U.

Let $f(x) = 1 + 3x + x^2 - x^3 \in U$. Then

$$[f]_E = \begin{bmatrix} 1 \\ 3 \\ 1 \\ -1 \end{bmatrix} \quad [f]_F = \begin{bmatrix} -2 \\ 3 \\ 1 \\ -1 \end{bmatrix}.$$

These are two different vectors of real numbers, but they represent the *same* element of U, just in different bases.

Example 3.26. Let $U = \mathbb{R}^3$ and let $E = \{(1,0,0), (1,1,0), (1,1,1)\}$. Then if $\mathbf{u} = (1,3,2)$, then

$$[\mathbf{u}]_E = \begin{bmatrix} -2 \\ 1 \\ 2 \end{bmatrix}.$$

Remark 3.27. If B is the standard basis for $\mathbb{R}^n$, then any time we write a column vector there's an implicit $\begin{bmatrix} a_1 \\ \vdots \\ a_n \end{bmatrix}_B$ that we just don't bother to write down.

Lemma 3.28. *If U is a vector space and $E = \{\mathbf{e}_1, \dots, \mathbf{e}_n\}$ is a basis for U, then the function $[\cdot]_E : U \to \mathbb{R}^n$ which sends $\mathbf{u}$ to $[\mathbf{u}]_E$ is a linear function.*

Proof. See HW 5. □

Theorem 3.29. *Let U and V be finite-dimensional vector spaces, with $E = \{\mathbf{e}_1, \dots, \mathbf{e}_n\}$ a basis for U and $F = \{\mathbf{f}_1, \dots, \mathbf{f}_m\}$ a basis for V. Let $L : U \to V$ be a linear transformation.*

Then there is a matrix A that represents L with respect to E and F, such that $L\mathbf{u} = \mathbf{v}$ if and only if $A[\mathbf{u}]_E = [\mathbf{v}]_F$. The columns of A are given by $\mathbf{c}_j = [L(\mathbf{e}_j)]_F$.

Remark 3.30. This looks really complicated, but it really just says that any v linear transformation is determined entirely by what it does to the elements of some basis; if you have a basis and you know where your transformation sends each element of that basis, you know what it does to everything in your space.

In particular, if we have coordintes for our vector spaces, we can use a matrix to map one set of coordinates to the other, as if we were working in $\mathbb{R}^n$.

$$\begin{array}{ccc} U & \xrightarrow{L} & V \\ \downarrow{\scriptstyle [\cdot]_E} & & \downarrow{\scriptstyle [\cdot]_F} \\ \mathbb{R}^n & \xrightarrow{A} & \mathbb{R}^m \end{array} \qquad \begin{array}{ccc} \mathbf{u} & \xmapsto{L} & L(\mathbf{u}) \\ \downarrow{\scriptstyle [\cdot]_E} & & \downarrow{\scriptstyle [\cdot]_F} \\ [\mathbf{u}]_E & \xmapsto{A} & A[\mathbf{u}]_E = [L(\mathbf{u})]_F \end{array}$$

Proof. We just want to show that $A[\mathbf{u}]_E = [L(\mathbf{u})]_F$ for any $\mathbf{u} \in U$, where

$$A = [\mathbf{c}_1 \dots \mathbf{c}_n] = [[L(\mathbf{e}_1)]_F \dots [L(\mathbf{e}_n)]_F] .$$

Let $\mathbf{u} \in U$. Since E is a basis for U we can write $u = a_1\mathbf{e}_1 + \dots + a_n\mathbf{e}_n$. Then we have

$$\begin{aligned} [L(\mathbf{u})]_F &= [a_1 L(\mathbf{e}_1) + \dots + a_n L(\mathbf{e}_n)]_F = a_1 [L(\mathbf{e}_1)]_F + \dots + a_n [L(\mathbf{e}_n)]_F \\ &= a_1\mathbf{c}_1 + \dots + a_n\mathbf{c}_n; \\ A[\mathbf{u}]_E &= A [a_1\mathbf{e}_1 + \dots + a_n\mathbf{e}_n]_E = A(a_1, \dots, a_n) = [\mathbf{c}_1 \dots \mathbf{c}_n] (a_1, \dots, a_n) \\ &= \mathbf{c}_1 a_1 + \dots + \mathbf{c}_n a_n. \end{aligned}$$

Thus we have $[L(\mathbf{u})]_F = A [\mathbf{u}]_E$, so the matrix A does in fact represent the linear operator L. □

Example 3.31. Let $F = \{(1,1), (-1,1)\}$ be a basis for $\mathbb{R}^2$, and let $L : \mathbb{R}^3 \to \mathbb{R}^2$ be given by $L(x,y,z) = (x - y - z, x + y + z)$. Find a matrix for L with respect to the standard basis in the domain and F in the codomain.

$$\begin{aligned} L(1,0,0) &= (1,1) = \mathbf{f}_1 \\ L(0,1,0) &= (-1,1) = \mathbf{f}_2 \\ L(0,0,1) &= (-1,1) = \mathbf{f}_2 \\ A &= \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \end{bmatrix}. \end{aligned}$$

Example 3.32. Let S be the subspace of $\mathcal{C}([a,b], \mathbb{R})$ spanned by $\{e^x, xe^x, x^2e^x\}$, and let D be the differentiation operator on S. Find the matrix of D with respect to $\{e^x, xe^x, x^2e^x\}$.

We compute:

$$
\begin{aligned}
D(e^x) &= e^x = \mathbf{s}_1 \\
D(xe^x) &= e^x + xe^x = \mathbf{s}_1 + \mathbf{s}_2 \\
D(x^2e^x) &= 2xe^x + x^2e^x = 2\mathbf{s}_2 + \mathbf{s}_3 \\
A &= \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 2 \\ 0 & 0 & 1 \end{bmatrix}.
\end{aligned}
$$

Example 3.33. Let $E = \{(1,1,0),(1,0,1),(0,1,1)\}$ and $F = \{(1,0,0),(1,1,0),(1,1,1)\}$ be bases for $\mathbb{R}^3$, and define $L(x,y,z) = (x+y+z, 2z, -x+y+z)$. We can check this is a linear transformation.

To find the matrix of L with respect to E and the standard basis, we compute

$$
\begin{aligned}
L(1,1,0) &= (2,0,0) \\
L(1,0,1) &= (2,2,0) \\
L(0,1,1) &= (2,2,2).
\end{aligned}
$$

Thus the matrix with respect to E and the standard basis is

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

If we want to find the matrix with respect to E and F, we observe that

$$
\begin{aligned}
L(1,1,0) &= (2,0,0) = 2(1,0,0) = 2\mathbf{f}_1 \\
L(1,0,1) &= (2,2,0) = 2(1,1,0) = 2\mathbf{f}_2 \\
L(0,1,1) &= (2,2,2) = 2(1,1,1) = 2\mathbf{f}_3.
\end{aligned}
$$

Thus the matrix is

$$
\begin{bmatrix} 2 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 2 \end{bmatrix}.
$$

We notice that this matrix is really simple; this is a "good" choice of bases for this linear transformation.

In contrast, let's look at the transformation $T(x, y, z) = (x, y, z)$. Then we have

$$\begin{aligned} T(1,1,0) &= (1,1,0) = (1,1,0) = \mathbf{f}_2 \\ T(1,0,1) &= (1,0,1) = (1,0,0) - (1,1,0) + (1,1,1) = \mathbf{f}_1 - \mathbf{f}_2 + \mathbf{f}_3 \\ T(0,1,1) &= (0,1,1) = -(1,0,0) + (1,1,1) = -\mathbf{f}_1 + \mathbf{f}_3. \end{aligned}$$

Thus the matrix of T with respect to E and F is

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

Thus this transformation, which is really simple with respect to the standard basis, is much more complicated with respect to these bases.

These matrices, finally, allow us to do easy calculations of the kernel and image of a transformation. We start with the kernel: we're looking for the solutions to $L(\mathbf{v}) = \mathbf{0}$. But this is the same as looking for solutions of $A[\mathbf{v}] = \mathbf{0}$. Further, if we take $A = (a_{ij})$ and $[\mathbf{v}] = (v_1, \ldots, v_n)$, then this equation becomes

$$\begin{bmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ a_{21} & a_{22} & \ldots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \ldots & a_{mn} \end{bmatrix} \begin{bmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix}$$

$$\begin{bmatrix} a_{11}x_1 + \cdots + a_{1n}x_n \\ a_{21}x_1 + \cdots + a_{2n}x_n \\ \vdots \\ a_{m1}x_1 + \cdots + a_{mn}x_n \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix}$$

which gives us the system

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

And since we have a system of equations, we can turn it into an augmented matrix:

$$\left[\begin{array}{cccc|c} a_{11} & a_{12} & \dots & a_{1n} & 0 \\ a_{21} & a_{22} & \dots & a_{2n} & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} & 0 \end{array}\right]$$

but this is just the matrix we started with! So we can find the kernel by row-reducing this matrix.

Similarly, if we want to check if a vector $\mathbf{u}$ is in the image, that corresponds to solving the equation $L(\mathbf{v}) = \mathbf{u}$, and thus $A[\mathbf{v}] = [\mathbf{u}]$; working through the same computations, this leads us to row reduce the matrix

$$\left[\begin{array}{cccc|c} a_{11} & a_{12} & \dots & a_{1n} & u_1 \\ a_{21} & a_{22} & \dots & a_{2n} & u_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} & u_m \end{array}\right].$$

Example 3.34. Consider again S the subspace of $\mathcal{C}([a,b],\mathbb{R})$ spanned by $\{e^x, xe^x, x^2e^x\}$, and let D the differentiation operator on S. We want to find the kernel and image of D.

We found the matrix with respect to $\{e^x, xe^x, x^2e^x\}$ to be

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

We can then set up the equation

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

and find for which $\mathbf{b}$ there is a $\mathbf{x}$ that solves this equation. So we have

$$\begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 2 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = \begin{bmatrix} b_1 \\ b_2 \\ b_3 \end{bmatrix}$$

$$\begin{bmatrix} x_1 + x_2 \\ x_2 + 2x_3 \\ x_3 \end{bmatrix} = \begin{bmatrix} b_1 \\ b_2 \\ b_3 \end{bmatrix}$$

which gives us the system of equations

$$\begin{aligned} x_1 + x_2 \qquad &= b_1 \\ x_2 + 2x_3 &= b_2 \\ x_3 &= b_3 \end{aligned}$$

which we can solve by row reducing a matrix:

$$\left[\begin{array}{ccc|c} 1 & 1 & 0 & b_1 \\ 0 & 1 & 2 & b_2 \\ 0 & 0 & 1 & b_3 \end{array}\right] \to \left[\begin{array}{ccc|c} 1 & 0 & -2 & b_1 - b_2 \\ 0 & 1 & 2 & b_2 \\ 0 & 0 & 1 & b_3 \end{array}\right] \to \left[\begin{array}{ccc|c} 1 & 0 & 0 & b_1 - b_2 + 2b_3 \\ 0 & 1 & 0 & b_2 - 2b_3 \\ 0 & 0 & 1 & b_3 \end{array}\right].$$

First, we observe that this has solutions for any $\mathbf{b} = (b_1, b_2, b_3)$; that means that the image of our matrix is $\mathbb{R}^3$, and thus the image of D is S. So if we want to obtain, say, $3e^x + 5xe^x - 2x^2e^2$ we have $b_1 = 3, b_2 = 5, b_3 = -2$, and so we must have $x_1 = -6, x_2 = 9, x_3 = -2$; and indeed we can check that

$$\begin{aligned} \frac{d}{dx} - 6e^x + 9xe^x - 2x^2e^x &= -6e^x + 9e^x + 9xe^2 - 4xe^x - 2x^2e^x \\ &= 3e^x + 5xe^x - 2x^2e^x. \end{aligned}$$

Second, if we look at the matrix we were reducing, it's just an augmented version of A—which isn't an accident. We pushed our symbols around through three or four different forms of the question, but throughout we were asking essentially the same question.

Finally, we can just as well try to identify the kernel of this transformation. We would set up the same equations, except instead of looking at an arbitrary output $\mathbf{b}$, we want to see how we can obtain $\mathbf{0}$. So we would take our same solutions as before, but with all the $b_i = 0$. So we have

$$\begin{aligned} x_1 &= b_1 - b_2 + 2b_3 = 0 \\ x_2 &= b_2 - 2b_3 = 0 \\ x_3 &= b_3 = 0. \end{aligned}$$

Thus the only solution is $x_1 = x_2 = x_3 = 0$, and the kernel of the transformation is $\{\mathbf{0}\}$.

3.4 The space of linear transformations

We know the set of $m \times n$ matrices is a vector space: we can add matrices, and multiply them by scalars. We now have a function that takes in a linear transformation and gives us a matrix. In fact, this function should give us some sort of equivalence—which would mean that the linear transformations should also be a vector space!

And indeed we can add and scalar multiply linear transformations.

Definition 3.35. Let $L, T : U \to V$ be linear transformations. We define a function $(L+T)(\mathbf{u}) = L(\mathbf{u}) + T(\mathbf{u})$.

Let $r \in F$ be a scalar. Then we define a function $(rT)(\mathbf{u}) = r(T(\mathbf{u}))$.

Proposition 3.36. *Let U, V be vector spaces over $\mathbb{F}$, and $r \in F$ be a scalar. If $L, T : U \to V$ are linear transformations, then the function $rL + T$ is also a linear transformation.*

Proof. HW 6. □

From here we can conclude that the set of linear transformations from U to V is a vector space. We have two operations; we just have to check all ten axioms, which is tedious but not difficult. The zero vector is the zero linear transformation, defined by $L(\mathbf{v}) = \mathbf{0}$.

Definition 3.37. Let U, V be vector spaces over $\mathbb{F}$. We denote the *space of linear transformations from U to V* by $\mathcal{L}(U, V)$.

Proposition 3.38. *Let V, W be finite-dimensional vector spaces over $\mathbb{F}$ with ordered bases β, γ, and let $L, T : V \to W$ be linear transformations. Then*

(a) $[L+T]_\beta^\gamma = [L]_\beta^\gamma + [T]_\beta^\gamma$

(b) $[rL]_\beta^\gamma = r[L]_\beta^\gamma$ *for all* $r \in \mathbb{F}$.

Proof. Let $\beta = \{v_1, \dots, v_n\}$ and $\gamma = \{w_1, \dots, w_m\}$. We know that since γ is a basis for W, there are unique scalars a_{ij} and b_{ij} for $1 \leq i \leq m$ and $1 \leq j \leq n$ such that

$$L(v_j) = \sum_{i=1}^m a_{ij} w_i \quad \text{and} \quad T(v_j) = \sum_{i=1}^m b_{ij} w_i.$$

And that the matrix $[L]_\beta^\gamma = (a_{ij})$ and $[T]_\beta^\gamma = (b_{ij})$. To compute the matrix $[L+T]_\beta^\gamma$, we need to compute the coefficients on $(L+T)(v_j)$ in terms of the w_i. But now note that

$$(L+T)(v_j) = L(v_j) + T(v_j) = \sum_{i=1}^m a_{ij} w_i + \sum_{i=1}^m b_{ij} w_i = \sum_{i=1}^m (a_{ij} + b_{ij}) w_i.$$

Hence, the matrix $[L+T]_\beta^\gamma = (a_{ij} + b_{ij})$. But by definition of matrix addition, this is the same as $[L]_\beta^\gamma + [T]_\beta^\gamma$.

Part (2) is proved similarly, and you should go through it as an exercise.

□

Finally, we can *compose* two linear transformations and get another linear transformation.

Proposition 3.39. *Let U, V, W be vector spaces over $\mathbb{F}$, and let $L : U \to V$ and $T : V \to W$ be linear functions. Then $T \circ L : U \to W$ is also linear.*

Proof. Let $\mathbf{u}_1, \mathbf{u}_2 \in U$, and $r \in \mathbb{F}$. Then

$$\begin{aligned} TL(\mathbf{u}_1 + \mathbf{u}_2) &= T\big(L(\mathbf{u}_1) + L(\mathbf{u}_2)\big) \\ &= T(L(\mathbf{u}_1)) + T(L(\mathbf{u}_2)) \\ TL(r\mathbf{u}_1) &= T\big(rL(\mathbf{u}_1)\big) \\ &= rTL(\mathbf{u}_1). \end{aligned}$$

□

The composition of linear transformations also behaves very well, and respects a lot of properties we'd like to preserve.

Proposition 3.40. *Let U, V, W, Y be vector spaces over $\mathbb{F}$. Let $L_1, L_2 : U \to V, T_1, T_2 : V \to W$, and $S : W \to Y$. Then*

(a) $(T_1 + T_2)L_1 = T_1L_1 + T_2L_1$ *and* $T_1(L_1 + L_2) = T_1L_1 + T_1L_2$.

(b) $S(T_1L_1) = (ST_1)L_1$.

(c) $a(T_1L_1) = (aT_1)L_1 = T_1(aL_1)$.

There's also another special linear transformation:

Definition 3.41. Let V be a vector space over $\mathbb{F}$. We define the *identity transformation* I_V by $I_V(\mathbf{v}) = \mathbf{v}$.

We now want to relate all this to matrices. We can compose two linear transformations. What does that do to the matrices? In fact, it does the best possible thing:

Proposition 3.42. *Let U, V, W be finite-dimensional vector spaces over $\mathbb{F}$, with ordered bases α, β, γ. Let $L : U \to V$ and $T : V \to W$ be linear transformations. Then*

$$[TL]_\alpha^\gamma = [T]_\beta^\gamma [L]_\alpha^\beta.$$

That is, composition of linear transformations is just the same as multiplying the corresponding matrices. And this is essentially where the definition of matrix multiplication came from.

Proof. □

3.5 Injectivity, Surjectivity, and Isomorphism

Here are some definitions you should be familiar with from 2971:

Definition 3.43.
- Let $f : U \to V$ be any function. If there is a $g : V \to U$ such that $g(f(\mathbf{u})) = \mathbf{u}$ for all $u \in U$, and $f(g(\mathbf{v})) = \mathbf{v}$ for all $\mathbf{v} \in V$, then we say that $g = f^{-1}$ is the *inverse* of f, and that f is *invertible.*
- A function f is *one-to-one* or *injective* if it has the property that: if $f(x) = f(y)$ then $x = y$. This tells us that anything in the image of f is only in the image once.
- A function $f : A \to B$ is *onto* or *surjective* if the image of f is B. That is, f is onto if for every $b \in B$ there is an $a \in A$ with $f(a) = b$. This tells us we can reach every element of the codomain from some element of the domain.
- A function f is *bijective* if it is both one-to-one and onto.

Fact 3.44. *A function $f : U \to V$ is invertible if and only if it is bijective.*

Definition 3.45. If $L : U \to V$ is an invertible linear transformation, we say that L is an *isomorphism* between U and V.

If U and V are vector spaces, we say they are *isomorphic* if there exists an isomorphism from U to V. We write $U \cong V$.

Because linear transformations are so structured, we can check these things more easily than usual.

Proposition 3.46. *Let $L : U \to V$ be a linear transformation. Then L is injective if and only if* $\ker(L) = \{\mathbf{0}\}$.

Proof. See hw6? □

This makes it easy to check if a linear transformation is injective. We just need to check the kernel, and we can check the kernel of the transformation by row-reducing the associated matrix.

Surjectivity is a little harder to check, at least directly. We can still do this with the matrix form of a transformation:

Example 3.47. Consider again S the subspace of $\mathcal{C}([a, b], \mathbb{R})$ spanned by $\{e^x, xe^x, x^2e^x\}$, and let D the differentiation operator on S. We want to find the kernel and image of D. We got the matrix

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

and then reduced to get

$$\left[\begin{array}{ccc|c} 1 & 1 & 0 & b_1 \\ 0 & 1 & 2 & b_2 \\ 0 & 0 & 1 & b_3 \end{array}\right] \to \left[\begin{array}{ccc|c} 1 & 0 & -2 & b_1 - b_2 \\ 0 & 1 & 2 & b_2 \\ 0 & 0 & 1 & b_3 \end{array}\right] \to \left[\begin{array}{ccc|c} 1 & 0 & 0 & b_1 - b_2 + 2b_3 \\ 0 & 1 & 0 & b_2 - 2b_3 \\ 0 & 0 & 1 & b_3 \end{array}\right].$$

So we saw the image of A was $\mathbb{R}^3$, and thus the image of D was S, making D surjective. And the kernel of D is $\{\mathbf{0}\}$, so D is injective.

But it's often simpler to use the rank-nullity theorem. If we know the dimension of the kernel, then we know the dimension of the image, and thus we can figure out if it's surjective. As a corollary, we can observe that if two spaces are isomorphic, they must have the same dimension. But we can actually say something stronger.

Proposition 3.48. *Let $U, V/\mathbb{F}$ be finite-dimensional vector spaces. Then $U \cong V$ if and only if $\dim(U) = \dim(V)$.*

Proof. Suppose $U \cong V$. Then there is an isomorphism $L : U \to V$. Since L is injective, we know $\ker(L) = \{\mathbf{0}\}$ and so $\dim(\ker(L)) = 0$. Since L is surjective, we know that $\operatorname{Im}(L) = V$ and thus $\dim(\operatorname{Im}(L)) = \dim(V)$. But by the rank-nullity theorem, we know that

$$\dim(U) = \dim(\ker(L)) + \dim(\operatorname{Im}(L)) = 0 + \dim(V) = \dim(V).$$

Conversely: suppose $\dim(U) = \dim(V)$. We have a basis $\beta = \{\mathbf{u}_1, \dots, \mathbf{u}_n\}$ for U, and a basis $\gamma = \{\mathbf{v}_1, \dots, \mathbf{v}_n\}$ for V. (These two bases have the same size, since $\dim(U) = \dim(V)$.)

Define a transformation $L : U \to V$ by

$$L(a_1\mathbf{u}_1 + \cdots + a_n\mathbf{u}_n) = a_1\mathbf{v}_1 + \cdots + a_n\mathbf{v}_n.$$

First we need to prove that this is "well-defined"—that is, we need to prove that L is actually a function. But we know that given a vector $\mathbf{u} \in U$ there is a unique way to write it as a linear combination of our basis vectors. So there's only one way to represent the input, and so this is a proper function.

We need to check that this is linear, and that it's invertible. Suppose $a \in \mathbb{F}$, and that

$$\mathbf{u}_1 = b_1\mathbf{u}_1 + \cdots + b_n\mathbf{u}_n$$
$$\mathbf{u}_2 = c_1\mathbf{u}_! + \cdots + c_n\mathbf{v}_n \in U.$$

Then

$$\begin{aligned}
L(a\mathbf{u}_1 + \mathbf{u}_2) &= L\Big(a\big(b_1\mathbf{u}_1 + \cdots + b_n\mathbf{u}_n\big) + c_1\mathbf{u}_1 + \cdots + c_n\mathbf{v}_n\Big) \\
&= L\Big((ab_1 + c_1)\mathbf{u}_1 + \cdots + (ab_n + c_n)\mathbf{u}_n\Big) \\
&= (ab_1 + c_1)\mathbf{v}_1 + \cdots + (ab_n + c_n)\mathbf{v}_n
\end{aligned}$$

and

$$\begin{aligned}
aL(u_1) + L(\mathbf{u}_2) &= a\big(b_1\mathbf{v}_1 + \cdots + b_n\mathbf{v}_n\big) + c_1\mathbf{v}_1 + \cdots + c_n\mathbf{v}_n \\
&= (ab_1 + c_1)\mathbf{v}_1 + \cdots + (ab_n + c_n)\mathbf{v}_n.
\end{aligned}$$

So L is linear.

To show that L is a bijection, we can do two things. We could check that it's injective and surjective, which is annoying; but we can also just find an inverse. So we define a function $T : V \to U$ by the formula

$$T(a_1\mathbf{v}_1 + \cdots + a_n\mathbf{v}_n) = a_1\mathbf{u}_1 + \cdots + a_n\mathbf{u}_n,$$

and we see that $T(L(\mathbf{u})) = \mathbf{u}$ for all $\mathbf{u} \in U$. Thus L is invertible.

□

But this sort of rule isn't very helpful for actually finding inverses to transformations, that we can compute. For that we have to use matrices again.

Definition 3.49. Let $\mathbb{F}$ be a field and $n \in \mathbb{N}$. We define the *identity matrix* to be the matrix $I_n \in M_{n\times n}$ that has a 1 on every entry in the main diagonal, and 0s everywhere else. For example,

$$I_4 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}.$$

If $A \in M_n$ then $I_nA = A = AI_n$. Thus it is a *multiplicative identity* in the ring of $n \times n$ matrices.

Let A and B be $n \times n$ matrices, such that $AB = I_n = BA$. Then we say that B is the *inverse* (or *multiplicative inverse*) of A, and write $B = A^{-1}$.

If such a matrix exists, we say that A is *invertible* or *nonsingular*. If no such matrix exists, we say that A is *singular*.

Example 3.50. The identity matrix I_n is its own inverse, and thus invertible.

The matrices

$$\begin{bmatrix} 2 & 4 \\ 3 & 1 \end{bmatrix} \quad \text{and} \quad \begin{bmatrix} -1/10 & 2/5 \\ 3/10 & -1/5 \end{bmatrix}$$

are inverses to each other, as you can check.

Example 3.51. The matrix $\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$ has no inverse, since

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

won't be the identity for any a, b, c, d. Thus this matrix is singular.

As the last example shows, finding the inverse to a matrix is a matter of solving a big pile of linear equations at the same time (one for each coefficient of the inverse matrix). Fortunately, we just got good at solving linear equations. Even more fortunately, there's an easy way to organize the work for these problems.

Proposition 3.52. *Let A be a $n \times n$ matrix. Then if we form the augmented matrix $\begin{bmatrix} A & I_n \end{bmatrix}$, then A is invertible if and only if the reduced row echelon form of this augmented matrix is $\begin{bmatrix} I_n & B \end{bmatrix}$ for some matrix B, and furthermore $B = A^{-1}$.*

Proof. Let X be a $n \times n$ matrix of unknowns, and set up the system of equations implied by $AX = I_n$. Thus we have

$$\begin{bmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{bmatrix} \begin{bmatrix} x_{11} & x_{12} & \dots & x_{1n} \\ x_{21} & x_{22} & \dots & x_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ x_{n1} & x_{n2} & \dots & x_{nn} \end{bmatrix} = \begin{bmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 0 \end{bmatrix}$$

which gives us a *huge* pile of equations like

$$\begin{aligned}
a_{11}x_{11} + a_{12}x_{21} + \cdots + a_{1n}x_{n1} &= 1 \\
a_{11}x_{12} + a_{12}x_{22} + \cdots + a_{1n}x_{n2} &= 0 \\
\vdots \quad & \quad \vdots \\
a_{11}x_{1n} + a_{12}x_{2n} + \cdots + a_{1n}x_{nn} &= 0 \\
-&-- \\
a_{21}x_{11} + a_{22}x_{21} + \cdots + a_{2n}x_{n1} &= 0 \\
a_{21}x_{12} + a_{22}x_{22} + \cdots + a_{2n}x_{n2} &= 1 \\
\vdots \quad & \quad \vdots \\
a_{21}x_{1n} + a_{22}x_{2n} + \cdots + a_{2n}x_{nn} &= 0 \\
-&-- \\
\vdots \quad & \quad \vdots \\
-&-- \\
a_{n1}x_{11} + a_{n2}x_{21} + \cdots + a_{nn}x_{n1} &= 0 \\
a_{n1}x_{12} + a_{n2}x_{22} + \cdots + a_{nn}x_{n2} &= 0 \\
\vdots \quad & \quad \vdots \\
a_{n1}x_{1n} + a_{n2}x_{2n} + \cdots + a_{nn}x_{nn} &= 1
\end{aligned}$$

Now we can solve this system by turning it into an augmented matrix. And in theory, maybe the matrix should be n^2 rows and n^2 columns, and then one augmented column. But it's really the same matrix of coefficients repeated n times, so we'll have to do the exact same set of row operations n times. Instead we can do them all at once, by taking the single column with n^2 entries and rewriting it as n columns with n entries each.

Then if the matrix A has a reduced row echelon form equal to the identity, this system will have a unique solution, which will give us A^{-1}. If the RREF of A isn't the identity, then it will have a row of all zeroes, and thus there will be no solution, and A has no inverse. □

Example 3.53. Let's find an inverse for $A = \begin{bmatrix} 1 & 2 & 3 \\ 0 & 1 & 4 \\ 0 & 0 & 1 \end{bmatrix}$.

We form and reduce the augmented matrix

$$\left[\begin{array}{ccc|ccc} 1 & 2 & 3 & 1 & 0 & 0 \\ 0 & 1 & 4 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 \end{array}\right] \to \left[\begin{array}{ccc|ccc} 1 & 0 & -5 & 1 & -2 & 0 \\ 0 & 1 & 4 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 \end{array}\right] \to \left[\begin{array}{ccc|ccc} 1 & 0 & 0 & 1 & -2 & 5 \\ 0 & 1 & 0 & 0 & 1 & -4 \\ 0 & 0 & 1 & 0 & 0 & 1 \end{array}\right].$$

Thus $A^{-1} = \begin{bmatrix} 1 & -2 & 5 \\ 0 & 1 & -4 \\ 0 & 0 & 1 \end{bmatrix}$. We can check this by multiplying the matrices back together.

Example 3.54. Find the inverse of $B = \begin{bmatrix} 1 & 0 & 4 \\ 1 & 1 & 6 \\ -3 & 0 & -10 \end{bmatrix}$.

We form and reduce the augmented matrix

$$\left[\begin{array}{ccc|ccc} 1 & 0 & 4 & 1 & 0 & 0 \\ 1 & 1 & 6 & 0 & 1 & 0 \\ -3 & 0 & -10 & 0 & 0 & 1 \end{array}\right] \to \left[\begin{array}{ccc|ccc} 1 & 0 & 4 & 1 & 0 & 0 \\ 0 & 1 & 2 & -1 & 1 & 0 \\ 0 & 0 & 2 & 3 & 0 & 1 \end{array}\right]$$
$$\to \left[\begin{array}{ccc|ccc} 1 & 0 & 4 & 1 & 0 & 0 \\ 0 & 1 & 2 & -1 & 1 & 0 \\ 0 & 0 & 1 & 3/2 & 0 & 1/2 \end{array}\right] \to \left[\begin{array}{ccc|ccc} 1 & 0 & 0 & -5 & 0 & -2 \\ 0 & 1 & 2 & -4 & 1 & -1 \\ 0 & 0 & 1 & 3/2 & 0 & 1/2 \end{array}\right].$$

Thus $B^{-1} = \begin{bmatrix} -5 & 0 & -2 \\ -4 & 1 & -1 \\ 3/2 & 0 & 1/2 \end{bmatrix}$.

Example 3.55. What happens if we try to find an inverse for $C = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$? We start with

$$\left[\begin{array}{cc|cc} 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{array}\right]$$

but then there is no way to make the left-side block of the matrix into the identity I_2. Thus this matrix C is not invertible.

Proposition 3.56. *Let $L : U \to V$ be a linear transformation of finite dimensional vector spaces, and let E, F be bases for U, V respectively. Let A be the matrix of L with respect to E, F. Then L is invertible if and only if A is invertible, and the matrix of L^{-1} is A^{-1}.*

Proof. Suppose L is invertible, and that the matrix of L is A and the Let B be the matrix of L^{-1}. Then for any $\mathbf{u} \in U$,

$$[L^{-1}(L(\mathbf{u}))]_E = B[L(\mathbf{u})]_F = BA[\mathbf{u}]_E$$
$$[L^{-1}(L(\mathbf{u}))]_E = [\mathbf{u}]_E$$

and thus $BA[\mathbf{u}]_E = [\mathbf{u}]_E$ for all $\mathbf{u} \in U$. Thus $BA\mathbf{x} = \mathbf{x}$ for all $\mathbf{x} \in \mathbb{R}^n$, and thus $BA = I_n$. So by definition $B = A^{-1}$.

Conversely, suppose the matrix of L is A, and A has an inverse A^{-1}. Let T be the function corresponding to A^{-1}, so for all $\mathbf{v} \in V$ we have $[T(\mathbf{v})]_E = A^{-1}[\mathbf{v}]_F$. Then for any $\mathbf{u} \in U, \mathbf{v} \in V$, we compute

$$[T(L(\mathbf{u}))]_E = A^{-1}[L(\mathbf{u})]_F = A^{-1}A[\mathbf{u}]_E = [\mathbf{u}]_E$$
$$[L(T(\mathbf{v}))]_F = A[T(\mathbf{v})]_E = AA^{-1}[\mathbf{v}]_F = [\mathbf{v}]_F.$$

Thus $T(L(\mathbf{u})) = \mathbf{u}$ and $L(T(\mathbf{v})) = \mathbf{v}$, so by definition $T = L^{-1}$. □

Example 3.57. Consider again S the subspace of $\mathcal{C}([a,b],\mathbb{R})$ spanned by $\{e^x, xe^x, x^2e^x\}$, and let D the differentiation operator on S.We got the matrix

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

and we can invert this matrix:

$$\left[\begin{array}{ccc|ccc} 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 2 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 \end{array}\right] \to \left[\begin{array}{ccc|ccc} 1 & 0 & -2 & 1 & -1 & 0 \\ 0 & 1 & 2 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 \end{array}\right] \to \left[\begin{array}{ccc|ccc} 1 & 0 & 0 & 1 & -1 & 2 \\ 0 & 1 & 0 & 0 & 1 & -2 \\ 0 & 0 & 1 & 0 & 0 & 1 \end{array}\right].$$

Thus we have an inverse matrix

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

What does this say as a function from $S \to S$? Well, this is the function that sends $e^x \mapsto e^x$, sends $xe^x \mapsto -e^x + xe^x$, and sends $x^2e^x \mapsto 2e^x - 2xe^x + x^2e^x$. So it's the antidifferentiation operator on S!

We've done a lot of work on the relationship between linear functions and matrices. This also gives us an actual isomorphism.

Proposition 3.58. *Let V, W be finite-dimensional vector spaces over $\mathbb{F}$ of dimension n and m, respectively; and fix ordered bases β, γ of V and W. We can define a function*

$$\Phi_\beta^\gamma : \mathcal{L}(V, W) \to M_{m\times n}(\mathbb{F})$$

by $\Phi_\beta^\gamma(T) = [T]_\beta^\gamma$. Then Φ_β^γ is an isomorphism.

Proof. In proposition 3.38 we showed that Φ_β^γ is a linear transformation. So we just need to show it has an inverse.

Let $A \in M_{m\times n}$, and fix bases $\beta = \{\mathbf{v}_1, \ldots, \mathbf{v}_n\}$ and $\gamma = \{\mathbf{w}_1, \ldots, \mathbf{w}_m\}$. Then we can define a unique linear transformation $T : V \to W$ by setting

$$T(\mathbf{v}_j) = \sum_{i=1}^m a_{ij} w_i$$

for each basis element $\mathbf{v}_j \in \beta$. Then we can extend this by linearity to get a unique linear transformation on all of V. Thus $\Phi_\beta^\gamma(T) = A$, so Φ_β^γ is surjective.

Now suppose $\Phi_\beta^\gamma(T) = \Phi_\beta^\gamma(L)$. Then $[T]_\beta^\gamma = [L]_\beta^\gamma$. Thus $T(\mathbf{v}_j) = L(\mathbf{v}_j)$ for each j, and thus $T = L$. So Φ_β^γ is injective. □

Corollary 3.59. *If $\dim(V) = n$ and $\dim(W) = m$ then $\dim(\mathcal{L}(V, W)) = mn$.*

3.6 Change of Basis

We will sometimes use the notation ϕ_β for the map $\mathbf{x} \mapsto [\mathbf{x}]_\beta$.

Proposition 3.60. *If V is a finite-dimensional vector space with ordered basis β, then ϕ_β is an isomorphism.*

Proof. We've already shown this is linear.

Let $\mathbf{x} = (x_1, \ldots, x_n) \in \mathbb{R}^n$. Then if $\beta = \{\mathbf{v}_1, \ldots, \mathbf{v}_n\}$, we can set $\mathbf{v} = x_1\mathbf{v}_1 + \cdots + x_n\mathbf{v}_n$, and $\phi_\beta(\mathbf{v}) = \mathbf{x}$. So ϕ_β is surjective. Since V and $\mathbb{R}^n$ have the same dimension, it must also be injective.

□

We return to theorem 3.29, and the diagram that follows it, now with our new notation:

$$\begin{array}{ccc} U & \xrightarrow{L} & V \\ \updownarrow{\scriptstyle \phi_\beta} & & \updownarrow{\scriptstyle \phi_\gamma} \\ \mathbb{R}^n & \xrightarrow{A} & \mathbb{R}^m \end{array} \qquad \begin{array}{ccc} \mathbf{u} & \xmapsto{L} & L(\mathbf{u}) \\ \downarrow{\scriptstyle \phi_\beta} & & \downarrow{\scriptstyle \phi_\gamma} \\ [\mathbf{u}]_\beta & \xmapsto{A} & A[\mathbf{u}]_\beta = [L(\mathbf{u})]_\gamma \end{array}$$

The new information, in addition to changing the notation, is that the vertical maps are invertible, which means that we can go either way. Specifically, this tells us that if we have a linear transformation $L : U \to V$, and its matrix is $A \in M_{m\times n}$ with implied linear transformation $L_A : \mathbb{R}^n \to \mathbb{R}^m$, then we have

$$L = \phi_\gamma^{-1} \circ L_A \circ \phi_\beta.$$

So this gives us a whole family of isomorphisms: every basis for V gives an isomorphism $\phi_\beta : V \xrightarrow{\sim} \mathbb{R}^n$. If we have another basic γ we get another isomorphism $\phi_\gamma : V \xrightarrow{\sim} \mathbb{R}^n$; but since isomorphisms are invertible this in fact gives us an isomorphism $\phi_\gamma^{-1}\phi_\beta$ from V to itself!

Proposition 3.61. *Let β and γ be two ordered bases of a finite-dimensional vector space V, and let $Q = [I_V]_\gamma^\beta$. Then Q is an invertible matrix, and for any $\mathbf{v} \in V$, $[\mathbf{v}]_\beta = Q[\mathbf{v}]_\gamma$.*

Proof. Since I_V is invertible, its matrix is also invertible. For any $\mathbf{v} \in V$, we have

$$[\mathbf{v}]_\beta = [I_V(\mathbf{v})]_\beta = [I_V]_\gamma^\beta[\mathbf{v}]_\gamma = Q[\mathbf{v}]_\gamma.$$

□

So this matrix Q changes the coordinates of our vector: it changes γ-coordinates into β-coordinates. The inverse, of course, goes the other way, and Q^{-1} changes β coordinates into γ coordinates.

Definition 3.62. We call such an isomorphism a *change of basis map*. The matrix of such an isomorphism is called a *transition matrix*.

Example 3.63. We know that $\beta = \{(1, 0, 0), (0, 1, 0), (0, 0, 1)\}$ and $\gamma = \{(1, 0, 0), (1, 1, 0), (1, 1, 1)\}$ are both bases for $\mathbb{R}^3$. Then we have

$$\begin{aligned} [I_V(1, 0, 0)]_\beta &= [(1, 0, 0)]_\beta = (1, 0, 0) \\ [I_V(1, 1, 0)]_\beta &= [(1, 1, 0)]_\beta = (1, 1, 0) \\ [I_V(1, 1, 1)]_\beta &= [(1, 1, 1)]_\beta = (1, 1, 1) \\ [I_V]_\gamma^\beta &= \begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix}. \end{aligned}$$

If we have the γ coordinates of a vector, this gives us the β coordinates; so if $[\mathbf{v}]_\gamma = (3, 1, 4)$ then we have

$$\begin{aligned}[\mathbf{v}]_\beta &= [I_V]_\gamma^\beta [\mathbf{v}]_\gamma \\ &= \begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 3 \\ 1 \\ 4 \end{bmatrix} = \begin{bmatrix} 8 \\ 5 \\ 4 \end{bmatrix}.\end{aligned}$$

Of course we could have figured this out directly, in this case. Because we know that

$$\mathbf{v} = 3 \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix} + 1 \begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix} + 4 \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix} = \begin{bmatrix} 8 \\ 5 \\ 4 \end{bmatrix}.$$

The really cool bit is that we can invert it. Row reduction gives

$$\left[\begin{array}{ccc|ccc} 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 \end{array}\right] \to \left[\begin{array}{ccc|ccc} 1 & 0 & 0 & 1 & -1 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 \end{array}\right] \to \left[\begin{array}{ccc|ccc} 1 & 0 & 0 & 1 & -1 & 0 \\ 0 & 1 & 0 & 0 & 1 & -1 \\ 0 & 0 & 1 & 0 & 0 & 1 \end{array}\right]$$

and thus we have

$$\left([I_v]_\gamma^\beta\right)^{-1} = \begin{bmatrix} 1 & -1 & 0 \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{bmatrix}.$$

But this is just the matrix that changes coordinates from β to γ. So if I have the vector $\mathbf{v} = (5, -2, 3)$, then we can find

$$\begin{aligned}[\mathbf{v}]_\gamma &= \begin{bmatrix} 1 & -1 & 0 \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 5 \\ -2 \\ 3 \end{bmatrix} \\ &= \begin{bmatrix} 7 \\ -5 \\ 3 \end{bmatrix}.\end{aligned}$$

And indeed we can see that

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

Definition 3.64. A linear transformation $L : V \to V$ is called a *linear operator on* V. We denote the space of linear operators on V by $\mathcal{L}(V) = \mathcal{L}(V, V)$.

If we have a linear operator on V, and a basis on V, then we can get a matrix for that operator. But which matrix we get depends on the basis we choose.

Example 3.65. Let $R_{\pi/2} : \mathbb{R}^2 \to \mathbb{R}^2$ be the linear transformation given by a rotation ninety degrees counterclockwise. We saw earlier that with respect to the standard basis, this transformation has matrix $A = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$. But we can also compute the matrix with respect to, say, $\gamma = \{(1,0),(1,1)\}$. Then we have

$$\begin{aligned} R_{\pi/2}(1,0) &= (0,1) = (1,1) - (1,0) \to (-1,1) \\ R_{\pi/2}(1,1) &= (-1,1) = (1,1) - 2(1,0) \to (-2,1) \\ B &= \begin{bmatrix} -1 & -2 \\ 1 & 1 \end{bmatrix}. \end{aligned}$$

These two matrices represent the same transformation, with respect to different bases. But they are clearly not the same matrix! What's going on here?

The answer is that we changed the coordinate system, and so our matrix changed. After we account for that, we should get the same matrix. To account for this, we need the change of basis matrix between γ and the standard basis β. We have

$$U[I]_\gamma^\beta = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$$

the transition matrix from γ to the standard basis, and thus

$$U^{-1} = \begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix} = [I]_\beta^\gamma$$

is the transition matrix from the standard basis to γ.

If we want to perform the operation $R_{\pi/2}$ on the vectors of F, we can use the matrix B that we found. Alternatively, we can transform our vectors into E-coordinates, use the matrix A, and then transform back into F-coordinates. This operation would be given by $U^{-1}AU$. We calculate that

$$\begin{aligned} U^{-1}AU = [I]_\beta^\gamma [R_{\pi/2}]_\beta^\beta [I]_\gamma^\beta &= \begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \\ &= \begin{bmatrix} -1 & -1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} -1 & -2 \\ 1 & 1 \end{bmatrix} = B = [R_{\pi/2}]_\gamma^\gamma. \end{aligned}$$

This is the same as the matrix $B = [R_{\pi/2}]_\gamma^\gamma$, as it should be.

We can generalize this. Sometimes two different *matrices* are representing the same *transformation*, just in different bases. and in this case, the matrices have to have some basic properties in common. We call these matrices *similar*.

Definition 3.66. If A and B are $n \times n$ matrices, we say they are *similar* if there is some invertible matrix U such that $B = U^{-1}AU$. We write $A \sim B$.

Proposition 3.67. *Let $E = \{\mathbf{e}_1, \dots, \mathbf{e}_n\}, F = \{\mathbf{f}_1, \dots, \mathbf{f}_n\}$ be two bases for V, and let $L : V \to V$ be a linear function. Let U be the transition matrix from F to E.*

If A is the matrix representing L with respect to E, and B is the matrix representing L with respect to F, then $B = U^{-1}AU$.

Example 3.68. Let $D : \mathcal{P}_2(x) \to \mathcal{P}_2(x)$ be the differentiation operator. Let's find the matrix of D with respect to $E = \{1, x, x^2\}$ and with respect to $F = \{1, 2x, 4x^2 - 2\}$.

We've already seen that the matrix of D with spect to E is $A = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 2 \\ 0 & 0 & 0 \end{bmatrix}$.

We can work out the matrix with respect to F directly:

$$\begin{aligned}
D(1) &= 0 \to (0, 0, 0) \\
D(2x) &= 2 \to (2, 0, 0) \\
D(4x^2 - 2) &= 8x \to (0, 4, 0) \\
B &= \begin{bmatrix} 0 & 2 & 0 \\ 0 & 0 & 4 \\ 0 & 0 & 0 \end{bmatrix}
\end{aligned}$$

Alternatively, we could recall that the change of basis matrices between E and F:

$$\begin{aligned}
[I]_F^E &= \begin{bmatrix} 1 & 0 & 1/2 \\ 0 & 1/2 & 0 \\ 0 & 0 & 1/4 \end{bmatrix} = U^{-1} \\
[I]_E^F &= \begin{bmatrix} 1 & 0 & -2 \\ 0 & 2 & 0 \\ 0 & 0 & 4 \end{bmatrix} = U.
\end{aligned}$$

So we can compute the matrix B for D by saying

$$B = U^{-1}AU = \begin{bmatrix} 1 & 0 & 1/2 \\ 0 & 1/2 & 0 \\ 0 & 0 & 1/4 \end{bmatrix} \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 2 \\ 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 & -2 \\ 0 & 2 & 0 \\ 0 & 0 & 4 \end{bmatrix}$$
$$= \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 & -2 \\ 0 & 2 & 0 \\ 0 & 0 & 4 \end{bmatrix} = \begin{bmatrix} 0 & 2 & 0 \\ 0 & 0 & 4 \\ 0 & 0 & 0 \end{bmatrix}.$$

Example 3.69. Let $L : \mathbb{R}^3 \to \mathbb{R}^3$ be given by $L(x, y, z) = (x + 3y + z, 2x - y + 3z, y - z)$. Find the matrix of L with respect to $\{(4, 1, 2), (3, 0, 1), (1, -1, 0)\}$, and show it is similar to the matrix with respect to the standard basis.

We have

$$\begin{aligned} L(1,0,0) &= (1,2,0) \\ L(0,1,0) &= (3,-1,1) \\ L(0,0,1) &= (1,3,-1) \\ A = [L]_E^E &= \begin{bmatrix} 1 & 3 & 1 \\ 2 & -1 & 3 \\ 0 & 1 & -1 \end{bmatrix}. \end{aligned}$$

We can compute the change of basis matrices. If U is the matrix from F to E, then we have

$$U = [I]_F^E \begin{bmatrix} 4 & 3 & 1 \\ 1 & 0 & -1 \\ 2 & 1 & 0 \end{bmatrix}$$

and

$$\left[\begin{array}{ccc|ccc} 4 & 3 & 1 & 1 & 0 & 0 \\ 1 & 0 & -1 & 0 & 1 & 0 \\ 2 & 1 & 0 & 0 & 0 & 1 \end{array}\right] \to \left[\begin{array}{ccc|ccc} 1 & 0 & -1 & 0 & 1 & 0 \\ 4 & 3 & 1 & 1 & 0 & 0 \\ 2 & 1 & 0 & 0 & 0 & 1 \end{array}\right] \to \left[\begin{array}{ccc|ccc} 1 & 0 & -1 & 0 & 1 & 0 \\ 0 & 3 & 5 & 1 & -4 & 0 \\ 0 & 1 & 2 & 0 & -2 & 1 \end{array}\right]$$
$$\to \left[\begin{array}{ccc|ccc} 1 & 0 & -1 & 0 & 1 & 0 \\ 0 & 1 & 2 & 0 & -2 & 1 \\ 0 & 3 & 5 & 1 & -4 & 0 \end{array}\right] \to \left[\begin{array}{ccc|ccc} 1 & 0 & -1 & 0 & 1 & 0 \\ 0 & 1 & 2 & 0 & -2 & 1 \\ 0 & 0 & -1 & 1 & 2 & -3 \end{array}\right]$$
$$\to \left[\begin{array}{ccc|ccc} 1 & 0 & -1 & 0 & 1 & 0 \\ 0 & 1 & 2 & 0 & -2 & 1 \\ 0 & 0 & 1 & -1 & -2 & 3 \end{array}\right] \to \left[\begin{array}{ccc|ccc} 1 & 0 & 0 & -1 & -1 & 3 \\ 0 & 1 & 0 & 2 & 2 & -5 \\ 0 & 0 & 1 & -1 & -2 & 3 \end{array}\right]$$

so we have

$$[I]_E^F = U^{-1} = \begin{bmatrix} -1 & -1 & 3 \\ 2 & 2 & -5 \\ -1 & -2 & 3 \end{bmatrix}.$$

Thus to find the matrix with respect to F, we can compute

$$\begin{aligned} B = U^{-1}AU &= \begin{bmatrix} -1 & -1 & 3 \\ 2 & 2 & -5 \\ -1 & -2 & 3 \end{bmatrix} \begin{bmatrix} 1 & 3 & 1 \\ 2 & -1 & 3 \\ 0 & 1 & -1 \end{bmatrix} \begin{bmatrix} 4 & 3 & 1 \\ 1 & 0 & -1 \\ 2 & 1 & 0 \end{bmatrix} \\ &= \begin{bmatrix} -3 & 1 & -7 \\ 6 & -1 & 13 \\ -5 & 2 & -10 \end{bmatrix} \begin{bmatrix} 4 & 3 & 1 \\ 1 & 0 & -1 \\ 2 & 1 & 0 \end{bmatrix} = \begin{bmatrix} -25 & -16 & -4 \\ 49 & 31 & 7 \\ -38 & -25 & -7 \end{bmatrix}. \end{aligned}$$

There's not a really efficient way to determine whether two matrices are similar in general, although we have a few tools that can tell us two matrices are *not* similar. For instance, any property that belongs to the *transformation*, and not just to the matrix, has to be the same for similar matrices. One example:

Proposition 3.70. *Let $A, B \in M_{n\times n}$ with $A \sim B$. Then A is invertible if and only if B is invertible.*

Proof. HW 8 □

We call properties like these *similarity invariants*. We can never use similarity invariants to prove that two matrices *are* similar, but we can definitely use them to prove that two matrices are *not* similar.

Example 3.71. $A = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ is invertible, but $B = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$ is not. So A is not similar to B.

A less obvious similarity invariant is the *trace*. Recall we defined the trace of a matrix to be the sum of the entries on the main diagonal. It's not at all obvious that this is a similarity invariant, but we'll see soon that it is. That allows us to separate more matrices:

Example 3.72. Let $C = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ and $D = \begin{bmatrix} 2 & 0 \\ 0 & 1 \end{bmatrix}$. Then $\operatorname{Tr}(C) = 2$ and $\operatorname{Tr}(D) = 3$, so C is not similar to D.

But to talk about this more, we first need to spend a bit of time understanding the matrices themselves, and invariants we can attach to them.

4 Matrices and Systems of Equations

In this section we want to spend some time dealing with matrices directly. We've seen a lot of facts about matrices already; here we can collect some of them, and prove some basic facts about matrices.

4.1 Elementary Matrices

Recall in definition 2.56 we had three "elementary matrix operations":

I Interchange two rows.

II Multiply a row by a nonzero real number.

III Replace a row by its sum with a multiple of another row.

At the time we justified these purely in terms of thinking of the corresponding system of equations. But now that we understand matrices themselves better, we can built a theoretical framework for them.

In particular, we can encode the elementary row operations as matrices:

Definition 4.1. An $n \times n$ *elementary matrix* is a matrix obtained by performing an elementary operation on I_n. The elementary matrix is said to be of type 1, type 2, or type 3, depending on which elementary operation was performed on I_n.

Example 4.2. For example, interchanging the second and third rows of I_3 produces the elementary matrix

$$E_1 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}.$$

Multiplying the third row by 2 produces the elementary matrix

$$E_2 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 2 \end{bmatrix}.$$

Subtracting 4 times the first row from the second row yields the elementary matrix

$$E_3 = \begin{bmatrix} 1 & 0 & 0 \\ -4 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

And these elementary matrices do in fact encode everything there is to know about the corresponding row operations.

Proposition 4.3. *Let $A \in M_{m \times n}(\mathbb{F})$ and suppose that B is obtained from A by performing an elementary row operation. Then there exists an $m \times m$ elementary matrix E such that $B = EA$.*

In fact, E is obtained from I_m by performing the same elementary row operation as that which was performed on A to obtain B.

Conversely, if E is an elementary $m \times m$ matrix, then EA is the matrix obtained from A by performing the same elementary row operation as which produces E from I_m.

Proving this is not interesting. But we can do a couple examples and see how the logic works out.

Example 4.4.

$$E_1 A = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & -1 & 3 \\ 4 & 0 & 1 & 2 \end{bmatrix} = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 4 & 0 & 1 & 2 \\ 2 & 1 & -1 & 3 \end{bmatrix} = B,$$

as desired. Similarly,

$$E_2 B = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 2 \end{bmatrix} \begin{bmatrix} 1 & 2 & 3 & 4 \\ 4 & 0 & 1 & 2 \\ 2 & 1 & -1 & 3 \end{bmatrix} = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 4 & 0 & 1 & 2 \\ 4 & 2 & -2 & 6 \end{bmatrix} = C.$$

Finally,

$$E_3 C = \begin{bmatrix} 1 & 0 & 0 \\ -4 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 2 & 3 & 4 \\ 4 & 0 & 1 & 2 \\ 4 & 2 & -2 & 6 \end{bmatrix} = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 0 & -8 & -11 & -14 \\ 4 & 2 & -2 & 6 \end{bmatrix} = D.$$

Proposition 4.5. *Elementary matrices are invertible, and their inverses are also elementary matrices of the same type.*

Proof. Let E be an elementary $n \times n$ matrix. Then by definition, E is obtained by performing an elementary row operation on I_n.

We have already seen that this means that we can obtain I_n from E by performing an elementary row operation. This means that there is an elementary matrix E' such that $E'E = I_n$.

But this means that E is invertible and $E^{-1} = E'$, so its inverse is also an elementary matrix. □

Proposition 4.6. *Every invertible matrix is a product of elementary matrices.*

Proof. By our algorithm, a matrix is invertible if and only if we can row-reduce it to the identity. So if A is an invertible matrix, there is some sequence of row operations that turns it into the identity. Thus we can write

$$\begin{aligned} I_n &= E_1 E_2 \dots E_k A \\ A &= E_k^{-1} \dots E_2^{-1} E_1^{-1} I_n \\ &= E_k^{-1} \dots E_2^{-1} E_1^{-1}. \end{aligned}$$

□

These elementary matrices don't yet allow us to do anything we couldn't do just by identifying row operations. But they're a really useful tool for understanding what those row operations will do.

4.2 Rowspace and Columnspace

Definition 4.7. Let A be a $m \times n$ matrix. The *column space* of A, denoted $\text{col}(A)$, is the subspace of $\mathbb{R}^m$ spanned by the columns of A. The *rowspace* of A, denoted $\text{row}(A)$, is the space spanned by the rows of A.

Remark 4.8. We now have three subspaces attached to a given matrix: the rowspace, columnspace, and nullspace. Some sources will also point to a fourth space $N(A^T)$, but I won't really discuss this until we have the tools to explain why it matters.

There are two facts about these spaces that we can obtain from the work we've already done.

Proposition 4.9. *If A and B are row-equivalent matrices, then they have the same rowspace.*

Proof. We need to check that each elementary row operation doesn't change the span of the set of vectors.

I. (Switch two rows) Switching the order of two vectors does not affect the span at all.

II. (Multiply a row by a nonzero scalar) Multiplying a vector by a non-zero scalar won't change the span of the set of vectors, since in any linear combination we can always just multiply the relevant coefficient by the inverse of our non-zero scalar.

III. (Add a multiple of one row to another) This won't add anything to the span, since a linear combination of the new vectors will still be a linear combination of the old vectors.

This won't lose anything from the span, since we can undo the row operation, and so every old vector is a linear combination of new vectors.

□

This means that it's very easy to find a basis for the rowspace of a matrix: just row reduce it, and look at the result.

Example 4.10. Let

$$A = \begin{bmatrix} 1 & 5 & -9 & 11 \\ -2 & -9 & 15 & -21 \\ 3 & 17 & -30 & 36 \\ -1 & 2 & -3 & -1 \end{bmatrix}.$$

We can row reduce this matrix

$$\begin{bmatrix} 1 & 5 & -9 & 11 \\ -2 & -9 & 15 & -21 \\ 3 & 17 & -30 & 36 \\ -1 & 2 & -3 & -1 \end{bmatrix} \to \begin{bmatrix} 1 & 5 & -9 & 11 \\ 0 & 1 & -3 & 1 \\ 0 & 2 & -3 & 3 \\ 0 & 7 & -12 & 10 \end{bmatrix} \to \begin{bmatrix} 1 & 0 & 6 & 6 \\ 0 & 1 & -3 & 1 \\ 0 & 0 & 3 & 1 \\ 0 & 0 & 9 & 3 \end{bmatrix}$$

$$\to \begin{bmatrix} 1 & 0 & 6 & 6 \\ 0 & 1 & -3 & 1 \\ 0 & 0 & 1 & 1/3 \\ 0 & 0 & 9 & 3 \end{bmatrix} \to \begin{bmatrix} 1 & 0 & 0 & 4 \\ 0 & 1 & 0 & 2 \\ 0 & 0 & 1 & 1/3 \\ 0 & 0 & 0 & 0 \end{bmatrix} \to \begin{bmatrix} 1 & 0 & 0 & 4 \\ 0 & 1 & 0 & 2 \\ 0 & 0 & 1 & 1/3 \\ 0 & 0 & 0 & 0 \end{bmatrix}.$$

Thus a basis for the rowspace of A is $\{(1,0,0,4),(0,1,0,2),(0,0,1,1/3)\}$.

In fact, we can use this technique any time we have a set of vectors and want to find a nice basis for their span: write your vectors as the rows of a matrix, and then row-reduce.

Unfortunately, it's a little tricky to make this into more than a useful computational trick. It's not totally clear what the rowspace means, in terms of the underlying linear transformation. (It's something called the *coimage*, which we won't be worrying about; but we will revisit the geometric interpretation of the rowspace towards the end of the course.)

In contrast, the column space has a straightforward interpretation in terms of the linear function:

Proposition 4.11. *Let A be a $m \times n$ matrix. Then* $\operatorname{col}(A)$ *is the image in* $\mathbb{R}^m$ *of the linear transformation* $L_A : \mathbb{R}^n \to \mathbb{R}^m$ *associated to* A.

Proof. We did all the hard work here way back in section 2.5. We observed that $A\mathbf{x} = \mathbf{b}$ has a solution if and only if $\mathbf{b}$ is in the span of the columns of A, which is precisely the columnspace of A. □

Definition 4.12. We define the *rank* of a matrix A to be the dimension of $\operatorname{col}(A)$.

If A is the matrix of a linear transformation L, then $\operatorname{rk}(L) = \operatorname{rk}(A)$.

It's relatively easy to find the rank, by the following proposition:

Proposition 4.13. *Let A be an $m \times n$ matrix. If P and Q are invertible $m \times m$ and $n \times n$ matrices respectively, then*

(a) $\operatorname{rk}(AQ) = \operatorname{rk}(A)$,

(b) $\operatorname{rk}(PA) = \operatorname{rk}(A)$,

and therefore

(c) $\operatorname{rk}(PAQ) = \operatorname{rk}(A)$.

Proof. (a) Notice that

$$\operatorname{Im}(L_{AQ}) = \operatorname{Im}(L_A L_Q) = L_A L_Q(\mathbb{F}^n) = L_A(\mathbb{F}^n) = \operatorname{Im}(L_A)$$

since $L_Q(\mathbb{F}^n) = \mathbb{F}^n$, since L_Q is surjective. Therefore,

$$\operatorname{rk}(AQ) = \dim \operatorname{Im}(L_{AQ}) = \dim \operatorname{Im}(L_A) = \operatorname{rk}(A).$$

(b) This is a bit more subtle. We have

$$\operatorname{Im}(L_{PA}) = \operatorname{Im}(L_P L_A) = L_P \operatorname{Im}(L_A).$$

Since L_P is an isomorphism, it maps $\operatorname{Im}(L_A)$ to a subspace of the same dimension, and hence it will be true that

$$\dim \operatorname{Im}(L_{PA}) = \dim \operatorname{Im}(L_A)$$

whence $\operatorname{rk}(PA) = \operatorname{rk}(A)$.

(c) Follows from applying (a) and then (b). □

Corollary 4.14. *Elementary row and column operations on a matrix are rank-preserving.*

Remark 4.15. We haven't talked about column operations yet, but they're the same idea as row operations, just on columns. They're less theoretically useful but we can get a bit of work out of them.

But finding a basis for the column space is a little trickier. One option is just to row-reduce the transpose of the matrix. But there's something a little slicker we can do.

Proposition 4.16. *Let A be a $m \times n$ matrix. Let B be the reduced row echelon form of A. Then the set of columns of A that correspond to columns with leading 1s in B is a basis for the columnspace of A.*

Example 4.17. Consider again the matrix

$$A = \begin{bmatrix} 1 & 5 & -9 & 11 \\ -2 & -9 & 15 & -21 \\ 3 & 17 & -30 & 36 \\ -1 & 2 & -3 & -1 \end{bmatrix}.$$

We saw that this has reduced row echelon form

$$\begin{bmatrix} 1 & 0 & 0 & 4 \\ 0 & 1 & 0 & 2 \\ 0 & 0 & 1 & 1/3 \\ 0 & 0 & 0 & 0 \end{bmatrix},$$

which has leading 1s in the first, second, and third columns. So a basis for $\operatorname{col}(A)$ is $\{(1, -2, 3, -1), (5, -9, 17, 2), (-9, 15, -30, -3)\}$.

Remark 4.18. Note that the columns of the reduced matrix do not themselves give a basis for the columnspace/image; we need to take columns from the *original* matrix.

Proof. Clearly the set of columns of A is a spanning set for the columnspace of A. So we just need to figure out which, if any, vectors to remove. Which means we need to determine which vectors have linear dependences.

We claim that row operations don't affect dependences between columns. The columns of A are linearly independent if and only if there is a vector $\mathbf{x}$ such that $A\mathbf{x} = \mathbf{0}$. But the set of solutions to $A\mathbf{x} = \mathbf{0}$ is the same as the set of solutions to $B\mathbf{x} = \mathbf{0}$; that's why row reduction works to solve systems of equations. And that means that the columns of B have the same set of linear dependencies that the columns of A have.

Thus we can remove the columns of A that correspond to dependent columns in B; what is left is the columns in A that correspond to columns with leading ones in B.

□

Corollary 4.19. *Let A be a matrix. Then* $\dim(\text{row}(A)) = \text{rk}(A) = \dim(\text{col}(A))$.

Proof. Let B be the RREF of A. By proposition 4.16, the dimension of the columnspace of A is the number of leading ones in B. But the non-zero rows of B form a basis for $\text{row}(A)$, and thus the dimension of $\text{row}(A)$ is also the number of leading ones in B. □

Proposition 4.20. *Let A be an $m \times n$ matrix of rank r. Then $r \leq m$, $r \leq n$, and by means of a finite number of elementary row and column operations, A can be transformed into the matrix*

$$D = \begin{bmatrix} I_r & O_1 \\ O_2 & O_3 \end{bmatrix}$$

where O_1, O_2, and O_3 are zero matrices [of size $(m-r)\times r$, $r\times(n-r)$ and $(m-r)\times(n-r)$].

Corollary 4.21. *Let A be an $m \times n$ matrix of rank r. Then there exist invertible matrices B and C of sizes $m \times m$ and $n \times n$ such that $D = BAC$ where*

$$D = \begin{bmatrix} I_r & O_1 \\ O_2 & O_3 \end{bmatrix}.$$

Proof. We perform elementary row operations on A by multiplying on the left by $m \times m$ elementary matrices $E_1, \dots, E_p$. We perform elementary column by multiplying on the right by $n \times n$ elementary matrices $G_1, \dots, G_q$. Then in the previous theorem, we have

$$D = E_p E_{p-1} \cdots E_1 A G_1 G_2 \cdots G_q.$$

We know that elementary matrices are invertible, and the product of invertible matrices is invertible. Hence, letting $B = E_p E_{p-1} \cdots E_1$ and $C = G_1 G_2 \cdots G_q$ yields the result. □

4.3 Systems of equations and the Nullspace

Recall we defined:

Definition 4.22. A *system of linear equations* is a system of the form

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

with the a_{ij} and b_is all elements of some field $\mathbb{F}$.

We say this is a system of m equations in n unknowns.

If we take A to be the coefficient matrix

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

and we set

$$\mathbf{x} = \begin{bmatrix} x_1 \\ x_2 \\ \dots \\ x_n \end{bmatrix} \in \mathbb{F}^n \qquad \mathbf{b} = \begin{bmatrix} b_1 \\ b_2 \\ \dots \\ b_m \end{bmatrix} \in \mathbb{F}^m$$

then we can rewrite this system as the matrix equation

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

Then a *solution* to the system is a vector

$$\mathbf{s} = \begin{bmatrix} s_1 \\ s_2 \\ \dots \\ s_n \end{bmatrix} \in \mathbb{F}^n.$$

Some systems of equations are especially nice.

Definition 4.23. A system $A\mathbf{x} = \mathbf{b}$ is *homogeneous* if $\mathbf{b} = \mathbf{0}$. Otherwise it's *nonhomogeneous*.

The set of solutions to a homogeneous system $A\mathbf{x} = \mathbf{0}$ is the *nullspace* of the matrix A, sometimes written $N(A)$. The dimension of the nullspace is the *nullity* of A.

Proposition 4.24. *The nullspace of A is the kernel of the linear transformation associate to A. Consequently it is a subspace of $\mathbb{R}^n$.*

Proof. Let $L : \mathbb{R}^n \to \mathbb{R}^m$ be defined by $L(\mathbf{x}) = A\mathbf{x}$. Then $\ker(L) = \{\mathbf{x} \in \mathbb{R}^n : A\mathbf{x} = \mathbf{0}\}$, which is precisely the definition of the nullspace of A. □

Corollary 4.25 (Rank-Nullity Theorem for matrices)**.** *If $A \in M_{m\times n}$ then* $\operatorname{rk}(A)+\dim(N(A)) = n$.

Proof. The linear transformation associate to A has domain $\mathbb{R}^n$. The rank of this transformation is the rank of A, and the dimension of the kernel is the nullity of A, so this follows from the rank-nullity theorem. □

Corollary 4.26. *If $m < n$, then the system $A\mathbf{x} = \mathbf{0}$ has a nonzero solution.*

Proof. Since the rank is the dimension of the image of the transformation, we have $\operatorname{rk}(A) \leq m$. Thus the nullity is at least $n - m \geq 1$, so the space of solutions has dimension at least 1. Then $\ker(A) \neq \{\mathbf{0}\}$ and thus there is a nonzero element in $\ker(A)$. □

Remark 4.27. If we work over the field $\mathbb{R}$ or $\mathbb{C}$, this in fact implies that $A\mathbf{x} = \mathbf{0}$ has infinitely many solutions. But in a finite field, a finite-dimensional vector space still has finitely many elements. (See homework 9.)

This tells us all the theory we need for homogeneous systems. And we already know how to solve them in practice, using row-reduction. What about non-homogeneous systems? The solution set to a homogeneous system is always a vector space, which gave us all our theory. But the set of solutions to a non-homogeneous system is *never* a vector space:

(a) The zero vector is never a solution, since $A\mathbf{0} = \mathbf{0} \neq \mathbf{b}$.

(b) Adding two solutions doesn't give you another solution:

$$\begin{aligned} A(\mathbf{x}_1 + \mathbf{x}_2) &= A\mathbf{x}_1 + A\mathbf{x}_2 \\ &= \mathbf{b} + \mathbf{b} = 2\mathbf{b} \neq \mathbf{b}. \end{aligned}$$

(c) Multiplying a solution by a scalar doesn't give another solution: $Ar\mathbf{x} = r\mathbf{b} \neq \mathbf{b}$ unless $r = 1$.

But if homogeneous systems are straightforward, we'd like to use what we know about them to answer our new questions.

Definition 4.28. Let $A\mathbf{x} = \mathbf{b}$ be a nonhomogeneous system of linear equations. We say the system $A\mathbf{x} = \mathbf{0}$ is the homogeneous system *corresponding to* $A\mathbf{x} = \mathbf{b}$.

Proposition 4.29. *Suppose $A\mathbf{x} = \mathbf{b}$ is a non-homogeneous linear system.*

If $U = N(A))$ and $\mathbf{x}_0$ is a solution to $A\mathbf{x} = \mathbf{b}$, then the set of solutions to the system $A\mathbf{x} = \mathbf{b}$ is the set

$$N(A) + \mathbf{x}_0 = \{\mathbf{y} + \mathbf{x}_0 : \mathbf{y} \in N(A)\}.$$

Proof. We want to show that two sets are equal, so we show that each is a subset of the other.

First, suppose that $\mathbf{x}_1$ is a solution to $A\mathbf{x}_1 = \mathbf{b}$. Then we have

$$\begin{aligned} b &= A\mathbf{x}_0 \\ b &= A\mathbf{x}_1 \\ b - b &= A\mathbf{x}_1 - A\mathbf{x}_0 = A(\mathbf{x}_1 - \mathbf{x}_0) \\ \mathbf{0} &= A(\mathbf{x}_1 - \mathbf{x}_0). \end{aligned}$$

Thus $\mathbf{y} = \mathbf{x}_1 - \mathbf{x}_0$ is a solution to $A\mathbf{x} = \mathbf{0}$, and then $\mathbf{x}_1 = \mathbf{x}_0 + \mathbf{y}$ for some $\mathbf{y} \in U$.

Conversely, suppose $\mathbf{x}_1 = \mathbf{x}_0 + \mathbf{y}$ for some $\mathbf{y} \in U$. Then

$$A\mathbf{x}_1 = A(\mathbf{x}_0 + \mathbf{y}) = A\mathbf{x}_0 + A\mathbf{y} = \mathbf{b} + \mathbf{0} = \mathbf{b}.$$

Thus x_1 is a solution to $A\mathbf{x} = \mathbf{b}$. □

Remark 4.30. This proof basically used linearity and nothing else. So the same argument works for any linear transformation $L : U \to V$, and any vector equation $L(\mathbf{x}) = \mathbf{b}$.

Example 4.31. Let's find a set of solutions to the system

$$\begin{aligned} x_1 + x_2 + x_3 &= 3 \\ x_1 + 2x_2 + 3x_3 &= 6 \\ 2x_1 + 3x_2 + 4x_2 &= 9. \end{aligned}$$

Gaussian elimination gives

$$\left[\begin{array}{ccc|c} 1 & 1 & 1 & 3 \\ 1 & 2 & 3 & 6 \\ 2 & 3 & 4 & 9 \end{array}\right] \to \left[\begin{array}{ccc|c} 1 & 1 & 1 & 3 \\ 0 & 1 & 2 & 3 \\ 0 & 1 & 2 & 3 \end{array}\right] \to \left[\begin{array}{ccc|c} 1 & 1 & 1 & 3 \\ 0 & 1 & 2 & 3 \\ 0 & 0 & 0 & 0 \end{array}\right] \to \left[\begin{array}{ccc|c} 1 & 0 & -1 & 0 \\ 0 & 1 & 2 & 3 \\ 0 & 0 & 0 & 0 \end{array}\right].$$

Taking $x_3 = \alpha$ as a free variable, our solution set is $\{(\alpha, 3-2\alpha, \alpha)\} = \{(0,3,0)+\alpha(1,-2,1)\}$. Indeed, we see that this set corresponds to elements of the vector space spanned by $\{(1,-2,1)\}$, plus a specific solution $(0,3,0)$.

Alternatively, we could have solved the homogeneous system first, and seen that the solution was $x_1 - x_3 = 0, x_2 + 2x_3 = 0$, telling us that $N(A) = \{\alpha(1,-2,1)\}$. Then we just need to find a solution; to my eyes the obvious solution is $(1,1,1)$. So our theorem tells us that the solution set is $\{(1,1,1) + \alpha(1,-2,1)\}$. This may not *look* like the solution we got before, but it is in fact the same set, since $(1,1,1) = (0,3,0) + (1,-2,1)$.

Corollary 4.32. *Let $A \in M_{n \times n}$. Then the system $A\mathbf{x} = \mathbf{b}$ has exactly one solution if and only if A is invertible.*

Proof. See homework 9 □

We can summarize a lot of our work with

Theorem 4.33. *Let V be an n-dimensional vector space, $L : V \to V$ a linear operator, and A the matrix of V with respect to some ordered basis β. Then the following are equivalent:*

(a) L is an invertible operator.

(b) A is an invertible matrix.

(c) A is injective

(d) A is surjective

(e) $\ker(A) = \{\mathbf{0}\}$.

(f) $\operatorname{rk}(A) = n$

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

(h) For any $b \in V$, the system $A\mathbf{x} = \mathbf{b}$ has a unique solution.

(i) The columns of A are linearly independent.

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

(k) The rows of A are linearly independent.

(l) The rows of A span $\mathbb{R}^n$.

In the next section we'll add a few more items to this list.

5 Eigenvectors and Eigenvalues

In this section we will study a special type of basis, called an eigenbasis. For (almost) any given operator, we get a specific basis which will make most our computations easier.

5.1 Eigenvectors

Definition 5.1. Let $L : V \to V$ be a linear transformation, and let λ be a scalar. If there is a vector $\mathbf{v} \in V$ such that $L\mathbf{v} = \lambda\mathbf{v}$, then we say that λ is an *eigenvalue* of L, and $\mathbf{v}$ is an *eigenvector* with eigenvalue λ.

Geometrically, an eigenvector corresponds to a direction in which our linear operator purely stretches or shrinks vectors, without rotating or reflecting them at all. It can often be an axis of rotation.

Example 5.2. Let $A = \begin{bmatrix} 4 & -2 \\ 1 & 1 \end{bmatrix}$. We can check that if $\mathbf{x} = (2, 1)$, then

$$A\mathbf{x} = \begin{bmatrix} 4 & -2 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} 2 \\ 1 \end{bmatrix} = \begin{bmatrix} 6 \\ 3 \end{bmatrix} = 3 \begin{bmatrix} 2 \\ 1 \end{bmatrix},$$

so $\mathbf{x}$ is an eigenvector with eigenvalue 3. Similarly, we can check that if $\mathbf{y} = (1, 1)$, then

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

Thus $\mathbf{y}$ is an eigenvector with eigenvalue 2.

Example 5.3. Let $R_{\pi/2} : \mathbb{R}^2 \to \mathbb{R}^2$ be the rotation map. We can see geometrically that this has no non-trivial eigenvectors, since it changes the direction of any vector. Algebraically, if (x, y) is an eigenvector, then we would have

$$R_{\pi/2}(x, y) = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} -y \\ x \end{bmatrix} = \begin{bmatrix} \lambda x \\ \lambda y \end{bmatrix}$$

and thus we have $\lambda y = x, \lambda x = -y$, which gives $\lambda^2 y = -y$. So either $y = 0$, or $\lambda^2 = -1$, and the second isn't possible in $\mathbb{R}$. So the only solution here is $x = y = 0$.

Example 5.4. But now suppose we take the same operator, given by the matrix $A = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$, but view it as a map from $\mathbb{C}^2$ to $\mathbb{C}^2$. We have the same calculation, and the same conclusion that $\lambda^2 = -1$, but now this has a solution. In fact, it has two: i and $-i$. So these are the two eigenvalues.

To find eigenvectors, we solve

$$\begin{aligned} A\mathbf{x} &= i\mathbf{x} \\ \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} &= \begin{bmatrix} ix \\ iy \end{bmatrix} \\ \begin{bmatrix} -y \\ x \end{bmatrix} &= \begin{bmatrix} ix \\ iy \end{bmatrix}. \end{aligned}$$

This gives the system

$$\begin{aligned} -y &= ix \\ x &= iy \end{aligned}$$

which is, of course, the same system we found before. So we conclude from the first equation that if $x = 1$ then $y = -i$; we confirm that this is consistent with the second equation. So the vector $\begin{bmatrix} 1 \\ -i \end{bmatrix}$ is an eigenvector with eigenvalue i.

Similarly, if we take $\lambda = -i$ then we get the system

$$\begin{aligned} -y &= -ix \\ x &= -iy \end{aligned}$$

and then if $x = 1$ we have $y = i$. Thus $\begin{bmatrix} 1 \\ i \end{bmatrix}$ is an eigenvector with eigenvalue $-i$.

Example 5.5. In contrast, if we take the rotation map $R : \mathbb{R}^3 \to \mathbb{R}^3$ that rotates around the z-axis, the vector $(0, 0, 1)$ will be an eigenvector with eigenvalue 1.

Example 5.6. Let $V = \mathcal{D}(\mathbb{R}, \mathbb{R})$ be the space of differentiable real functions, and let $\frac{d}{dx} : V \to V$ be the derivative map. If $f(x) = e^{rx}$, then $\frac{d}{dx} f(x) = re^{rx} = rf(x)$, so f is an eigenvector with eigenvalue r.

Proposition 5.7. *Let V be a vector space and $L : V \to V$ a linear transformation.* $\mathbf{v}$ *is an eigenvector with eigenvalue λ if and only if* $\mathbf{v} \in \ker(L - \lambda I)$.

Proof. $\mathbf{v}$ is an eigenvector with eigenvalue λ if and only if $L\mathbf{v} = \lambda\mathbf{v} = \lambda I\mathbf{v}$, if and only if $\mathbf{0} = L\mathbf{v} - \lambda I\mathbf{v} = (L - \lambda I)\mathbf{v}$, if and only if $\mathbf{v} \in \ker(L - \lambda I)$. □

Corollary 5.8. *The set of eigenvectors with eigenvalue λ is a subspace of V, called the* eigenspace *corresponding to λ. We denote this space E_λ.*

Corollary 5.9. *A transformation L is invertible if and only if* 0 *is not an eigenvalue of L.*

Proposition 5.10. *Let $L : V \to V$ be a linear transformation. If $E = \{\mathbf{e}_1, \ldots, \mathbf{e}_n\}$ is a set of eigenvectors each with a distinct eigenvalue, then E is linearly independent.*

Proof. Let λ_i be the eigenvalue corresponding to $\mathbf{e}_i$. Suppose (for contradiction) that E is linearly dependent, and let k be the smallest positive integer such that $\{\mathbf{e}_1, \ldots, \mathbf{e}_k\}$ is linearly dependent; then we must have $a_k \neq 0$, and we can compute

$$\begin{aligned}
\mathbf{e}_k &= \frac{-a_1}{a_k}\mathbf{e}_1 + \cdots + \frac{-a_{k-1}}{a_k}\mathbf{e}_{k-1} \\
L(\mathbf{e}_k) &= L\left(\frac{-a_1}{a_k}\mathbf{e}_1 + \cdots + \frac{-a_{k-1}}{a_k}\mathbf{e}_{k-1}\right) = \frac{-a_1}{a_k}L(\mathbf{e}_1) + \cdots + \frac{-a_{k-1}}{a_k}L(\mathbf{e}_{k-1}) \\
\lambda_k\mathbf{e}_k &= \frac{-a_1}{a_k}\lambda_1\mathbf{e}_1 + \cdots + \frac{-a_{k-1}}{a_k}\lambda_{k-1}\mathbf{e}_{k-1}.
\end{aligned}$$

We can multiply the first equation by λ_1 and subtract from the last equation; this gives us

$$\mathbf{0} = \frac{-a_1}{a_k}(\lambda_1 - \lambda_k)\mathbf{e}_1 + \cdots + \frac{-a_{k-1}}{a_k}(\lambda_{k-1} - \lambda_k)\mathbf{e}_{k-1}.$$

But we know by hypothesis that the set $\{\mathbf{e}_1, \ldots, \mathbf{e}_{k-1}\}$ is linearly independent, so all these coefficients must be zero. Since the a_i are not all zero, we must have at least some $\lambda_i - \lambda_k = 0$. □

Corollary 5.11. *Let V be finite-dimensional, and $L : V \to V$ a linear operator. Then L has at most* $\dim(V)$ *distinct eigenvalues.*

So the set of eigenvectors is linearly independent. If it happens to span V then it's a basis, and that's really nice. Unfortunately that often isn't true.

Example 5.12. Let $A = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$. It's pretty easy to see that 1 should be an eigenvalue of this thing, since

$$A - 1 \cdot I = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$$

has kernel spanned by $(1, 0)$. With a little more work you can convince yourself there's no other eigenvalues; I won't do that here. And that means that the eigenvectors don't span all of $\mathbb{R}^2$.

But you might notice another thing. The eigenspace E_1 is one-dimensional, but it seems like it's *almost* two-dimensional. And in fact if we do our operator *twice*, everything goes away.

$$(A - I)^2 = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$$

has kernel $\mathbb{R}^2$.

Definition 5.13. Let A be a $n \times n$ matrix, and λ and eigenvalue of A. If $\mathbf{v} \in \ker(A - \lambda I)^n$ then we say $\mathbf{v}$ is a *generalized eigenvector* of A.

These aren't critical but we'll be coming back to them a few times.

It's straightforward enough to *check* that a vector is an eigenvector if we already have a candidate; but how do we find them? Sometimes this is easy

Example 5.14. Let $A = \begin{bmatrix} 3 & 0 \\ 0 & 2 \end{bmatrix}$. What are the eigenvalues and eigenspaces of A?

We see that

$$A\mathbf{x} = \begin{bmatrix} 3 & 0 \\ 0 & 2 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 3x \\ 2y \end{bmatrix}.$$

Thus the eigenvalues are 3 and 2; the corresponding eigenspaces are spanned by $(1, 0)$ and $(0, 1)$, respectively.

When things aren't this easy, there is still a fairly straightforward approach we can take:

Example 5.15. Let $B = \begin{bmatrix} 7 & 2 \\ 3 & 8 \end{bmatrix}$. Find the eigenvalues and eigenvectors of B.

If $\mathbf{x} = (x, y)$ is an eigenvector with eigenvalue λ, then we have

$$B\mathbf{x} = \begin{bmatrix} 7x + 2y \\ 3x + 8y \end{bmatrix} = \begin{bmatrix} \lambda x \\ \lambda y \end{bmatrix}$$

so we have the system of equations $7x + 2y = \lambda x, 3x + 8y = \lambda y$. Equivalently, we have $(7 - \lambda)x + 2y = 0$ and $(3x + (8 - \lambda)y = 0$. We row-reduce

$$\begin{bmatrix} 7 - \lambda & 2 \\ 3 & 8 - \lambda \end{bmatrix} \to \begin{bmatrix} 3 & 8 - \lambda \\ 0 & 2 + (8 - \lambda)(\lambda - 7)/3 \end{bmatrix}$$
$$\to \begin{bmatrix} 3 & 8 - \lambda \\ 0 & 6 + (-56 + 15\lambda - \lambda^2) \end{bmatrix} = \begin{bmatrix} 3 & 8 - \lambda \\ 0 & -\lambda^2 + 15\lambda - 50 \end{bmatrix}.$$

We first see that this is solveable if and only if $0 = \lambda^2 - 15\lambda + 50 = (\lambda - 5)(\lambda - 10)$, and thus if $\lambda = 5$ or $\lambda = 10$. Thus these are the two eigenvalues for B.

If $\lambda = 5$ then we have $3x + 3y = 0$ so $y = -x$. Any vector $(\alpha, -\alpha)$ will be an eigenvector with eigenvalue 5, so the eigenspace for 5 is the span of $\{(1, -1)\}$. And indeed, we compute

$$B(1, -1) = \begin{bmatrix} 7 & 2 \\ 3 & 8 \end{bmatrix} \begin{bmatrix} 1 \\ -1 \end{bmatrix} = \begin{bmatrix} 5 \\ -5 \end{bmatrix} = 5 \begin{bmatrix} 1 \\ -1 \end{bmatrix}.$$

If $\lambda = 10$ then we have $3x - 2y = 0$ and $y = 3/2x$. Thus any vector $(2\alpha, 3\alpha)$ will be an eigenvector with eigenvalue 10, and the corresponding eigenspace is spanned by $\{(2, 3)\}$. We check:

$$B(2, 3) = \begin{bmatrix} 7 & 2 \\ 3 & 8 \end{bmatrix} \begin{bmatrix} 2 \\ 3 \end{bmatrix} = \begin{bmatrix} 20 \\ 30 \end{bmatrix} = 10 \begin{bmatrix} 2 \\ 3 \end{bmatrix}.$$

As the previous example shows, it is completely possible to find the eigenvectors and eigenvalues with the tools we have already, but it's pretty fiddly even for a small example. We'd like to streamline the process, and this leads us to define the determinant.

5.2 Determinants

Definition 5.16. Let $A \in M_{n \times n}$. If A has n distinct eigenvalues, we say that the *determinant* of A, written $\det A$, is the product of the eigenvalues.

More generally, the determinant of A is the product of the eigenvalues "up to multiplicity". Thus if the generalized eigenspace of $\lambda = 2$ is three-dimensional, we will multiply in λ three times.

Definition 5.17 (Formal definition)**.**

$$\det A = \prod_{\lambda} \lambda^{e_\lambda} \qquad \text{where} \quad e_\lambda = \dim \ker(A - \lambda I)^n.$$

We can also take a geometric perspective: we will eventually prove the determinant represents the volume of the n-dimensional solid that our matrix sends the n-dimensional unit cube to. Thus it tells us how much our matrix stretches its inputs.

Example 5.18. The determinant of $A = \begin{bmatrix} 3 & 0 \\ 0 & 2 \end{bmatrix}$ is $3 \cdot 2 = 6$.

The determinant of $B = \begin{bmatrix} 7 & 2 \\ 3 & 8 \end{bmatrix}$ is $5 \cdot 10 = 50$.

The determinant of $C = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ is $1^2 = 1$.

The determinant is (roughly) the product of the eigenvalues, so it can tell something about what the eigenvalues are. But this doesn't help if we don't have a way of finding the determinant without already knowing the eigenvalues. Fortunately, there is a straightforward way to compute it.

5.2.1 The Laplace Formula

We first need to develop some notation.

Definition 5.19. Let $A = (a_{ij})$ be a $n \times n$ matrix. We define the i,j*th minor matrix* of A to be the $(n-1) \times (n-1)$ matrix $\widetilde{A}_{ij}$ obtained by deleting the row and column containing a_{ij}—that is, deleting the ith row and jth column.

We define the i,j*th minor* of A to be $\det \widetilde{A}_{ij}$. We define the i,j*th cofactor* to be $A_{ij} = (-1)^{i+j} \det(\widetilde{A}_{ij})$.

Example 5.20. Let

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

Then we have

$$M_{1,1} = \begin{bmatrix} -2 & -1 \\ 3 & 3 \end{bmatrix} \qquad M_{3,2} = \begin{bmatrix} 3 & 2 \\ 5 & -1 \end{bmatrix}.$$

Fact 5.21 (Cofactor Expansion)**.** *Let A be a $n \times n$ matrix.*

If $A \in M_{1\times 1}$ then $A = \begin{bmatrix} a_{11} \end{bmatrix}$ and $\det A = a_{11}$.

Otherwise, for any k we have

$$\begin{aligned} \det(A) &= \sum_{i=1}^n a_{ki}A_{ki} = a_{k1}A_{k1} + a_{k2}A_{k2} + \cdots + a_{kn}A_{kn} \\ &= \sum_{i=1}^n a_{ik}A_{ik} = a_{1k}A_{1k} + a_{2k}A_{2k} + \cdots + a_{nk}A_{nk}. \end{aligned}$$

Thus we may compute the determinant of a matrix inductively, using cofactor expansion. We can expand along any row or column; we should pick the one that makes our job easiest.

Remark 5.22. This is usually taken to be the definition of determinant. Feel free to think of it that way, and the fact about eigenvectors as a theorem.

You can also think of the determinant as the unique multilinear map that satisfies certain properties. You probably shouldn't, at the moment. But you can.

Example 5.23. Let $A = \begin{bmatrix} 3 & 2 & 1 \\ 0 & 5 & 1 \\ 0 & 0 & 2 \end{bmatrix}$. If we expand along the last row, we get

$$\begin{aligned} \det A &= 0 \cdot (-1)^{3+1} \det \begin{bmatrix} 2 & 1 \\ 5 & 1 \end{bmatrix} + 0 \cdot (-1)^{3+2} \det \begin{bmatrix} 3 & 1 \\ 0 & 1 \end{bmatrix} + 2 \cdot (-1)^{3+3} \det \begin{bmatrix} 3 & 2 \\ 0 & 5 \end{bmatrix} \\ &= 2 \det \begin{bmatrix} 3 & 2 \\ 0 & 5 \end{bmatrix} = 2 \left(0 \cdot (-1)^{2+1} \det \begin{bmatrix} 2 \end{bmatrix} + 5 \cdot (-1)^{2+2} \det \begin{bmatrix} 3 \end{bmatrix} \right) \\ &= 2(0 + 5 \cdot 3) = 30. \end{aligned}$$

Example 5.24. Let

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

We'd like to expand along the row or column wiht the most zeros, but we don't have any. I'm going to expand along the bottom row because at least everything is the same.

$$\begin{aligned} \det A &= 3(-1)^{3+1} \det \begin{bmatrix} 1 & 2 \\ -2 & -1 \end{bmatrix} + 3(-1)^{3+2} \det \begin{bmatrix} 3 & 2 \\ 5 & -1 \end{bmatrix} + 3(-1)^{3+3} \begin{bmatrix} 3 & 1 \\ 5 & -2 \end{bmatrix} \\ &= 3\left(1(-1)^{1+1}(-1) + 2(-1)^{1+2}(-2)\right) - 3\left(3(-1)^{1+1}(-1) + 2(-1)^{1+2}5\right) \\ &\quad + 3\left(3(-1)^{1+1}(-2) + 1(-1)^{1+2}(5)\right) \\ &= 3(-1+4) - 3(-3-10) + 3(-6-5) = 9 + 39 - 33 = 15. \end{aligned}$$

Using this method, we can compute the determinant of any size of matrix. But for small matrices we can work out quick formulas that encode all this information.

Proposition 5.25.

$$\det \begin{bmatrix} a & b \\ c & d \end{bmatrix} = ad - bc \qquad \det \begin{bmatrix} a & b & c \\ d & e & f \\ g & h & i \end{bmatrix} = aei + bfg + cdh - gec - hfa - idb.$$

5.2.2 Properties of Determinants

We'd like to do things to make computing determinants easier, in addition to the formulas I just gave. We can start by proving some simple results. This will also allow us to show that the determinant is in fact the product of the eigenvalues.

The most important fact is that the determinant is a *multilinear map*. That is, it's a function of multiple vectors that is linear in each of them.

Proposition 5.26. *If A is a $n \times n$ matrix, then the (Laplace computation of the) determinant is a linear function of each row. Thus for $1 \leq r \leq n$, we have*

$$\det \begin{bmatrix} a_1 \\ \vdots \\ a_{r-1} \\ u + kv \\ a_{r+1} \\ \vdots \\ a_n \end{bmatrix} = \det \begin{bmatrix} a_1 \\ \vdots \\ a_{r-1} \\ u \\ a_{r+1} \\ \vdots \\ a_n \end{bmatrix} + k \det \begin{bmatrix} a_1 \\ \vdots \\ a_{r-1} \\ v \\ a_{r+1} \\ \vdots \\ a_n \end{bmatrix}$$

where $k \in \mathbb{F}$, and u, v and each a_i are row vectors in $\mathbb{F}^n$.

Proof. Let A be an $n \times n$ matrix with rows $a_1, a_2, \dots, a_n$, and suppose that for some $1 \leq r \leq n$, we have that $a_r = u + tv$ for some row vectors u, v and some scalar $t \in \mathbb{F}$. So we have that

$$A = \begin{bmatrix} a_1 \\ \vdots \\ a_{r-1} \\ u + tv \\ a_{r+1} \\ \vdots \\ a_n \end{bmatrix}.$$

Write $u = (b_1, \dots, b_n)$ and $v = (c_1, \dots, c_n)$. Further, let B and C be the matrices obtained from A by replacing row r of A with u and v, respectively. That is,

$$B = \begin{bmatrix} a_1 \\ \vdots \\ a_{r-1} \\ u \\ a_{r+1} \\ \vdots \\ a_n \end{bmatrix} \quad \text{and} \quad C = \begin{bmatrix} a_1 \\ \vdots \\ a_{r-1} \\ v \\ a_{r+1} \\ \vdots \\ a_n \end{bmatrix}.$$

We wish to prove that $\det(A) = \det(B) + t\det(C)$.

We do a cofactor expansion along the first row to compute $\det(A)$, we see that

$$\begin{aligned}\det(A) &= \sum_{i=1}^{n} a_{ri} A_{ri} \\ &= \sum_{i=1}^{n} (u_{ri} + t v_{ri}) A_{ri} \\ &= \sum_{i=1}^{n} u_{ri} A_{ri} + t \sum_{i=1}^{n} v_{ri} A_{ri}.\end{aligned}$$

But we know that $A_{ri} = B_{ri} = C_{ri}$ because all three matrices are identical outside of row r, and thus we have

$$\det(A) = \sum_{i=1}^{n} u_{ri} B_{ri} + t \sum_{i=1}^{n} v_{ri} C_{ri} = \det(B) + t \det(C)$$

as desired. □

Corollary 5.27. *If $A \in M_{n\times n}(\mathbb{F})$ has a row consisting entirely of zeros, then* $\det(A) = 0$*.*

Proof. This is because we can write $\mathbf{0} = \mathbf{0} + \mathbf{0}$. Hence, we have

$$A = \begin{bmatrix} a_1 \\ \vdots \\ \mathbf{0} \\ \vdots \\ a_n \end{bmatrix} = \begin{bmatrix} a_1 \\ \vdots \\ \mathbf{0} + \mathbf{0} \\ \vdots \\ a_n \end{bmatrix}.$$

By the above theorem, we therefore know that

$$\det(A) = \det \begin{bmatrix} a_1 \\ \vdots \\ \mathbf{0} \\ \vdots \\ a_n \end{bmatrix} + \det \begin{bmatrix} a_1 \\ \vdots \\ \mathbf{0} \\ \vdots \\ a_n \end{bmatrix} = \det(A) + \det(A).$$

This shows that $\det(A) = 0$. □

Remark 5.28. We can also prove this pretty easily by doing cofactor expansion along the row of zeroes, but this argument is fun and standard.

There are two basic types of operations we do with matrices. One is elementary row operations, and the other is matrix multiplication; by proposition 4.3 about elementary matrices, row operations are a form of matrix multiplication so those are basically the same thing. So let's think about what elementary row operations do to the determinant. Fortunately, we can figure all of them out by applications of proposition 5.26.

Proposition 5.29. *If $A \in M_{n\times n}(\mathbb{F})$ and B is the matrix obtained from A by interchanging any two rows of A, then* $\det(B) = -\det(A)$.

Proof. Label the rows of A as $a_1, \ldots, a_n$ and suppose that B is obtained by interchanging row r with row s. That is, we have

$$A = \begin{bmatrix} a_1 \\ \vdots \\ a_r \\ \vdots \\ a_s \\ \vdots \\ a_n \end{bmatrix} \quad \text{and} \quad B = \begin{bmatrix} a_1 \\ \vdots \\ a_s \\ \vdots \\ a_r \\ \vdots \\ a_n \end{bmatrix}.$$

We now take the determinant of a cleverly chosen matrix. Namely,

$$0 = \det \begin{bmatrix} a_1 \\ \vdots \\ a_r + a_s \\ \vdots \\ a_r + a_s \\ \vdots \\ a_n \end{bmatrix} = \det \begin{bmatrix} a_1 \\ \vdots \\ a_r \\ \vdots \\ a_r + a_s \\ \vdots \\ a_n \end{bmatrix} + \det \begin{bmatrix} a_1 \\ \vdots \\ a_s \\ \vdots \\ a_r + a_s \\ \vdots \\ a_n \end{bmatrix}$$

$$= \det \begin{bmatrix} a_1 \\ \vdots \\ a_r \\ \vdots \\ a_r \\ \vdots \\ a_n \end{bmatrix} + \det \begin{bmatrix} a_1 \\ \vdots \\ a_r \\ \vdots \\ a_s \\ \vdots \\ a_n \end{bmatrix} + \det \begin{bmatrix} a_1 \\ \vdots \\ a_s \\ \vdots \\ a_r \\ \vdots \\ a_n \end{bmatrix} + \det \begin{bmatrix} a_1 \\ \vdots \\ a_s \\ \vdots \\ a_s \\ \vdots \\ a_n \end{bmatrix} = 0 + \det(A) + \det(B) + 0$$

and so $\det(B) = -\det(A)$. □

Proposition 5.30. *Let $A \in M_{n\times n}(\mathbb{F})$ and let B be the matrix obtained by adding a multiple of one row of A to another row of A. Then* $\det(B) = \det(A)$.

Proof. Again, let $a_1, \dots, a_n$ be the rows of A, and suppose that B is obtained by adding k times row s to row r. We then have

$$\det(B) = \det \begin{bmatrix} a_1 \\ \vdots \\ a_r + ka_s \\ \vdots \\ a_s \\ \vdots \\ a_n \end{bmatrix} = \det \begin{bmatrix} a_1 \\ \vdots \\ a_r \\ \vdots \\ a_s \\ \vdots \\ a_n \end{bmatrix} + k \det \begin{bmatrix} a_1 \\ \vdots \\ a_s \\ \vdots \\ a_s \\ \vdots \\ a_n \end{bmatrix} = \det(A) + 0,$$

as desired. □

Theorem 5.31 (Row Operations)**.** *Let $A \in M_{n\times n}(\mathbb{F})$. Then if we do an elementary row operation:*

(a) Interchanging two rows multiplies the determinant by -1.

(b) Multiplying a row by a scalar multiplies the determinant by that scalar.

(c) Adding a multiple of one row to another row does not change the determinant.

Proof. (a) This is proposition 6.21.

(b) This follows directly from proposition 5.26.

(c) This is proposition 5.30.

□

Example 5.32.

$$\det \begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & 0 \\ 1 & 1 & 2 \end{bmatrix} = 1 \qquad \det \begin{bmatrix} 3 & 3 & 3 \\ 0 & 1 & 0 \\ 1 & 1 & 2 \end{bmatrix} = 3$$

$$\det \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix} = -1 \qquad \det \begin{bmatrix} 4 & 4 & 4 \\ 0 & 1 & 0 \\ 1 & 1 & 2 \end{bmatrix} = 3 + 1 = 4.$$

This is enough to tell us all about invertible matrices, but we need a to briefly discuss singular matrices before we can tie everything together.

Lemma 5.33. *Let* $A \in M_{n\times n}(\mathbb{F})$*. If* $\mathrm{rk}(A) < n$ *then* $\det(A) = 0$*.*

Proof. If $\mathrm{rk}(A) < n$ then the rows of A are linearly dependent. Then we can write some row as a linear combination of the others; without loss of generality, say

$$a_n = c_1 a_1 + c_2 a_2 + \dots c_{n-1} a_{n-1}.$$

If we subtract $c_i a_i$ from the nth row, that for every i, we get a matrix with a row of all zeroes, and thus this new matrix has determinant 0. But these row operations don't change the determinant, and thus $\det(A) = 0$. □

Theorem 5.34. *Let* $A, B \in M_{n\times n}(\mathbb{F})$*. Then* $\det(AB) = \det(A)\det(B)$*.*

Proof. If either A or B is singular, then AB is singular, so $\det(AB) = \det(A)\det(B) = 0$.

Suppose A and B are both invertible. Then we can write A as a product of elementary matrices.

First let's consider the case where A is an elementary matrix. Because we know how row operations affect the determinant, we can check that:

(a) If A is a type 1 elementary matrix, then $\det(A) = -1$ and $\det(AB) = -\det(B)$.

(b) If A is a type 2 elementary matrix, then $\det(A) = k$ and $\det(AB) = k\det(B)$.

(c) If A is a type 3 elementary matrix, then $\det(A) = 1$ and $\det(AB) = \det(B)$.

Now let A be any invertible matrix. We can write $A = E_m \dots E_2 E_1$, and we have

$$\begin{aligned}
\det(AB) &= \det(E_m \cdots E_2 E_1 B) \\
&= \det(E_m) \cdot \det(E_{m-1} \cdots E_2 E_1 B) \\
&\vdots \\
&= \det(E_m) \cdots \det(E_2) \cdot \det(E_1) \cdot \det(B) \\
&= \det(E_m \cdots E_1) \cdot \det(B) \\
&= \det(A) \cdot \det(B)
\end{aligned}$$

as desired.

□

Corollary 5.35. *Let $A \in M_{n\times n}(\mathbb{F})$. Then A is invertible if and only if* $\det(A) \neq 0$. *If A is invertible, then* $\det(A^{-1}) = \frac{1}{\det(A)}$.

Proof. We know that if A is not invertible, then $\det(A) = 0$.

If A is invertible, then A^{-1} exists, and we can write

$$1 = \det(I_n) = \det(AA^{-1}) = \det(A)\det(A^{-1}).$$

This proves that $\det(A) \neq 0$, and further dividing both sides by $\det(A^{-1})$ gives the desired equality.

□

Remark 5.36. We can add this to theorem 4.33 as another characterization of invertibility.

There are a few other ways to think about why this result is true.

From the eigenvalue perspective: $\det A$ is the product of the eigenvalues. Thus $\det A = 0$ if and only if 0 is an eigenvalue of A. But 0 is an eigenvalue of A if and only if A has non-trivial kernel, and A is invertible if and only if $\ker(A)$ is trivial.

From the cofactor perspective: if A is invertible it is row-equivalent to the identity matrix, which has determinant 1. None of the row operations can change a determinant from zero to non-zero or vice versa, so $\det A$ is nonzero.

Conversely, if A is not invertible, it is row-equivalent to a matrix with a row of all zeros, which has determinant zero. Since row operations cannot change a determinant from non-zero to zero, $\det A = 0$ as well.

We end with a couple final useful facts about the determinant:

Proposition 5.37. $\det A^T = \det A$.

Proof. Do a cofactor expansion along the column of A^T that corresponds to the row you expanded along in A, or vice versa. □

Proposition 5.38. *If A is a $n\times n$ triangular matrix, then* $\det A$ *is the product of the diagonal entries of A.*

Proof. Homework 10. □

Fact 5.39. *If* $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ *then* $A^{-1} = \frac{1}{\det A}\begin{bmatrix} d & -b \\ -c & a \end{bmatrix} = \frac{1}{ad-bc}\begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$.

We check this by multiplying the two of them:

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}\frac{1}{ad-bc}\begin{bmatrix} d & -b \\ -c & a \end{bmatrix} = \frac{1}{ad-bc}\begin{bmatrix} ad-bc & -ab+ba \\ cd-dc & -bc+ad \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}.$$

5.3 Characteristic Polynomials

Now that we've figured out how determinants work, we can use them to find eigenvalues.

Definition 5.40. We say that $\chi_A(\lambda) = \det(A - \lambda I)$ is the *characteristic polynomial* of A. This is a polynomial in one variable, λ. We call the equation $\chi_A(\lambda) = 0$ the *characteristic equation* of A.

Proposition 5.41. *The real number λ is an eigenvalue of A if and only if it is a root of the characteristic polynomial of A. That is, the roots of $\chi_A(\lambda)$ is the set of eigenvalues of A.*

Proof. Recall that $\mathbf{v}$ is an eigenvector with eigenvalue λ if and only if $\mathbf{v} \in \ker(A - \lambda I)$. Thus λ is an eigenvalue if and only if $\ker(A - \lambda I)$ has nontrivial kernel, which occurs if and only if $\det(A - \lambda I) = 0$. □

Definition 5.42. If

$$\chi_A(\lambda) = (\lambda - \lambda_1)^{n_1}(\lambda - \lambda_2)^{n_2} \dots (\lambda - \lambda_k)^{n_k}$$

then we say that the *algebraic multiplicity* of the eigenvalue λ_i is n_i.

We say that the *geometric multiplicity* of λ_i is $\dim(\ker(A - \lambda_i I_n)^n)$.

We will (hopefully) see that the algebraic and geometric multiplicities are the same.

Remark 5.43. This definition implicitly assumes we're working in the complex numbers, because every polynomial can be factored completely in that field.

Example 5.44. Find the eigenvalues and corresponding eigenspaces of $A = \begin{bmatrix} 3 & 2 \\ 3 & -2 \end{bmatrix}$.

The characteristic equation is

$$\begin{aligned} 0 = \chi_A(\lambda) &= \begin{vmatrix} 3-\lambda & 2 \\ 3 & -2-\lambda \end{vmatrix} \\ &= (3-\lambda)(-2-\lambda) - 2 \cdot 3 = -6 - 3\lambda + 2\lambda + \lambda^2 - 6 \\ &= \lambda^2 - \lambda - 12 = (\lambda - 4)(\lambda + 3) \end{aligned}$$

so the eigenvalues are 4 and -3. We compute

$$A - 4I = \begin{bmatrix} -1 & 2 \\ 3 & -6 \end{bmatrix} \to \begin{bmatrix} 1 & -2 \\ 0 & 0 \end{bmatrix}$$

so $\ker(A-4I) = \{\alpha(2,1)\}$. Thus the eigenspace corresponding to 4 is $E_4 = \operatorname{span}\{(2,1)\}$. Similarly,

$$A + 3I = \begin{bmatrix} 6 & 2 \\ 3 & 1 \end{bmatrix} \to \begin{bmatrix} 3 & 1 \\ 0 & 0 \end{bmatrix}$$

so $\ker(A+3I) = \{\alpha(-1,3)\}$. Thus the eigenspace $E_{-3} = \operatorname{span}\{(-1,3)\}$.

Example 5.45. Find the eigenvalues and corresponding eigenspaces of $A = \begin{bmatrix} 5 & 1 \\ 3 & 3 \end{bmatrix}$.

The characteristic equation is

$$\begin{aligned} 0 = \chi_A(\lambda) &= \left| \begin{pmatrix} 5-\lambda & 1 \\ 3 & 3-\lambda \end{pmatrix} \right| \\ &= (3-\lambda)(5-\lambda) - 1\cdot 3 = 15 - 8\lambda + \lambda^2 - 3 \\ &= \lambda^2 - 8\lambda + 12 = (\lambda-6)(\lambda-2) \end{aligned}$$

so the eigenvalues are 6 and 2.

$$A - 6I = \begin{bmatrix} -1 & 1 \\ 3 & -3 \end{bmatrix} \to \begin{bmatrix} -1 & 1 \\ 0 & 0 \end{bmatrix}$$

has kernel $\{\alpha(1,1)\}$, so the eigenspace $E_6 = \operatorname{span}\{(1,1)\}$.

$$A - 2I = \begin{bmatrix} 3 & 1 \\ 3 & 0 \end{bmatrix} \to \begin{bmatrix} 3 & 1 \\ 0 & 0 \end{bmatrix}$$

has kernel $\{\alpha(-1,3)\}$, so the eigenspace $E_2 = \operatorname{span}\{(-1,3)\}$.

Example 5.46. Find the eigenvalues and corresponding eigenspaces of $A = \begin{bmatrix} 2 & -3 & 1 \\ 1 & -2 & 1 \\ 1 & -3 & 2 \end{bmatrix}$.

The characteristic equation is

$$\begin{aligned} 0 = \chi_A(\lambda) &= \left| \begin{pmatrix} 2-\lambda & -3 & 1 \\ 1 & -2-\lambda & 1 \\ 1 & -3 & 2-\lambda \end{pmatrix} \right| \\ &= (2-\lambda)(-2-\lambda)(2-\lambda) - 3 - 3 - ((-2-\lambda) - 3(2-\lambda) - 3(2-\lambda)) \\ &= -\lambda^3 + 2\lambda^2 + 4\lambda - 8 - 6 + 2 + \lambda + 12 - 6\lambda \\ &= -\lambda^3 + 2\lambda^2 - \lambda = -\lambda(\lambda-1)^2 \end{aligned}$$

so the eigenvalues are 0 and 1 (twice). We have

$$A - 0I = \begin{bmatrix} 2 & -3 & 1 \\ 1 & -2 & 1 \\ 1 & -3 & 2 \end{bmatrix} \to \begin{bmatrix} 1 & 0 & -1 \\ 0 & 1 & -1 \\ 0 & 0 & 0 \end{bmatrix}$$

so $\ker(A) = \{\alpha(1,1,1)\}$, and $E_0 = \operatorname{span}\{(1,1,1)\}$. We also have

$$A - I = \begin{bmatrix} 1 & -3 & 1 \\ 1 & -3 & 1 \\ 1 & -3 & 1 \end{bmatrix} \to \begin{bmatrix} 1 & -3 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}$$

so $\ker(A - I) = \{\alpha(3,1,0) + \beta(-1,0,1)\}$, and $E_1 = \operatorname{span}\{(3,1,0), (-1,0,1)\}$.

We can use this same setup to find eigenvalues and eigenvectors for an operator on some other finite-dimensional space.

Example 5.47. Let T be the linear operator on $\mathcal{P}_2(\mathcal{R})$ defined by $T(f(x)) = f(x) + (x + 1)f'(x)$, and let $\beta = \{1, x, x^2\}$. Then we have the matrix

$$A = [T]_\beta = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 2 & 2 \\ 0 & 0 & 3 \end{bmatrix}.$$

The characteristic polynomial of T is then

$$\det(A - \lambda I_3) = \det \begin{bmatrix} 1-\lambda & 1 & 0 \\ 0 & 2-\lambda & 2 \\ 0 & 0 & 3-\lambda \end{bmatrix} = (1-\lambda)(2-\lambda)(3-\lambda).$$

Hence, the eigenvalues of T are precisely $\lambda = 1$, 2, or 3.

We can think about finding the eigenvectors in two ways. One is to work directly: We can for instance try to solve

$$\begin{aligned} T(ax^2 + bx + c) &= ax^2 + bx + c \\ ax^2 + bx + c + (x+1)(2ax + b) &= ax^2 + bx + c \\ 2ax^2 + (2a + b)x + b &= 0 \end{aligned}$$

and thus we find that $a = 0, b = 0$, and c is a free variable; thus E_1 is spanned by $\{1\}$.

But that's a lot of work when we've done the work already! We can say that

$$[E_1]_\beta = \ker\left(\begin{bmatrix} 0 & 1 & 0 \\ 0 & 1 & 2 \\ 0 & 0 & 2 \end{bmatrix}\right) = \ker\left(\begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{bmatrix}\right) = \operatorname{span}\left\{\begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}\right\}$$
$$[E_2]_\beta = \ker\left(\begin{bmatrix} -1 & 1 & 0 \\ 0 & 0 & 2 \\ 0 & 0 & 1 \end{bmatrix}\right) = \ker\left(\begin{bmatrix} 1 & -1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{bmatrix}\right) = \operatorname{span}\left\{\begin{bmatrix} -1 \\ 1 \\ 0 \end{bmatrix}\right\}$$
$$[E_3]_\beta = \ker\left(\begin{bmatrix} -2 & 1 & 0 \\ 0 & -1 & 2 \\ 0 & 0 & 0 \end{bmatrix}\right) = \ker\left(\begin{bmatrix} 1 & 0 & -1 \\ 0 & 1 & -2 \\ 0 & 0 & 0 \end{bmatrix}\right) = \operatorname{span}\left\{\begin{bmatrix} 1 \\ 2 \\ 1 \end{bmatrix}\right\}$$

and thus

$$E_1 = \operatorname{span}\{1\}$$
$$E_2 = \operatorname{span}\{x-1\}$$
$$E_2 = \operatorname{span}\{x^2+2x+1\}$$

Proposition 5.48. *If A is a $n \times n$ matrix over $\mathbb{R}$ and n is odd, then A has at least one eigenvalue.*

Proof. Recall that a degree n polynomial always has at least one real root if n is odd. Thus if $A \in M_{n\times n}$, $\chi_A(\lambda)$ is degree n, and has a real root, which is an eigenvalue of A. □

Example 5.49. Find the eigenvalues and corresponding eigenspaces of $B = \begin{bmatrix} 2 & 0 & 0 \\ 0 & 4 & 0 \\ 1 & 0 & 2 \end{bmatrix}$.

Since this matrix is triangluar, we know the eigenvalues are $2, 4, 2$. We solve

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

and $\ker(A-2I) = \{\alpha(0,0,1)\}$, so $E_2 = \operatorname{span}\{(0,0,1)\}$. Similarly,

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

so $\ker(A - 4I) = \{\alpha(0, 1, 0)\}$ so $E_4 = \operatorname{span}\{(0, 1, 0)\}$.

Notice that in this case, the span of the eigenvectors is only 2-dimensional; the eigenvectors don't span the whole domain.

Over the complex numbers, things work a little better.

Proposition 5.50. *If A is a $n \times n$ matrix over $\mathbb{C}$, then it has at least one eigenvalue.*

Proof. The characteristic polynomial will have at least one root over the complex numbers by the Fundamental Theorem of Alebra. □

Lemma 5.51. *Let $A \in M_{n\times n}(\mathbb{R})$. If $\lambda \in \mathbb{C}$ is an eigenvalue for A, then $\overline{\lambda} \in \mathbb{C}$ is also an eigenvalue, with the same multiplicity.*

Proof. If all the entries of A are real numbers, then $\chi_A(\lambda)$ will be a real polynomial, and complex roots of a real polynomial always come in complex-conjugate pairs. □

Example 5.52. Let $B = \begin{bmatrix} .5 & -.6 \\ .75 & 1.1 \end{bmatrix}$. We can work out the characteristic polynomial is

$$\chi_B(\lambda) = \det \begin{bmatrix} .5 - \lambda & -.6 \\ .75 & 1.1 - \lambda \end{bmatrix} = (.5 - \lambda)(1.1 - \lambda) - (-.6)(.75) = \lambda^2 - 1.6\lambda + 1.$$

By the Fundamental Theorem of Algebra, this quadratic must have two complex roots; by the Quadratic Formula, we see that they are $.8 \pm .6i$. Let's set $\lambda = .8 + .6i$ and find the λ eigenspace. We have

$$\begin{bmatrix} .5 - (.8 + .6i) & -.6 \\ .75 & 1.1 - (.8 + .6i) \end{bmatrix} = \begin{bmatrix} -.3 - .6i & -.6 \\ .75 & .3 - .6i \end{bmatrix}$$

This would be a pain to row-reduce, but we don't actually have to; we already know this has non-trivial kernel, so the second row must be some multiple of the first, even if we're too lazy to figure out which multiple. So we can just say that we want to solve $.75x_1 + (.3 - .6i)x_2 = 0$, and we get $x_1 = (-.4 + .8i)x_2$, so the eigenspace is $E_\lambda = \{((-.4 + .8i)x_2, x_2)\}$. To find an eigenvector, we can take $x_2 = 10$ so $x_1 = -4 + 8i$, and we have that one eigenvector is $(-4 + 8i, 10)$.

We might also want to find the other eigenspace, corresponding to $E_{\overline{\lambda}}$. But we don't have to do any more work here! Our matrix B was defined over the real numbers, so everything is preserved by complex conjugation. We know that $E_\lambda = \left\{ \begin{bmatrix} (-4 + 8i)\alpha \\ 10\alpha \end{bmatrix} \right\}$, so we know that

$$E_{\overline{\lambda}} = \overline{\left\{ \begin{bmatrix} (-4 + 8i)\alpha \\ 10\alpha \end{bmatrix} \right\}} = \left\{ \begin{bmatrix} (-4 - 8i)\alpha \\ 10\alpha \end{bmatrix} \right\}$$

What does this tell us? We see that while neither eigenvalue is 1 or -1, both eigenvalues have *magnitude* 1: $|.8 + .6i| = .64 + .36 = 1$. This tells us that the linear transformation will give some sort of rotation.

It turns out that a matrix with complex eigenvalues always represents some sort of rotation.

5.4 Diagonalization

We now reach the payoff to all this. Throughout section 3, and particularly in section 3.6, we saw that we could choose a basis to work in, and different bases would produce nicer or more awkward matrices for the same linear operator. Now we can say, if we find the eigenvectors of a linear operator and the give us a (eigen)basis for our space, we can always find a matrix representation of our linear operator with a *particularly* nice matrix.

Definition 5.53. If D is a $n \times n$ matrix such that $a_{ij} = 0$ whenever $i \neq j$, we say that D is *diagonal*.

Proposition 5.54. *Let* $D = \begin{bmatrix} d_{11} & 0 & \dots & 0 \\ 0 & d_{22} & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & d_{nn} \end{bmatrix}$ *be a diagonal* $n \times n$ *matrix. Then:*

- *Each standard basis vector* $\mathbf{e}_i$ *is an eigenvector of* D *with eigenvalue* d_{ii}.
- $\det(D) = \prod_{i=1}^n d_{ii}$ *is the product of the diagonal entries.*
- $\mathbb{R}^n$ *is spanned by the eigenvectors of* D.

Proof.

- We have

$$D\mathbf{e}_i = \begin{bmatrix} d_{11} & 0 & \dots & 0 \\ 0 & d_{22} & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & d_{nn} \end{bmatrix} \begin{bmatrix} 0 \\ \vdots \\ 1 \\ \vdots \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ \vdots \\ d_{ii} \\ \vdots \\ 0 \end{bmatrix} = d_{ii}\mathbf{e}_i.$$

- The determinant is the product of the eigenvalues, which are the diagonal entries.
- The standard basis vectors are eigenvalues, and span $\mathbb{R}^n$.

∎

Definition 5.55. We say a linear transformation is *diagonalizable* if its matrix in some basis is diagonal.

We say a matrix is *diagonalizable* if its linear transformation is diagonalizable. Thus A is diagonalizable if A is similar to some diagonal matrix.

Proposition 5.56. *Let A be a $n \times n$ matrix. Then:*

(a) A is diagonalizable if and only if the eigenvectors of A span $\mathbb{R}^n$.

(b) A is diagonalizable if and only if it has n linearly independent eigenvectors.

(c) If A has n distinct eigenvalues, then A is diagonalizable.

Proof. (a) Suppose A is diagonalizable, i.e. there is an invertible matrix U and a diagonal matrix D such that $A = U^{-1}DU$. Let F be the image of the standard basis under U^{-1}; then

$$A\mathbf{f}_i = U^{-1}DU\mathbf{f}_i = U^{-1}D\mathbf{e}_i = U^{-1}d_{ii}\mathbf{e}_i = d_{ii}U^{-1}\mathbf{e}_i = d_{ii}\mathbf{f}_i.$$

Thus $\mathbf{f}_i$ is an eigenvector for each i, so we have a basis of eigenvectors.

Conversely Suppose the eigenvectors of A span $\mathbb{R}^n$. Then in particular there is a basis $F = \{\mathbf{f}_1, \dots, \mathbf{f}_n\}$ of eigenvectors. Let U be the matrix that sends the standard basis to F. Then for each i we have

$$U^{-1}AU\mathbf{e}_i = U^{-1}A\mathbf{f}_i = U^{-1}\lambda_i\mathbf{f}_i = \lambda_i U^{-1}\mathbf{f}_i = \lambda_i\mathbf{e}_i$$

and thus $U^{-1}AU$ is a diagonal matrix with $d_{ii} = \lambda_i$. Thus A is diagonalizable.

(b) A set of n linearly independent vectors is a basis for $\mathbb{R}^n$. Thus A has n linearly indpendent eigenvectors if and only if the eigenvectors span $\mathbb{R}^n$.

(c) Let $F = \{\mathbf{f}_1, \dots, \mathbf{f}_n\}$ be a set of eigenvectors corresponding to each eigenvalue. Then this set is linearly independent by proposition 5.10, and thus A has n linearly independent eigenvectors.

□

Remark 5.57. Notice that the converse of (3) is not true, by which we mean that it would be false if we said "if and only if". For instance, the identity has only one eigenvalue, but is clearly diagonalizable (and actually diagonal already).

Corollary 5.58. *If A is a $n \times n$ matrix and $F = \{\mathbf{f}_1, \dots, \mathbf{f}_n\}$ is a basis of eigenvectors, and U is the matrix sending the standard basis to F, then $D = U^{-1}AU$ is a diagonal matrix.*

We say that the matrix U diagonalizes *A.*

Remark 5.59. Diagonalization is not unique; the matrix U depends on the choice of basis. However, since the diagonal entries are the eigenvalues, they will be the same (up to reordering) for any diagonalization.

Example 5.60. Let $A = \begin{bmatrix} 3 & 2 \\ 3 & -2 \end{bmatrix}$. We know (from example 5.44) that the eigenvalues are 4 and -3, so the matrix is diagonalizable; the corresponding eigenvectors are $(2, 1)$ and $(-1, 3)$. So we set

$$\begin{aligned} U &= \begin{bmatrix} 2 & -1 \\ 1 & 3 \end{bmatrix} \\ U^{-1} &= \frac{1}{7}\begin{bmatrix} 3 & 1 \\ -1 & 2 \end{bmatrix} \\ U^{-1}AU &= \frac{1}{7}\begin{bmatrix} 3 & 1 \\ -1 & 2 \end{bmatrix}\begin{bmatrix} 3 & 2 \\ 3 & -2 \end{bmatrix}\begin{bmatrix} 2 & -1 \\ 1 & 3 \end{bmatrix} = \frac{1}{7}\begin{bmatrix} 3 & 1 \\ -1 & 2 \end{bmatrix}\begin{bmatrix} 8 & 3 \\ 4 & -9 \end{bmatrix} \\ &= \frac{1}{7}\begin{bmatrix} 28 & 0 \\ 0 & -21 \end{bmatrix} = \begin{bmatrix} 4 & 0 \\ 0 & -3 \end{bmatrix}. \end{aligned}$$

Example 5.61. Let $A = \begin{bmatrix} 2 & -3 & 1 \\ 1 & -2 & 1 \\ 1 & -3 & 2 \end{bmatrix}$. We saw in example 5.46 that the eigenvalues are $0, 1, 1$. The eigenvectors are $(1, 1, 1), (3, 1, 0), (-1, 0, 1)$, so we set

$$\begin{aligned} U &= \begin{bmatrix} 1 & 3 & -1 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix} \\ U^{-1} &= \begin{bmatrix} -1 & 3 & -1 \\ 1 & -2 & 1 \\ 1 & -3 & 2 \end{bmatrix} \end{aligned}$$

and then

$$U^{-1}AU = \begin{bmatrix} -1 & 3 & -1 \\ 1 & -2 & 1 \\ 1 & -3 & 2 \end{bmatrix} \begin{bmatrix} 2 & -3 & 1 \\ 1 & -2 & 1 \\ 1 & -3 & 2 \end{bmatrix} \begin{bmatrix} 1 & 3 & -1 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix}$$
$$= \begin{bmatrix} -1 & 3 & -1 \\ 1 & -2 & 1 \\ 1 & -3 & 2 \end{bmatrix} \begin{bmatrix} 0 & 3 & -1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

Example 5.62. We saw in example 5.49 that the matrix $B = \begin{bmatrix} 2 & 0 & 0 \\ 0 & 4 & 0 \\ 1 & 0 & 2 \end{bmatrix}$ had eigenspaces $E_2 = \text{span}\{(0,0,1)\}$ and $E_4 = \text{span}\{(0,1,0)\}$. The eigenvectors do not span $\mathbb{R}^3$, so A is not diagonalizable.

In general I don't really expect triangular matrices with repeated eigenvalues to be diagonal, but treating this thought fully is beyond the scope of this course.

There are a few major uses for diagonalization. The first is to tell us the basis we "should" be working in, and to allow us to change bases to that basis. The basis in which your operator is diagonal is the basis in which your operator is "really" working; it divides your space up into the dimensions along which your operator really works.

Eigenvectors and diagonalization are often used in various sorts of data analysis. The eigenvector corresponding to the largest eigenvalue is the most significant input, so diagonalization can tell us which components of our data are most important to whatever phenomenon we're studying; this is the idea behind "principal component analysis". If we have time we'll return to this at the end of class.

They are also used in various sorts of approximate computations: if your linear operator has eigenvalues of 5, 3, 1, .1, .1, -.1, .0005, you can get a pretty good approximation of your operator by ignoring the eigenvectors corresponding to the small eigenvalues, and only worrying about the large ones. This is important in a lot of numeric computation.

Finally, we can use diagonalization to simplify many matrix computations. We need to make two observations: one about diagonal matrices, the other about similar matrices.

Proposition 5.63. *Suppose C and D are two diagonal matrices with diagonal entries given* *by c_{ii}, d_{ii} respectively. Then their product is a diagonal matrix given by*

$$\begin{bmatrix} c_{11} & 0 & 0 & \dots & 0 \\ 0 & c_{22} & 0 & \dots & 0 \\ 0 & 0 & c_{33} & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & c_{nn} \end{bmatrix} \begin{bmatrix} d_{11} & 0 & 0 & \dots & 0 \\ 0 & d_{22} & 0 & \dots & 0 \\ 0 & 0 & d_{33} & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & d_{nn} \end{bmatrix} = \begin{bmatrix} c_{11}d_{11} & 0 & 0 & \dots & 0 \\ 0 & c_{22}d_{22} & 0 & \dots & 0 \\ 0 & 0 & c_{33}d_{33} & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & c_{nn}d_{nn} \end{bmatrix}.$$

Proposition 5.64. *If $A = U^{-1}BU$, then $A^n = U^{-1}B^nU$.*

Proof.

$$\begin{aligned} A^n = (U^{-1}BU)^n &= U^{-1}BUU^{-1}BU \dots U^{-1}BUU^{-1}BU \\ U^{-1}BI_nB \dots IBIBU &= U^{-1}BB \dots BBU = U^{-1}B^nU. \end{aligned}$$

□

Example 5.65. Let Let $A = \begin{bmatrix} 3 & 2 \\ 3 & -2 \end{bmatrix}$. Find A^5.

If $U^{-1}AU = D$, then $UU^{-1}AUU^{-1} = UDU^{-1}$ and thus $A = UDU^{-1}$. So

$$\begin{aligned} D = \begin{bmatrix} 4 & 0 \\ 0 & -3 \end{bmatrix} &= \frac{1}{7}\begin{bmatrix} 3 & 1 \\ -1 & 2 \end{bmatrix}\begin{bmatrix} 3 & 2 \\ 3 & -2 \end{bmatrix}\begin{bmatrix} 2 & -1 \\ 1 & 3 \end{bmatrix} = U^{-1}AU \\ A = \begin{bmatrix} 3 & 2 \\ 3 & -2 \end{bmatrix} &= \begin{bmatrix} 2 & -1 \\ 1 & 3 \end{bmatrix}\begin{bmatrix} 4 & 0 \\ 0 & -3 \end{bmatrix}\frac{1}{7}\begin{bmatrix} 3 & 1 \\ -1 & 2 \end{bmatrix} = UDU^{-1} \\ A^5 = \begin{bmatrix} 3 & 2 \\ 3 & -2 \end{bmatrix}^5 &= \left(\begin{bmatrix} 2 & -1 \\ 1 & 3 \end{bmatrix}\begin{bmatrix} 4 & 0 \\ 0 & -3 \end{bmatrix}\frac{1}{7}\begin{bmatrix} 3 & 1 \\ -1 & 2 \end{bmatrix}\right)^5 \\ &= \begin{bmatrix} 2 & -1 \\ 1 & 3 \end{bmatrix}\begin{bmatrix} 4 & 0 \\ 0 & -3 \end{bmatrix}^5\frac{1}{7}\begin{bmatrix} 3 & 1 \\ -1 & 2 \end{bmatrix} \\ &= \begin{bmatrix} 2 & -1 \\ 1 & 3 \end{bmatrix}\begin{bmatrix} 1024 & 0 \\ 0 & -243 \end{bmatrix}\frac{1}{7}\begin{bmatrix} 3 & 1 \\ -1 & 2 \end{bmatrix} \\ &= \frac{1}{7}\begin{bmatrix} 2 & -1 \\ 1 & 3 \end{bmatrix}\begin{bmatrix} 3072 & 1024 \\ 243 & -486 \end{bmatrix} \\ &= \frac{1}{7}\begin{bmatrix} 5901 & 2534 \\ 3801 & -434 \end{bmatrix} = \begin{bmatrix} 843 & 362 \\ 543 & -62 \end{bmatrix}. \end{aligned}$$

Example 5.66. Let $A = \begin{bmatrix} 2 & -3 & 1 \\ 1 & -2 & 1 \\ 1 & -3 & 2 \end{bmatrix}$. Find a formula for A^n.

We have

$$\begin{aligned}
\begin{bmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} &= \begin{bmatrix} -1 & 3 & -1 \\ 1 & -2 & 1 \\ 1 & -3 & 2 \end{bmatrix} \begin{bmatrix} 2 & -3 & 1 \\ 1 & -2 & 1 \\ 1 & -3 & 2 \end{bmatrix} \begin{bmatrix} 1 & 3 & -1 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix} \\
\begin{bmatrix} 2 & -3 & 1 \\ 1 & -2 & 1 \\ 1 & -3 & 2 \end{bmatrix} &= \begin{bmatrix} 1 & 3 & -1 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix} \begin{bmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} -1 & 3 & -1 \\ 1 & -2 & 1 \\ 1 & -3 & 2 \end{bmatrix} \\
\begin{bmatrix} 2 & -3 & 1 \\ 1 & -2 & 1 \\ 1 & -3 & 2 \end{bmatrix}^n &= \left(\begin{bmatrix} 1 & 3 & -1 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix} \begin{bmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} -1 & 3 & -1 \\ 1 & -2 & 1 \\ 1 & -3 & 2 \end{bmatrix} \right)^n \\
&= \begin{bmatrix} 1 & 3 & -1 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix} \begin{bmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}^n \begin{bmatrix} -1 & 3 & -1 \\ 1 & -2 & 1 \\ 1 & -3 & 2 \end{bmatrix} \\
&= \begin{bmatrix} 1 & 3 & -1 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix} \begin{bmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} -1 & 3 & -1 \\ 1 & -2 & 1 \\ 1 & -3 & 2 \end{bmatrix} \\
&= \begin{bmatrix} 2 & -3 & 1 \\ 1 & -2 & 1 \\ 1 & -3 & 2 \end{bmatrix}.
\end{aligned}$$

Corollary 5.67. *If A is a diagonalizable matrix whose eigenvalues are only zero or one, then $A^n = A$ for any n.*

We can actually extend this even further, and talk about matrix exponentiation.

At first it's not even clear what it would mean to compute e^A where A is a matrix. But we know from Calculus 2 that we can define $e^x = \exp(x)$ by its Taylor series:

$$\exp(x) = \sum_{k=0}^{\infty} \frac{x^k}{k!} = 1 + x + \frac{x^2}{2} + \frac{x^3}{3!} + \frac{x^4}{4!} + \dots$$

We are perfectly capable of plugging a matrix into this formula, so we can define

$$e^A = 1 + A + \frac{1}{2}A^2 + \frac{1}{3!}A^3 + \frac{1}{4!}A^4 + \dots$$

But if D is diagonal, we can compute e^D just by exponentiating each entry; and it turns out that this whole operation plays nicely with transition matrices and changing coordinates. So if $A = U^{-1}DU$ then $e^A = U^{-1}e^D U$ is easy to compute.

This sort of matrix exponentiation is really important in a lot of differential equations modeling problems. It solves multi-dimensional differential equations similar to the single-variable $y' = ky$ that is solved by the regular exponential function.

5.4.1 The Jordan Canonical Form

Not every operator is diagonalizable. But over $\mathbb{C}$, every operator is almost diagonalizable, in a specific way.

Fact 5.68. *Suppose $T : \mathbb{F} \to \mathbb{F}$ is a linear operator whose characteristic polynomial factors completely into linear terms. (If $\mathbb{F} = \mathbb{C}$ then this is always true.) Then there is a basis β for $\mathbb{F}^n$ such that*

$$[T]_\beta = \begin{bmatrix} A_1 & 0 & \dots & 0 \\ 0 & A_2 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & A_k \end{bmatrix},$$

where each A_i has the form

$$A_i = \begin{bmatrix} \lambda & 1 & 0 & \dots & 0 & 0 \\ 0 & \lambda & 1 & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & \lambda & 1 \\ 0 & 0 & 0 & \dots & 0 & \lambda \end{bmatrix}$$

for some eigenvalue λ of T.

We call this the Jordan Canonical Form *of T. It is unique up to the ordering of the blocks. It reflects the structure of the eigenvectors and generalized eigenvectors of T.*

I'm not going to prove this because we're out of time. But from here you can see that $\det(T)$ is the product of the eigenvalues up to multiplicity, which we claimed at the beginning of this section.

5.5 Application: Markov Chains

We can combine all these ideas about eigenvalues, similarity, and diagonalization to provide tools to analyze random processes.

Example 5.69. Suppose at a certain time. 70% of the population lives in the suburbs, and 30% lives in the city. But each year, 6% of the people living in the suburbs move to the city, and 2% of the people living in the city move to the suburbs. What happens after a year? Five years? Ten years?

And what is the equilibrium distribution?

Because these rates of transition are *constant*, we can model this with a matrix. If s is the number of people in the suburbs, and c is the number in the city, then next year we'll have $.94s + .02c$ people in the suburbs, and $.06s + .98c$ people in the city. With our numbers, that gives 66.4% in the suburbs, and 33.6% in the city.

We could repeat this calculation to find out what happens in two years, and then three, et cetera. But it's simpler, first, if we turn this into a matrix. If we think of (s, c) as a vector in $\mathbb{R}^2$, then the population changes according to the following matrix:

$$A = \begin{bmatrix} .94 & .02 \\ .06 & .98 \end{bmatrix}.$$

Thus after one year the population distribution will be $A \begin{bmatrix} .7 \\ .3 \end{bmatrix}$ and after five years it will be $A^5 \begin{bmatrix} .7 \\ .3 \end{bmatrix}$. This matrix A is called a *transition matrix*, although it has nothing to do with the change of basis matrices we discussed in section 3.6. Instead, it measures what fraction of a population transitions from one state to another—in this case, from the suburbs to the city or vice versa. Notice that every column sums up to 1. This isn't an accident; exactly 100% of a population has to go somewhere.

So now we can answer our earlier questions, if we can compute A^5 and A^{10}. We saw in 5.4 that this is easy if we *diagonalize* the matrix A. We can compute the eigenvectors, and see that A has an eigenvector $(1, 3)$ with eigenvalue 1, and an eigenvector $(-1, 1)$ with eigenvalue .92. Then we compute

$$\begin{aligned} U &= \begin{bmatrix} 1 & -1 \\ 3 & 1 \end{bmatrix} \\ U^{-1} &= \frac{1}{4} \begin{bmatrix} 1 & 1 \\ -3 & 1 \end{bmatrix} \\ A = UDU^{-1} &= \frac{1}{4} \begin{bmatrix} 1 & -1 \\ 3 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & .92 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ -3 & 1 \end{bmatrix}. \end{aligned}$$

This allows us to compute our exponentials:

$$\begin{aligned}
A^5 = UD^5U^{-1} &= \frac{1}{4}\begin{bmatrix} 1 & -1 \\ 3 & 1 \end{bmatrix}\begin{bmatrix} 1 & 0 \\ 0 & .92^5 \end{bmatrix}\begin{bmatrix} 1 & 1 \\ -3 & 1 \end{bmatrix} \\
&\approx \frac{1}{4}\begin{bmatrix} 1 & -1 \\ 3 & 1 \end{bmatrix}\begin{bmatrix} 1 & 0 \\ 0 & .66 \end{bmatrix}\begin{bmatrix} 1 & 1 \\ -3 & 1 \end{bmatrix} \approx \begin{bmatrix} .744 & .085 \\ .256 & .915 \end{bmatrix} \\
A^5 \begin{bmatrix} .7 \\ .3 \end{bmatrix} \approx \begin{bmatrix} .55 \\ .45 \end{bmatrix}.
\end{aligned}$$

Thus after five years we'll have about 55% of people in the suburbs, and 45% in the city.

For ten years, we can do the same computation.

$$\begin{aligned}
A^{10} = UD^5U^{-1} &= \frac{1}{4}\begin{bmatrix} 1 & -1 \\ 3 & 1 \end{bmatrix}\begin{bmatrix} 1 & 0 \\ 0 & .92^{10} \end{bmatrix}\begin{bmatrix} 1 & 1 \\ -3 & 1 \end{bmatrix} \\
&\approx \frac{1}{4}\begin{bmatrix} 1 & -1 \\ 3 & 1 \end{bmatrix}\begin{bmatrix} 1 & 0 \\ 0 & .60 \end{bmatrix}\begin{bmatrix} 1 & 1 \\ -3 & 1 \end{bmatrix} \approx \begin{bmatrix} .576 & .141 \\ .424 & .859 \end{bmatrix} \\
A^{10} \begin{bmatrix} .7 \\ .3 \end{bmatrix} \approx \begin{bmatrix} .45 \\ .55 \end{bmatrix}.
\end{aligned}$$

So after ten years, we'll have 45% of people in the suburbs, and 55% in the city.

But how do we answer our final question, about the equilibrium? Here we want something like $\lim_{n\to\infty} A^n$. Without diagonalization this would be really hard to compute. But it's easy to see that $\lim_{n\to\infty} D^n = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$, and thus we get

$$\begin{aligned}
\lim_{n\to\infty} A^n = \lim_{n\to\infty} UD^nU^{-1} &= \frac{1}{4}\begin{bmatrix} 1 & -1 \\ 3 & 1 \end{bmatrix}\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}\begin{bmatrix} 1 & 1 \\ -3 & 1 \end{bmatrix} = \begin{bmatrix} 1/4 & 1/4 \\ 3/4 & 3/4 \end{bmatrix} \\
\lim_{n\to\infty} A^n \begin{bmatrix} .7 \\ .3 \end{bmatrix} \approx \begin{bmatrix} 1/4 \\ 3/4 \end{bmatrix}.
\end{aligned}$$

Thus the equilibrium state is where 25% of people live in the suburbs and 75% live in the cities. Which maybe we could have guessed from the start, since that makes the populations moving each way equal.

This entire process is very flexible. Any time the probability of transitioning from one state to another is constant, and only depends on which state you start in, we can model our system with a matrix like A, which we call a *Markov process*. In that case, the sequence of vectors $\mathbf{v}_1 = A\mathbf{v}, \mathbf{v}_2 = A^2\mathbf{v}, \ldots$ is called a *Markov chain*.

Each column of A is a *probability vector*, which is a vector of non-negative numbers that add up to one. Each row and each column corresponds to a particular possible state, and each entry tells us the probability of moving into the column-state if we start out in the row-state.

We can use this system to find the projected state after a finite number of steps, but even more usefully we can use it to project the equilibrium state.

Example 5.70. Suppose our matrix of transition probabilities is $B = \begin{bmatrix} .7 & .2 \\ .3 & .8 \end{bmatrix}$. This matrix has eigenvalues $1/2, 1$ with eigenvectors $(1, -1)$ and $(2, 3)$. Then we can diagonalize:

$$U = \begin{bmatrix} 1 & 2 \\ -1 & 3 \end{bmatrix}$$
$$U^{-1} = \frac{1}{5}\begin{bmatrix} 3 & -2 \\ 1 & 1 \end{bmatrix}$$

$$\begin{aligned} D = U^{-1}BU &= \frac{1}{5}\begin{bmatrix} 3 & -2 \\ 1 & 1 \end{bmatrix}\begin{bmatrix} .7 & .2 \\ .3 & .8 \end{bmatrix}\begin{bmatrix} 1 & 2 \\ -1 & 3 \end{bmatrix} = \frac{1}{5}\begin{bmatrix} 3 & -2 \\ 1 & 1 \end{bmatrix}\begin{bmatrix} .5 & 2 \\ -.5 & 3 \end{bmatrix} \\ &= \frac{1}{5}\begin{bmatrix} 2.5 & 0 \\ 0 & 5 \end{bmatrix} = \begin{bmatrix} .5 & 0 \\ 0 & 1 \end{bmatrix} \\ B = UDU^{-1} &= \begin{bmatrix} 1 & 2 \\ -1 & 3 \end{bmatrix}\begin{bmatrix} .5 & 0 \\ 0 & 1 \end{bmatrix}\frac{1}{5}\begin{bmatrix} 3 & -2 \\ 1 & 1 \end{bmatrix} \end{aligned}$$

Then we can easily exponentiate.

$$\begin{aligned} B^n &= \left(\begin{bmatrix} 1 & 2 \\ -1 & 3 \end{bmatrix}\begin{bmatrix} .5 & 0 \\ 0 & 1 \end{bmatrix}\frac{1}{5}\begin{bmatrix} 3 & -2 \\ 1 & 1 \end{bmatrix}\right)^n \\ &= \begin{bmatrix} 1 & 2 \\ -1 & 3 \end{bmatrix}\begin{bmatrix} .5 & 0 \\ 0 & 1 \end{bmatrix}^n\frac{1}{5}\begin{bmatrix} 3 & -2 \\ 1 & 1 \end{bmatrix} \\ \lim_{n\to\infty} B^n &= \begin{bmatrix} 1 & 2 \\ -1 & 3 \end{bmatrix}\begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}\frac{1}{5}\begin{bmatrix} 3 & -2 \\ 1 & 1 \end{bmatrix} = \frac{1}{5}\begin{bmatrix} 1 & 2 \\ -1 & 3 \end{bmatrix}\begin{bmatrix} 0 & 0 \\ 1 & 1 \end{bmatrix} = \frac{1}{5}\begin{bmatrix} 2 & 2 \\ 3 & 3 \end{bmatrix} = \begin{bmatrix} .4 & .4 \\ .6 & .6 \end{bmatrix}. \end{aligned}$$

Thus in the equilibrium, we will have 40% of people in state one, and 60% in state two.

You might have noticed something both of these examples have in common. Both A and B had 1 as an eigenvalue. And our steady-state vectors were in fact eigenvectors with eigenvalue 1. As you might guess, this isn't a coincidence.

Not every Markov process converges to a steady-state vector. But if it converges, the steady state will be an eigenvector with eigenvalue 1.

Further, convergence is guaranteed if all the entries of the matrix are positive (and nonzero). And convergence is also guaranteed if there is only one eigenvector of magnitude 1 (even after taking absolute values).

Example 5.71. Suppose you run a car dealership that does long-term car leases. You lease sedans, sports cars, minivans, and SUVs. At the end of each year, your clients have the option to trade in to a different style of car. Empirically, you find that you get the following transition matrix:

$$C = \begin{bmatrix} .80 & .10 & .05 & .05 \\ .10 & .80 & .05 & .05 \\ .05 & .05 & .80 & .10 \\ .05 & .05 & .10 & .80 \end{bmatrix}$$

Thus if someone has a sedan this year, they are 80% likely to take a sedan next year, 10% likely to take a sports car, and 5% each likely to take a minivan or an SUV.

We find that C has the eigenvalues $1, .8, .7, .7$, with corresponding eigenvalues

$$\begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \end{bmatrix}, \begin{bmatrix} -1 \\ -1 \\ 1 \\ 1 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \\ -1 \\ 1 \end{bmatrix}, \begin{bmatrix} -1 \\ 1 \\ 0 \\ 0 \end{bmatrix}$$

Thus it will have a steady-state equilibrium. In particular, in a steady state, equal numbers of customers will lease each type of car, no matter what the distribution is right now.

Example 5.72. As a final, non-numerical example, this is how the Google PageRank algorithm works.

They treat web browsing as a random process: given that you are currently on one web page, you have some (small) probability of winding up on any other web page. Of course, this probability is higher if the page you're on links to the new page prominently, so the probability of winding up on any given page is not equal.

Then they build a giant $n \times n$ matrix, where n is the number of web pages they have analyzed. Each column corresponds to a particular web page, and the entries tell you how likely you are to go to any other web page next.

Then they compute the eigenvectors and eigenvalues of this matrix. Or at least, they compute the eigenvector with eigenvalue 1. (Since the matrix is all positive, this is guaranteed to exist, and there are relatively efficient ways to find it.) This gives you an equilibrium probability: if you browse the web for an arbitrarily long period of time, how likely are you to land on this page?

And that is, roughly speaking, the page rank. The more likely you are to land on a given web page, from this Markov chain model, the more highly ranked the page is.

6 Inner Product Spaces and Geometry

In this section we're going to consider vector spaces from a more geometric perspective. In $\mathbb{R}^3$ we have the geometric ideas of "distance" and "angle", but neither of those is necessarily present in an arbitrary vector space. Here we will introduce a new structure called an "Inner Product" that allows us to generalize the angles and distances of $\mathbb{R}^3$ to any vector space with an inner product structure.

6.1 The Dot Product and Inner Products

Definition 6.1. Let $\mathbf{u} = (u_1, \dots, u_n), \mathbf{v} = (v_1, \dots, v_n) \in \mathbb{R}^n$. We define the *dot product* of $\mathbf{u}$ and $\mathbf{v}$ by

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

This is sometimes also called the *scalar product* on $\mathbb{R}^n$.

Remark 6.2. If we think of $\mathbf{u}$ and $\mathbf{v}$ as $n \times 1$ matrices, we can think of $\mathbf{u} \cdot \mathbf{v} = \mathbf{u}^T \mathbf{v}$, the product of a $n \times 1$ matrix with a $1 \times n$ matrix.

The dot product has a number of useful properties. First of all, it allows us to define the length or magnitude of a vector.

Definition 6.3. Let $\mathbf{v} = (v_1, \dots, v_n) \in \mathbb{R}^n$. We define the *magnitude* of $\mathbf{v}$ to be

$$\|\mathbf{v}\| = \sqrt{\mathbf{v} \cdot \mathbf{v}} = \sqrt{v_1^2 + v_2^2 + \cdots + v_n^2}.$$

Notice that this is just the usual definition of distance; in the plane this is

$$\|(x, y)\| = \sqrt{x^2 + y^2},$$

which is just the pythagorean theorem.

Sometimes it's useful to talk about the distance between two points, rather than the length of a vector. But the distance between two points is the length of the vector between them, so we can define the distance between $\mathbf{x}$ and $\mathbf{y}$ to be

$$d(\mathbf{x}, \mathbf{y}) = \|\mathbf{x} - \mathbf{y}\|.$$

We sometimes want to be able to talk about the direction of a vector without worrying about the magnitude. In this case we may wish to comput the *unit vector* given by $\frac{\mathbf{u}}{\|\mathbf{u}\|}$. This vector will clearly have magnitude 1, and point in the same direction that $\mathbf{u}$ does.

The dot product has a few important properties:

Proposition 6.4. *Let* $\mathbf{u}, \mathbf{v} \in \mathbb{R}^n$. *Then:*

(a) *(Positive definite)* $\mathbf{u} \cdot \mathbf{u} \geq 0$, *and if* $\mathbf{u} \cdot \mathbf{u} = 0$ *then* $\mathbf{u} = \mathbf{0}$.

(b) *(Symmetric)* $\mathbf{u} \cdot \mathbf{v} = \mathbf{v} \cdot \mathbf{u}$.

(c) *(Bilinear) The function defined by* $L(\mathbf{x}) = \mathbf{x} \cdot \mathbf{v}$ *is linear, and the function defined by* $T(\mathbf{y}) = \mathbf{u} \cdot \mathbf{y}$ *is linear.*

Proof. (a) $\mathbf{u} \cdot \mathbf{u} = u_1^2 + u_2^2 + \cdots u_n^2$. Each term is non-negative since each term is a real square, so the sum is non-negative. The sum is zero if and only if each term is zero, if and only if $\mathbf{u} = (0, \ldots, 0) = \mathbf{0}$.

(b) $\mathbf{u} \cdot \mathbf{v} = u_1 v_1 + \cdots + u_n v_n = v_1 u_1 + \cdots + v_n u_n = \mathbf{v} \cdot \mathbf{u}$.

(c) We'll prove linearity in the first coordinate; the proof for the second coordinate is identical.

Fix $\mathbf{v} \in \mathbb{R}^n$ and let $\mathbf{x}, \mathbf{y} \in \mathbb{R}^n$ and $r \in \mathbb{R}$. Define $L(\mathbf{x}) = \mathbf{x} \cdot \mathbf{v}$. Then

$$\begin{aligned} L(r\mathbf{x}) &= (r\mathbf{x}) \cdot \mathbf{v} = (rx_1)v_1 + \cdots + (rx_n)v_n = r(x_1 v_1 + \cdots + x_n v_n) = rL(\mathbf{x}) \\ L(\mathbf{x} + \mathbf{y}) &= (\mathbf{x} + \mathbf{y}) \cdot \mathbf{v} = (x_1 + y_1)v_1 + \cdots + (x_n + y_n)v_n \\ &= (x_1 v_1 + \cdots + x_n v_n) + (y_1 v_1 + \cdots + y_n v_n) = L(\mathbf{x}) + L(\mathbf{y}). \end{aligned}$$

□

The dot product also allows us to compute the angle between two vectors.

Proposition 6.5. *If* $\mathbf{u}, \mathbf{v}$ *are two nonzero vectors in* $\mathbb{R}^n$, *and the angle between them is* θ, *then*

$$\mathbf{u} \cdot \mathbf{v} = \|\mathbf{u}\| \|\mathbf{v}\| \cos\theta.$$

Proof. We can form a triangle with sides $\mathbf{u}, \mathbf{v}$, and $\mathbf{u} - \mathbf{v}$. Then by the law of cosines (which I'm sure you all remember from high school trigonometry), we have

$$\|\mathbf{u} - \mathbf{v}\|^2 = \|\mathbf{u}\|^2 + \|\mathbf{v}\|^2 - 2\|\mathbf{u}\| \|\mathbf{v}\| \cos\theta.$$

Then we compute

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

□

Thus the angle between two vectors is given by $\cos\theta = \frac{\mathbf{u}\cdot\mathbf{v}}{\|\mathbf{u}\|\|\mathbf{v}\|}$.

Example 6.6. Let $\mathbf{u} = (3,4)$ and $\mathbf{v} = (-1,7)$. Then $\mathbf{u}\cdot\mathbf{v} = 3\cdot(-1) + 4\cdot 7 = 25$.

We can compute $\|u\| = \sqrt{3^2+4^2} = 25$ and $\|\mathbf{v}\| = \sqrt{(-1)^2+7^2} = 5\sqrt{2}$. The distance between them is $\|\mathbf{u}-\mathbf{v}\| = \|(4,-3)\| = \sqrt{4^2+(-3)^2} = 5$.

The angle between them is given by

$$\cos\theta = \frac{\mathbf{u}\cdot\mathbf{v}}{\|\mathbf{u}\|\|\mathbf{v}\|} = \frac{25}{5\cdot 5\sqrt{2}} = \frac{1}{\sqrt{2}} = \frac{\sqrt{2}}{2}$$
$$\theta = \arccos\left(\frac{\sqrt{2}}{2}\right) = \frac{\pi}{4}.$$

We'd like to extend this idea to other vector spaces. But first we have to think a bit about other *fields*. In particular, we have to say something about the complex numbers $\mathbb{C}$.

In the real numbers we can define the absolute value as $|x| = \sqrt{x^2}$. But in the complex numbers that doesn't quite work, because z^2 may not be a positive real number. So, you may recall, we defined $|z| = \sqrt{z\overline{z}}$. In order to get our positive definiteness, we need to do something similar.

Definition 6.7. Let $\mathbf{u} = (u_1,\dots,u_n), \mathbf{v} = (v_1,\dots,v_n) \in \mathbb{C}^n$. We define the *dot product* of $\mathbf{u}$ and $\mathbf{v}$ by

$$\mathbf{u}\cdot\mathbf{v} = u_1\overline{v_1} + \cdots + u_n\overline{v_n} = \sum_{i=1}^n u_i\overline{v_i}.$$

Then just as we did before, we can define

$$\begin{aligned}\|\mathbf{u}\| &= \sqrt{\mathbf{u}\cdot\mathbf{u}}\\ &= \sqrt{u_1\overline{u_1} + \cdots + u_n\overline{u_n}}\\ &= \sqrt{|u_1|^2 + \cdots + |u_n|^2}.\end{aligned}$$

This resulting product is positive definite, just as the real dot product was. But it's not *quite* symmetric or bilinear. In particular, we can see that

$$\begin{aligned}\mathbf{u}\cdot\mathbf{v} &= u_1\overline{v_1} + \cdots + u_n\overline{v_n}\\ &= \overline{v_1}u_1 + \cdots + \overline{v_n}u_n\\ &= \overline{v_1\overline{u_1} + \cdots + v_n\overline{u_n}}\\ &= \overline{\mathbf{v}\cdot\mathbf{u}}.\end{aligned}$$

Similarly, we still see that $(r\mathbf{u}) \cdot \mathbf{v} = r(\mathbf{u} \cdot \mathbf{v})$, but $\mathbf{u} \cdot (r\mathbf{v}) = \overline{r}(\mathbf{u} \cdot \mathbf{v})$. Thus the complex dot product is linear in the first coordinate, but *conjugate linear* in the second coordinate; we call such a product *sesquilinear*.

(Note that the real dot product is also conjugate linear and sesquilinear: because the conjugate of a real number is just the original number, we can just ignore the conjugation.)

And now we are ready to define:

Definition 6.8. Let $\mathbb{F} = \mathbb{R}$ or $\mathbb{C}$, and let V be a vector space over $\mathbb{F}$. An *inner product* on V is an operation that takes in two vectors $\mathbf{u}, \mathbf{v} \in V$ and returns a real number $\langle \mathbf{u}, \mathbf{v} \rangle$, satisfying the following conditions:

(a) (Positive Definite) $\langle \mathbf{u}, \mathbf{u} \rangle \geq 0$, and $\langle \mathbf{u}, \mathbf{u} \rangle = 0$ if and only if $\mathbf{u} = \mathbf{0}$.

(b) (Conjugate Symmetric) $\langle \mathbf{u}, \mathbf{v} \rangle = \overline{\langle \mathbf{v}, \mathbf{u} \rangle}$.

(c) (Sesquilinear) $\langle \alpha\mathbf{u}+\beta\mathbf{v}, \mathbf{w} \rangle = \alpha\langle \mathbf{u}, \mathbf{w} \rangle + \beta\langle \mathbf{v}, \mathbf{w} \rangle$, and $\langle \mathbf{u}, \alpha\mathbf{v}+\beta\mathbf{w} \rangle = \overline{\alpha}\langle \mathbf{u}, \mathbf{v} \rangle + \overline{\beta}\langle \mathbf{u}, \mathbf{w} \rangle$.

We write the *norm* of a vector $\mathbf{v}$ as $\|\mathbf{v}\| = \sqrt{\langle \mathbf{v}, \mathbf{v} \rangle}$; the norm is always ≥ 0, and is equal to zero if and only if $\mathbf{v} = \mathbf{0}$.

Remark 6.9. Why are we limiting ourselves to just the reals and complexes? We could study symmetric bilinear products (or "bilinear symmetric forms") over any field. The sticking point is the first issue: we require $\langle \mathbf{u}, \mathbf{u} \rangle \geq 0$, and this requires us to have a field with some sense of "positive number", which a finite field does not. Similarly, we want to define the norm, which requires the square root to be a real thing.

The dot products, both real and complex, are examples of inner products, but there are other important examples we can see.

Example 6.10. Let $V = \mathcal{C}([a,b], \mathbb{R})$ be the space of continuous functions on $[a,b]$, and define an inner product by

$$\langle f, g \rangle = \int_a^b f(t)g(t)\,dt.$$

Then

(a) $\langle f, f \rangle = \int_a^b f(t)^2\,dt \geq 0$ since $f(t)^2 \geq 0$; and further the integral is zero if and only if $f(t)^2 = 0$ everywhere.

(b) $\langle f, g \rangle = \int_a^b f(t)g(t)\,dt = \int_a^b g(t)f(t)\,dt = \langle g, f \rangle$.

(c) $\langle \alpha f + \beta g, h\rangle = \int_a^b (\alpha f(t) + \beta g(t))h(t)\,dt = \alpha \int_a^b f(t)h(t)\,dt + \beta \int_a^b g(t)h(t)\,dt = \alpha\langle f, h\rangle + \beta\langle g, h\rangle$.

Thus this is an inner product on $\mathcal{C}([a, b], \mathbb{R})$ by definition.

In fact, we can extend this to a complex inner product easily enough. Let $V = \mathcal{C}([a, b], \mathbb{C})$ be the space of continuous functions on $[a, b]$ with values in $\mathbb{C}$. We can define an inner product by

$$\langle f, g\rangle = \int_a^b f(t)\overline{g(t)}\,dt.$$

Example 6.11. Let $V = \mathcal{P}_n(x)$ and fix real numbers $x_0, x_1, \dots, x_n$ be distinct real numbers. For $f, g \in V$, define

$$\langle f, g\rangle = \sum_{i=0}^{n} f(x_i)g(x_i).$$

Then we can see $\langle f, f\rangle = \sum_{i=0}^n f(x_i)^2 \geq 0$, and the sum is equal to zero if and only if $f(x_i) = 0$ for all i. But then f is a degree n polynomial with $n + 1$ roots, and so must be constantly zero.

You will check the other two conditions on your homework.

6.2 Properties of the Inner Product

Proposition 6.12. *Let V be an inner product space. Then for $x, y, z \in V$ and $c \in \mathcal{F}$, the following are true.*

(a) $\langle \mathbf{0}, \mathbf{x}\rangle = \langle \mathbf{x}, \mathbf{0}\rangle = 0$.

(b) $\langle \mathbf{x}, \mathbf{x}\rangle = 0$ *if and only if* $\mathbf{x} = \mathbf{0}$.

(c) If $\langle \mathbf{x}, \mathbf{y}\rangle = \langle \mathbf{x}, \mathbf{z}\rangle$ *for all* $\mathbf{x} \in V$*, then* $\mathbf{y} = \mathbf{z}$.

Proof. (1) Since $\langle \mathbf{0}, \mathbf{x}\rangle = \langle \mathbf{0} + \mathbf{0}, \mathbf{x}\rangle = \langle \mathbf{0}, \mathbf{x}\rangle + \langle \mathbf{0}, \mathbf{x}\rangle$, this implies that $\langle \mathbf{0}, \mathbf{x}\rangle = 0$. You can use the same argument in the other component.

(2) If $\mathbf{x} \neq \mathbf{0}$, then by positivity, we know $\langle \mathbf{x}, \mathbf{x}\rangle > 0$. Conversely, if $\mathbf{x} = \mathbf{0}$, then part (1) says that $\langle \mathbf{x}, \mathbf{x}\rangle = \langle \mathbf{0}, \mathbf{0}\rangle = 0$.

(3) If $\langle \mathbf{x}, \mathbf{y}\rangle = \langle \mathbf{x}, \mathbf{z}\rangle$ for every $\mathbf{x} \in V$, then by additivity in the second component, we have $\langle \mathbf{x}, \mathbf{y} - \mathbf{z}\rangle = 0$ for all $\mathbf{x} \in V$. In particular, this is true for $\mathbf{x} = \mathbf{y} - \mathbf{z}$, whence $\mathbf{y} - \mathbf{z} = \mathbf{0}$ and so $\mathbf{y} = \mathbf{z}$. □

We remarked that the norm $\|v\| = \sqrt{\langle \mathbf{v}, \mathbf{v} \rangle}$ should be thought of as some notion of the length of a vector. So we should check that the norm actually behaves like a length, in the following theorem. (For (c), keep in mind that for the dot product on $\mathbb{R}^n$, $\mathbf{x} \cdot \mathbf{y} = \|\mathbf{x}\| \|\mathbf{y}\| \cos \theta$ where θ is the angle between them.)

Proposition 6.13. *Let V be an inner product space over $\mathbb{F}$. Suppose $x, y \in V$ and $c \in \mathbb{F}$. Then*

(a) $\|cx\| = |c| \cdot \|x\|$.

(b) $\|x\| = 0$ *if and only if* $x = \mathbf{0}$. *In any case,* $\|x\| \geq 0$.

(c) (Cauchy–Schwarz inequality). $|\langle x, y \rangle| \leq \|x\| \|y\|$.

(d) (Triangle inequality). $\|x + y\| \leq \|x\| + \|y\|$.

Proof. (a) We compute

$$\|cx\|^2 = \langle cx, cx \rangle = c\overline{c} \langle x, x \rangle = |c|^2 \|x\|^2.$$

(b) By positivity of inner products, we know that $\langle x, x \rangle \geq 0$ and $\langle x, x \rangle = 0$ if and only if $x = \mathbf{0}$. And $\|x\| = \langle x, x \rangle^2$ so $\|x\| \geq 0$ and $\|x\| = 0$ if and only if $x = \mathbf{0}$.

(c) If $y = \mathbf{0}$, then the result is immediate, since both sides are then equal to 0. So assume that $y \neq \mathbf{0}$. For any $c \in \mathbb{F}$, we have

$$0 \leq \langle x - cy, x - cy \rangle = \langle x, x - cy \rangle - c\langle y, x - cy \rangle = \langle x, x \rangle - \langle x, cy \rangle - c\langle y, x \rangle - c\langle y, -cy \rangle$$
$$= \langle x, x \rangle - \overline{c}\langle x, y \rangle - c\langle y, x \rangle + c\overline{c}\langle y, y \rangle.$$

In particular, if we set $c = \frac{\langle x, y \rangle}{\langle y, y \rangle}$, then we have

$$\frac{\langle x, y \rangle \langle y, x \rangle}{\langle y, y \rangle} = \overline{c}\langle x, y \rangle = c\langle y, x \rangle = c\overline{c}\langle y, y \rangle.$$

Hence, the preceding inequality becomes

$$0 \leq \langle x, x \rangle - \frac{\langle x, y \rangle \langle y, x \rangle}{\langle y, y \rangle} = \langle x, x \rangle - \frac{|\langle x, y \rangle|^2}{\langle y, y \rangle} = \|x\|^2 - \frac{|\langle x, y \rangle|^2}{\|y\|^2}$$

and the Cauchy–Schwarz inequality follows.

(d) We have

$$\begin{aligned}
\|x+y\|^2 &= \langle x+y, x+y\rangle = \langle x,x\rangle + \langle y,y\rangle + \langle x,y\rangle + \langle y,x\rangle \\
&= \langle x,x\rangle + \langle y,y\rangle + \langle x,y\rangle + \overline{\langle x,y\rangle} = \|x\|^2 + \|y\|^2 + 2\Re\langle x,y\rangle \\
&\leq \|x\|^2 + \|y\|^2 + 2|\langle x,y\rangle| \overset{\text{C–S}}{\leq} \|x\|^2 + \|y\|^2 + 2\|x\|\|y\| \\
&= (\|x\| + \|y\|)^2.
\end{aligned}$$

Taking square roots (noting that norms are nonnegative) gives the result.

□

Definition 6.14. Let $\|\cdot\| : V \to \mathbb{R}^{\geq 0}$ be a function that satisfies properties a–d of proposition 6.13, that is:

(a) $\|cx\| = |c| \cdot \|x\|$.

(b) $\|x\| = 0$ if and only if $x = \mathbf{0}$. In any case, $\|x\| \geq 0$.

(c) (Cauchy–Schwarz inequality). $|\langle x, y\rangle| \leq \|x\|\|y\|$.

(d) (Triangle inequality). $\|x + y\| \leq \|x\| + \|y\|$.

Then we say that $\|\cdot\|$ is a *norm* on V.

Proposition 6.13 tells us that any inner product gives us a norm. However it is *not* true that every norm comes from an inner product. A good example is the norm on $\mathbb{R}^n$ given by $\|(a_1, a_2, \ldots, a_n\|_1 = |a_1| + |a_2| + \cdots + |a_n|$. But norms that come from inner product are especially nice, and we tend to like them best.

You will sometimes hear the term *Hilbert space* tossed around here. A Hilbert space is a space with an inner product which is *complete*, which means that limits and calculus behave well. Every finite-dimensional inner product space is a Hilbert space, but not every infinite-dimensional inner product space is complete.

So now we'd like to see some of the extra value we get from the inner product. We already saw we got distances, but what about angles? We start by looking at the most important angle: a right angle. In $\mathbb{R}^n$, if two vectors are perpendicular then their dot product is

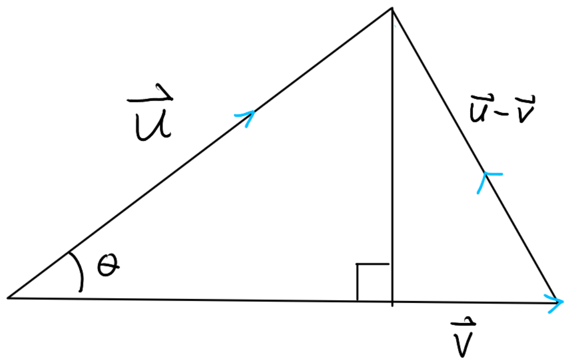
$$\mathbf{u} \cdot \mathbf{v} = \|\mathbf{u}\| \cdot \|\mathbf{v}\| \cos(\theta) = \|\mathbf{u}\| \cdot \|\mathbf{v}\| \cos(\pi/2) = \|\mathbf{u}\| \cdot \|\mathbf{v}\| \cdot 0 = 0.$$

That leads to the following definition:

Definition 6.15. Let $\mathbf{u}, \mathbf{v}$ be elements of an inner product space V. If $\langle \mathbf{u}, \mathbf{v} \rangle = 0$, we say that $\mathbf{u}$ and $\mathbf{v}$ are *orthogonal*.

If vectors are orthogonal, they're independent in a very specific way: we can break any vector up into two pieces that are orthogonal, and re-combine into the original vector. To see this we should start by considering $\mathbb{R}^2$ again.

Suppose we have two vectors $\mathbf{u}$ and $\mathbf{v}$, with angle θ between them. These form two sides of a triangle, with the third side given by $\mathbf{u} - \mathbf{v}$. But we can also draw a line from the endpoint of $\mathbf{u}$ that is perpendicular to $\mathbf{v}$.



We now have a right trangle. The hypotenuse has length $\|\mathbf{u}\|$, so by definition of cosine the length of the adjacent side is $\|\mathbf{u}\| \cos\theta$. But we know that

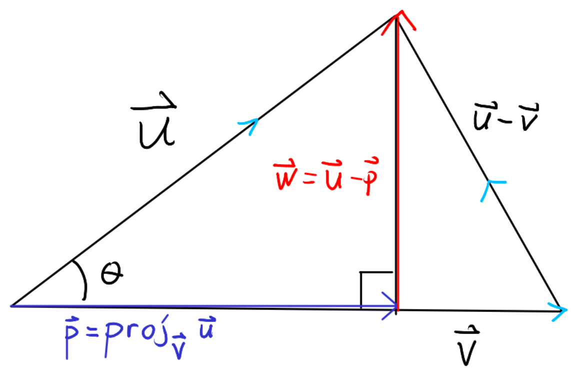
$$\mathbf{u} \cdot \mathbf{v} = \|\mathbf{u}\|\|\mathbf{v}\| \cos\theta$$
$$\mathbf{u} \cdot \frac{\mathbf{v}}{\|\mathbf{v}\|} = \|\mathbf{u}\| \cos\theta$$

so the length of the adjacent side is $\mathbf{u} \cdot \frac{\mathbf{v}}{\|\mathbf{v}\|}$. We sometimes call this number the *scalar projection of* $\mathbf{u}$ *onto* $\mathbf{v}$.

Further, we know the direction that the adjacent side is pointing: it's the same direction as $\mathbf{v}$! So we can find this adjacent side as a vector with the formula

$$\mathbf{p} = \mathbf{u} \cdot \frac{\mathbf{v}}{\|\mathbf{v}\|}\frac{\mathbf{v}}{\|\mathbf{v}\|} = \frac{\mathbf{u} \cdot \mathbf{v}}{\mathbf{v} \cdot \mathbf{v}}\mathbf{v}.$$

It is not immediately obvious that this is a vector; but most of the dot products give us scalars, with the final $\mathbf{v}$ giving direction.



Finally, we can write $\mathbf{w} = \mathbf{u} - \mathbf{p}$. We will have that $\mathbf{p} \cdot \mathbf{v} = \|\mathbf{p}\|\|\mathbf{v}\|$ since the two vectors point in the same direction; we will have

$$\begin{aligned} \mathbf{w} \cdot \mathbf{v} &= (\mathbf{u} - \mathbf{p}) \cdot \mathbf{v} = \mathbf{u} \cdot \mathbf{v} - \mathbf{p} \cdot \mathbf{v} \\ &= \mathbf{u} \cdot \mathbf{v} - \frac{\mathbf{u} \cdot \mathbf{v}}{\mathbf{v} \cdot \mathbf{v}}(\mathbf{v} \cdot \mathbf{v}) \\ &= \mathbf{u} \cdot \mathbf{v} - \mathbf{u} \cdot \mathbf{v} = \mathbf{0}. \end{aligned}$$

Thus $\mathbf{w}$ is orthogonal to $\mathbf{v}$. We have written $\mathbf{u} = \mathbf{p} + \mathbf{w}$ so that $\mathbf{w}$ is orthogonal to $\mathbf{v}$, and $\mathbf{p}$ points in the same direction as $\mathbf{v}$.

Definition 6.16. If $\mathbf{u}, \mathbf{v}$ are two vectors in $\mathbb{R}^n$, we define the *projection map onto* $\mathbf{v}$ by

$$\operatorname{proj}_{\mathbf{v}} \mathbf{u} = \frac{\mathbf{u} \cdot \mathbf{v}}{\mathbf{v} \cdot \mathbf{v}} \mathbf{v}.$$

Example 6.17. Let's look back at our earlier vectors $\mathbf{u} = (3, 4)$ and $\mathbf{v} = (-1, 7)$. Then we compute

$$\begin{aligned} \operatorname{proj}_{\mathbf{v}} \mathbf{u} &= \frac{\mathbf{u} \cdot \mathbf{v}}{\mathbf{v} \cdot \mathbf{v}} \mathbf{v} = \frac{25}{50} \begin{bmatrix} -1 \\ 7 \end{bmatrix} = \begin{bmatrix} -1/2 \\ 7/2 \end{bmatrix} \\ \mathbf{u} - \operatorname{proj}_{\mathbf{v}} \mathbf{u} &= \begin{bmatrix} 3 \\ 4 \end{bmatrix} - \begin{bmatrix} -1/2 \\ 7/2 \end{bmatrix} = \begin{bmatrix} 7/2 \\ 1/2 \end{bmatrix}. \end{aligned}$$

Now that all worked in $\mathbb{R}^2$, and even in $\mathbb{R}^n$. So what does it look like in another vector space?

Definition 6.18. Suppose $\mathbf{u}, \mathbf{v}$ are vectors in an inner product space V, and $\mathbf{v} \neq 0$. We define the projection of $\mathbf{u}$ onto $\mathbf{v}$ by

$$\operatorname{proj}_{\mathbf{v}} \mathbf{u} = \frac{\langle \mathbf{u}, \mathbf{v} \rangle}{\langle \mathbf{v}, \mathbf{v} \rangle} \mathbf{v}.$$

Proposition 6.19. *Let* $\mathbf{u}, \mathbf{v}$ *be vectors in an inner product space* V*, with* $\mathbf{v} \neq 0$*. Let* $\mathbf{p} = \text{proj}_{\mathbf{v}}\mathbf{u}$*. Then:*

(a) $\langle \mathbf{u} - \mathbf{p}, \mathbf{p} \rangle = 0$*—that is,* $\mathbf{u} - \mathbf{p}$ *is orthogonal to* $\mathbf{p}$*.*

(b) $\mathbf{u} = \mathbf{p}$ *if and only if* $\mathbf{u}$ *is a scalar multiple of* $\mathbf{v}$*.*

Proof. (a) See Homework 13

(b) If $\mathbf{u} = \beta\mathbf{v}$, then

$$\text{proj}_{\mathbf{v}}\mathbf{u} = \frac{\langle \beta\mathbf{v}, \mathbf{v} \rangle}{\langle \mathbf{v}, \mathbf{v} \rangle}\mathbf{v} = \beta\mathbf{v} = \mathbf{u}.$$

Conversely, suppose $\mathbf{u} = \text{proj}_{\mathbf{v}}\mathbf{u}$. Then by definition

$$\mathbf{u} = \frac{\langle \mathbf{u}, \mathbf{v} \rangle}{\langle \mathbf{v}, \mathbf{v} \rangle}\mathbf{v},$$

so set $\beta = \frac{\langle \mathbf{u}, \mathbf{v} \rangle}{\langle \mathbf{v}, \mathbf{v} \rangle}$ and we have $\mathbf{u} = \beta\mathbf{v}$.

□

Example 6.20. Let $V = \mathcal{C}([-1,1], \mathbb{R})$ be the space of continuous functions on the closed interval $[-1, 1]$, with the inner product given as above. Consider the vectors $1, x$. We compute:

$$\begin{aligned}
\|1\| &= \sqrt{\int_{-1}^{1} 1\,dx} = \sqrt{x|_{-1}^{1}} = \sqrt{2} \\
\|x\| &= \sqrt{\int_{-1}^{1} x^2\,dx} = \sqrt{x^3/3|_{-1}^{1}} = \sqrt{2/3} \\
\langle 1, x \rangle &= \int_{-1}^{1} x\,dx = x^2/2|_{-1}^{1} = 0
\end{aligned}$$

so 1 and x are orthogonal. Thus the projection of x onto 1 will give the zero vector: the two vectors have no "direction" in common.

Let's consider now the vector $1 + x$. We have

$$\begin{aligned}
\langle 1 + x, 1 \rangle &= \int_{-1}^{1} 1 + x\,dx = x + x^2/2|_{-1}^{1} = 2 \\
\langle 1 + x, x \rangle &= \int_{-1}^{1} x + x^2\,dx = x^2/2 + x^3/3|_{-1}^{1} = 2/3.
\end{aligned}$$

Now we compute

$$\begin{aligned}
\text{proj}_1 1 + x &= \frac{\langle 1 + x, 1 \rangle}{\langle 1, 1 \rangle}1 = \frac{2}{2}1 = 1 \\
\text{proj}_x 1 + x &= \frac{\langle 1 + x, x \rangle}{\langle x, x \rangle}x = \frac{2/3}{2/3}x = x.
\end{aligned}$$

Thus we can use the inner product to decomopose $1 + x$ into its 1 component and its x component (and the remainder, if there were any).

We can squeeze some extra geometry out of this. If two vectors are orthogonal, then they are independent; they don't have any reasonable sub-components pointing in the same direction. This means their lengths are in some sense independent.

Proposition 6.21 (Pythagorean Law)**.** *If* $\mathbf{u}, \mathbf{v}$ *are orthogonal, then*

$$\|\mathbf{u} + \mathbf{v}\|^2 = \|\mathbf{u}\|^2 + \|\mathbf{v}\|^2.$$

Proof. See homework 13. □

Example 6.22. Returning to our previous example, we can compute that

$$\|1 + x\| = \sqrt{\int_{-1}^{1} 1 + 2x + x^2 \, dx} = \sqrt{x + x^2 + x^3/3|_{-1}^{1}} = \sqrt{8/3}.$$

We can confirm that indeed,

$$\|1 + x\|^2 = 8/3 = 2 + 2/3 = \|1\| + \|x\|.$$

Using projections we can prove that the Cauchy-Schwarz Inequality, which we saw briefly in our discussion of the dot product, holds for any inner product.

Theorem 6.23 (Cauchy-Schwarz Inequality)**.** *If* $\mathbf{u}, \mathbf{v}$ *are in an inner product space* V*, then*

$$|\langle \mathbf{u}, \mathbf{v} \rangle| \leq \|\mathbf{u}\|\|\mathbf{v}\|. \tag{1}$$

Equality holds if and only if $\mathbf{u}$ *and* $\mathbf{v}$ *are linearly dependent.*

Proof. If $\mathbf{v} = \mathbf{0}$, both sides are zero. So assume $\mathbf{v} \neq 0$.

Let $\mathbf{p} = \text{proj}_{\mathbf{v}}\mathbf{u}$. By the Pythagorean law 6.21, we know that

$$\|\mathbf{u}\|^2 = \|\mathbf{p}\|^2 + \|\mathbf{u} - \mathbf{p}\|^2.$$

But we know that

$$\|\mathbf{p}\|^2 = \left\| \frac{\langle \mathbf{u}, \mathbf{v} \rangle}{\langle \mathbf{v}, \mathbf{v} \rangle} \mathbf{v} \right\|^2 = \left(\frac{\langle \mathbf{u}, \mathbf{v} \rangle}{\langle \mathbf{v}, \mathbf{v} \rangle} \right)^2 \|\mathbf{v}\|^2 = \frac{\langle \mathbf{u}, \mathbf{v} \rangle^2}{\langle \mathbf{v}, \mathbf{v} \rangle}.$$

Thus we have

$$\begin{aligned}
\frac{\langle \mathbf{u}, \mathbf{v} \rangle^2}{\langle \mathbf{v}, \mathbf{v} \rangle} &= \|\mathbf{u}\|^2 - \|\mathbf{u} - \mathbf{p}\|^2 \\
\langle \mathbf{u}, \mathbf{v} \rangle^2 &= \|\mathbf{u}\|^2\|\mathbf{v}\|^2 - \|\mathbf{u} - \mathbf{p}\|^2\|\mathbf{v}\|^2 \leq \|\mathbf{u}\|^2\|\mathbf{v}\|^2 \\
|\langle \mathbf{u}, \mathbf{v} \rangle| &\leq \|\mathbf{u}\|\|\mathbf{v}\|.
\end{aligned}$$

Further, we can easily see that we get equality if and only if $\mathbf{u} - \mathbf{p} = \mathbf{0}$, if and only if $\mathbf{u} = \mathbf{p}$, if and only if $\mathbf{u}$ is a scalar multiple of $\mathbf{v}$. $\square$

Notice that this allows us to define an "angle" between two vectors. Cauchy-Schwarz tells us that

$$-1 \leq \frac{\langle \mathbf{u}, \mathbf{v} \rangle}{\|\mathbf{u}\| \|\mathbf{v}\|} \leq 1,$$

so we can coherently define:

Definition 6.24. If $\mathbf{u}, \mathbf{v}$ are non-zero vectors in an inner product space, we define the angle between them to be

$$\theta = \arccos\left(\frac{\langle \mathbf{u}, \mathbf{v} \rangle}{\|\mathbf{u}\| \|\mathbf{v}\|} \right).$$

6.3 Orthonormal Bases

Throughout the course, we've been suggesting that we would often like to change from one coordinate system into another which is easier to work with. In this section we'll discuss one particular type of nice basis: one in which all the basis elements are orthogonal.

Definition 6.25. A set $S = \{\mathbf{u}_1, \ldots, \mathbf{u}_n\}$ is said to be *orthogonal* if $\langle \mathbf{u}_i, \mathbf{u}_j \rangle = 0$ whenever $i \neq j$. We say it is *orthonormal* if every vector has magnitude 1.

Proposition 6.26. *Any orthogonal set of non-zero vectors is linearly independent.*

Proof. Suppose

$$a_1 \mathbf{u}_1 + \cdots + a_n \mathbf{u}_n = \mathbf{0}.$$

Then dotting the equation with itself, we get

$$\langle a_1 \mathbf{u}_1 + \cdots + a_n \mathbf{u}_n, a_1 \mathbf{u}_1 + \cdots + a_n \mathbf{u}_n \rangle = 0$$
$$\sum_{i,j=1}^{n} a_i a_j \langle \mathbf{u}_i, \mathbf{u}_j \rangle = 0$$

But since the $\mathbf{u}_i$ are orthogonal, $\langle \mathbf{u}_i, \mathbf{u}_j \rangle = 0$ when $i \neq j$, so this just gives us

$$\sum_{i=1}^{n} a_i^2 \langle \mathbf{u}_i, \mathbf{u}_i \rangle = 0$$
$$a_1^2 \|\mathbf{u}_1\|^2 + \cdots + a_n^2 \|\mathbf{u}_n\|^2 = 0.$$

And thus, since $\|\mathbf{u}_i\| > 0$, we must have $a_i = 0$ for each i. $\square$

Thus every orthogonal set is a basis for its span.

Definition 6.27. Let $E = \{\mathbf{e}_1, \dots, \mathbf{e}_n\}$ be a basis for V. We say that E is an *orthogonal basis* if $\langle \mathbf{e}_i, \mathbf{e}_j \rangle = 0$ whenever $i \neq j$.

We say that E is an *orthonormal basis* if, furthermore, $\|\mathbf{e}_i\| = 1$. Thus E is an orthonormal basis if and only if

$$\langle \mathbf{e}_i, \mathbf{e}_j \rangle = \begin{cases} 1 & i = j \\ 0 & i \neq j \end{cases}.$$

Example 6.28.

- The standard basis for $\mathbb{R}^3$ is orthonormal.
- The basis $\{(1,1,0),(1,-1,0),(0,0,1)\}$ for $\mathbb{R}^3$ is orthogonal but not orthonormal.
  But $\{(\sqrt{2}/2, \sqrt{2}/2, 0), (\sqrt{2}/2, -\sqrt{2}/2, 0), (0,0,1)\}$ is orthornormal.
- Let $V = \mathcal{P}_2(x)$ with inner product given by $\langle f, g \rangle = \int_{-1}^1 f(t)g(t)\,dt$. The basis $E = \{1, x, 3x^2 - 1\}$ is an orthogonal basis for V, but not orthonormal.
  The basis $F = \left\{\frac{1}{\sqrt{2}}, \frac{x\sqrt{3}}{\sqrt{2}}, \frac{\sqrt{5}}{2\sqrt{2}}(3x^2-1)\right\}$ is orthonormal.
- Let $V = \mathcal{P}_2(x)$ with inner product given by $\langle f, g \rangle = f(-1)g(-1) + f(0)g(0) + f(1)g(1)$. Then $E = \{1, x, x^2 - 2/3\}$ is an orthogonal basis for V.
  An orthonormal basis is $F = \left\{\frac{\sqrt{3}}{3}, \frac{x\sqrt{2}}{2}, \frac{\sqrt{3}}{\sqrt{2}}\left(x^2 - \frac{2}{3}\right)\right\}$.

Orthonormal bases are particularly nice, for a few reasons.

Proposition 6.29. *Suppose $E = \{\mathbf{e}_1, \dots, \mathbf{e}_n\}$ is an orthonormal basis for V. Then if $\mathbf{u} = \sum_{i=1}^n a_i \mathbf{e}_i$ and $\mathbf{v} = \sum_{i=1}^n b_i \mathbf{e}_i$, then $\langle \mathbf{u}, \mathbf{v} \rangle = \sum_{i=1}^n a_i b_i$.*

Consequently $\|\mathbf{u}\| = |a_1|^2 + \cdots + |a_n|^2$.

Remark 6.30. We use this all the time when we're computing the norm of vectors in $\mathbb{R}^n$. This also gives us our "normal" dot product.

Mor importantly, orthonormal bases make projection, coordinates, and changes of basis very easy.

Proposition 6.31. *Let $E = \{\mathbf{e}_1, \dots, \mathbf{e}_n\}$ be a basis for V, with $\langle e_i, e_j \rangle = 0$ when $i \neq j$. Then if $\mathbf{v} \in V$, we have*

$$\mathbf{v} = \sum_{i=1}^n \left(\text{proj}_{\mathbf{e}_i} \mathbf{v}\right) \mathbf{e}_i = \left(\text{proj}_{\mathbf{e}_1} \mathbf{v}\right) \mathbf{e}_1 + \cdots + \left(\text{proj}_{\mathbf{e}_n} \mathbf{v}\right) \mathbf{e}_n.$$

Proof. Write $\mathbf{v} = a_1\mathbf{e}_1 + \cdots + a_n\mathbf{e}_n$ and compute each projection. □

Corollary 6.32. *Let $E = \{\mathbf{e}_1, \ldots, \mathbf{e}_n\}$ be an orthonormal basis for V. Then*

$$\mathbf{v} = \sum_{i=1}^{n} \langle \mathbf{v}, \mathbf{e}_i \rangle \mathbf{e}_i = \langle \mathbf{v}, \mathbf{e}_1 \rangle \mathbf{e}_1 + \cdots + \langle \mathbf{v}, \mathbf{e}_n \rangle \mathbf{e}_n.$$

Example 6.33. $E = \{(1,1,0), (1,-1,0), (0,0,1)\}$ is orthogonal. Find the E coordinates of $(6,2,1)$.

We compute:

$$\begin{aligned}
\operatorname{proj}_{\mathbf{e}_1}(6,2,1) &= \frac{(6,2,1)\cdot(1,1,0)}{(1,1,0)\cdot(1,1,0)} \begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix} = \frac{8}{2} \begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix} = 4 \begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix} \\
\operatorname{proj}_{\mathbf{e}_2}(6,2,1) &= \frac{(6,2,1)\cdot(1,-1,0)}{(1,-1,0)\cdot(1,-1,0)} \begin{bmatrix} 1 \\ -1 \\ 0 \end{bmatrix} = \frac{4}{2} \begin{bmatrix} 1 \\ -1 \\ 0 \end{bmatrix} = 2 \begin{bmatrix} 1 \\ -1 \\ 0 \end{bmatrix} \\
\operatorname{proj}_{\mathbf{e}_3}(6,2,1) &= \frac{(6,2,1)\cdot(0,0,1)}{(0,0,1)\cdot(0,0,1)} \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix} = \frac{1}{1} \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix} \\
[(6,2,1)]_E &= (4,2,1)
\end{aligned}$$

Example 6.34. Let $V = \mathcal{P}_2(x)$, with inner product given by $\langle f, g \rangle = \int_{-1}^{1} f(t)g(t)\,dt$. Then $E = \{1, x, 3x^2 - 1)$ is orthogonal. Write $3x^2 - 6x + 4$ in E-coordinates.

We compute

$$\begin{aligned}
\operatorname{proj}_{\mathbf{e}_1} 3x^2 - 6x + 4 &= \frac{\langle 3x^2 - 6x + 4, 1 \rangle}{\langle 1, 1 \rangle}(1) = \frac{1}{2} \int_{-1}^{1} 3x^2 - 6x + 4\,dx(1) \\
&= \frac{1}{2}\left(x^3 - 3x^2 + 4x \mid |_{-1}^{1}\right)(1) = 5(1) \\
\operatorname{proj}_{\mathbf{e}_2} 3x^2 - 6x + 4 &= \frac{\langle 3x^2 - 6x + 4, x \rangle}{\langle x, x \rangle}(x) = \frac{3}{2} \int_{-1}^{1} 3x^3 - 6x^2 + 4x\,dx(x) \\
&= \frac{3}{2}\left(\frac{x^4}{4} - 2x^3 + 2x^2 \mid |_{-1}^{1}\right)(x) = -6(x) \\
\operatorname{proj}_{\mathbf{e}_3} 3x^2 - 6x + 4 &= \frac{\langle 3x^2 - 6x + 4, 3x^2 - 1 \rangle}{\langle 3x^2 - 1, 3x^2 - 1 \rangle}(3x^2 - 1) \\
&= \frac{5}{8} \int_{-1}^{1} (3x^2 - 6x + 4)(3x^2 - 1)\,dx(3x^2 - 1) \\
&= \frac{5}{8}\left(9x^5/5 - 9x^4/2 + 3x^3 + 3x^2 - 4x \mid |_{-1}^{1}\right)(3x^2 - 1) = 1(3x^2 - 1) \\
\left[3x^2 - 6x + 4\right]_E &= (5, -6, 1).
\end{aligned}$$

Example 6.35. Let $V = \mathbb{R}^3$ with the usual dot product. Then the standard basis $\{(1,0,0),(0,1,0),(0,0,1)\}$ is an orthonormal basis. Use the dot product to find the coordinates of $(2,3,4)$.

We don't need to use the full projection operator; we just need to compute the inner products, since our basis is orthonormal and not just orthogonal.

$$\operatorname{proj}_{\mathbf{e}_1}(2,3,4) = (2,3,4)\cdot(1,0,0)\begin{bmatrix}1\\0\\0\end{bmatrix} = 2\begin{bmatrix}1\\0\\0\end{bmatrix}$$

$$\operatorname{proj}_{\mathbf{e}_2}(2,3,4) = (2,3,4)\cdot(0,1,0)\begin{bmatrix}0\\1\\0\end{bmatrix} = 3\begin{bmatrix}0\\1\\0\end{bmatrix}$$

$$\operatorname{proj}_{\mathbf{e}_3}(2,3,4) = (2,3,4)\cdot(0,0,1)\begin{bmatrix}0\\0\\1\end{bmatrix} = 4\begin{bmatrix}0\\0\\1\end{bmatrix}$$

$$[(2,3,4)]_E = (2,3,4).$$

This isn't a surprise because it was already in coordinates with respect to the standard basis. But this also illustrates a more general principle: if your vector is already written in orthonormal coordinates, your inner product just becomes a dot product.

We'd like a way to generate an orthonormal basis if we don't already have one. This turns out to be straightforward; start with any basis, and one-by-one "fix" elements so that they're orthogonal to all the others.

Proposition 6.36 (Gram-Schmidt Process)**.** *Let $E = \{\mathbf{e}_1, \dots, \mathbf{e}_n\}$ be a basis for V. Then there is an orthonormal basis $\{\mathbf{u}_1, \dots, \mathbf{u}_n\}$, where we set:*

$$\begin{aligned}
\mathbf{f}_1 &= \mathbf{e}_1 & \mathbf{u}_1 &= \frac{\mathbf{f}_1}{\|\mathbf{f}_1\|}\\
\mathbf{f}_2 &= \mathbf{e}_2 - \operatorname{proj}_{\mathbf{u}_1}\mathbf{e}_2 & \mathbf{u}_2 &= \frac{\mathbf{f}_2}{\|\mathbf{f}_2\|}\\
\mathbf{f}_3 &= \mathbf{e}_3 - \left(\operatorname{proj}_{\mathbf{u}_1}\mathbf{e}_3 + \operatorname{proj}_{\mathbf{u}_2}\mathbf{e}_3\right) & \mathbf{u}_3 &= \frac{\mathbf{f}_3}{\|\mathbf{f}_3\|}\\
&\vdots & &\vdots\\
\mathbf{f}_n &= \mathbf{e}_n - (\operatorname{proj}_{\mathbf{u}_1}\mathbf{e}_n + \cdots + \operatorname{proj}_{\mathbf{u}_{n-1}}\mathbf{e}_n) & \mathbf{u}_n &= \frac{\mathbf{f}_n}{\|\mathbf{f}_n\|}.
\end{aligned}$$

Proof. It's clear that each $\mathbf{u}_i$ has norm 1, so we just need to check that they are pairwise orthogonal, which is the same as checking that the $\mathbf{f}_i$ are all orthogonal

But we have constructed the $\mathbf{f}_i$ to be orthogonal by subtracting off the pieces they have in common. For instance, we see that

$$\begin{aligned}\langle \mathbf{f}_1, \mathbf{f}_2\rangle &= \left\langle \mathbf{e}_1, \mathbf{e}_2 - \frac{\langle \mathbf{e}_2, \mathbf{e}_1\rangle}{\langle \mathbf{e}_1, \mathbf{e}_1\rangle}\mathbf{e}_1 \right\rangle = \langle \mathbf{e}_1, \mathbf{e}_2\rangle - \frac{\langle \mathbf{e}_2, \mathbf{e}_1\rangle}{\langle \mathbf{e}_1, \mathbf{e}_1\rangle}\langle \mathbf{e}_1, \mathbf{e}_1\rangle \\ &= \langle \mathbf{e}_1, \mathbf{e}_2\rangle - \langle \mathbf{e}_2, \mathbf{e}_1\rangle = 0.\end{aligned}$$

In general, we see that

$$\langle \mathbf{f}_j, \mathrm{proj}_{\mathbf{f}_j}\mathbf{f}_i\rangle = \left\langle \mathbf{f}_i, \frac{\langle \mathbf{f}_j, \mathbf{f}_j\rangle}{\langle \mathbf{f}_j, \mathbf{f}_j\rangle}\mathbf{f}_j \right\rangle = \langle \mathbf{f}_i, \mathbf{f}_j\rangle$$

and all the other projections will be zero since the $\mathbf{f}_i$ are orthogonal, so each $\mathbf{f}_j$ is orthogonal to all the previous $\mathbf{f}_i$. □

Example 6.37. Let $V = \mathbb{R}^3$ with the usual dot product, and let $E = \{(1, 1, -1), (1, -1, 1), (-1, 1, 1)\}$. Use Gram-Schmidt to orthonormalize this basis.

We take $\mathbf{f}_1 = (1, 1, -1)$, and then we compute $\|\mathbf{f}_1\| = \sqrt{3}$ so $\mathbf{u}_1 = \left(\frac{1}{\sqrt{3}}, \frac{1}{\sqrt{3}}, \frac{-1}{\sqrt{3}}\right)$.

Then we set

$$\begin{aligned}\mathbf{f}_2 &= \begin{bmatrix} 1 \\ -1 \\ 1 \end{bmatrix} - \mathrm{Proj}_{(1,1,-1)} \begin{bmatrix} 1 \\ -1 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ -1 \\ 1 \end{bmatrix} - \frac{(1,-1,1)\cdot(1,1,-1)}{(1,1,-1)\cdot(1,1,-1)} \begin{bmatrix} 1 \\ 1 \\ -1 \end{bmatrix} \\ &= \begin{bmatrix} 1 \\ -1 \\ 1 \end{bmatrix} - \frac{-1}{3} \begin{bmatrix} 1 \\ 1 \\ -1 \end{bmatrix} = \begin{bmatrix} 4/3 \\ -2/3 \\ 2/3 \end{bmatrix} \\ \mathbf{u}_2 &= \frac{\mathbf{f}_2}{\|\mathbf{f}_2\|} = \frac{(4/3, -2/3, 2/3)}{\sqrt{24/9}} = \frac{\sqrt{3}}{2\sqrt{2}} \begin{bmatrix} 4/3 \\ -2/3 \\ 2/3 \end{bmatrix} = \begin{bmatrix} \sqrt{6}/3 \\ -\sqrt{6}/6 \\ \sqrt{6}/6 \end{bmatrix}.\end{aligned}$$

Finally we have

$$\begin{aligned}
\mathbf{f}_3 &= \begin{bmatrix} -1 \\ 1 \\ 1 \end{bmatrix} - \operatorname{proj}_{(1,1,-1)} \begin{bmatrix} -1 \\ 1 \\ 1 \end{bmatrix} - \operatorname{proj}_{(4,-2,2)} \begin{bmatrix} -1 \\ 1 \\ 1 \end{bmatrix} \\
&= \begin{bmatrix} -1 \\ 1 \\ 1 \end{bmatrix} - \frac{(-1,1,1)\cdot(1,1,-1)}{(1,1,-1)\cdot(1,1,-1)} \begin{bmatrix} 1 \\ 1 \\ -1 \end{bmatrix} - \frac{(-1,1,1)\cdot(4,-2,2)}{(4,-2,2)\cdot(4,-2,2)} \begin{bmatrix} 4 \\ -2 \\ 2 \end{bmatrix} \\
&= \begin{bmatrix} -1 \\ 1 \\ 1 \end{bmatrix} - \frac{-1}{3} \begin{bmatrix} 1 \\ 1 \\ -1 \end{bmatrix} - \frac{-4}{24} \begin{bmatrix} 4 \\ -2 \\ 2 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 1 \end{bmatrix} \\
\mathbf{u}_3 &= \frac{\mathbf{f}_3}{\|\mathbf{f}_3\|} = \frac{(0,1,1)}{\sqrt{2}} = \begin{bmatrix} 0 \\ \sqrt{2}/2 \\ \sqrt{2}/2 \end{bmatrix}.
\end{aligned}$$

Thus an orthonormal basis for $\mathbb{R}^3$ is

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

Notice that while this is an orthonormal basis for $\mathbb{R}^3$, it is not the usual one. We will get different orthonormal bases out of the end, depending on which vector we start with.

Example 6.38. Let $V = \mathcal{P}_2(x)$ with the inner product given by $\langle f, g\rangle = \int_0^1 f(t)g(t)\,dt$. (Note this is a *different* inner product from the one we've been using!) Let's form an orthonormal basis from the set $\{1, x, x^2\}$.

We set $\mathbf{f}_1 = 1$. We compute that

$$\|1\|^2 = \langle 1, 1\rangle = \int_0^1 1\,dx = 1$$

so this is already a unit vector; we set $\mathbf{u}_1 = 1$.

We take

$$\mathbf{f}_2 = x - \frac{\langle 1, x\rangle}{\langle 1, 1\rangle}(1) = x - \frac{1}{2}(1) = x - 1/2.$$

We compute

$$\|\mathbf{f}_2\| = \sqrt{\int_0^1 (x-1/2)^2\,dx} = \sqrt{12} = 2\sqrt{3}$$

so we set

$$\mathbf{u}_2 = \frac{\mathbf{f}_2}{\|\mathbf{f}_2\|} = 2\sqrt{3}(x - 1/2) = \sqrt{3}(2x - 1).$$

Finally, we have

$$\begin{aligned}
\mathbf{f}_3 &= x^2 - \frac{\langle 1, x^2 \rangle}{\langle 1, 1 \rangle}(1) - \frac{\langle \sqrt{3}(2x-1), x^2 \rangle}{\langle \sqrt{3}(2x-1), \sqrt{3}(2x-1) \rangle}\sqrt{3}(2x-1) \\
&= x^2 - \int_0^1 x^2 \, dx(1) - \sqrt{3}\int_0^1 2x^3 - x^2 \, dx(\sqrt{3}(2x-1)) \\
&= x^2 - \frac{1}{3} - \frac{1}{2}(2x-1) = x^2 - x + \frac{1}{6}.
\end{aligned}$$

Then we compute

$$\begin{aligned}
\|\mathbf{f}_3\| &= \sqrt{\int_0^1 (x^2 - x + 1/6)^2 \, dx} = \sqrt{\frac{1}{180}} = \frac{1}{6\sqrt{5}} \\
\mathbf{u}_3 &= \frac{\mathbf{f}_3}{\|\mathbf{f}_3\|} = 6\sqrt{5}x^2 - 6\sqrt{5}x + \sqrt{5}.
\end{aligned}$$

Thus an orthonormal basis for $\mathcal{P}_2(x)$ with this inner product is

$$\{1, \sqrt{3}(2x-1), \sqrt{5}(6x^2 - 6x + 1)\}.$$

6.4 Orthogonal Subspaces

We have used orthogonality to give a vector space a particularly nice basis. We can also break the vector space into two (or more) independent subspaces.

Definition 6.39. If V is an inner product space and U, W are subspaces, we say that U and W are *orthogonal* and write $U \perp W$ if $\langle \mathbf{u}, \mathbf{w} \rangle = 0$ for every $\mathbf{u} \in U, \mathbf{w} \in W$.

If $U \subset V$, we define the *orthogonal complement of* U to be the set of all vectors perpendicular to everything in U:

$$U^\perp = \{\mathbf{v} \in V : \langle \mathbf{v}, \mathbf{u} \rangle = 0 \forall \mathbf{u} \in U\}.$$

Example 6.40.

- In $\mathbb{R}^2$, the orthogonal complement of a line is a line. The orthogonal complement to a set with two points in it is also a line.
- In $\mathbb{R}^3$, the orthogonal complement of a line is a plane, and the orthogonal complement of a plane is a line.

Proposition 6.41. *If U is a subset of V, then $U^\perp$ is a subspace of V.*

Proof. (a) $\mathbf{0}$ is orthogonal to everything, and thus is in $U^\perp$.

(b) Suppose $\mathbf{v} \in U^\perp$, and $r \in \mathbb{R}$. Then for any $\mathbf{u} \in U$ we have $\langle r\mathbf{v}, \mathbf{u}\rangle = r\langle \mathbf{v}, \mathbf{u}\rangle = r \cdot 0 = 0$, so $r\mathbf{v} \in U^\perp$ by definition.

(c) Suppose $\mathbf{v}, \mathbf{w} \in U^\perp$, and let $\mathbf{u} \in U$. Then

$$\langle \mathbf{v} + \mathbf{w}, \mathbf{u}\rangle = \langle \mathbf{v}, \mathbf{u}\rangle + \langle \mathbf{w}, \mathbf{u}\rangle = 0 + 0 = 0.$$

Thus $\mathbf{v} + \mathbf{w}$ is orthogonal to $\mathbf{u}$ for every $\mathbf{u} \in U$, and so $\mathbf{v} + \mathbf{w} \in U^\perp$.

Thus by the subspace theorem, $\mathbf{U}^\perp$ is a subspace of V. □

Remark 6.42. We will usually consider cases where U is also a subspace of V, but this isn't necessary; nothing above assumes anything about the structure of U.

A basic thing we want to do is, given a subspace, find a basis for the subspace and for its orthogonal complement. As with everything else, we can solve this problem by row-reducing matrices.

Proposition 6.43. *Let A be a matrix. Then* $\ker(A) = (\text{row}(A))^\perp$.

Remark 6.44. In three dimensions, we can use this exact formula to find the normal vector to a plane.

Proof. If $\mathbf{r}_i$ are the rows of the matrix A, then

$$A\mathbf{x} = \begin{bmatrix} \mathbf{r}_1 \cdot \mathbf{x} \\ \vdots \\ \mathbf{r}_m \cdot \mathbf{x} \end{bmatrix}$$

and thus $\mathbf{x} \in \ker(A)$ precisely if $\mathbf{x}$ is orthogonal to every row of A. But if $\mathbf{x}$ is orthogonal to every row vector of A, it is orthogonal to every linear combination of them, and thus is orthogonal to their span, which is the rowspace. □

Example 6.45. Suppose we want to find the orthogonal complement to $U = \text{span}\{(1, 4, 2), (1, 1, 1)\}$. Then we write down the matrix

$$A = \begin{bmatrix} 1 & 4 & 2 \\ 1 & 1 & 1 \end{bmatrix} \to \begin{bmatrix} 1 & 1 & 1 \\ 0 & 3 & 1 \end{bmatrix} \to \begin{bmatrix} 1 & 0 & 2/3 \\ 0 & 3 & 1 \end{bmatrix}$$

so $U^\perp = \ker(A) = \{(-2\alpha, -\alpha, 3\alpha)\} = \text{span}\{(2, 1, -3)\}$. We can check that this is in fact orthogonal to the original two vectors.

There are a couple more useful facts we'd like to know about orthogonal complements, which show that they relate spaces in useful ways.

Proposition 6.46. *If U is a subspace of V and $\mathbf{v} \in V$, then there exist unique $\mathbf{v}_U \in U, \mathbf{v}_{U^\perp} \in U^\perp$ such that $\mathbf{v} = \mathbf{v}_U + \mathbf{v}_{U^\perp}$.*

We say that this is an orthogonal decomposition *of* $\mathbf{v}$.

Proof. Let $E = \{\mathbf{e}_1, \dots, \mathbf{e}_n\}$ be an orthogonal basis for U and $F = \{\mathbf{f}_1, \dots, \mathbf{f}_m\}$ an orthogonal basis for $U^\perp$.

We claim that $E \cup F = \{\mathbf{e}_1, \dots, \mathbf{e}_n, \mathbf{f}_1, \dots, \mathbf{f}_m\}$ is an orthogonal basis for V. It must be orthogonal since E and F are orthogonal sets, and thus it is linearly independent. So we need to show that it spans V.

Suppose $\mathbf{v} \in V$, and consider the element

$$\mathbf{v}' = \mathbf{v} - \sum_{i=1}^{n} \operatorname{proj}_{\mathbf{e}_i} \mathbf{v}.$$

This is an element of V, and by construction it is orthogonal to every $\mathbf{e}_i$ and thus all of U, so $\mathbf{v}' \in U^\perp$. Thus $\mathbf{v}' \in \operatorname{span}(F)$ and so $\mathbf{v} \in \operatorname{span}(E \cup F)$. Thus $E \cup F$ spans V.

Then every element of V can be expressed uniquely as a linear combination of elements of E and F. This gives us a unique representation as a sum of an element of U and an element of $U^\perp$.

□

Corollary 6.47. $\dim U + \dim U^\perp = \dim V$.

Example 6.48. Give the orthogonal decomposition of $(3, -1, 2)$ with respect to the subspace given by $x - y + 2z = 0$ and its complement.

We need to find an orthonormal basis for either $x - y + 2z = 0$ or its orthogonal complement. But we can see that the normal vector to this plane is in the orthogonal complement, so $\{(1, -1, 2)\}$ is a basis for $U^\perp$.

We project $(3, -1, 2)$ onto $\operatorname{span}\{(1, -1, 2)\}$. We have

$$\operatorname{proj}_{(1,-1,2)} \begin{bmatrix} 3 \\ -1 \\ 2 \end{bmatrix} = \frac{(3,-1,2) \cdot (1,-1,2)}{(1,-1,2) \cdot (1,-1,2)} \begin{bmatrix} 1 \\ -1 \\ 2 \end{bmatrix} = \frac{8}{6} \begin{bmatrix} 1 \\ -1 \\ 2 \end{bmatrix} = \begin{bmatrix} 4/3 \\ -4/3 \\ 8/3 \end{bmatrix}$$

So this is the projection into $U^\perp$. The projection into U then is just what's left over: it's

$$\begin{bmatrix} 3 \\ -1 \\ 2 \end{bmatrix} - \operatorname{proj}_{(1,-1,2)} \begin{bmatrix} 3 \\ -1 \\ 2 \end{bmatrix} = \begin{bmatrix} 3 - 4/3 \\ -1 + 4/3 \\ 2 - 8/3 \end{bmatrix} = \begin{bmatrix} 5/3 \\ 1/3 \\ -2/3 \end{bmatrix}.$$

(We check that this vector is in fact in the plane U). Then we have an orthogonal decomposition: $(3, -1, 2) = (5/3, 1/3, -2/3) + (4/3, -4/3, 8/3)$.

Example 6.49. Let $V = \mathbb{R}^4$ and let $U = \operatorname{span}\{(1, 2, 3, 4), (2, 1, -1, -2)\}$. Find the orthogonal decomposition of $(1, 1, 1, 1)$ into its components in U and $U^\perp$.

We write a matrix

$$A = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & -1 & -2 \end{bmatrix} \to \begin{bmatrix} 3 & 0 & -5 & -8 \\ 0 & 3 & 7 & 10 \end{bmatrix}$$

so $\ker(A) = (5\alpha + 8\beta, -7\alpha - 10\beta, 3\alpha, 3\beta) = \operatorname{span}\{(5, -7, 3, 0), (8, -10, 0, 3)\}$.

We need to find an orthogonal basis for either U or $U^\perp$.We compute

$$\mathbf{f}_1 = \begin{bmatrix} 1 \\ 2 \\ 3 \\ 4 \end{bmatrix}$$

$$\mathbf{f}_2 = \begin{bmatrix} 2 \\ 1 \\ -1 \\ -2 \end{bmatrix} - \operatorname{proj}_{(1,2,3,4)} \begin{bmatrix} 2 \\ 1 \\ -1 \\ -2 \end{bmatrix} = \begin{bmatrix} 2 \\ 1 \\ -1 \\ -2 \end{bmatrix} - \frac{(2, 1, -1, -2) \cdot (1, 2, 3, 4)}{(1, 2, 3, 4) \cdot (1, 2, 3, 4)} \begin{bmatrix} 1 \\ 2 \\ 3 \\ 4 \end{bmatrix}$$

$$= \begin{bmatrix} 2 \\ 1 \\ -1 \\ -2 \end{bmatrix} - \frac{-7}{30} \begin{bmatrix} 1 \\ 2 \\ 3 \\ 4 \end{bmatrix} = \frac{1}{30} \begin{bmatrix} 67 \\ 44 \\ -9 \\ -32 \end{bmatrix}$$

We compute

$$\operatorname{proj}_{\mathbf{f}_1}\begin{bmatrix}1\\1\\1\\1\end{bmatrix} = \frac{(1,2,3,4)\cdot(1,1,1,1)}{(1,2,3,4)\cdot(1,2,3,4)}\begin{bmatrix}1\\2\\3\\4\end{bmatrix} = \frac{10}{30}\begin{bmatrix}1\\2\\3\\4\end{bmatrix} = \begin{bmatrix}1/3\\2/3\\1\\4/3\end{bmatrix}$$

$$\operatorname{proj}_{\mathbf{f}_2}\begin{bmatrix}1\\1\\1\\1\end{bmatrix} = \frac{(1,1,1,1)\cdot(67,44,-9,-32)}{(67,44,-9,-32)\cdot(67,44,-9,-32)}\begin{bmatrix}67\\44\\-9\\-32\end{bmatrix} = \frac{70}{7530}\begin{bmatrix}67\\44\\-9\\-32\end{bmatrix} = \frac{7}{753}\begin{bmatrix}67\\44\\-9\\-32\end{bmatrix}$$

$$\begin{bmatrix}1\\1\\1\\1\end{bmatrix}_U = \begin{bmatrix}1/3\\2/3\\1\\4/3\end{bmatrix} + \frac{7}{753}\begin{bmatrix}67\\44\\-9\\-32\end{bmatrix} = \frac{10}{251}\begin{bmatrix}24\\27\\23\\26\end{bmatrix}$$

$$\begin{bmatrix}1\\1\\1\\1\end{bmatrix}_{U^\perp} = \begin{bmatrix}1\\1\\1\\1\end{bmatrix} - \begin{bmatrix}1\\1\\1\\1\end{bmatrix}_U = \begin{bmatrix}1\\1\\1\\1\end{bmatrix} - \frac{10}{251}\begin{bmatrix}24\\27\\23\\26\end{bmatrix} = \frac{1}{251}\begin{bmatrix}11\\-19\\21\\-9\end{bmatrix}.$$

Proposition 6.50. *If U is a subspace of V, then $(U^\perp)^\perp = U$.*

Proof. If $\mathbf{u} \in U$, then $\mathbf{u}$ is orthogonal to every $\mathbf{w} \in U^\perp$ by definition. So $U \subset (U^\perp)^\perp$.

Conversely, suppose $\mathbf{w} \in (U^\perp)^\perp$. We can write $\mathbf{w} = \mathbf{w}_U + \mathbf{w}_{U^\perp}$. Then $\mathbf{w} \in (U^\perp)^\perp$ so we know $\langle \mathbf{w}, \mathbf{w}_{U^\perp}\rangle = \mathbf{0}$.

But $\langle \mathbf{w}, \mathbf{w}_{U^\perp}\rangle = \langle \mathbf{w}_{U^\perp}, \mathbf{w}_{U^\perp}\rangle = 0$ if and only if $\mathbf{w}_{U^\perp} = 0$. Thus $\mathbf{w}_{U^\perp} = \mathbf{0}$, and $\mathbf{w} = \mathbf{w}_U \in U$. □