Contents

IV Matrix Nullspaces And Ranges

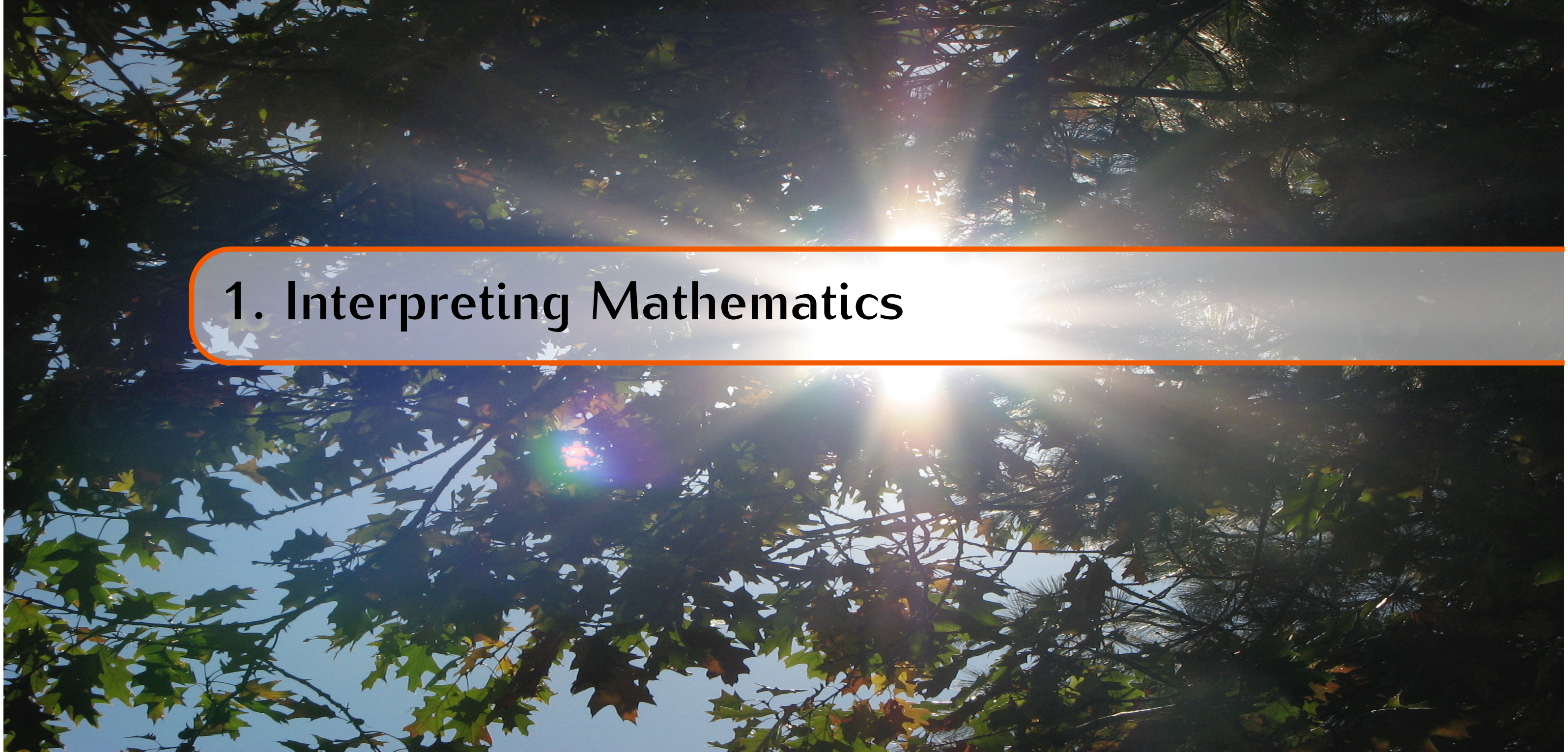
IX Invariant Subspaces And Eigentheory

X General Linearity

XII Further Applications

I

Preliminaries



1. Interpreting Mathematics

Last modified on December 8, 2018

2. The Anatomy of Functions

Last modified on December 8, 2018

2.1 Functions As Route Maps Of Budget Airlines

Definition 2.1.1 ☞ **Functions**

A **function** f acting from a collection A of some objects to a collection B of some objects is a non-empty bunch of arrows emanating from objects in A and pointing to objects in B, which has one additional property: there is *at most one* arrow emanating from any object in A.

In this case we say that A is the **initial space** of the function (or better yet: its **departure space**). B is the **final space** (or the **destination space**).

When describing a function one must indicate its departure space and its destination space.

INSERT PICTURE

Imagine a peculiar airline flying from Land A to Land B described by a collection of arrows indicating its routes, of which there is at least one. (It may happen that Land A and Land B are one an the same.) Surely the reader is familiar with such depictions. The peculiarity of the airline is in the fact that it flies to *at most one* destination in Land B from any given location in Land A.

In this way the airline is a “budget” one: there is no choice of destinations for departures from any point of Land A. It may very well happen that there are no departing flights at all from some locations in Land A.

Surely the reader perceives the analogy between functions and route maps of budget airlines just described. We will exploit this analogy for the sake of easy visualization, and shall interpret functions as maps of routes of budget airlines flying from one collection of objects to another.

INSERT PICTURE

Test Your Comprehension 2.1.2 ☞ **Creating new functions by renaming departure and destination points**

Suppose that f is a function from $\mathcal{A}$ to $\mathcal{B}$, and think of it as a route map for a budget airline. Argue that if one replaces elements of $\mathcal{A}$ with distinct objects constituting a collection $\mathcal{C}$, and elements of $\mathcal{B}$ – with some objects from a collection $\mathcal{D}$, then one has created a function acting from $\mathcal{C}$ to $\mathcal{D}$.

INSERT PICTURE

Definition 2.1.3 ☞ **Domains and ranges**

We can write $a \xrightarrow{f} b$ to indicate that the corresponding airline flies from a departure point a to a destination b, but a more common notation is

$$f(a) = b\ .$$

The collection of all departure points of a function is said to be its **domain**. The collection of all arrival points is said to be its **range**. The domain lies within the departure space, and the range lies within the destination space.

INSERT PICTURE

Example 2.1.4

For example, the function f acting from $\mathbb{R}$ to $\mathbb{R}$ and defined by a formula $f(\star) := -\sqrt{\star + 1}$ has domain $[-1, \infty)$ and range $(-\infty, 0]$.

Identifying the domain of the function is usually much easier than figuring out its range. For example, the function f acting from $\mathbb{R}$ to $\mathbb{R}$ and defined by a formula $f(x) := x + \frac{1}{x^7 - 1}$, clearly has domain $(-\infty, 1) \cup (1, \infty)$. Its range is much less obvious.

In general the domain of a function may not be its entire departure space, but *for the functions we shall study in this book such equality holds.*

Notation 2.1.5 ☞ $f : \Omega \longrightarrow \Gamma$

The notation $f : \Omega \longrightarrow \Gamma$ indicates that f is a function with departure space Ω *all of which is the domain of* f, and a destination space Γ.

INSERT PICTURE

A function $f : \mathcal{X} \longrightarrow \mathcal{X}$ is said to be a **function <u>on</u>** $\mathcal{X}$.

Definition 2.1.6 ☞ **Identity functions**

Consider the following lazy function f on A. For any $a \in A$:

$$f(a) = a\ .$$

In other words, $f : A \longrightarrow A$ is a route map of a "sight-seeing tours" airline, every flight of which returns to the point of its departure. The domain of f is all of A, as is the range.

INSERT PICTURE

This function is said to be **the identity function on** A, and is denoted by the symbols $\mathcal{I}_A$ and id_A.

Test Your Comprehension 2.1.7

Describe the identity function on $\mathbb{R}$ as a familiar function from Calculus.

Notation 2.1.8

The collection of all functions $f : \mathcal{X} \longrightarrow \mathcal{Y}$ is denoted by the symbol $\mathcal{Y}^{\mathcal{X}}$.

It turns out that $\mathbb{R}^2$ can be naturally interpreted as $\mathbb{R}^{\{0,1\}}$, and $\mathbb{R}^5$ – as $\mathbb{R}^{\{0,1,2,3,4\}}$. What may puzzle the reader even further is that in a language of set-theoretic foundations of mathematics, 2 actually stands for $\{0, 1\}$, and 5 actually stands for $\{0, 1, 2, 3, 4\}$. An interested reader can pursue these ideas, but we shall not do so here. We simply state these facts to motivate the use of the notation $\mathcal{Y}^{\mathcal{X}}$ as quite natural.

2.2 Surjections, Injections, Bijections

Terminology 2.2.1 ☞ **Surjections**

The range of a function f may not be all of its destination space. When it is, we say that the function is **surjective**, or is a **surjection**.

In loose terms, a function is surjective when one can use the corresponding airline to fly to any destination in its destination space.

Another way to express this is to say that for any d in the destination space of f, the equation

$$f(z) = d$$

has *at least one* solution for z in the domain of f.

INSERT PICTURE

Example 2.2.2

For example, $f : \mathbb{R} \longrightarrow \mathbb{R}$ defined by the formula

$$f(z) := z^2$$

is NOT surjective, while the function $g : \mathbb{R} \longrightarrow [0, \infty)$ defined by the formula

$$g(t) := t^2$$

is surjective, as is the function $h : (-\frac{\pi}{2}, \frac{\pi}{2}) \longrightarrow \mathbb{R}$ defined by the formula

$$h(*) := \tan(*) .$$

Comment 2.2.3

While a function describes an airline that flies to exactly one destination from each departure point in its domain, that airline may fly to the same destination from different departure points.

INSERT PICTURE

Example 2.2.4

For example, $f : \mathbb{R} \longrightarrow \mathbb{R}$ defined by the formula

$$f(z) := z^2$$

flies to 4 from departure points -2 and 2.

Terminology 2.2.5 **Injections**

If corresponding airline departures from distinct points cannot produce arrivals at the same destination, we say that the function is **injective**.

In this sense the injective functions are those for which the departure point is completely determined by the arrival point.

In a more precise language, for any d in the destination space of f, the equation

$$f(z) = d$$

has *at most one* solution for z in the domain of f.

INSERT PICTURE

Test Your Comprehension 2.2.6

Convince yourself that the following statements are equivalent.

1. Function f is injective.

2. $f(a) = f(c)$ can happen only when $a = c$.

Example 2.2.7

For example, $f : \mathbb{R} \longrightarrow \mathbb{R}$ defined by the formula

$$f(z) := z^k ,$$

with a positive integer k, is injective exactly when k is odd, and not injective when k is even.

Terminology 2.2.8

A function that is neither surjective, nor injective, is said to be **non-jective**.

Test Your Comprehension 2.2.9

Give an example of a non-jective function on $\mathbb{R}$.

Test Your Comprehension 2.2.10 ☞ **Reversing functions**

If we reverse all of the arrows/flights of a given function acting from A to B, we obtain a route map for an airline flying from B to A, but such an airline is not necessarily a budget airline, and so its route map is not necessarily a function.

Argue that the **reverse** $f^{\looparrowleft}$ of a function f acting from A to B is a function acting from B to A exactly when f is injective.

Argue that in this case the domain of $f^{\looparrowleft}$ is the range of f, and the range of $f^{\looparrowleft}$ is the domain of f.

INSERT PICTURE

Test Your Comprehension 2.2.11

What can you say about the reverse of the identity function on A?

Exercise 2.2.12

Argue that the following claims are equivalent* for a function $f : \mathcal{X} \longrightarrow \mathcal{Y}$.

1. f is injective and surjective.
2. $f^{\looparrowleft} : \mathcal{Y} \longrightarrow \mathcal{X}$; i.e. $f^{\looparrowleft}$ is a function with domain $\mathcal{Y}$.

Hint: Consult Ntn. 2.1.5, definitions of injectivity, surjectivity, and TYC 2.2.10.

*In the sense that when one is true so is the other.

Terminology 2.2.13 ☞ **Bijections**

A function that is both injective and surjective is said to be **bijective**, or, equivalently, is a **bijection**.

Test Your Comprehension 2.2.14

Argue that a function f is bijective exactly when for any d in the destination space of f, the equation

$$f(z) = d$$

has *exactly one* solution for z in the domain of f.

Test Your Comprehension 2.2.15

Argue that the identity function on A is bijective. Give an example of a bijective function on $\mathbb{R}$ that is not $\mathcal{I}_{\mathbb{R}}$.

Exercise 2.2.16

Argue that the reverse of a bijection $f : \mathcal{X} \longrightarrow \mathcal{Y}$ is also a bijection.

Test Your Comprehension 2.2.17 ☞ **Graphs and the jectivity**

For functions $f : \mathbb{R} \longrightarrow \mathbb{R}$, how does one discern the jectivity of the function from its graph?

2.3 Composing Functions

Suppose that f-airline and g-airline, described by functions $f : \mathcal{X} \longrightarrow \mathcal{Y}$ and $g : \mathcal{Y} \longrightarrow \mathcal{Z}$, decide to form an alliance in order to fly customers from $\mathcal{X}$ to $\mathcal{Z}$. Customers will travel the first leg of the trip with the f-airline, and the second – with g-airline. Let h be the route map of the composite airline.

A customer can depart with the f-airline from any point in $\mathcal{X}$ (since $\mathcal{X}$ is the domain of f), consequently arriving at some point in $\mathcal{Y}$. Since $\mathcal{Y}$ is the domain of g, there will be a g-flight departing from every point in $\mathcal{Y}$, and so the customer can continue the travels, eventually arriving in $\mathcal{Z}$.

We can go ahead and create the arrows depicting all of the possible routes from $\mathcal{X}$ to $\mathcal{Z}$: this gives the route map h. If a customer can depart at a point a in $\mathcal{X}$ and, after a stopover in $\mathcal{Y}$, arrive at a point c in $\mathcal{Z}$ (i.e. fly with h from a to c with one stop), we draw an h-arrow from a to c.

INSERT PICTURE

Does this alliance constitute a budget airline from $\mathcal{X}$ to $\mathcal{Z}$? In other words, is there at most one h-arrow emanating from each point of $\mathcal{X}$? Since we can fly with f to exactly one destination in $\mathcal{Y}$ from each point of $\mathcal{X}$, and we can fly with g to exactly one destination in $\mathcal{Z}$ from each point of $\mathcal{Y}$, the answer is affirmative. So, h is a function from $\mathcal{X}$ to $\mathcal{Z}$.

Furthermore, it should be clear to the reader than the domain of h is all of $\mathcal{X}$; so, h has the same as the domain of f. The function $h : \mathcal{X} \longrightarrow \mathcal{Z}$ thus obtained is said to be the **composition** of f and g, and is denoted by $g \circ f$.

Comment 2.3.1

Note the reversal of the order in the notation! Why is it so? If we depart from x with the f-airline, we will arrive at the destination $f(x)$ in $\mathcal{Y}$. Departing from this place in $\mathcal{Y}$ and now traveling with the g-airline, we will arrive at $g\big(f(x)\big)$ in $\mathcal{Z}$.

INSERT PICTURE

So,

$$\boxed{(g \circ f)(x) = g\big(f(x)\big) \ .}$$

When we write $g \circ f$ and remember that the inputs (x) are listed from the right, we will see that f is closer to the inputs and will grab them first, passing the outputs to g, in turn.

Test Your Comprehension 2.3.2 ☞ **Composing with an identity function is pointless**

Suppose that $f : \mathcal{X} \longrightarrow \mathcal{Y}$. Argue that

$$id_{\mathcal{Y}} \circ f = f \quad \text{and} \quad f \circ id_{\mathcal{X}} = f \ .$$

In this sense the role of the identity function for the operation of composition of functions is similar to that zero plays for the addition of numbers, or to that 1 plays for the multiplication of numbers.

Comment 2.3.3 ☞ **Composition of functions is not commutative**

Given functions $f : \mathcal{X} \longrightarrow \mathcal{Y}$ and $g : \mathcal{Y} \longrightarrow \mathcal{Z}$, we can form

$$g \circ f : \mathcal{X} \longrightarrow \mathcal{Z} \ ,$$

but $f \circ g$ will not even make sense if $\mathcal{Z}$ does not equal $\mathcal{X}$. (Do you see why?)

Even if we have functions $f : \mathcal{X} \longrightarrow \mathcal{Y}$ and $g : \mathcal{Y} \longrightarrow \mathcal{X}$, so that we can form

$$g \circ f : \mathcal{X} \longrightarrow \mathcal{X} \quad \text{and} \quad f \circ g : \mathcal{Y} \longrightarrow \mathcal{Y} \ ,$$

these functions will certainly not be equal, if $\mathcal{X}$ is distinct from $\mathcal{Y}$.

Even when our functions are $f : \mathcal{X} \longrightarrow \mathcal{X}$ and $g : \mathcal{X} \longrightarrow \mathcal{X}$, so that

$$g \circ f : \mathcal{X} \longrightarrow \mathcal{X} \quad \text{and} \quad f \circ g : \mathcal{X} \longrightarrow \mathcal{X} ,$$

these functions may still not be equal (see TYC 2.3.4).

The order of composition is important when dealing with functions. The operation of composition is not commutative, in contrast to the addition and multiplication of numbers.

Test Your Comprehension 2.3.4

Let functions $f : \mathbb{R} \longrightarrow \mathbb{R}$ and $g : \mathbb{R} \longrightarrow \mathbb{R}$ be defined by formulas

$$f(s) = s^2 \quad \text{and} \quad g(t) = t + 1 .$$

Argue that

$$f \circ g \neq g \circ f .$$

Theorem 2.3.5 ☞ **Composition of functions is associative**

When $f : \mathcal{X} \longrightarrow \mathcal{Y}$, $g : \mathcal{Y} \longrightarrow \mathcal{Z}$ and $h : \mathcal{Z} \longrightarrow \mathcal{W}$,

$$\big(h \circ g\big) \circ f = h \circ \big(g \circ f\big) .$$

Proof of Theorem 2.3.5. Clearly $h \circ g : \mathcal{Y} \longrightarrow \mathcal{W}$ and $g \circ f : \mathcal{X} \longrightarrow \mathcal{Z}$. Hence

$$\big(h \circ g\big) \circ f : \mathcal{X} \longrightarrow \mathcal{W} \quad \text{and} \quad h \circ \big(g \circ f\big) : \mathcal{X} \longrightarrow \mathcal{W} .$$

Thus, to show the equality of these functions we simply need to verify that the corresponding airlines fly to identical destinations from each departure point in $\mathcal{X}$. In other words that

$$\Big(\big(h \circ g\big) \circ f\Big)(x) = \Big(h \circ \big(g \circ f\big)\Big)(x) ,$$

for every x in $\mathcal{X}$.

This is a matter of calculations based on the formula in Comment 2.3.1:

$$\Big(\big(h \circ g\big) \circ f\Big)(x) = \Big(\big(h \circ g\big)\big(f(x)\big) = h\Big(g\big(f(x)\big)\Big) ,$$

and

$$\Big(h \circ \big(g \circ f\big)\Big)(x) = h\Big(\big(g \circ f\big)(x)\Big) = h\Big(g\big(f(x)\big)\Big) . \qquad \blacksquare$$

Comment 2.3.6

The associativity of composition allows us to leave out the grouping brackets when we compose more than two functions together. Please do keep in mind that the order in which the functions are composed matters and may not be switched in general without affecting the outcome.

2.3.1 — Range Of A Composition Of Functions

Observation 2.3.7

It is obvious that we cannot fly with $g \circ f$ to a destination that is outside of the range of g (since the second leg of a $(g \circ f)$-flight is implemented by g). Hence the range of $g \circ f$ lies within the range of g. It may very well happen that the two are not equal (see TYC 2.3.8). Let us record this.

$$\mathit{Range}\,(g \circ f) \subseteq \mathit{Range}\,(g)\ .$$

Test Your Comprehension 2.3.8

Suppose that the function $f : \mathbb{R} \longrightarrow \mathbb{R}$ is defined by the formula

$$f(u) := u^2\ ,$$

and the function $g : \mathbb{R} \longrightarrow \mathbb{R}$ is defined by the formula

$$g(w) := w^3\ .$$

Argue that the range of $g \circ f$ is a **proper subset** of the range of g (i.e. is within the range of g, but is not all of it).

Terminology 2.3.9

If $\boldsymbol{S}$ is a subset of $\boldsymbol{\Omega}$, and $f : \boldsymbol{\Omega} \longrightarrow \boldsymbol{\Delta}$, **the image** $f\,\langle \boldsymbol{S}]$ **of** $\boldsymbol{S}$ **under** f is defined as follows:

$$f\,\langle \boldsymbol{S}] := \{\ f(s) \mid s \in \boldsymbol{S}\ \} \subset \boldsymbol{\Delta}\ .$$

In other words, $f\,\langle \boldsymbol{S}]$ is the set of all destinations one can get to via the airline described by f with departures restricted to the locations in $\boldsymbol{S}$.

Exercise 2.3.10 ☞ **Range of a composition**

Suppose that $f : X \longrightarrow Y$ and $g : Y \longrightarrow Z$. Argue that

$$\mathit{Range}\,(g \circ f) = g\left\langle \mathit{Range}\,(f)\right]\ .$$

Conclude that

$$\mathit{Range}\,(g \circ f) = \mathit{Range}\,(g), \text{ whenever } f \text{ is a surjection.}$$

2.4 Composition And The Jectivity Of Functions

Exercise 2.4.1 ☞ **A composition of —jections is a —jection**

Argue that a composition of two injections is an injection, and a composition of two surjections is a surjection. Conclude that a composition of two bijections is a bijection.

Theorem 2.4.2 ☞ **The jectivity of a composition tells us something about the jectivities of the functions involved**

For functions $f : \mathcal{X} \longrightarrow \mathcal{Y}$ and $g : \mathcal{Y} \longrightarrow \mathcal{Z}$, each of the following claims is true.

1. If $g \circ f$ is an injection then so is f.
2. If $g \circ f$ is a surjection then so is g.

Proof of Theorem 2.4.2.

1. : We will assume that $g \circ f$ is an injection and argue that $f(a) = f(c)$ can happen only when $a = c$. Suppose that $f(a) = f(c)$. Then

$$g\big(f(a)\big) = g\big(f(b)\big) \ .$$

In other words,

$$\big(g \circ f\big)(a) = \big(g \circ f\big)(b) \ .$$

Since we are assuming that $g \circ f$ is an injection, the desired conclusion

$$a = c$$

follows.

2. : We will assume that $g \circ f : \mathcal{X} \longrightarrow \mathcal{Z}$ is a surjection; i.e. that

$$Range\,(g \circ f) = \mathcal{Z} \ ,$$

and argue that g is a surjection; i.e. that

$$Range\,(g) = \mathcal{Z} \ .$$

To this end observe that,

$$\mathcal{Z} = Range\,(g \circ f) \overset{\text{Obs. 2.3.7}}{\subseteq} Range\,(g) \subseteq \mathcal{Z} \ ,$$

and so the required equality follows. ■

Test Your Comprehension 2.4.3

Suppose that $f : \mathcal{X} \longrightarrow \mathcal{Y}$ and $g : \mathcal{Y} \longrightarrow \mathcal{X}$ are such that

$$g \circ f \text{ is a bijection.}$$

Argue that g is surjective and f is injective.

Exercise 2.4.4

1. Give (and justify) a concrete example of sets $\mathcal{X}$, $\mathcal{Y}$ and $\mathcal{Z}$, and functions $f : \mathcal{X} \longrightarrow \mathcal{Y}$ and $g : \mathcal{Y} \longrightarrow \mathcal{Z}$ such that $g \circ f$ is an injection, but g is non-jective.

2. Give (and justify) a concrete example of sets $\mathcal{X}$, $\mathcal{Y}$ and $\mathcal{Z}$, and functions $f : \mathcal{X} \longrightarrow \mathcal{Y}$ and $g : \mathcal{Y} \longrightarrow \mathcal{Z}$ such that $g \circ f$ is a surjection, but f is non-jective.

3. Give (and justify) a concrete example of sets $\mathcal{X}$, $\mathcal{Y}$ and $\mathcal{Z}$, and functions $f : \mathcal{X} \longrightarrow \mathcal{Y}$ and $g : \mathcal{Y} \longrightarrow \mathcal{Z}$ such that $g \circ f$ is a bijection, but neither f nor g is bijective.

Hint: Your sets can be small with just a few elements in each, and your functions can be described as route maps of budget airlines.

Comment 2.4.5 ☞ **Cancellation**

Let us recall the cancellation properties for multiplication of real numbers. There, if $3x = 3y$ then $x = y$. This deduction is known as "cancel the 3 from both sides". Its validity has to do with the fact that there is a real number $\frac{1}{3}$ that is antipodal to 3 with respect to multiplication, in the sense that

$$\frac{1}{3} \cdot 3 = 1.$$

"Cancelling the 3" refers to the following argument:

> If $3x = 3y$, then $\frac{1}{3} \cdot \big(3x\big) = \frac{1}{3} \cdot \big(3y\big)$. Thus, by the associativity of multiplication,
>
> $$\left(\frac{1}{3} \cdot 3\right) \cdot x = \left(\frac{1}{3} \cdot 3\right) \cdot y\ ,$$
>
> which leads to $1 \cdot x = 1 \cdot y$. Since 1 is the multiplicative identity,
>
> $$x = 1 \cdot x = 1 \cdot y = y\ .$$

Below we shall demonstrate that certain functions enjoy "cancellability" properties with respect to composition. We will argue that surjective functions are right-cancellable, and that injective functions are left-cancellable (see Lem. 2.4.6, Exc. 2.4.8, as well as Facts 2.5.3 and 2.5.5).

The reason for having two separate concepts is the non-commutativity of composition. The multiplication of real numbers is commutative and so we need not be concerned with the order of multiplication when working in $\mathbb{R}$.

In the next section, we will also show that left-/right- cancellability of functions has to do with the existence of left-/right- antipodal functions, which play the role of "$\frac{1}{3}$" if a function is thought of as playing the role of "3", and the identity functions are playing the role of "1".

Lemma 2.4.6 ☞ **Surjective functions are right-cancellable**

Suppose that $f : \mathcal{X} \longrightarrow \mathcal{Y}$ and $g, k : \mathcal{Y} \longrightarrow \mathcal{Z}$, and that

$$g \circ f = k \circ f \ .$$

If f is surjective then $g = k$.

This is what we mean when we say that surjective functions are **right-cancellable** (or **cancellable from the right**).

Proof of Lemma 2.4.6. Let us suppose that f is a surjective function such that $g \circ f = k \circ f$. Then

$$\big(g \circ f\big)(x) = \big(k \circ f\big)(x), \quad \text{for all} \quad x \in \mathcal{X} \ .$$

In other words, for all $x \in \mathcal{X}$,

$$g\big(f(x)\big) = k\big(f(x)\big) \ .$$

This shows that

$$g(y) = k(y), \quad \text{for all} \quad y \in \mathit{Range}\,(f) \ .$$

Since f is surjective, $\mathit{Range}\,(f) = \mathcal{Y}$, and therefore g and k agree on all inputs in $\mathcal{Y}$, which is their common domain (and departure space). This shows that g and k are equal as functions. ∎

It is not hard to show that every right-cancellable function must be surjective, so that surjective and right-cancellable functions are the same objects. We record this claim, but leave the proof out of the presentation.

⇩

Fact 2.4.7 ☞ **surjective $\iff$ right-cancellable**

The following are equivalent for $f : \mathcal{X} \longrightarrow \mathcal{Y}$.

1. f is surjective.

2. f is right-cancellable.

Exercise 2.4.8 ☞ **Injective functions are left-cancellable**

Suppose that $f, h : \mathcal{X} \longrightarrow \mathcal{Y}$ and $g : \mathcal{Y} \longrightarrow \mathcal{Z}$, and

$$g \circ f = g \circ h \ .$$

Argue that if g is injective then $f = h$.

This is what we mean when we say that injective functions are **left-cancellable** (or **cancellable from the left**).

Again, it turns out that every left-cancellable function must be injective, so that injective and left-cancellable functions are the same objects. We leave the proof out of the presentation. It is not difficult, and the reader is encouraged to think about it.

Fact 2.4.9 ☞ **injective $\Longleftrightarrow$ left-cancellable**

The following are equivalent for $f : \mathcal{X} \longrightarrow \mathcal{Y}$.

1. f is injective.

2. f is left-cancellable.

2.5 Invertibility Of Functions

Test Your Comprehension 2.5.1 ☞ **Composition with the reverse function**

Suppose that $f : \mathcal{X} \longrightarrow \mathcal{Y}$ is a *bijection*. Argue that

$$f^{\leftrightarrow} \circ f = id_{\mathcal{X}} \quad \text{and} \quad f \circ f^{\leftrightarrow} = id_{\mathcal{Y}} \ .$$

In this sense the reverse of a bijective function plays a role (with respect to the composition of functions) similar to that the reciprocal of a non-zero number plays with respect to the multiplication in $\mathbb{R}$.

Terminology 2.5.2 ☞ **Left-invertible functions**

A function $f : \mathcal{X} \longrightarrow \mathcal{Y}$ is said to be **left-invertible**, if there is a partner function $g : \mathcal{Y} \longrightarrow \mathcal{X}$ such that

$$g \circ f = id_{\mathcal{X}} \ ,$$

or in other words,

$$g\big(f(x)\big) = x \ ,$$

for all x in $\mathcal{X}$.

Loosely speaking, g can serve as a return flight airline for f: when the first leg of the flight is with f and the second is with g, the traveller returns to the original point of departure in $\mathcal{X}$.

Such a g is then said to be a **left inverse** of f, and can be thought of as a left-antipodal function for f with respect to the operation of composition.

The strategy of looking for equivalent but very distinct descriptions of the same phenomena is one of the central themes in mathematics. Looking at a situation from a different vantage point has proven to be key for finding solutions to many problems. One may even say that most of the very difficult problems in mathematics are solved this way.

We know from Theorem 2.4.2 that only injective functions may be possibly left-invertible. The following fact, presented here without proof, affirms that all injective functions are left-invertible. In this way the notions of left-invertibility, left-cancellability and injectivity describe exactly the same functions.

Fact 2.5.3 ☞ Injective $\iff$ left-invertible $\iff$ left-cancellable

Every injective function is left-invertible, and every left-invertible function is injective.

A left-invertible function may have a number of left inverses.

Terminology 2.5.4 ☞ Right-invertible functions

A function $f : \mathcal{X} \longrightarrow \mathcal{Y}$ is said to be **right-invertible**, if there is a partner function $h : \mathcal{Y} \longrightarrow \mathcal{X}$ such that

$$f \circ h = id_{\mathcal{Y}} \ ,$$

or in other words,

$$f\big(h(y)\big) = y \ ,$$

for all y in $\mathcal{Y}$.

Loosely speaking, f can serve as a return flight airline for h: when the first leg of the flight is with h and the second is with f, the traveller returns to his/her original point of departure in $\mathcal{Y}$.

Such an h is then said to be a **right inverse** of f, and can be thought of as a right-antipodal function for f with respect to the operation of composition.

We know from Theorem 2.4.2 that only surjective functions may be possibly right-invertible. The following fact, that we present here without proof, affirms that all surjective functions are in fact right-invertible. In this way the concepts of right-invertibility and surjectivity describe exactly the same functions.

Fact 2.5.5 ☞ **Surjective $\Longleftrightarrow$ right-invertible $\Longleftrightarrow$ right-cancellable**

Every surjective function is right-invertible, and every right-invertible function is surjective.

A right-invertible function may have a number of right inverses.

This claim turns out to be far more treacherous than the corresponding result about injectivity (Fact 2.5.3).
The statement that every surjective function is right invertible cannot be proved or disproved based on the standard set of mathematical axioms known as ZF. We shall accept the statement as true, making it an additional axiom (Axiom of Choice), and so shall follow the ZFC theory of mathematics.
Were we to reject the claim as false, we would follow a different but still perfectly consistent mathematics theory ZF¬C.
Even though the two mathematics theories are in conflict with each other, they are equally legitimate descriptions of our reality. An interested reader is encouraged to research topics on the axiomatic foundation of mathematics for further information.

Test Your Comprehension 2.5.6

Verify the following claims.

1. The function $EXP : \mathbb{R} \longrightarrow \mathbb{R}$ defined by
$$EXP(t) := e^t ,$$
is left-invertible, but is not right-invertible.

2. The function $Exp : \mathbb{R} \longrightarrow (0, \infty)$ defined by
$$Exp(t) := e^t ,$$
is both left-invertible and right-invertible.

Test Your Comprehension 2.5.7

Argue that the following are equivalent for a function $f : \mathcal{X} \longrightarrow \mathcal{Y}$.

1. f is cancellable from the left and is cancellable from the right.

2. f is left-invertible and right-invertible.

3. f is a bijection.

Terminology 2.5.8 ☞ **Invertible functions**

Functions f that are both left-invertible and right-invertible are said to be **invertible** (or **cancellable**).

As TYC 2.5.7 shows,

the invertible functions are exactly the bijections.

An injective function may have a number of left inverses, and a surjective function may have a number of right inverses. As we shall show momentarily, *a bijective function f has exactly one left inverse and exactly one right inverse, and in fact these are one and the same.*

If one were to take this for granted (for just a moment), one could use Exc. 2.2.12 and TYC 2.5.1 to conclude that the reverse function $f^{\hookleftarrow}$ must be that one and only "two-sided" inverse of f.

Theorem 2.5.9 **Reverse is the inverse**

Given a bijective function $f : \mathcal{X} \longrightarrow \mathcal{Y}$, $f^{\looparrowleft}$ is the only left inverse of f and the only right inverse of f.

Proof of Theorem 2.5.9. We already know from TYC 2.5.1 that $f^{\looparrowleft}$ is a left inverse of f and a right inverse of f. So it shall be sufficient to argue that every left inverse of our f equals to every right inverse of f. (That way every left inverse of our f equals $f^{\looparrowleft}$, as does every right inverse.)

Suppose that $g : \mathcal{Y} \longrightarrow \mathcal{X}$ is a left inverse of f, and $h : \mathcal{Y} \longrightarrow \mathcal{X}$ is a right inverse of f. Then

$$g \overset{\text{TYC 2.3.2}}{=} g \circ id_{\mathcal{X}} = g \circ \big(f \circ h\big) \overset{\text{Thm. 2.3.5}}{=} \big(g \circ f\big) \circ h = id_{\mathcal{Y}} \circ h \overset{\text{TYC 2.3.2}}{=} h\,. \qquad \blacksquare$$

Terminology 2.5.10

Based on the result of Theorem 2.5.9 we shall refer to the reverse $f^{\looparrowleft}$ of a bijective function as its (one and only) **two-sided inverse**, and we shall use the more common alternate notation f^{-1} to denote this function. It is also common to drop “two-sided” off in this terminology, so that we shall just speak of **the inverse of** f.

The reader should keep in mind that f^{-1} is the inverse/reverse of f, and NOT its reciprocal!

Test Your Comprehension 2.5.11 **Equivalent conditions for invertibility**

Argue that the following statements for a function $f : \mathcal{X} \longrightarrow \mathcal{Y}$ are equivalent.

1. There is a function $g : \mathcal{Y} \longrightarrow \mathcal{X}$ such that
$$f \circ g = id_{\mathcal{Y}} \quad \text{and} \quad g \circ f = id_{\mathcal{X}}\,.$$
2. f is invertible.
3. f is a bijection.

When these conditions hold,

$$g = f^{-1} = f^{\looparrowleft}\,.$$

Comment 2.5.12

Let us return to cancellation properties for the multiplication of real numbers (see Com. 2.4.5). One common maneuver is to move a factor from one side of an equation to the other via reciprocating. For example,

> If $3x = y$ then $x = \frac{1}{3}y$.

Let us deconstruct the argument.

> If $3x = y$ then $\frac{1}{3} \cdot (3x) = \frac{1}{3} \cdot y$. By associativity of multiplication we arrive at
> $$\left(\frac{1}{3} \cdot 3\right) \cdot x = \frac{1}{3} \cdot y \ ,$$
> which leads to $x = 1 \cdot x = \frac{1}{3} \cdot y$.

If instead of starting with $3x = y$, we start with $ax = y$, we can carry out a similar procedure as long as a has a multiplicatively antipodal element (denoted by $\frac{1}{a}$), namely as long as a is not zero. Every non-zero real number has a unique multiplicatively antipodal element.

We trust that the reader has been convinced through past experience that this algebraic maneuver is very useful. Can we replicate it somehow for the compositions of functions? As we know, not all functions have left/right antipodal functions with respect to the operation of composition. Yet bijections do, and these functions f have a unique antipode f^{-1} (i.e. $f^{\leftrightarrow}$).

In Exercise 2.5.13 the reader is asked to develop the required analogue by mimicking a deconstructed argument carried out above in the case of real numbers.

This result is part of the reason we use the notation f^{-1} more often than $f^{\leftrightarrow}$, as it reminds us of the cancellation properties analogous to those implemented by the reciprocals of real numbers.

Exercise 2.5.13 ☞ **Moving bijections to the other side of an equation**

Suppose that $f : \mathcal{X} \longrightarrow \mathcal{Y}$ is a bijection. Verify the following claims.

1. If $g : \mathcal{Y} \longrightarrow \mathcal{Z}$ and $g \circ f = h$, then
$$g = h \circ f^{-1} \ .$$
2. If $k : \mathcal{W} \longrightarrow \mathcal{X}$ and $f \circ k = r$, then
$$k = f^{-1} \circ r \ .$$

Theorem 2.5.14 ☞ **Composing with a bijection does not alter the jectivity**

Suppose that f is a *bijection*. Then

$$f \circ g \text{ has the same jectivity as } g \ ,$$

and

$$h \circ f \text{ has the same jectivity as } h \ .$$

Proof of Theorem 2.5.14. If g is injective, then $f \circ g$ is a composition of two injections and so is an injection (Exc. 2.4.1).

If g is surjective, then $f \circ g$ is a composition of two surjections and so is a surjection (Exc. 2.4.1).

If $f \circ g$ is an injection, then from the observation that

$$f^{-1} \circ (f \circ g) = \left(f^{-1} \circ f\right) \circ g = id \circ g = g \,,$$

it follows that g is a composition of two injections: f^{-1} and $f \circ g$ (Exc. 2.2.16 and Thm. 2.5.9), and hence is an injection.

If $f \circ g$ is a surjection, then g is a surjection by a similar argument.

This settles the first claim of the theorem. We leave the second as TYC 2.5.15 for the reader. ■

Test Your Comprehension 2.5.15

Verify the second claim of Theorem 2.5.14.

Theorem 2.5.16 ☞ **Inverse of a composition is a composition of the inverses in reversed order**

If $f : \mathcal{X} \longrightarrow \mathcal{Y}$ and $g : \mathcal{Y} \longrightarrow \mathcal{Z}$ are bijections,* then

$$\left(g \circ f\right)^{-1} = f^{-1} \circ g^{-1} . \;^{\dagger}$$

*Hence $g \circ f$ is also a bijection by Exc. 2.4.1 or by Thm. 2.5.14.
†Notice the reversal of order.

Proof of Theorem 2.5.16. Since $g \circ f$ is a bijection, by Theorem 2.5.9 it has exactly one left inverse: $\left(g \circ f\right)^{-1}$. Let us show that $f^{-1} \circ g^{-1}$ is also a left inverse of $g \circ f$, so that the desired equality will follow from the uniqueness of left inverses of bijections. Here is the calculation:

$$\begin{aligned}
\left(f^{-1} \circ g^{-1}\right) \circ (g \circ f) &= f^{-1} \circ g^{-1} \circ g \circ f \\
&= f^{-1} \circ \left(g^{-1} \circ g\right) \circ f \\
&= f^{-1} \circ id_{\mathcal{Y}} \circ f \\
&= f^{-1} \circ \left(id_{\mathcal{Y}} \circ f\right) \\
&\overset{\text{TYC 2.3.2}}{=} f^{-1} \circ f \\
&= id_{\mathcal{X}} .
\end{aligned}$$

Of course we have made much use of the associativity of composition. ■

Test Your Comprehension 2.5.17

Suppose that $\boldsymbol{T}$ is a subset of $\boldsymbol{\Delta}$, and $f : \boldsymbol{\Omega} \longrightarrow \boldsymbol{\Delta}$ is a bijection. Argue that $f^{-1}\left\langle \boldsymbol{T} \right]$ is the collection of all departure points in $\boldsymbol{\Omega}$, from which f flies to points in $\boldsymbol{T}$.

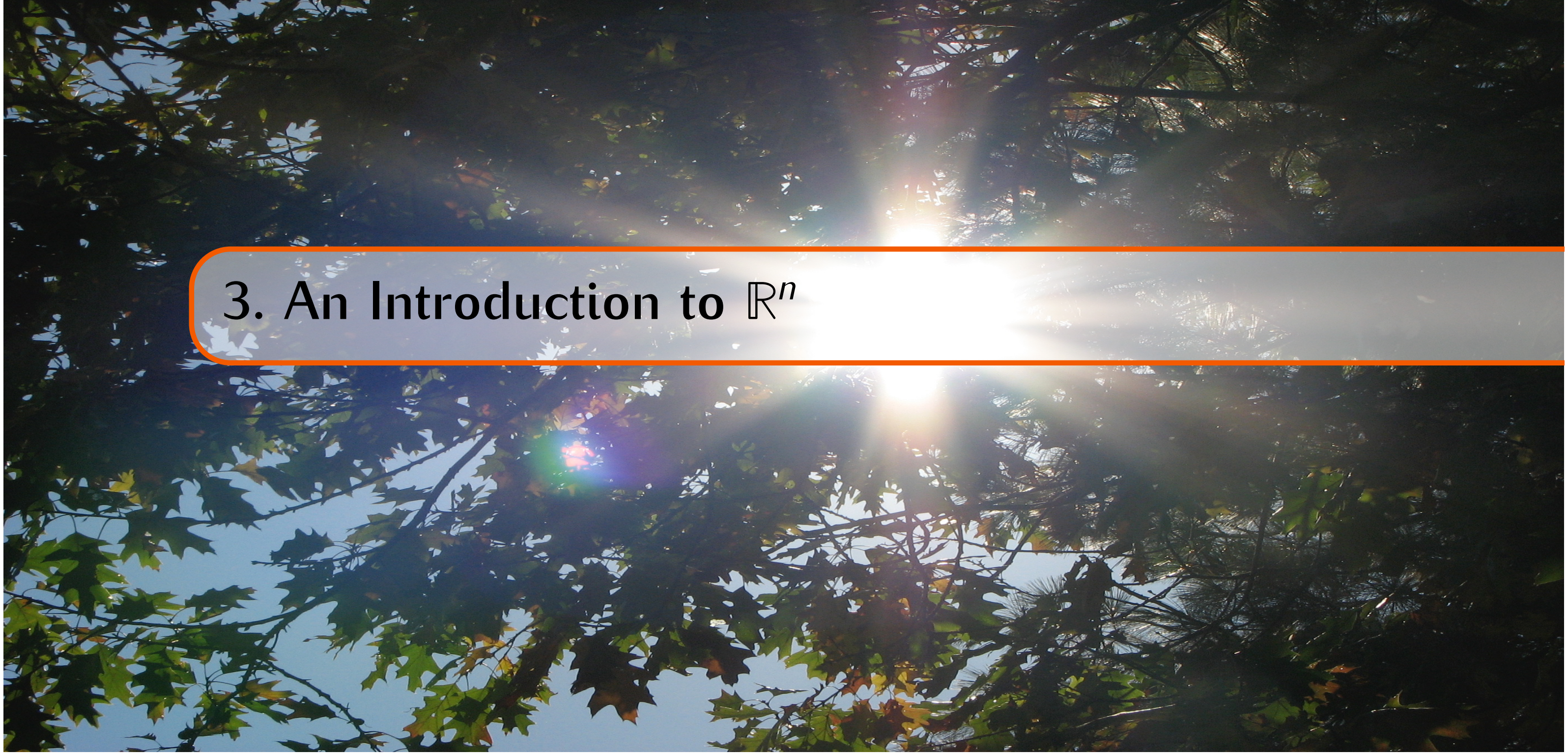
Hint: Remember that $f^{-1} = f^{\leftarrow\!\!\!\!\mathsf{P}}$. Draw yourself some pictures.

Exercise 2.5.18

Suppose that $\boldsymbol{S}$ is a subset of $\boldsymbol{\Omega}$, and $f : \boldsymbol{\Omega} \longrightarrow \boldsymbol{\Delta}$ is a bijection. Argue that

$$f^{-1}\left\langle f \left\langle \boldsymbol{S} \right] \right] = \boldsymbol{S} .$$

Hint: Apply TYC 2.5.17, with $\boldsymbol{T} = f\left\langle \boldsymbol{S} \right]$. Argue that f cannot fly to a point in $f\left\langle \boldsymbol{S} \right]$ from a point not in $\boldsymbol{S}$, as this would contradict the injectivity of f.



3. An Introduction to $\mathbb{R}^n$

Last modified on December 8, 2018

3.1 Tuples

Terminology 3.1.1

Suppose we have 23 slots numbered 1 through 23, and 23 objects, some of which may be identical. By placing all of the objects into the slots we create a **list** of these objects, and refer to the objects as **the entries of/on the list**.

We shall not deal with empty or infinite lists. All our lists are assumed to have at least one entry, and have finitely many entries each.

We shall not discriminate against lists with just one entry. When we add all of the entries of a given list of numbers, we shall not care whether there are six numbers on the list, or just one. In this way the sum of the entries on the list with a single entry is the entry itself.

A list A obtained by removing some entries from a list B is said to be a **sub-list** of B. Here we are effectively removing the slots and renumbering the remaining slots, but it is simpler just to imagine the removed entries of a list becoming invisible.

For example, the third entry of a list is the object that was placed into the third slot, and it may happen that the fourth entry of a list equals the second and twentieth entries.

A list is NOT a geometric object and the very same list can be represented visually in many ways. Here are some examples of various common representations of the *same list*.

$$p, a, b, c, a, e, f \qquad \begin{matrix} p \\ a \\ b \\ c \\ a \\ e \\ f \end{matrix} \qquad p \quad a \quad b \quad c \quad a \quad e \quad f \qquad \begin{matrix} p & & & & & & \\ & a & & & & & \\ & & b & & & & \\ & & & c & & & \\ & & & & a & & \\ & & & & & e & \\ & & & & & & f \end{matrix}$$

We often use brackets to delineate a list. Here is the *same list* represented in three more ways.

$$(p, a, b, c, a, e, f) \qquad \begin{pmatrix} p \\ a \\ b \\ c \\ a \\ e \\ f \end{pmatrix} \qquad (p \quad a \quad b \quad c \quad a \quad e \quad f)$$

If no special mention is made, one assumes that the first entry of a horizontal list is its left-most entry, and the first entry of a vertical list is its top-most entry.

The first entry of a leaning North-West-to-South-East list is its North-West-most entry. There is no convention for the position of the first entry in a leaning North-East-to-South-West list.

A choice for a representation of a list is made based on various considerations, including purely typographical ones, and it will vary depending on the context.

If a list is fairly short it can be given explicitly. When a list is too long to be written out, or when one is presenting an unspecified list, it is common to use subscripts and ellipsis, with the understanding that a subscript i indicates the i-th entry of the list. Here are some examples:

$$(a_1, a_2, \ldots, a_{23}) \qquad \begin{matrix} a_1 \\ a_2 \\ \vdots \\ a_{23} \end{matrix} \qquad a_1 \quad a_2 \quad \cdots \quad a_{23} \qquad \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_{23} \end{pmatrix} \qquad \begin{matrix} a_1 & & & \\ & a_2 & & \\ & & \ddots & \\ & & & a_{23} \end{matrix}$$

Terminology 3.1.2

A $\mathbb{R}$eal **tuple** is a list of real numbers. A tuple with n entries is an n**-tuple**. We will also use the words **singleton**, **pair, triple**, **quadruple**, etc., to refer to 1-tuple, 2-tuple, 3-tuple, 4-tuple, etc., (respectively).

Being a list, a tuple does NOT have a preset representation or orientation on a page. The same n-tuple can be horizontal when it is "sleeping", vertical when it is "standing", and tilted when it is subject to a strong wind.

Notation 3.1.3

$\mathbb{R}^n$ stands for the collection of all n-tuples of real numbers. For example, $\mathbb{R}^3$

is the set of all triples of numbers, and $\mathbb{R}^4$ is the set of all quadruples.

By convention, we shall say that $\mathbb{R}^0$ is the singleton set $\{\emptyset\}$.

Please note that $\mathbb{R}^1$ *is NOT the same construct as* $\mathbb{R}$. This is subtle. A list with a single entry is NOT the same thing as that entry itself. For an analogy think of a shopping list that only has one entry: "Eggs". The word "Eggs" is itself a list with four entries (the letters), and as such cannot be the same thing as the original shopping list which only has one entry.

Most of the time, it will be clear from the context whether an expression such as $(3+2)$ indicates the real number 5, or the singleton (5).

Notation 3.1.4

The k-th entry of a tuple U is denoted by $U[\![k]\!]$. For example: the third entry of the tuple $\begin{pmatrix} 0 \\ e \\ \ln(4) \\ -\frac{5}{3} \end{pmatrix}$ is the scalar $\ln(4)$; i.e.

$$\begin{pmatrix} 0 \\ e \\ \ln(4) \\ -\frac{5}{3} \end{pmatrix}[\![3]\!]=\ln(4).$$

Terminology 3.1.5

The n-tuple which has only zero entries is known as the **null n-tuple** and is denoted by $\mathbb{O}_n$. It plays a special role, similar to that of the real number zero.

We shall write E_k for a tuple that has 1 as its k-th entry, with all other entries being zero. Whether E_k represents a 17-tuple or a 15768-tuple, depends on the context. For example,

$$E_4 = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} \text{ in } \mathbb{R}^6 .$$

The list $E_1, E_2, \ldots, E_n$ in $\mathbb{R}^n$ is said to be **the standard basis of** $\mathbb{R}^n$ and E_k is called **the k-th standard basis tuple**.

3.2 Algebra For n-Tuples

3.2.1 — Addition

We have marked the operation of addition in $\mathbb{R}^n$ in red. Even though we are "recycling" familiar terminology and the symbol $+$ used to designate addition of real numbers, this is a new operation. $+$ pertains to $\mathbb{R}^n$, not $\mathbb{R}$. We shall rely on the reader to discern the difference in the context and will not be making the distinction explicit henceforth.

Definition 3.2.1

Two n-tuples can be "added" entry-by-entry to create another n-tuple:

$$\begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix} + \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{pmatrix} := \begin{pmatrix} a_1+b_1 \\ a_2+b_2 \\ \vdots \\ a_n+b_n \end{pmatrix}.$$

Example 3.2.2

For example,

$$\begin{pmatrix} 3 \\ -2.7 \\ \pi \\ 0 \\ 0 \end{pmatrix} + \begin{pmatrix} 0 \\ 4 \\ -x \\ 0 \\ \frac{e}{2} \end{pmatrix} = \begin{pmatrix} 3 \\ 1.3 \\ \pi-x \\ 0 \\ \frac{e}{2} \end{pmatrix},$$

while

$$\begin{pmatrix} 3 \\ -2.7 \\ \pi \\ \frac{e}{2} \end{pmatrix} + \begin{pmatrix} 0 \\ 4 \\ 0 \\ 0 \\ 0 \end{pmatrix} \quad \text{makes no sense,}$$

since the summands do not come from the same $\mathbb{R}^n$.

Observation 3.2.3

Since the addition of tuples amounts to a simultaneous addition of scalars, it is not hard to see that the operation of addition in $\mathbb{R}^n$ is commutative and associative. In other words, it satisfies the conditions

$$U + W = W + U$$

$$U + (W + Z) = (U + W) + Z.$$

The commutativity and associativity of n-tuple addition allow us to talk about sums of many n-tuples at a time, without having to specify the order of the summands and without a use of brackets to specify the order of the operations of addition.

3.2.2 — Scaling

Definition 3.2.4

An n-tuple can be "scaled" by a real number to create another n-tuple:

$$\lambda \cdot \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix} := \begin{pmatrix} \lambda \cdot a_1 \\ \lambda \cdot a_2 \\ \vdots \\ \lambda \cdot a_n \end{pmatrix} .$$

It is no accident that not all dots in the above formula are red! Do you see why?

Example 3.2.5

For example,

$$3.2 \cdot \begin{pmatrix} -1 \\ 0 \\ 2.5 \\ \pi \end{pmatrix} = \begin{pmatrix} -3.2 \\ 0 \\ 8 \\ 3.2\pi \end{pmatrix} .$$

Observation 3.2.6

It is easy to see that scaling distributes over addition in $\mathbb{R}^n$:

$$\alpha \cdot (U + W) = (\alpha \cdot U) + (\alpha \cdot W).$$

This is true because the operations of addition and scaling in $\mathbb{R}^n$ are carried out in an entry-by-entry fashion, and multiplication distributes over addition in $\mathbb{R}$.

Similarly, the following identity holds as well:

$$(\alpha \cdot \beta) \cdot U = \alpha \cdot (\beta \cdot U) .$$

3.2.3 — Linear Combinations

Definition 3.2.7

Addition and scaling are often intertwined. Given 32-tuples $U_1, U_2, \ldots, U_k$ and scalars $\alpha_1, \alpha_2, \ldots, \alpha_k$, we can form a 32-tuple

$$\alpha_1 U_1 + \alpha_2 U_2 + \cdots + \alpha_k U_k$$

which is said to be **a linear combination of the tuples** $U_1, U_2, \ldots, U_k$ with respective **coefficients** $\alpha_1, \alpha_2, \ldots, \alpha_k$.

A linear combination of tuples involving at least one non-zero coefficient is said to be a **non-trivial linear combination**. A linear combination with zero coefficients is said to be a **trivial linear combination**.

Notice that we have omitted the $\cdot$'s here, based on the similar practice of omitting multiplication signs when working with the real numbers.
We will still include $\cdot$'s whenever there is an advantage to doing so.

Please note that in the case $k = 1$ the definition does state that $\alpha_1 \cdot U_1$ **IS** a linear combination of the (single) tuple U_1.
In other words, if a tuple Z is a scalar multiple of a tuple X, then Z is a linear combination of X. This slight bending of the language will simplify future arguments.

Example 3.2.8

For example,

$$-2\cdot\begin{pmatrix}3\\-2.7\\\pi\\0\\0\end{pmatrix}+\begin{pmatrix}0\\4\\-x\\0\\\frac{e}{2}\end{pmatrix}-\begin{pmatrix}0\\0\\0\\0\\0\end{pmatrix}$$

is a linear combination of the tuples

$$\begin{pmatrix}3\\-2.7\\\pi\\0\\0\end{pmatrix},\quad\begin{pmatrix}0\\4\\-x\\0\\\frac{e}{2}\end{pmatrix},\quad\begin{pmatrix}0\\0\\0\\0\\0\end{pmatrix},$$

with respective coefficients -2, 1, and $\mathbf{-5}$.

(Why, do you think, we are trying to bring -5 to your attention here?)

We can also say that tuple $\begin{pmatrix}1\\-11\\-22\end{pmatrix}$ is a linear combination of tuples $\begin{pmatrix}3\\2\\-1\end{pmatrix}$ and $\begin{pmatrix}1\\3\\4\end{pmatrix}$, because

$$\begin{pmatrix}1\\-11\\-22\end{pmatrix}=2\cdot\begin{pmatrix}3\\2\\-1\end{pmatrix}-5\cdot\begin{pmatrix}1\\3\\4\end{pmatrix}.$$

Similarly, $\begin{pmatrix}1\\-11\\-22\end{pmatrix}$ is a linear combination of tuples $\begin{pmatrix}3\\2\\-1\end{pmatrix}$, $\begin{pmatrix}1\\3\\4\end{pmatrix}$, and $\begin{pmatrix}1\\2\\3\end{pmatrix}$, because $\begin{pmatrix}1\\-11\\-22\end{pmatrix}=2\cdot\begin{pmatrix}3\\2\\-1\end{pmatrix}-5\cdot\begin{pmatrix}1\\3\\4\end{pmatrix}+0\cdot\begin{pmatrix}1\\2\\3\end{pmatrix}$.

Deciding whether a given tuple can be expressed as a linear combination of several other given tuples is not an easy task. Eventually we will learn an algorithmic method to answer such a question.

Observation 3.2.9

Every n-tuple is a linear combination of the standard basis tuples $E_1, E_2, \ldots, E_n$. Indeed:

$$\begin{pmatrix}a_1\\a_2\\\vdots\\a_n\end{pmatrix}=a_1\cdot\begin{pmatrix}1\\0\\0\\\vdots\\0\end{pmatrix}+a_2\cdot\begin{pmatrix}0\\1\\0\\\vdots\\0\end{pmatrix}+\cdots+a_n\cdot\begin{pmatrix}0\\0\\0\\\vdots\\1\end{pmatrix}$$

$$=a_1E_1+a_2E_2+\cdots+a_nE_n\,.$$

Test Your Comprehension 3.2.10

Argue that each n-tuple can be expressed as a linear combination of the standard basis tuples in *exactly one way*.

Test Your Comprehension 3.2.11

1. Suppose that the third entry of each of the tuples $A, B, C, \ldots, Y$ is zero, while the third entry of the tuple Z is not zero. Argue that Z cannot be expressed as a linear combination of the tuples $A, B, C, \ldots, Y$.

2. Argue that no standard basis tuple can be expressed as a linear combination of some other standard basis tuples.

Test Your Comprehension 3.2.12

Suppose that tuple X can be expressed as a linear combination of the tuples U, V, W and Z using non-zero coefficients. Argue that V can be expressed as a linear combination of X, U, W and Z.

3.2.4 — Concatenation

Notation 3.2.13

The **concatenation** $V \oplus W$ of tuples $V = (v_1, v_2, v_3, \ldots, v_7)$ and $W = (w_1, w_2, w_3, \ldots, w_9)$ is the tuple $(v_1, v_2, v_3, \ldots, v_7, w_1, w_2, w_3, \ldots, w_9)$.

We will write $\begin{pmatrix} V \\ W \end{pmatrix}$ and (V, W) instead of $V \oplus W$, when convenient.

A statement of the form

$$X \oplus Y \in \mathbb{R}^{13} \oplus \mathbb{R}^{5} \quad (= \mathbb{R}^{18})$$

shall indicate that $X \in \mathbb{R}^{13}$ and $Y \in \mathbb{R}^{5}$.

Test Your Comprehension 3.2.14

Argue that every element of $\mathbb{R}^{23}$ can be written in exactly one way as $\begin{pmatrix} Z \\ V \end{pmatrix}$, where $Z \oplus V \in \mathbb{R}^4 \oplus \mathbb{R}^{19}$.

Test Your Comprehension 3.2.15 ☞ **Concatenation of tuples is not commutative**

Give an example of $U \in \mathbb{R}^8$ and $Z \in \mathbb{R}^{12}$, such that $U \oplus Z \neq Z \oplus U$.

Test Your Comprehension 3.2.16 ☞ **Concatenation of tuples is associative**

Suppose that $X \in \mathbb{R}^8$, $Y \in \mathbb{R}^4$ and $Z \in \mathbb{R}^{12}$. Argue that

$$(X \oplus Y) \oplus Z = X \oplus (Y \oplus Z)\ .$$

The concept of a concatenation of more than two tuples at a time is now aparent, as is the interpretation of a statement of the form

$$X \oplus Y \oplus Z \in \mathbb{R}^{13} \oplus \mathbb{R}^5 \oplus \mathbb{R}^{14} .$$

Test Your Comprehension 3.2.17

Suppose that $X \oplus Y$ and $U \oplus W$ are in $\mathbb{R}^8 \oplus \mathbb{R}^3$ and $\alpha, \beta \in \mathbb{R}$. Argue that

$$\alpha \cdot (X \oplus Y) + \beta \cdot (U \oplus W) = (\alpha \cdot X + \beta \cdot U) \oplus (\alpha \cdot Y + \beta \cdot W) .$$

In other words,

$$\alpha \cdot \begin{pmatrix} X \\ Y \end{pmatrix} + \beta \cdot \begin{pmatrix} U \\ W \end{pmatrix} = \begin{pmatrix} \alpha \cdot X + \beta \cdot U \\ \alpha \cdot Y + \beta \cdot W \end{pmatrix}$$

3.2.5 — Dot Product

Definition 3.2.18

The **dot product** $\bullet$ of two n-tuples *is a scalar* defined according to the following rule:

$$\begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix} \bullet \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{pmatrix} := a_1 \cdot b_1 + a_2 \cdot b_2 + \cdots + a_n \cdot b_n .$$

Example 3.2.19

For example,

$$\begin{pmatrix} 3 \\ -2.7 \\ \pi \\ 0 \\ 0 \end{pmatrix} \bullet \begin{pmatrix} 0 \\ 4 \\ -x \\ 0 \\ \frac{e}{2} \end{pmatrix} = -10.8 - \pi x ,$$

while

$$\begin{pmatrix} 3 \\ -2.7 \\ \pi \\ \frac{e}{2} \end{pmatrix} \bullet \begin{pmatrix} 0 \\ 4 \\ -x \\ 0 \\ 0 \end{pmatrix} \quad \text{makes no sense.}$$

Test Your Comprehension 3.2.20

You are asked to evaluate

$$\begin{pmatrix} 3 \\ -2.7 \\ \pi \\ 0 \\ 0 \end{pmatrix} \bullet \begin{pmatrix} 0 \\ 4 \\ -x \\ 0 \\ \frac{e}{2} \end{pmatrix} \bullet \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} .$$

What is your answer?

Test Your Comprehension 3.2.21

1. What are all of the possible values of $X \bullet X$, as X ranges over all 7-tuples?

2. When does it happen that $X \bullet X = 0$?

Test Your Comprehension 3.2.22

Argue that each of the following identities holds true in $\mathbb{R}^5$.

1. $A \bullet B = B \bullet A$

2. $(A + B) \bullet C = (A \bullet C) + (B \bullet C)$

3. $A \bullet (B + C) = (A \bullet B) + (A \bullet C)$

4. $\delta \cdot (A \bullet B) = (\delta \cdot A) \bullet B = A \bullet (\delta \cdot B)$

These formulas tell us that the dot product on $\mathbb{R}^5$ is commutative, it distributes over addition, and the scalars can be taken in and out of the product. Similar results hold in a general $\mathbb{R}^n$.

- Can you see a way of using the first two identities to demonstrate the third in a quick fashion?

- Why are *not all* dots in the last formula red?

- Are you confused by the use of the same "•" symbol to designate the entries of this list of remarks and the scalar product on $\mathbb{R}^n$? :-)

Test Your Comprehension 3.2.23

Interpret and justify the following claim:

the dot product distributes over linear combinations.

Test Your Comprehension 3.2.24

Suppose that $X, U \in \mathbb{R}^7$ and $Y, W \in \mathbb{R}^{65}$. Argue that

$$\left(\begin{smallmatrix} X \\ Y \end{smallmatrix}\right) \bullet \left(\begin{smallmatrix} U \\ W \end{smallmatrix}\right) = X \bullet U + Y \bullet W \ .$$

3.3 Orthogonality

Definition 3.3.1

Tuples U and V are said to be **orthogonal** (to each other) if

$$U \bullet V = 0.$$

Example 3.3.2

For example, tuples $\begin{pmatrix} 2 \\ 6 \\ -x \\ 4 \\ 0 \\ 1 \end{pmatrix}$ and $\begin{pmatrix} 2 \\ 2 \\ 1 \\ -4 \\ 5 \\ x \end{pmatrix}$ are orthogonal.

The null tuple $\mathbb{O}_n$ is orthogonal to every tuple in $\mathbb{R}^n$.

Test Your Comprehension 3.3.3

Suppose that tuples X and Y are orthogonal. Argue that αX and βY are also orthogonal.

Exercise 3.3.4

A friend of mine tells me that s/he has selected five concrete tuples U, V, W, Y, Z in $\mathbb{R}^5$, but that s/he intends to keep them private. S/he does tell me that U is orthogonal to each of the tuples V, W and Y, and that Z is a linear combination of V, W and Y.

Is it possible for me to decide whether U is orthogonal to Z, knowing neither any of the tuples involved nor the coefficients used to express Z as a linear combination of V, W and Y?

If you think the answer is "yes", provide a strong general mathematical argument to support your claim.

If you think the answer is "no", provide two concrete examples for the tuples and the scalars involved, such that in one case U is orthogonal to Z and in the other case it is not. These two examples will show that there is not enough information for the desired conclusion to be drawn unequivocally.

Exercise 3.3.5

1. Give a strong mathematical argument to support the claim that the only 7-tuple which is orthogonal to every 7-tuple is the null 7-tuple.

2. What happens if we only assume that a given 7-tuple is orthogonal to every *other* 7-tuple? Can one still conclude that the 7-tuple must be

the null 7-tuple?

3. Suppose that X and Y are 7-tuples such that

$$X \bullet Z = Y \bullet Z$$

for every $Z \in \mathbb{R}^7$. Is it necessarily true that $X = Y$?

Test Your Comprehension 3.3.6

Argue that for any tuple U,

$$U \bullet E_i = U[\![i]\!] \;= \text{the } i\text{-th entry of } U.$$

Consequently, the standard basis tuples in $\mathbb{R}^n$ are mutually orthogonal.

Terminology 3.3.7

A list of mutually orthogonal n-tuples is referred to as an **orthogonal list**.

3.4 Euclidean Length

Definition 3.4.1

To each tuple Z we associate a non-negative number $\|Z\|$ defined as follows:

$$\left\| \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix} \right\| := \sqrt{a_1^2 + a_2^2 + \cdots + a_n^2}.$$

We refer to $\|Z\|$ as the **(Euclidean) length** of Z.

Tuples of length 1 are said to be **the unit tuples**.

A list of mutually orthogonal *unit* n-tuples is an **orthonormal list**. For example, the standard basis of $\mathbb{R}^7$ is an orthonormal list.

Test Your Comprehension 3.4.2

Argue that the following hold for any tuple Z.

1. $\|Z\|^2 = Z \bullet Z$.

2. $\|\alpha Z\| = |\alpha| \cdot \|Z\|$.

3. The only tuples that have the (Euclidean) length zero are the null tuples.

4. $\|\alpha Z\| = 1$ exactly when Z is not null and $\alpha = \pm\frac{1}{\|Z\|}$.

Terminology 3.4.3

When Z is a non-null tuple, $\frac{1}{\|Z\|} \cdot Z$ is said to be **the unit tuple in the direction of Z**, and $\frac{-1}{\|Z\|} \cdot Z$ is said to be **the unit tuple in the direction opposite to Z**.

The process of replacing a non-null tuple Z with $\frac{1}{\|Z\|} \cdot Z$ is said to be a **normalization** of Z.

Fact 3.4.4

The following inequalities hold in every $\mathbb{R}^n$.

The Triangle Inequality: $\|X + Y\| \leq \|X\| + \|Y\|$.

The equality holds exactly when either X is a non-negative scalar multiple of Y, or Y is a non-negative scalar multiple of X.

The Reverse Triangle Inequality: $\|X - Y\| \geq \Big| \|X\| - \|Y\| \Big|$.

The equality holds exactly when either $X = \alpha Y$ or $Y = \alpha X$, with some $\alpha \geq 1$.

Cauchy-Schwarz Inequality: $|X \bullet Y| \leq \|X\| \cdot \|Y\|$.

The equality holds exactly when either X is a scalar multiple of Y, or Y is a scalar multiple of X.

Theorem 3.4.5 ☞ **Pythagorean Theorem in $\mathbb{R}^n$**

The following statements about n-tuples X and Y are equivalent.

1. X and Y are orthogonal.

2. $\|X + Y\|^2 = \|X\|^2 + \|Y\|^2$.

Proof of Theorem 3.4.5. Let us verify the following identity (which clearly entails the required result):

$$\|X + Y\|^2 - \|X\|^2 - \|Y\|^2 = 2\, X \bullet Y\,. \tag{3.1}$$

This identity is referred to as the **Real Polarization Identity**.

To this end,

$$\|X+Y\|^2 - \|X\|^2 - \|Y\|^2 \overset{\text{TYC 3.4.2}}{=} (X+Y) \bullet (X+Y) - X \bullet X - Y \bullet Y$$

$$\overset{\text{TYC3.2.22}}{=} X \bullet X + X \bullet Y + Y \bullet X + Y \bullet Y - X \bullet X - Y \bullet Y$$

$$= X \bullet Y + Y \bullet X$$

$$\overset{\text{TYC3.2.22}}{=} 2\, X \bullet Y\,.$$

■

Exercise 3.4.6

Suppose that the 9-tuples X, Y, Z, V, W are mutually orthogonal. Argue that

$$\|X+Y+Z+V+W\|^2 = \|X\|^2 + \|Y\|^2 + \|Z\|^2 + \|V\|^2 + \|W\|^2\,.$$

Hint: Exc. 3.3.4 can be useful here. Is it true that $X+Y+Z+V$ is necessarily orthogonal to W?

3.5 Subspaces of $\mathbb{R}^n$

Terminology 3.5.1

A subset $\boldsymbol{S}$ of $\mathbb{R}^n$ is said to be a **subspace** of $\mathbb{R}^n$ if it is *non-empty* and is **closed under addition and scaling**, in the sense that a sum of elements of $\boldsymbol{S}$ is again in $\boldsymbol{S}$, as is a scalar multiple of an element of $\boldsymbol{S}$.

It is easy to see that $\{\mathbb{0}_n\}$ is a subspace of $\mathbb{R}^n$. This subspace is said to be **the trivial subspace** of $\mathbb{R}^n$.

Similarly, it is clear that $\mathbb{R}^n$ is its own subspace. Subspaces of a $\mathbb{R}^n$ that are NOT equal to $\mathbb{R}^n$ are said to be **proper subspaces**.

Test Your Comprehension 3.5.2

Argue that every subspace of $\mathbb{R}^n$ contains $\mathbb{0}_n$.

Hint: A zero scalar multiple of a tuple is a null tuple.

Test Your Comprehension 3.5.3

Argue that every non-trivial subspace of $\mathbb{R}^n$ has infinitely many elements.

Hint: The set of all scalar multiples of a non-null tuple is an infinite set.

Hint: Use TYC 3.5.2 to show that the intersection is not empty. Then argue that the intersection is closed under addition and scaling.

Exercise 3.5.4

Argue that an intersection of two subspaces of $\mathbb{R}^n$ is a subspace of $\mathbb{R}^n$.

Exercise 3.5.5

Verify that the following are examples of non-trivial proper subspaces of $\mathbb{R}^8$.

1. The set of all 8-tuples whose third entry is zero.
2. The set of all 8-tuples X such that
$$X[\![2]\!] = -X[\![6]\!] .$$
3. The set of all 8-tuples whose entries add up to zero.
4. The set of all 8-tuples orthogonal to the tuple $\begin{pmatrix} 1 \\ 2 \\ 3 \\ 4 \\ 5 \\ 6 \\ \pi \\ 8 \end{pmatrix}$.
5. The set of all scalar multiples of $\begin{pmatrix} -4 \\ 3 \\ 0 \\ \frac{1}{\sqrt{2}} \\ 25 \\ -\pi^2 \\ 11 \\ e \end{pmatrix}$.
6. The set of all linear combinations of the tuples
$$\begin{pmatrix} 1 \\ 2 \\ 3 \\ 4 \\ 5 \\ 6 \\ \pi \\ 8 \end{pmatrix}, \begin{pmatrix} 0 \\ e \\ -3 \\ \sqrt{3} \\ 12 \\ \frac{1}{2} \\ \pi \\ 8 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ -11 \\ 0 \\ \ln 4 \\ 0 \\ 0 \\ 0 \end{pmatrix}.$$
7. The set of all linear combinations of the tuples
$$\begin{pmatrix} 1 \\ 2 \\ 3 \\ 4 \\ 5 \\ 6 \\ \pi \\ 8 \end{pmatrix}, \begin{pmatrix} 0 \\ e \\ -3 \\ \sqrt{3} \\ 12 \\ \frac{1}{2} \\ \pi \\ 8 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ -11 \\ 0 \\ \ln 4 \\ 0 \\ 0 \\ 0 \end{pmatrix}.$$
that are orthogonal to the tuple $\begin{pmatrix} 1 \\ 2 \\ 3 \\ 4 \\ 5 \\ 6 \\ \pi \\ 8 \end{pmatrix}$.

Test Your Comprehension 3.5.6

Argue that the following are NOT subspaces of $\mathbb{R}^7$.

1. The set of all 7-tuples whose fourth entry is 1.
2. The set of all 7-tuples X such that
$$X[\![2]\!] = 2 - X[\![6]\!] \ .$$
3. The set of all 7-tuples whose entries add up to 9.
4. The set of all 7-tuples X such that
$$X \bullet \begin{pmatrix} 1 \\ 2 \\ 3 \\ 4 \\ 5 \\ \pi \\ 7 \end{pmatrix} = -4 \ .$$
5. The set of all unit 7-tuples.
6. The set of all 7-tuples with non-negative entries.
7. The set of all tuples that are either a scalar multiple of $\begin{pmatrix} 1 \\ 2 \\ 3 \\ 4 \\ 5 \\ \pi \\ 7 \end{pmatrix}$ or are a scalar multiple of $\begin{pmatrix} 0 \\ 0 \\ -11 \\ 0 \\ \ln 4 \\ 0 \\ 0 \\ 0 \end{pmatrix}$.

Exercise 3.5.7

Find an example of two subspaces of $\mathbb{R}^5$ whose union is NOT a subspace of $\mathbb{R}^5$.

Hint: TYC 3.5.6.

Theorem 3.5.8

A non-empty subset $\boldsymbol{S}$ of $\mathbb{R}^n$ is a subspace exactly when
$$\alpha X + Y \in \boldsymbol{S}, \text{ whenever } X, Y \in \boldsymbol{S} \text{ and } \alpha \in \mathbb{R}.$$

Proof of Theorem 3.5.8. Since a subspace is closed under addition and scaling, any linear combination of elements of a subspace is again an element of that subspace. This establishes the forward implication.

To establish the reverse implication, let us assume that the stated condition holds for a subset $\boldsymbol{S}$ of $\mathbb{R}^n$.

When $\alpha = 1$ this condition becomes

$$X + Y \in \boldsymbol{S}, \text{ whenever } X, Y \in \boldsymbol{S} \text{ and } \alpha \in \mathbb{R},$$

which states that $\boldsymbol{S}$ is closed under addition.

When $Y = \mathbb{0}$, the condition becomes

$$\alpha X \in \boldsymbol{S}, \text{ whenever } X \in \boldsymbol{S} \text{ and } \alpha \in \mathbb{R},$$

and states that $\boldsymbol{S}$ is closed under scaling. ■

3.5.1 — Ortho-complements

Terminology 3.5.9

If S is a non-empty subset of $\mathbb{R}^n$, then the collection of the n-tuples that are orthogonal to ALL tuples in S is denoted by $S^\perp$, and is said to be the **orthogonal complement (a.k.a. ortho-complement)** of S.

Exercise 3.5.10 ☞ **Ortho-complements are always subspaces**

Argue that for any non-empty sub*set* S of $\mathbb{R}^n$, $S^\perp$ is a *subspace* of $\mathbb{R}^n$.

Test Your Comprehension 3.5.11

Argue that $\{\mathbb{0}_n\}^\perp = \mathbb{R}^n$ and $(\mathbb{R}^n)^\perp = \{\mathbb{0}_n\}$.

Test Your Comprehension 3.5.12

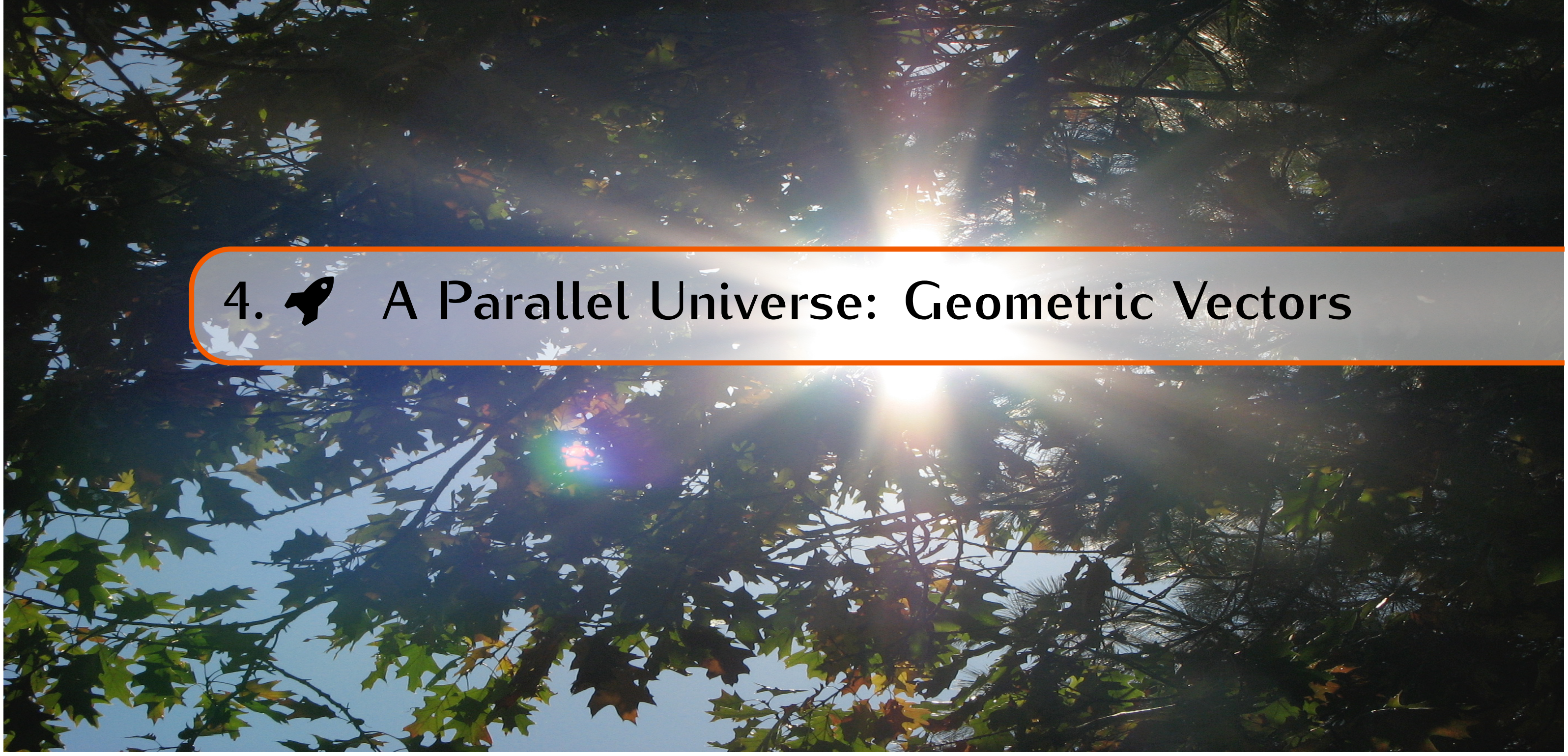
Hint: Which tuples are orthogonal to themselves?

Argue that $S \cap S^\perp = \{\mathbb{0}\}$.

Exercise 3.5.13

Show that

$$\left\{ \begin{pmatrix} x \\ y \\ y \\ x+y+z \end{pmatrix} \middle| \; x, y, z \in \mathbb{R} \right\}^\perp = \left\{ \begin{pmatrix} 0 \\ -t \\ t \\ 0 \end{pmatrix} \middle| \; t \in \mathbb{R} \right\}.$$



4. 🚀 A Parallel Universe: Geometric Vectors

Last modified on December 8, 2018

4.1 Why Vectors Are Not Directed Line Segments

The reader has surely encountered a concept of a directed line segment, usually called "a vector". These inhabit our idealized Euclidean 3-space $\mathbb{E}^3$.

$\mathbb{E}^3$ is our common model of the space around us that we perceive visually. This space is endowed with classical Euclidean geometry that allows us to talk about arbitrarily long perfectly straight lines which have no thickness, etc.

A directed line segment can be "scaled" by a positive real number α, producing another vector, whose length is α times that of the original, with no change in direction.

Scaling by a negative number β is a compound process that involves reversing the direction of the vector and then scaling the result by the positive number $|\beta|$.

Scaling by zero introduces the first conundrum and a peculiar object that results from such a scaling: a directed line segment of zero length and NO direction. This is the "zero vector" (a.k.a. the **null vector**). We denote it by $\vec{o}$.

Vectors may be added together to produce new vectors, but here enters the second conundrum: to do that one must usually "parallel-transport" one of the vectors into a favorable position with respect to the other.

Of course such a transport produces a directed line segment that is quite distinct from the original. This line segment is parallel to the original, has the same length as the original, and in our mind's eye[1] points in the same direction as the original. Yet it is definitely not identical to the original segment as it is in a different position.

This is where the other bit of strangeness happens: we are told to treat the new directed line segment as "equal" to the original. Consequently one is compelled to call a time out and demand a better definition of what is meant by a "vector". Defining vectors as directed line segments is clearly insufficient for the intended

[1] In a mind's eye, because presumably the vector can be so long (say a billion light years long) that we cannot behold it otherwise.

purposes, if we are to continue with the usual practice of interpreting "equal" to mean "is one and the same".

Let us offer an alternate definition, which does not take us too far afield.

Terminology 4.1.1

A **vector** is not a single directed line segment, but rather is a "club" (i.e. a collection) of directed line segments in $\mathbb{E}^3$ such that any one of these can be parallel-transported to match any other exactly. Furthermore, this club is "full up": the only directed line segments that can be parallel-transported to match a member of the club, are the members of the club.

The directed line segments in the club are **representatives of the vector**, not the vector itself. A vector has infinitely many representatives. The null vector is NOT an empty club: it is the club of all points on our space, and is as big a club as any other.

Scaling a club produces another club, obtained by scaling all of the representatives of the original one according to the scheme we had described above.

The addition of two clubs is accomplished by choosing an appropriate pair of representatives from the two clubs and then performing a familiar geometric procedure on the pair which produces a representative of the resulting club.

INSERT PICTURE

Here one has to prove that the choice of the original pair is immaterial, as long as the representatives fit together favorably, in the sense that any other chosen pair that fits together as favorably would have produced a representative of the same (resulting) club.

This intellectual maneuvering produces a sturdier foundation for the very shaky enterprise of operating on objects for which equality is unlike any one has encountered. We shall not belabor the technicalities of the issues at hand, but will indeed treat vectors as collections of directed (except in the case of $\vec{o}$) line segments, as in the preceding discussion.

The operations of addition and scaling on vectors enjoy the properties that match those of the identically named operations on $\mathbb{R}^n$. For example, the operation of addition of vectors is associative and commutative, and the scaling distributes over the addition. The null vector is the neutral object with respect to the addition: adding it to another vector returns that very vector as a result.

Definition 4.1.2

The collection of all vectors in $\mathbb{E}^3$ is denoted by Υ^3.

If we select a plane P within $\mathbb{E}^3$, we can restrict our attention only to those vectors that have a representative which falls within that plane. We shall denote this collection* by Υ^2_P.

Please note that $\Upsilon^2_P = \Upsilon^2_Q$ exactly when P and Q are parallel planes.

Clearly the null vector is common to every Υ^2_P, but is the only such vector.

The reader will sure agree that adding two vectors in Υ^2_P produces a vector in Υ^2_P, as does the scaling of such a vector by any scalar. Not surprisingly we shall summarize this by saying that Υ^2_P is a **subspace of** Υ^3. In particular, if need be, one can put the blinders on and operate only on the vectors in a given Υ^2_P, forgetting for the moment that there are other vectors in the universe.

In a similar fashion one may select a line L in $\mathbb{E}^3$, and focus on the collection Υ^1_L of the vectors that have a representative within L. Every such collection is clearly a subspace of Υ^3.

Again, $\Upsilon^1_L = \Upsilon^1_K$ exactly when the lines L and K are parallel.

Finally, one can get pedantic and introduce the set of vectors Υ^0_T that have a representative which fall entirely within the point T, but surely the reader can see that this is simply an overburdened way of identifying just the null vector (independently of the choice of T). Let us retain the notation Υ^0 to denote this collection with just one member.

Of course Υ^0 and Υ^3 are subspaces of Υ^3.

---

*Such a collection is like an association of clubs, in a sense that its members are clubs (i.e. vectors).

4.2 Vectors And Cartesian Coordinates

The reader is assumed to be familiar with the concept of **Cartesian coordinate systems** for $\mathbb{E}^3$. Once a unit of length is agreed upon and an origin $\mathfrak{O}$ is established, three mutually orthogonal directed lines intersecting in $\mathfrak{O}$ form the axis for such a coordinate system.

A different choice of unit of length, or of the point of origin, or of the axis, produces a different Cartesian coordinate system for $\mathbb{E}^3$.

INSERT PICTURE

Once a Cartesian coordinate system C is laid over $\mathbb{E}^3$, every point P in $\mathbb{E}^3$ receives a uniquely identifying C-address $(P)_C$. This address is a triple of numbers (i.e. an element of $\mathbb{R}^3$), and the entries of $(P)_C$ are said to be the **coordinates** of P.

INSERT PICTURE

Every triple in $\mathbb{R}^3$ is a C-address of a unique point in $\mathbb{E}^3$. Changing the coordinate system will result in points receiving new coordinates; i.e. new addresses.

Given a Cartesian coordinate system C, each vector $\vec{v}$ in Υ^3 has a unique representative that begins at the origin $\mathfrak{O}$. The C-address of the tip point of this representative is then assigned to $\vec{v}$ as its C-address $[\vec{v}]_C$. This way all vectors in Υ^3 are assigned uniquely identifying C-addresses/coordinates in $\mathbb{R}^3$.

Again, a different choice of a coordinate system will produce different addresses for the vectors. The vectors themselves do not change, and neither does $\mathbb{E}^3$, of course. A coordinate system can be thought of as an overlay for $\mathbb{E}^3$.

A vector that has a representative of unit length matching the direction of one of the coordinate axis is said to be a **standard unit vector**. These three vectors have C-addresses $\begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$, $\begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}$, and $\begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}$, and are traditionally denoted by symbols $\vec{i}, \vec{j}$ and $\vec{k}$ respectively.

If P is a plane in $\mathbb{E}^3$, one can follow similar procedures to generate planar Cartesian coordinate systems C for P and for Υ^2_P. This time the C-addresses will be pairs of numbers.

Similarly, we can talk about coordinatizing lines in $\mathbb{E}^3$.

The following fundamental properties of Cartesian coordinatization are the reason for its effectiveness. These provide a bridge between the geometric universe of $\mathbb{E}^3$ and the algebraic universe of $\mathbb{R}^3$. Mind you, the bridge (i.e. the correspondence) changes with each different choice of a Cartesian coordinate system for $\mathbb{E}^3$. This flexibility turns out to be absolutely crucial, as different coordinate systems can have advantage in different situations.

It is in this general sense that we talk about $\mathbb{R}^3$ and coordinatized $\mathbb{E}^3$ as "parallel universes".

Fact 4.2.1 **Properties of Cartesian coordinatization**

Given a Cartesian coordinate system C for $\mathbb{E}^3$, the following properties hold for all vectors $\vec{v}, \vec{w} \in \Upsilon^3$, and all scalars $a, b \in \mathbb{R}$.

1. The coordinatization function $\varphi_C : \Upsilon^3 \longrightarrow \mathbb{R}^3$ defined by
$$\varphi_C\left(\vec{u}\right) := \left[\vec{u}\right]_C ,$$
is a bijection.

2. $\left[a \cdot \vec{v} + b \cdot \vec{w}\right]_C = a \cdot \left[\vec{v}\right]_C + b \cdot \left[\vec{w}\right]_C$.

3. For non-null vectors $\vec{v}$ and $\vec{w}$,
$$\left[\vec{v}\right]_C \bullet \left[\vec{w}\right]_C = \text{Length}(\vec{v}) \cdot \text{Length}(\vec{w}) \cdot \cos\theta ,$$
where θ is an angle between the directions of vectors $\vec{v}$ and $\vec{w}$. In particular, $\left[\vec{v}\right]_C \bullet \left[\vec{w}\right]_C$ is independent of the coordinate system C.

4. $\left\|\left[\vec{v}\right]_C\right\| = \text{Length}(\vec{v})$. In other words, if $\left[\vec{v}\right]_C = \begin{pmatrix} a \\ b \\ c \end{pmatrix}$ then

$$\text{Length}(\vec{v}) = \sqrt{a^2 + b^2 + c^2}\ .$$

Test Your Comprehension 4.2.2

Use Fact 4.2.1 to argue that the following statements are equivalent for $\vec{w}, \vec{u}_1, \vec{u}_2, \ldots, \vec{u}_8 \in \Upsilon^3$.

1. $\vec{w} = a_1\vec{u}_1 + a_2\vec{u}_2 + \cdots + a_8\vec{u}_8$.
2. $\left[\vec{w}\right]_C = a_1 \cdot \left[\vec{u}_1\right]_C + a_2 \cdot \left[\vec{u}_2\right]_C + \cdots + a_8 \cdot \left[\vec{u}_8\right]_C$.

Consequently, argue that the following statements are equivalent.

1. $\left[\vec{v}\right]_C = \begin{pmatrix} a \\ b \\ c \end{pmatrix}$.
2. $\vec{v} = a \cdot \vec{i} + b \cdot \vec{j} + c \cdot \vec{k}$.

Exercise 4.2.3 ☞ The catalogue of the subspaces of Υ^3

Argue that every subspace* of Υ^3 has one of the following forms:

$$\Upsilon^0,\ \ \Upsilon^1_L,\ \ \Upsilon^2_P,\ \ \Upsilon^3\ .$$

*i.e. a non-empty collection of vectors that is closed under the operations of addition and scaling

Notation 4.2.4

Based on Fact 4.2.1, it is common to refer to the quantity

$$\text{Length}(\vec{v}) \cdot \text{Length}(\vec{w}) \cdot \cos\theta$$

as **the dot product of vectors $\vec{v}$ and $\vec{w}$**, and to denote it by $\vec{v} \bullet \vec{w}$.

Fact 4.2.1 tells us that

$$\vec{v} \bullet \vec{w} = \left[\vec{v}\right]_C \bullet \left[\vec{w}\right]_C\ ,$$

for any vectors $\vec{v}, \vec{w}$, and any Cartesian coordinate system C.

In particular, this formula is independent of the choice of a Cartesian coordinate system.

Exercise 4.2.5

Argue that each of the following identities holds true in Υ^3.

1. $\vec{v} \bullet \vec{v} = \Big(\text{Length}(\vec{v})\Big)^2$

2. $\vec{v} \bullet \vec{w} = 0$ exactly when the vectors are perpendicular or one of them is null

3. $\vec{v} \bullet \vec{w} = \vec{w} \bullet \vec{v}$

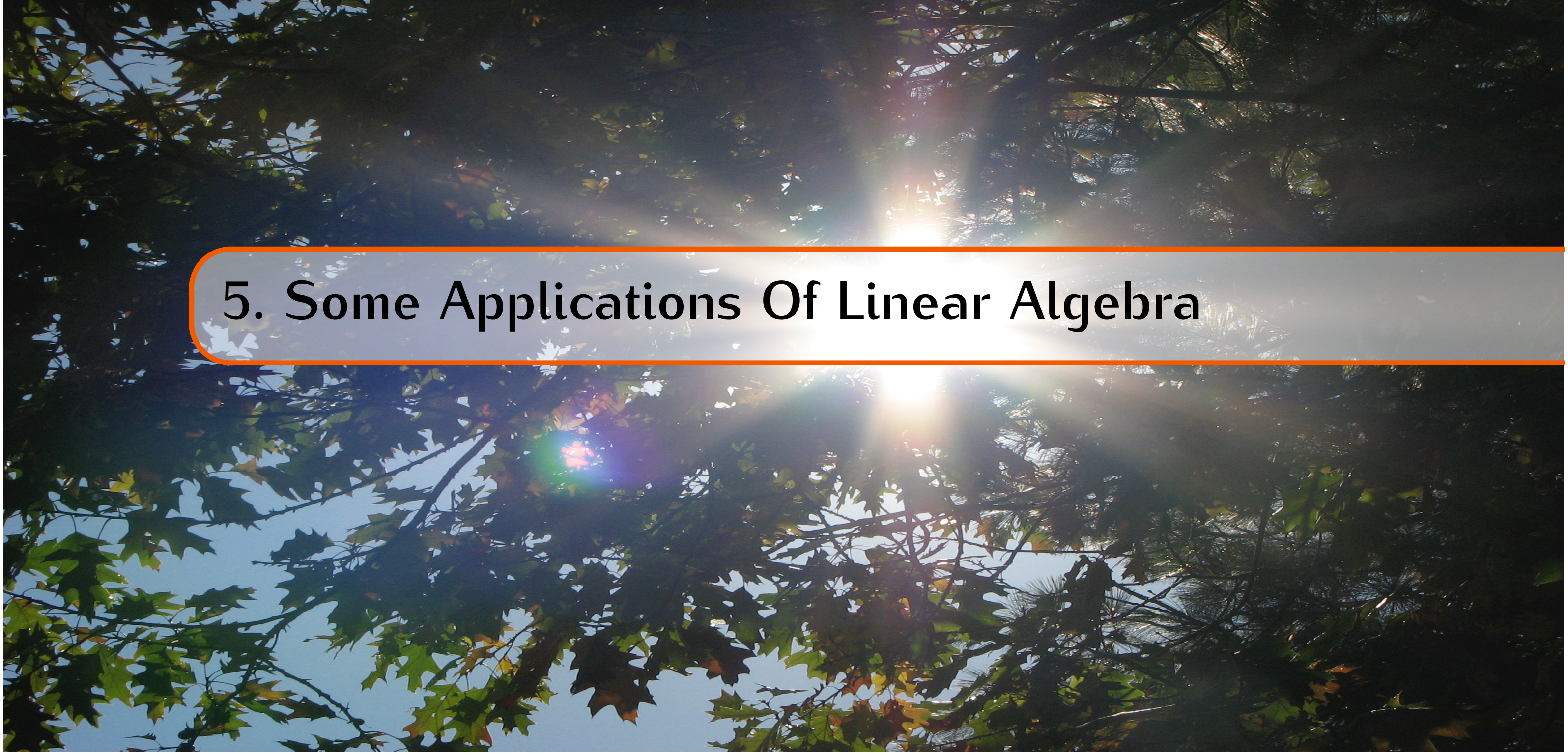
4. $(\vec{v} + \vec{w}) \bullet \vec{u} = (\vec{v} \bullet \vec{u}) + (\vec{w} \bullet \vec{u})$

5. $\vec{v} \bullet (\vec{w} + \vec{u}) = (\vec{v} \bullet \vec{w}) + (\vec{v} \bullet \vec{u})$

6. $\delta \cdot (\vec{v} \bullet \vec{w}) = (\delta \cdot \vec{v}) \bullet \vec{w} = \vec{v} \bullet (\delta \cdot \vec{w})$

Hint: Use the formula in Ntn. 4.2.4. Fact 4.2.1 and TYC 3.2.22 can be useful here.

4.2.1 — Orthogonal Complements



5. Some Applications Of Linear Algebra

Last modified on December 8, 2018

5.1 Decoupling A System Of Differential Equations

Consider a system of differential equations

$$\begin{cases} f'(x) = -f(x) + 2g(x) \\ \\ g'(x) = 3f(x) + 4g(x) \end{cases} \tag{5.1}$$

This is an example of a **coupled/intertwined** system, because each of f' and g' depends on *both* f and g.

Let us define two new auxiliary functions (we give no reason for our actions at the present time):

$$\begin{cases} h(x) := f(x) + 2g(x) \\ \\ k(x) := -3f(x) + g(x) \end{cases} . \tag{5.2}$$

Clearly h and k are differentiable functions and

$$\begin{cases} 3h + k = 7g \\ \\ h - 2k = 7f \end{cases} .$$

Therefore we can perform the following algebraic manipulation and differentiation:

$$\begin{cases} f = \frac{1}{7}h - \frac{2}{7}k \\ \\ g = \frac{3}{7}h + \frac{1}{7}k \end{cases} , \tag{5.3}$$

$$\begin{cases} f' = \frac{1}{7}h' - \frac{2}{7}k' \\ \\ g' = \frac{3}{7}h' + \frac{1}{7}k' \end{cases} .$$

Replacing f', g', f and g in the original system (5.1) with the corresponding expressions in h', k', h, k just obtained yields:

$$\begin{cases} \frac{1}{7}h' - \frac{2}{7}k' = -(\frac{1}{7}h - \frac{2}{7}k) + 2(\frac{3}{7}h + \frac{1}{7}k) \\ \\ \frac{3}{7}h' + \frac{1}{7}k' = 3(\frac{1}{7}h - \frac{2}{7}k) + 4(\frac{3}{7}h + \frac{1}{7}k) \end{cases},$$

i.e. (after collecting like terms)

$$\begin{cases} \frac{1}{7}h' - \frac{2}{7}k' = \frac{5}{7}h + \frac{4}{7}k \\ \\ \frac{3}{7}h' + \frac{1}{7}k' = \frac{15}{7}h - \frac{2}{7}k \end{cases}.$$

Let us multiply both equations in the last system through by 7 to clear the denominators:

$$\begin{cases} h' - 2k' = 5h + 4k \\ \\ 3h' + k' = 15h - 2k \end{cases}.$$

Now, if we add twice the second equation to the first, we get:

$$7h' = 35h.$$

Meanwhile, subtracting three times the first equation from the second, we get:

$$7k' = -14k.$$

Thus we have arrived at the following **decoupled** system of equations:

$$\begin{cases} h'(x) = 5h(x) \\ \\ k'(x) = -2k(x) \end{cases}. \tag{5.4}$$

After we solve for h and k (and this is indeed not hard) we can use our system (5.3) to find solutions f and g to the original system.

There are two natural questions that come to mind. The first asks whether we will find all possible solutions f and g this way. The second asks how we knew which auxiliary functions to introduce. Somehow these h and k were constructed just perfectly so that the equations got "decoupled". In due time we shall see how the theory of Linear Algebra gives answers to both of the questions.

Let us observe at this point that the original system (5.1) can be expressed in tuple notation as follows, and involves linear combinations of pairs in $\mathbb{R}^2$.

$$f'(x) \cdot \binom{1}{0} + g'(x) \cdot \binom{0}{1} = f(x) \cdot \binom{-1}{3} + g(x) \cdot \binom{2}{4}$$

5.2 A Curve In The Plane

What planar curve is described by the equation

$$x^2 + xy - y^2 = 1? \tag{5.5}$$

If the equation were just

$$x^2 - y^2 = 1,$$

we would know right away that the solutions describe a familiar planar curve called a "hyperbola". The presence of a **cross-term** term xy has made things less obvious; this term **intertwines** the variables x and y.

Let us set

$$\alpha := 10 + 4\sqrt{5} = 2\sqrt{5}(\sqrt{5} + 2),$$

and, again giving no justification for the maneuver, introduce auxiliary variables:

$$\begin{cases} u := \frac{-x+(\sqrt{5}+2)y}{\sqrt{\alpha}} \\ w := \frac{(\sqrt{5}+2)x+y}{\sqrt{\alpha}} \end{cases}. \tag{5.6}$$

Then

$$(\sqrt{5} + 2)u + w = \frac{(10 + 4\sqrt{5})y}{\sqrt{\alpha}} = \sqrt{\alpha}\ y$$

and

$$u - (\sqrt{5} + 2)w = \frac{-(10 + 4\sqrt{5})x}{\sqrt{\alpha}} = -\sqrt{\alpha}\ x.$$

In other words,

$$\begin{cases} x = -\frac{u-(\sqrt{5}+2)w}{\sqrt{\alpha}} \\ y = \frac{(\sqrt{5}+2)u+w}{\sqrt{\alpha}} \end{cases}$$

Change variables, replacing x and y in the original equation (5.5) by these expressions in u and w, to arrive at the equation

$$\frac{1}{\alpha}\left((u - (\sqrt{5} + 2)w)^2 - (u - (\sqrt{5} + 2)w)(\sqrt{5} + 2)u + w) - (\sqrt{5} + 2)u + w)^2\right) = 1,$$

which simplifies to

$$\frac{-5(\sqrt{5} + 2)(u^2 - w^2)}{\alpha} = 1,$$

and then to

$$w^2 - u^2 = \frac{\alpha}{5(\sqrt{5} + 2)} = \frac{2\sqrt{5}(\sqrt{5} + 2)}{5(\sqrt{5} + 2)} = \frac{2}{\sqrt{5}}.$$

As we have observed earlier, equation $w^2 - u^2 = \frac{2}{\sqrt{5}}$ describes a hyperbola in the u-w-plane.

The change of variables (5.6) caused the cross-terms to disappear (i.e. variables became **decoupled**) and has resulted in a simpler equation, but this is not quite the end of the original quest. The question we posed was about the x-y-plane, not the u-w-plane!

Is there a clever way to convert our knowledge about how things look in the u-w-plane into the knowledge about the x-y-plane? On top of this, one should wonder once again about the methodology behind the helpful change of variables. As we shall see, Linear Algebra provides the answers to these questions.

Please convince yourself that the original equation (5.5) can also be expressed in a tuple form as follows:

$$\begin{pmatrix} x \\ y \end{pmatrix} \bullet \left(x \cdot \begin{pmatrix} 1 \\ \frac{1}{2} \end{pmatrix} + y \cdot \begin{pmatrix} \frac{1}{2} \\ -1 \end{pmatrix} \right) = 1.$$

5.3 Least Squares

Suppose that five "data points" $(t_1, p_1), \ldots, (t_5, p_5)$ summarized in the following table are the measurements taken of a position of a body moving in a straight line with constant velocity. Here p_i is the (measured) position of the body along the line of travel at the (measured) time instance t_i.

t_i	p_i
2	2
3	5
5	6
8	9
10	11

Under ideal circumstances a body moving in this way with a constant speed v starting in position p_0 at time 0, will be at position $p_0 + tv$ at time t. Since a measurement process has imprecision inherent to it, the measured data does not precisely fit the ideal formula.

Here is the question: given our five somewhat imprecise data points, what would be a good estimate for the ideal values of p_0 and v?

For a given choice of p_0 and v we can consider the **residual** quantity

$$r_i(p_0, v) := p_i - (p_0 + t_i v),$$

which measures the error between our position measurement at time t_i and the ideal position value corresponding to p_0 and v at time t_i.

To make sure that the errors corresponding to different data points do not cancel each other when we gauge an aggregate error, we consider the sum of the squares of the residuals, i.e. the quantity

$$
\begin{aligned}
E(p_0, v) &:= r_1^2(p_0, v) + r_2^2(p_0, v) + \ldots + r_5^2(p_0, v) \\
&= \big(p_1 - (p_0 + t_1 v)\big)^2 + \big(p_2 - (p_0 + t_2 v)\big)^2 + \ldots + \big(p_5 - (p_0 + t_5 v)\big)^2 \\
&= \sum_{i=1}^{5} p_i^2 + 5p_0^2 + v^2 \sum_{i=1}^{5} t_i^2 + 2p_o v \sum_{i=1}^{5} t_i - 2p_0 \sum_{i=1}^{5} p_i - 2v \sum_{i=1}^{5} p_i t_i \\
&= 267 + 5p_0^2 + 202v^2 + 56p_0 v - 66p_0 - 462v
\end{aligned}
$$

We would like to find values p_0 and v that minimize $E(p_0, v)$, as these would be natural candidates to emulate the ideal values.

To this end, yet again we introduce auxiliary variables:

$$x := p_0 - \frac{99}{113} \quad \text{and} \quad y := v - \frac{231}{226}.$$

Then

$$
\begin{aligned}
5x^2 + 202y^2 + 56xy &= \ldots \\
&= 5p_0^2 + 202v^2 + 56p_0 v - 66p_0 - 462v + \frac{59895}{226} \\
&= E(p_0, v) + C
\end{aligned}
$$

where $C = \frac{59895}{226} - 267$.

All we have to do now is find the values of x and y that make $5x^2 + 202y^2 + 56xy$ smallest, and then the corresponding values of p_0 and v are the ones we seek!

At this point you know what to expect: we make another change of variables to uncouple x and y in $5x^2 + 202y^2 + 56xy$, just as we had done in the previous section. This time the new expression in the new variables u and w will have the form

$$\alpha u^2 + \beta w^2,$$

with positive α, β, and its minimum is clearly achieved when $u = 0 = w$. Unwinding the variable changes, we then go back to the required values of x and y, and then in turn to p_0 and v.

Alternatively, if one were versed in multivariable calculus and could argue successfully that $5x^2 + 202y^2 + 56xy$ does indeed have an absolute minimum on R^2

(which is not a totally trivial task, but is not exceedingly difficult either), then one can find the minimum by equating the gradient of the function to $\mathbb{0}_2$.

This would lead to the following equations:

$$\begin{cases} 10x + 56y = 0 \\ \\ 56x + 404y = 0 \end{cases} .$$

One would then solve the system to arrive at the sole solution $x = 0 = y$ which must therefore yield the absolute minimum of the function. It follows that $p_0 = \frac{99}{113}$ and $v = \frac{231}{226}$ minimize $E(p_0, v)$ and are the parameters we are after.

5.4 Fitting A Polynomial To Data

Given any five pairs $(a_1, b_1), \ldots, (a_5, b_5)$ of real numbers, where $a_1 < a_2 < \ldots < a_5$, how would one look for a polynomial p of degree at most 4 such that

$$p(a_i) = b_i?$$

We will deal with this and a more general question later in the term, but for now let us pick five particular points and see what is involved.

Let us be environmentally conscious and recycle the five data points from the last section:

a_i:	b_i:
2	2
3	5
5	6
8	9
10	11

Polynomial p we seek should have the form

$$p(x) = c_0 + c_1 x + c_2 x^2 + \ldots + c_4 x^4,$$

and must satisfy the following equations:

$$\begin{aligned} 2 &= c_0 + c_1 2 + c_2 2^2 + \ldots + c_4 2^4 \\ 5 &= c_0 + c_1 3 + c_2 3^2 + \ldots + c_4 3^4 \\ 6 &= c_0 + c_1 5 + c_2 5^2 + \ldots + c_4 5^4 \\ 9 &= c_0 + c_1 8 + c_2 8^2 + \ldots + c_4 8^4 \\ 11 &= c_0 + c_1 10 + c_2 10^2 + \ldots + c_4 10^4. \end{aligned}$$

In other words, are looking for real numbers $c_0, c_1, c_2, \ldots, c_4$ that satisfy the equations above.

The system of the five equations above can be expressed in a 5-tuple form as follows:

$$\begin{pmatrix} 2 \\ 5 \\ 6 \\ 9 \\ 11 \end{pmatrix} = c_0 \cdot \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \\ 1 \end{pmatrix} + c_1 \cdot \begin{pmatrix} 2 \\ 3 \\ 5 \\ 8 \\ 10 \end{pmatrix} + c_2 \cdot \begin{pmatrix} 2^2 \\ 3^2 \\ 5^2 \\ 8^2 \\ 10^2 \end{pmatrix} + \ldots + c_4 \cdot \begin{pmatrix} 2^4 \\ 3^4 \\ 5^4 \\ 8^4 \\ 10^4 \end{pmatrix},$$

and thus we see that our quest is reduced to the task of expressing a given 5-tuple as a linear combination of five other given 5-tuples, if possible.

This is a “bread and butter” problem of Linear Algebra, and we shall soon learn how to deal with it. We shall even show that for any m given data points (as described at the start of the section) there is exactly one polynomial of degree at most $m-1$ that fits the data.

5.5 Population Dynamics

A population of owls and a population of mice are placed into a small forrest and then observed at equal intervals of time. Each starts out with a small group unit. Previous experience seem to dictate that

$$\begin{cases} O(n+1) = \frac{1}{2} O(n) + bM(n) \\ \\ M(n+1) = \frac{-1}{8} O(n) + \frac{3}{2} M(n) \end{cases},$$

where $O(n)$ is the population of owls (measured in owl group units) observed after n periods of time and $M(n)$ is the corresponding population of mice. The value of the (positive) constant b seems to be in flux.

These equations reflect a natural expectation that a growth in a population of owls depends positively on the birthrate and on the availability of food (mice), while the growth in the population of mice depends positively on the birthrate, but negatively on the population of predators (owls).

The researchers are interested to know what affect different values of b will have on the LONG-TERM trend for the two inter-dependent populations.

Here again we can rewrite the original system as a single equation in $\mathbb{R}^2$:

$$O(n+1) \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix} + M(n+1) \cdot \begin{pmatrix} 0 \\ 1 \end{pmatrix} = O(n) \cdot \begin{pmatrix} \frac{1}{2} \\ \frac{-1}{8} \end{pmatrix} + M(n) \cdot \begin{pmatrix} b \\ \frac{3}{2} \end{pmatrix}.$$

It is possible to explore the long-term behavior of these populations by implementing an iterative calculation using a computing system. The reader who choses to do so will notice that something interesting happens as s/he explores the behavior for various values of b. Some values of b turn out to be "special", in that they result in a stable behavior of the system, while for other values the system experience either an uncontrolled growth of both populations, or their demise.

Discerning the special values of b is one of the things that Linear Algebra allows us to do.

5.6 A Moral Of The Story

The moral of our story is this: in all of these (and many other) problems, we come across an underlying construct of the form

$$x_1 \cdot V_1 + x_2 \cdot V_2 + \cdots + x_k \cdot V_k,$$

where x_i are real variables and $V_1, V_2, V_3, \ldots, V_k$ are some <u>fixed</u> tupples in some $\mathbb{R}^n$.

It is therefore only natural that functions $F : \mathbb{R}^k \longrightarrow \mathbb{R}^n$ of the form

$$F\begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_k \end{pmatrix} := x_1 \cdot V_1 + x_2 \cdot V_2 + \cdots + x_k \cdot V_k$$

are the central objects in the theory of Linear Algebra!

For example, in section 5.1 it is the function

$$F\begin{pmatrix} u_1 \\ u_2 \end{pmatrix} := u_1 \cdot \begin{pmatrix} -1 \\ 3 \end{pmatrix} + u_2 \cdot \begin{pmatrix} 2 \\ 4 \end{pmatrix}$$

that is central, in section 5.2 it is

$$F\begin{pmatrix} x \\ y \end{pmatrix} := x \cdot \begin{pmatrix} 1 \\ \frac{1}{2} \end{pmatrix} + y \cdot \begin{pmatrix} \frac{1}{2} \\ -1 \end{pmatrix},$$

and in section 5.4 it is

$$F\begin{pmatrix} c_0 \\ c_1 \\ c_2 \\ \vdots \\ c_4 \end{pmatrix} := c_0 \cdot \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \\ 1 \end{pmatrix} + c_1 \cdot \begin{pmatrix} 2 \\ 3 \\ 5 \\ 8 \\ 10 \end{pmatrix} + c_2 \cdot \begin{pmatrix} 2^2 \\ 3^2 \\ 5^2 \\ 8^2 \\ 10^2 \end{pmatrix} + \ldots + c_4 \cdot \begin{pmatrix} 2^4 \\ 3^4 \\ 5^4 \\ 8^4 \\ 10^4 \end{pmatrix}.$$

Such functions are called **matrix functions** for reasons that shall become clear shortly, and we will spend most of our effort in this book studying the behavior of such functions.

II

Matrix Functions

6. Introducing Matrix Functions

Last modified on December 8, 2018

6.1 What is a Matrix Function?

In Chapter 5 we offered a number of examples to demonstrate that a certain type of functions naturally appears in a variety of contexts. The study of these "matrix functions", as they are called, is the subject of Matrix Theory, a core part of Linear Algebra.

Definition 6.1.1

For any five *fixed* triples $V_1, V_2, V_3, \ldots, V_5$ in $\mathbb{R}^3$, we can define a function $\mathcal{M} : \mathbb{R}^5 \longrightarrow \mathbb{R}^3$ by the formula

$$\mathcal{M}\left(x_1, x_2, x_3, x_4, x_5\right) := x_1 \cdot V_1 + x_2 \cdot V_2 + x_3 \cdot V_3 + x_4 \cdot V_4 + x_5 \cdot V_5 \tag{6.1}$$

Every *output* of $\mathcal{M}$ equals a linear combination of the "generating" triples $V_1, V_2, V_3, \ldots, V_5$. This linear combination involves all five entries of the corresponding *input* as the scalar coefficients in front of the V_i's.

The function thus defined is called a **matrix function generated by the triples $V_1, V_2, V_3, \ldots, V_5$**.

Matrix functions generated by a list of m-tuples are defined similarly.

These triples need not be distinct, i.e. repetitions are allowed.

The *order* in which the triples are listed *matters*. It determines which entry of the input is to be used as a coefficient for each of the triples.

Example 6.1.2

For example, if the triples $V_1, V_2, V_3, \ldots, V_5$ are

$$\begin{pmatrix}1\\3\\0\end{pmatrix}, \begin{pmatrix}-2\\1.4\\0\end{pmatrix}, \begin{pmatrix}\pi\\0\\-8\end{pmatrix}, \begin{pmatrix}0\\0\\0\end{pmatrix}, \begin{pmatrix}-2\\1.4\\0\end{pmatrix}$$

then the corresponding matrix function $M : \mathbb{R}^5 \longrightarrow \mathbb{R}^3$ is described by the

Please recall that the tuple $\left(x_1, x_2, x_3, x_4, x_5\right)$ can be represented vertically, as well as horizontally.

formula:

$$\mathcal{M}\begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \end{pmatrix} := x_1 \cdot \begin{pmatrix} 1 \\ 3 \\ 0 \end{pmatrix} + x_2 \cdot \begin{pmatrix} -2 \\ 1.4 \\ 0 \end{pmatrix} + x_3 \cdot \begin{pmatrix} \pi \\ 0 \\ -8 \end{pmatrix} + x_4 \cdot \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix} + x_5 \cdot \begin{pmatrix} -2 \\ 1.4 \\ 0 \end{pmatrix}$$

$$= \begin{pmatrix} x_1 - 2x_2 + \pi x_3 - 2x_5 \\ 3x_1 + 1.4x_2 + 1.4x_5 \\ -8x_3 \end{pmatrix} .$$

Test Your Comprehension 6.1.3 ☞ **The range of a matrix is the set of all linear combinations of its generating tuples**

Argue that a tuple Y is an output from a matrix $\mathcal{A}$ exactly when Y can be expressed as a linear combination of the generating tuples of $\mathcal{A}$.

Notation 6.1.4

When a matrix function is generated by the list $V_1, V_2, V_3, \ldots, V_m$ of n-tuples we *name* it

$$\begin{bmatrix} V_1 & V_2 & V_3 & V_4 & \cdots & V_m \end{bmatrix} .$$

In particular

$$\begin{bmatrix} V_1 & V_2 & V_3 & V_4 & \cdots & V_m \end{bmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ \vdots \\ x_m \end{pmatrix} = x_1 \cdot V_1 + x_2 \cdot V_2 + x_3 \cdot V_3 + x_4 \cdot V_4 + \cdots + x_m \cdot V_m .$$

Changing the *order* in which the generating tuples are listed will commonly produce a different matrix function.

Furthermore, we forsake the delimiting brackets and express n-tuples V_i *vertically* when writing out $\begin{bmatrix} V_1 & V_2 & V_3 & V_4 & \cdots & V_m \end{bmatrix}$. This produces an array of numbers with n rows and m columns (i.e. an ***n*-by-*m* array**), which serves as a *name* of our matrix function.

A list of letters (i.e. language symbols) that has a meaning associated to it is called a "word" in the language.

Such a list of symbols is interpreted as representing that meaning. We grow accustomed to treating the list and its meaning as one whole. For example: a "tree".

In a similar fashion, "cotangent" is a list of letters that names a trigonometric function, and

$$\begin{bmatrix} -1 & 0 & e/5 \\ 2 & \pi & \sqrt{3} \end{bmatrix}$$

is a table of numbers that names a matrix function.

Based on this naming convention, we shall say that a matrix function from $\mathbb{R}^m$ to $\mathbb{R}^n$ is an $\boldsymbol{n \times m}$ **matrix** (function), and refer to "$n \times m$" as its **size**. ("$n \times m$" is vocalized as "n-by-m".) *The reader should quickly grow accustomed to the use of the word "matrix" as an abbreviation for "matrix function".*

The set of all $n \times m$ matrices is denoted by the symbol $\mathbb{M}_{n\times m}$, and we usually write $\mathbb{M}_n$ instead of $\mathbb{M}_{n\times n}$.

Example 6.1.5

When the tuples $V_1, V_2, V_3, \ldots, V_5$ are

$$\begin{pmatrix} 1 \\ 3 \\ 0 \\ \varphi \end{pmatrix}, \begin{pmatrix} -2 \\ 1.4 \\ 0 \\ 1 \end{pmatrix}, \begin{pmatrix} \pi \\ 0 \\ -8 \\ \sqrt{2} \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} -2 \\ 1.4 \\ 0 \\ 1 \end{pmatrix},$$

we have

$$\begin{bmatrix} V_1 & V_2 & V_3 & V_4 & \cdots & V_m \end{bmatrix} \begin{pmatrix} -1 \\ 2 \\ 3 \\ -4.2 \\ 1 \end{pmatrix}$$

$$= \begin{bmatrix} 1 & -2 & \pi & 0 & -2 \\ 3 & 1.4 & 0 & 0 & 1.4 \\ 0 & 0 & -8 & 0 & \sqrt{2} \\ \varphi & 1 & \sqrt{2} & 0 & 1 \end{bmatrix} \begin{pmatrix} -1 \\ 2 \\ 3 \\ -4.2 \\ 1 \end{pmatrix}$$

$$= -\begin{pmatrix} 1 \\ 3 \\ 0 \\ \varphi \end{pmatrix} + 2 \cdot \begin{pmatrix} -2 \\ 1.4 \\ 0 \\ 1 \end{pmatrix} + 3 \cdot \begin{pmatrix} \pi \\ 0 \\ -8 \\ \sqrt{2} \end{pmatrix} - 4.2 \cdot \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} + \begin{pmatrix} -2 \\ 1.4 \\ 0 \\ 1 \end{pmatrix}$$

$$= \begin{pmatrix} 3\pi-7 \\ 1.6 \\ -24 \\ 3+3\sqrt{2}-\varphi \end{pmatrix}.$$

Example 6.1.6

For example, if $\mathcal{M} = \begin{bmatrix} 2 & -1 & 3 \\ 0 & 1 & 2 \\ \gamma & 6 & 5 \\ 8 & 0 & -e \end{bmatrix}$ then $\mathcal{M} : \mathbb{R}^3 \longrightarrow \mathbb{R}^4$ and

$$\mathcal{M}\begin{pmatrix} x \\ y \\ z \end{pmatrix} = x \cdot \begin{pmatrix} 2 \\ 0 \\ \gamma \\ 8 \end{pmatrix} + y \cdot \begin{pmatrix} -1 \\ 1 \\ 6 \\ 0 \end{pmatrix} + z \cdot \begin{pmatrix} 3 \\ 2 \\ 5 \\ -e \end{pmatrix} = \begin{pmatrix} 2x-y+3z \\ y+2z \\ \gamma x+6y+5z \\ 8x-ez \end{pmatrix}. \tag{6.2}$$

In general, a function $\mathcal{F} : \mathbb{R}^3 \longrightarrow \mathbb{R}^4$ given by a formula

$$\mathcal{F}\begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} a_1 x + a_2 y + a_3 z \\ b_1 x + b_2 y + b_3 z \\ c_1 x + c_2 y + c_3 z \\ d_1 x + d_2 y + d_3 z \end{pmatrix} \tag{6.3}$$

is the matrix $\begin{bmatrix} a_1 & a_2 & a_3 \\ b_1 & b_2 & b_3 \\ c_1 & c_2 & c_3 \\ d_1 & d_2 & d_3 \end{bmatrix}$.

Test Your Comprehension 6.1.7

Argue that $id_{\mathbb{R}^m}$ and the constantly-$\mathbb{O}_m$ function $\mathcal{O}_m$ on $\mathbb{R}^m$ are examples of matrices, and write down the arrays that represent them.

Test Your Comprehension 6.1.8

Explain the difference between the number 3 and the 1×1 matrix $[3]_{1\times 1}$.

Exercise 6.1.9

Consider the functions $\mathcal{F}, \mathcal{G}, \mathcal{H}$ on $\mathbb{R}^5$ defined as follows.

$$\mathcal{F}\begin{pmatrix} v \\ \boldsymbol{w} \\ x \\ y \\ \boldsymbol{z} \end{pmatrix} := \begin{pmatrix} v \\ \boldsymbol{z} \\ x \\ y \\ \boldsymbol{w} \end{pmatrix}, \quad \mathcal{G}\begin{pmatrix} v \\ w \\ x \\ y \\ z \end{pmatrix} := \begin{pmatrix} v \\ w \\ x \\ 2y \\ z \end{pmatrix}, \quad \mathcal{H}\begin{pmatrix} v \\ w \\ x \\ y \\ z \end{pmatrix} := \begin{pmatrix} v \\ w \\ 3v+x \\ y \\ z \end{pmatrix}$$

Argue that $\mathcal{F}, \mathcal{G}$, and $\mathcal{H}$ are matrices, and write down the arrays that represent them.

When it is known that a function $\mathcal{F} : \mathbb{R}^m \longrightarrow \mathbb{R}^n$ is a matrix, the n-tuples that generate it can be recovered by applying $\mathcal{F}$ to the standard basis m-tuples. In particular, matrices are completely determined by their action on the standard basis tuples.

Theorem 6.1.10

If $\mathcal{F} : \mathbb{R}^m \longrightarrow \mathbb{R}^n$ is a matrix, then

$$\mathcal{F} = \begin{bmatrix} \mathcal{F}(E_1) & \mathcal{F}(E_2) & \ldots & \mathcal{F}(E_m) \end{bmatrix}$$

In other words, if $\mathcal{F}$ is generated by n-tuples $V_1, V_2, V_3, \ldots, V_m$, and E_k is the k-th standard basis tuple of $\mathbb{R}^m$ then

$$\mathcal{F}(E_k) = V_k \ ,$$

for all relevant k.

Proof of Theorem 6.1.10. By definition, every matrix $\mathcal{F} : \mathbb{R}^m \longrightarrow \mathbb{R}^n$ is generated by some n-tuples $V_1, V_2, V_3, \ldots, V_m$, and

$$\mathcal{F}(E_k) = \begin{bmatrix} V_1 & V_2 & V_3 & \cdots & V_m \end{bmatrix}(0, \ldots, 0, 1, 0, \ldots, 0)$$

$$= 0 \cdot V_1 + \ldots + 1 \cdot V_k + \ldots + 0 \cdot V_m = V_k \qquad \blacksquare$$

Test Your Comprehension 6.1.11

Argue that the same matrix function cannot be generated by two different lists of tuples.

Observation 6.1.12

Theorem 6.1.10 provides another way of identifying the matrices. If $\mathcal{F} : \mathbb{R}^m \longrightarrow \mathbb{R}^n$ is a matrix, then it is the function

$$\begin{bmatrix} \mathcal{F}(E_1) & \mathcal{F}(E_2) & \dots & \mathcal{F}(E_m) \end{bmatrix}$$

and therefore it satisfies the equality

$$\mathcal{F}\begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ \vdots \\ x_m \end{pmatrix} = x_1 \cdot \mathcal{F}(E_1) + x_2 \cdot \mathcal{F}(E_2) + \dots + x_m \cdot \mathcal{F}(E_m) \,, \tag{6.4}$$

for all $x_1, x_2, x_3, \dots, x_m \in \mathbb{R}$.

Conversely, if $\mathcal{F}$ satisfies the equality (6.4) for all $x_1, x_2, x_3, \dots, x_m \in \mathbb{R}$, then it is indeed a matrix generated by the tuples $\mathcal{F}(E_1)$, $\mathcal{F}(E_2), \dots, \mathcal{F}(E_m)$.

So, $\mathcal{F} : \mathbb{R}^m \longrightarrow \mathbb{R}^n$ *is a matrix exactly when it satisfies the equality* (6.4) *for all* $x_1, x_2, x_3, \dots, x_m \in \mathbb{R}$.

Example 6.1.13

The function $\mathcal{F} : \mathbb{R}^2 \longrightarrow \mathbb{R}^2$ defined by

$$\mathcal{F}\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 2|x|+y \\ xy \end{pmatrix}$$

is not a matrix, because it does not satisfy (6.4). Indeed,

$$\mathcal{F}(E_1) = \begin{pmatrix} 2 \\ 0 \end{pmatrix} \quad \text{and} \quad \mathcal{F}(E_2) = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$$

so that

$$x \cdot \mathcal{F}(E_1) + y \cdot \mathcal{F}(E_2) = \begin{pmatrix} 2x \\ 0 \end{pmatrix}$$

which does not always equal to $\mathcal{F}\begin{pmatrix} x \\ y \end{pmatrix}$, i.e. to $\begin{pmatrix} 2|x|+y \\ xy \end{pmatrix}$. For example, when $\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \end{pmatrix}$, the equality fails.

Test Your Comprehension 6.1.14

Suppose that U_o is a fixed 122-tuple (unknown to you). Consider the function $\mathcal{F} : \mathbb{R}^{122} \longrightarrow \mathbb{R}$ defined by

$$\mathcal{F}(X) := X \bullet U_o$$

Argue that $\mathcal{F}$ is a matrix.

Terminology 6.1.15

The (i, j)**-th entry of an array** is the entry that lies in the i-th row and the j-th column of the array.

The (i, j)**-th entry of a matrix** $\mathcal{M}$ is the (i, j)-th entry of its array. In other words, it is the i-th entry of the j-th generating tuple of $\mathcal{M}$. This scalar is denoted by $\mathcal{M}[\![i, j]\!]$.

In a similar fashion we identify **rows and columns of a matrix** $\mathcal{M}$. These are the tuples that appear as rows and columns of $\mathcal{M}$'s array. We enumerate the columns from left to right, and rows – from top to bottom, so that the first column is the left-most one, and the first row is the top row.

In this terminology, *the generating tuples of a matrix are its columns*, and a matrix acts by producing a linear combination of its columns with the coefficients given by the entries of the input.

Since rows and columns of a matrix are tuples, we can exploit the flexibility of their geometric orientation. For example, if a standing tuple is being identified as a row of a matrix, visualize the tuple "going to bed". Similarly, if a sleeping tuple is being identified as a column of a matrix, just "wake it up" in your mind's eye! The context will always make the orientation clear.

A **square** matrix has an equal number of rows and columns. A matrix that has at least as many rows as columns is said to be **portrait-shaped**. A matrix that has at least as many columns as rows is said to be **landscape-shaped**. A **strictly portrait-shaped** matrix has more rows than columns. **Strictly landscape-shaped** matrices have more columns than rows.

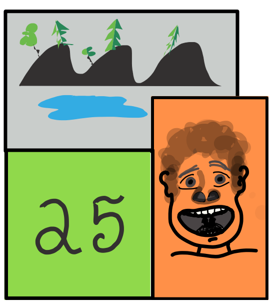


Figure 6.1

Exercise 6.1.16

Argue that a matrix produced from a matrix $\mathcal{A}$ by inserting or removing null columns has the same range as $\mathcal{A}$.

Test Your Comprehension 6.1.17

Suppose that $\mathcal{F} : \mathbb{R}^m \longrightarrow \mathbb{R}^n$ is a matrix. Argue that

$$\mathcal{F}[\![i, j]\!] = E_i \bullet \mathcal{F}(E_j)$$

for all appropriate i, j.

Test Your Comprehension 6.1.18

Argue that the only matrix function $\mathcal{F} : \mathbb{R}^m \longrightarrow \mathbb{R}^n$ such that

$$\mathcal{F}(X) \bullet Y = 0 \quad \text{for all} \quad X \in \mathbb{R}^m, \ Y \in \mathbb{R}^n ,$$

is the constantly-$\mathbb{O}_n$ function.

Terminology 6.1.19

1. An $n \times m$ matrix with only zero entries is called a **null matrix** and is denoted by $\mathcal{O}_{n\times m}$. It is easy to see that $\mathcal{O}_{n\times m} : \mathbb{R}^m \longrightarrow \mathbb{R}^n$ is the constantly-$\mathbb{0}_n$ function.

2. The matrix
$$\begin{bmatrix} \mathbf{1} & 0 & 0 & 0 & 0 & 0 \\ 0 & \mathbf{1} & 0 & 0 & 0 & 0 \\ 0 & 0 & \mathbf{1} & 0 & 0 & 0 \\ 0 & 0 & 0 & \mathbf{1} & 0 & 0 \\ 0 & 0 & 0 & 0 & \mathbf{1} & 0 \\ 0 & 0 & 0 & 0 & 0 & \mathbf{1} \end{bmatrix}$$
which is the identity function id_{R^6} (see TYC 6.1.7), is denoted by $\mathcal{I}_6$, and is called the 6×6 **identity matrix**. There are (square) identity matrices of all sizes.

3. The entries $M[\![i,i]\!]$ of a *square* matrix M are said to be its **diagonal entries**. The diagonal entries appear on **the (main) diagonal** of the matrix. Saying that **a tuple Z is the diagonal of a matrix $\mathcal{A}$** means that $\mathcal{A}[\![1,1]\!]$ is the first entry of Z, $\mathcal{A}[\![2,2]\!]$ is the second, etc. For example, the n-tuple $\mathbb{1}_n$ of all 1's is the diagonal of the identity matrix $\mathcal{I}_n$.

4. The entries of a square matrix that are not on the main diagonal are said to be the **off-diagonal entries**.
For example, the diagonal entries of the identity matrix are all equal to 1, and the off-diagonal ones are all equal to zero.

5. A *square* matrix M is said to be **upper-triangular** if $M[\![i,j]\!] = 0$ whenever $i > j$. In other words, when all entries of M appearing *below* the main diagonal are zero.
For example, upper-triangular 6×6 matrices have the following look:
$$\begin{bmatrix} \square & \square & \square & \square & \square & \square \\ 0 & \square & \square & \square & \square & \square \\ 0 & 0 & \square & \square & \square & \square \\ 0 & 0 & 0 & \square & \square & \square \\ 0 & 0 & 0 & 0 & \square & \square \\ 0 & 0 & 0 & 0 & 0 & \square \end{bmatrix},$$
where the entries in the boxes $\square$ may or may not be zero.
Lower-triangular matrices are defined in an analogous fashion.

6. A (square) matrix that is both lower- and upper-triangular is said to be a **diagonal matrix**. In other words, the diagonal matrices are such that all of their off-diagonal entries are zero. For example, an identity matrix is a diagonal matrix, and diagonal 6×6 matrices have the following look:
$$\begin{bmatrix} \square & 0 & 0 & 0 & 0 & 0 \\ 0 & \square & 0 & 0 & 0 & 0 \\ 0 & 0 & \square & 0 & 0 & 0 \\ 0 & 0 & 0 & \square & 0 & 0 \\ 0 & 0 & 0 & 0 & \square & 0 \\ 0 & 0 & 0 & 0 & 0 & \square \end{bmatrix},$$
where the entries in the boxes $\square$ may or may not be zero.

6.1.1 — Rows Vs. Columns

Observation 6.1.20

Let us revisit equation (6.2), and observe that

$$\mathcal{M}\begin{pmatrix} x\\ y\\ z\end{pmatrix} = \begin{bmatrix} 2 & -1 & 3\\ 0 & 1 & 2\\ \gamma & 6 & 5\\ 8 & 0 & -e\end{bmatrix}\begin{pmatrix} x\\ y\\ z\end{pmatrix} = \begin{pmatrix} 2x-y+3z\\ y+2z\\ \gamma x+6y+5z\\ 8x-ez\end{pmatrix} = \begin{pmatrix} \begin{pmatrix} 2\\ -1\\ 3\end{pmatrix}\bullet\begin{pmatrix} x\\ y\\ z\end{pmatrix}\\ \begin{pmatrix} 0\\ 1\\ 2\end{pmatrix}\bullet\begin{pmatrix} x\\ y\\ z\end{pmatrix}\\ \begin{pmatrix} \gamma\\ 6\\ 5\end{pmatrix}\bullet\begin{pmatrix} x\\ y\\ z\end{pmatrix}\\ \begin{pmatrix} 8\\ 0\\ -e\end{pmatrix}\bullet\begin{pmatrix} x\\ y\\ z\end{pmatrix}\end{pmatrix} = \begin{pmatrix} R_1\bullet\begin{pmatrix} x\\ y\\ z\end{pmatrix}\\ R_2\bullet\begin{pmatrix} x\\ y\\ z\end{pmatrix}\\ R_3\bullet\begin{pmatrix} x\\ y\\ z\end{pmatrix}\\ R_4\bullet\begin{pmatrix} x\\ y\\ z\end{pmatrix}\end{pmatrix},$$

where R_1, R_2, R_3, R_4 are the rows of the matrix $\mathcal{M}$. It is easy to see that this pattern holds generally.

$\Downarrow$

Theorem 6.1.21

If $\mathcal{M}$ is a matrix, then for each input tuple X the output tuple $\mathcal{M}(X)$ can be constructed by taking the dot products of X with the rows of $\mathcal{M}$.

Notation 6.1.22

Let us write

$$\begin{bmatrix} \longleftarrow & R_1 & \longrightarrow\\ \longleftarrow & R_2 & \longrightarrow\\ \longleftarrow & R_3 & \longrightarrow\\ & \vdots & \\ \longleftarrow & R_n & \longrightarrow\end{bmatrix}$$

for the $n \times m$ matrix whose rows are the m-tuples $R_1, R_2, R_3, \dots, R_n$. (In the future we will drop off the arrows when possible to unburden the notation.)

Theorem 6.1.21 gives us the formula

$$\begin{bmatrix} \longleftarrow & R_1 & \longrightarrow\\ \longleftarrow & R_2 & \longrightarrow\\ \longleftarrow & R_3 & \longrightarrow\\ & \vdots & \\ \longleftarrow & R_n & \longrightarrow\end{bmatrix}(X) = \begin{pmatrix} R_1\bullet X\\ R_2\bullet X\\ R_3\bullet X\\ \vdots\\ R_n\bullet X\end{pmatrix} \tag{6.5}$$

which expresses the output of a matrix in terms of the input and the *rows* of the matrix. The original definition of the matrix expressed the output in terms of the input and the *columns* of the matrix.

Synopsis 6.1.23

Given an n-by-m matrix $\mathcal{M}$ and an input $X \in \mathbb{R}^m$, one can calculate the output $\mathcal{M}(X) \in \mathbb{R}^n$ in *two different ways*:

Column-centric: Form a linear combination of the columns of $\mathcal{M}$ using the entries of X as scalar coefficients;

Row-centric: Make an n-tuple of the dot products of X with the rows of $\mathcal{M}$.

6.2 Linearity

According to our definition, a function $\mathcal{F} : \mathbb{R}^m \longrightarrow \mathbb{R}^n$ is a matrix exactly when it is generated in the prescribed way by some m n-tuples. This is equivalent to $\mathcal{F}$ being given by a formula of the type presented in (6.3).

We have noted in Observation 6.1.12 that another equivalent condition involves the outputs corresponding to the standard basis tuples, as described in (6.4).

In the present section we develop one more way of identifying matrices among the functions $\mathcal{F} : \mathbb{R}^m \longrightarrow \mathbb{R}^n$. This time the criterion does not deal explicitly with the generating tuples or a formula for the function. Instead it identifies matrices through their general behavior.

Our goal is the the following theorem, which we develop in a number of steps. **Please make sure you do *NOT* use the theorem itself to justify any of the claims preceding the end of its proof.**

Theorem 6.2.1 ☞ **Matrix functions are the linear functions**

A function $\mathcal{F} : \mathbb{R}^m \longrightarrow \mathbb{R}^n$ is a matrix exactly when

$$\begin{cases} \mathcal{F}(\alpha \cdot X) = \alpha \cdot \mathcal{F}(X) \\ \\ \mathcal{F}(X + Y) = \mathcal{F}(X) + \mathcal{F}(Y) \end{cases}, \tag{6.6}$$

for all $\alpha \in \mathbb{R}$ and $X, Y \in \mathbb{R}^m$.

This theorem can be loosely interpreted as stating that matrices are the functions that "commute" with the operations of addition and scaling. Performing the addition first and then applying the function to the result produces the same outcome as applying the function first and then adding the results. Similarly for scaling.

Terminology 6.2.2

The equalities (6.6) in Theorem 6.2.1 are referred to as the **linearity conditions**. Any function satisfying the linearity conditions is said to be a **linear function**. In this terminology Theorem 6.2.1 can be expressed as follows:

Among functions $\mathcal{F} : \mathbb{R}^m \longrightarrow \mathbb{R}^n$, matrices and linear functions are one and the same.

Since the definition of a linear function is "behavioral" and has no explicit reference to a particular representation of a function, it leads to a more general concept down the line. To reflect this we shall take the following philosophical stance from now on:

Linearity of functions is a primary and more general concept, which happens to coincide in our present particular setting with a secondary concept: that of a matrix.

Exercise 6.2.3

Argue that every linear function $\mathcal{F} : \mathbb{R}^m \longrightarrow \mathbb{R}^n$ has the property:

$$\mathcal{F}(\mathbb{O}_m) = \mathbb{O}_n \ .$$

In other words, such linear functions always map null tuples to null tuples.

Test Your Comprehension 6.2.4

Argue that each of the following formulas describes a function $f : \mathbb{R}^3 \longrightarrow \mathbb{R}^2$ which is NOT linear.

1. $f\left(\begin{smallmatrix} x \\ y \\ z \end{smallmatrix}\right) := \left(\begin{smallmatrix} 0 \\ xyz \end{smallmatrix}\right)$

2. $f\left(\begin{smallmatrix} x \\ y \\ z \end{smallmatrix}\right) := \left(\begin{smallmatrix} x+y \\ z-x+1 \end{smallmatrix}\right)$

3. $f\left(\begin{smallmatrix} x \\ y \\ z \end{smallmatrix}\right) := \left(\begin{smallmatrix} x^2+3y \\ y+z \end{smallmatrix}\right)$

Exercise 6.2.5

By verifying the validity of the chain

$$(5) \Rightarrow (4) \Rightarrow (3) \Rightarrow (2) \Rightarrow (1) \Rightarrow (5)$$

of implications, show that the following statements about a function $\mathcal{F} : \mathbb{R}^{123} \longrightarrow \mathbb{R}^{12}$ are mutually equivalent.

1. $\mathcal{F}$ is a linear function.

2. $\mathcal{F}(a \cdot X + Y) = a \cdot \mathcal{F}(X) + \mathcal{F}(Y)$
   for all $a \in \mathbb{R}$ and X, Y in $\mathbb{R}^{123}$.

3. $\mathcal{F}(a \cdot X + b \cdot Y) = a \cdot \mathcal{F}(X) + b \cdot \mathcal{F}(Y)$
   for all $a, b \in \mathbb{R}$ and X, Y in $\mathbb{R}^{123}$.

4. $\mathcal{F}(a \cdot X + b \cdot Y + c \cdot Z) = a \cdot \mathcal{F}(X) + b \cdot \mathcal{F}(Y) + c \cdot \mathcal{F}(Z)$
   for all $a, b, c \in \mathbb{R}$ and X, Y, Z in $\mathbb{R}^{123}$.

5. $\mathcal{F}(a \cdot X + b \cdot Y + c \cdot Z + d \cdot W)$
   $= a \cdot \mathcal{F}(X) + b \cdot \mathcal{F}(Y) + c \cdot \mathcal{F}(Z) + d \cdot \mathcal{F}(W)$
   for all $a, b, c, d \in \mathbb{R}$ and X, Y, Z, W in $\mathbb{R}^{123}$.

6. etc.

In loose terms, F is linear exactly when it "commutes" with a formation of linear combinations.

Terminology 6.2.6

We shall refer to the equality (2) in Exc. 6.2.5 as the **combined linearity condition**. Checking its validity for a given function $\mathcal{G}$ is often a quickest way of testing the linearity of $\mathcal{G}$.

Test Your Comprehension 6.2.7

Suppose that you are told that Y_o is a fixed but very secret 9-tuple of real numbers, known only to selected few, and not to you. Define a function $\mathcal{G} : \mathbb{R}^9 \longrightarrow \mathbb{R}$ by the formula

$$\mathcal{G}(X) := X \bullet Y_o \; .$$

Argue that this function is linear.

Exercise 6.2.8

Recalling the identity

$$\big(x_1, x_2, x_3, \ldots, x_m\big) = x_1 \cdot E_1 + x_2 \cdot E_2 + \cdots + x_m \cdot E_m$$

use Observation 6.1.12 and Exercise 6.2.5 to argue that every linear function $\mathcal{F} : \mathbb{R}^m \longrightarrow \mathbb{R}^n$ is a matrix.

Proof of Theorem 6.2.1. In view of the result of the Exercise 6.2.8, what remains to be verified is that every matrix $\mathcal{F} : \mathbb{R}^m \longrightarrow \mathbb{R}^n$ is a linear function.

To this end, suppose that $\mathcal{F} : \mathbb{R}^m \longrightarrow \mathbb{R}^n$ is a matrix, $\alpha \in \mathbb{R}$, $X = \big(x_1, x_2, x_3, \ldots, x_m\big)$ and $Y = \big(y_1, y_2, y_3, \ldots, y_m\big)$.

Then

$$\alpha \cdot X + Y = \begin{pmatrix} \alpha \cdot x_1 + y_1 \\ \alpha \cdot x_2 + y_2 \\ \vdots \\ \alpha \cdot x_m + y_m \end{pmatrix}$$

and

$$\mathcal{F}(\alpha \cdot X + Y) = \Big[\mathcal{F}(E_1) \;\; \mathcal{F}(E_2) \;\; \ldots \;\; \mathcal{F}(E_m)\Big](\alpha \cdot X + Y)$$

$$= (\alpha x_1 + y_1) \cdot \mathcal{F}(E_1) + \ldots + (\alpha x_m + y_m) \cdot \mathcal{F}(E_m)$$

$$= \alpha \cdot \Big(x_1 \cdot \mathcal{F}(E_1) + \ldots + x_m \cdot \mathcal{F}(E_m)\Big) + \Big(y_1 \cdot \mathcal{F}(E_1) + \ldots + y_m \cdot \mathcal{F}(E_m)\Big)$$

$$= \alpha \cdot \mathcal{F}(X) + \mathcal{F}(Y)\ .$$

We have verified that $\mathcal{F}$ satisfies the combined linearity condition, and so the proof is complete by Exc. 6.2.5. ■

Test Your Comprehension 6.2.9

Argue that if two *linear* functions $\mathcal{F} : \mathbb{R}^m \longrightarrow \mathbb{R}^n$ and $\mathcal{G} : \mathbb{R}^m \longrightarrow \mathbb{R}^n$ coincide on the standard basis tuples, they coincide at every input, i.e. are equal as functions.

More formally, if $\mathcal{F}(E_i) = \mathcal{G}(E_i)$ for all applicable i, then $\mathcal{F} = G$.

Proof of Theorem 8.4.7. Obviously $\mathcal{O}_n$ satisfies the described condition. Our task is to show that no other matrix does.

If $\mathcal{F}(X) \bullet X = 0$ for all $X \in \mathbb{R}^n$, then $\mathcal{F}(V) \bullet W = 0$ for all $V, W \in \mathbb{R}^n$ by the Polarization Identity (Exc. 8.4.6), the right hand side of which only involves expressions of the form $\mathcal{F}(X) \bullet X$. Hence $\mathcal{F} = \mathcal{O}_n$ by TYC 6.1.18. ■

Theorem 6.2.10 ☞ **Ranges of matrices are subspaces**

A range of an $n \times m$ matrix is a subspace of $\mathbb{R}^n$.

Proof of Theorem 6.2.10. A range of an $n \times m$ matrix $\mathcal{A}$ always contains the null n-tuple, since matrices map null tuples to null tuples. It remains to be shown that the range of $\mathcal{A}$ is closed under the formation of linear combinations.

If $X, Y \in \mathit{Range}(\mathcal{A})$ then $X = \mathcal{A}(V)$ and $Y = \mathcal{A}(W)$ for some $V, W \in \mathbb{R}^m$. Thus, for any $\alpha, \beta \in \mathbb{R}$,

$$\alpha \cdot X + \beta \cdot Y = \alpha \cdot \mathcal{A}(V) + \beta \cdot \mathcal{A}(W) = \mathcal{A}(\alpha \cdot V + \beta \cdot W),$$

which shows that $\alpha \cdot X + \beta \cdot Y \in \mathit{Range}(\mathcal{A})$. We have made use of the fact that every matrix, being a linear function, commutes with the formation of linear combinations. ■

Synopsis 6.2.11

Let us collect all of the various equivalent conditions that identify matrices among the functions $\mathcal{F} : \mathbb{R}^m \longrightarrow \mathbb{R}^n$. These are:

The Original Definition: Definition 6.1.1;

Images of the Standard Tuples Condition: (6.4);

Linearity Conditions: (6.6);

Combined Linearity Condition: part (2) of Exercise 6.2.5;

Commuting with Linear Combinations Condition: Exercise 6.2.5.

6.3 🚀 Linear Functions On Vectors

Cartesian coordinatization provides a bridge between vectors in $\mathbb{E}^3$ and triples in $\mathbb{R}^3$ (Fact 4.2.1). This bridge can be used to create a correspondence between functions $\mathcal{F}$ on Υ^3 and functions f on $\mathbb{R}^3$.

Given a function $\mathcal{F} : \Upsilon^3 \longrightarrow \Upsilon^3$, interpret it as a collection of routes describing a no-choice airline flying from everywhere in Υ^3 to Υ^3. By replacing each vector with its C-address, we arrive at a corresponding collection of routes describing a no-choice airline flying from everywhere in $\mathbb{R}^3$ to $\mathbb{R}^3$ (TYC 2.1.2). This is a function $f : \mathbb{R}^3 \longrightarrow \mathbb{R}^3$.

Here is another way to describe this construction. To apply f to a given tuple, we interpret the tuple as coordinates of a vector, apply $\mathcal{F}$ to that vector, and then find the coordinates of the result.

Of course this f depends on both $\mathcal{F}$ and C, but for sake of the the simplicity of notation we choose NOT to denote it by $f_{\mathcal{F},C}$.

INSERT PICTURE

Exercise 6.3.1

Continue to use the notation introduced in the preceding paragraph, and recall the coordinatization function $\varphi_C(\vec{u}) = [\vec{u}]_C$ defined in Fact 4.2.1.

1. Argue that
$$f = \varphi_C \circ \mathcal{F} \circ \varphi_C^{-1} .$$

2. Show that
$$f\left(\left[\vec{v}\right]_C\right) = \left[\mathcal{F}\left(\vec{v}\right)\right]_C .$$

3. Deduce that
$$f(X) = \left[\mathcal{F}\left(\varphi_C^{-1}(X)\right)\right]_C .$$

It is natural to ask for which functions $\mathcal{F}$ and coordinate systems C the resulting function $f : \mathbb{R}^3 \longrightarrow \mathbb{R}^3$ is a matrix function (i.e. satisfies the linearity conditions).

Theorem 6.3.2 ☞ **Vector-linear functions on Υ^3**

The following are equivalent for a function $\mathcal{F} : \Upsilon^3 \longrightarrow \Upsilon^3$ and a Cartesian coordinate system C on $\mathbb{E}^3$.

1. The corresponding function $f : \mathbb{R}^3 \longrightarrow \mathbb{R}^3$ is a matrix function.

2. $\mathcal{F}$ satisfies **the vector-linearity conditions**
$$\begin{cases} \mathcal{F}\left(\alpha \cdot \vec{v}\right) = \alpha \cdot \mathcal{F}(\vec{v}) \\ \mathcal{F}\left(\vec{v} + \vec{w}\right) = \mathcal{F}(\vec{v}) + \mathcal{F}(\vec{w}) \end{cases}$$
for all $\vec{v}, \vec{w} \in \Upsilon^3$ and $\alpha \in \mathbb{R}$.

3. $\mathcal{F}$ satisfies **the combined vector-linearity condition**
$$\mathcal{F}\left(\alpha \cdot \vec{v} + \vec{w}\right) = \alpha \cdot \mathcal{F}(\vec{v}) + \mathcal{F}(\vec{w})$$
for all $\vec{v}, \vec{w} \in \Upsilon^3$ and $\alpha \in \mathbb{R}$.

Terminology 6.3.3

We refer to the functions $\mathcal{F} : \Upsilon^3 \longrightarrow \Upsilon^3$ satisfying the vector-linearity conditions as **(vector-)linear functions** on Υ^3.

Exercise 6.3.4

By emulating a solution to Exercise 6.2.5, argue that the last two conditions of Theorem 6.3.2 are equivalent.

A proof of Theorem 6.3.2 is presented in the appendix to the chapter.

Test Your Comprehension 6.3.5

Argue that every linear function $\mathcal{F}$ on Υ^3 maps the null vector to the null vector.

Hint: $\vec{o} = 0 \cdot \vec{o}$.

Test Your Comprehension 6.3.6

Argue that each of the following functions is linear. In each case make sure that you understand the definition of the function.

1. The identity function on Υ^3.

2. The constantly $\vec{o}$ function on Υ^3.

3. A rotation function $\mathcal{C} : \Upsilon^3 \longrightarrow \Upsilon^3$, that rotates vectors by 37 radians clockwise about a given (axis) line L (where the meaning of "clockwise" needs to be established ahead of time). INSERT PICTURE

4. A reflection function $\mathcal{H} : \Upsilon^3 \longrightarrow \Upsilon^3$ that reflects vectors with respect to a given plane P. INSERT PICTURE

5. A vertical projection $\mathcal{P} : \Upsilon^3 \longrightarrow \Upsilon^2_P$ that projects vectors vertically onto the plane P. INSERT PICTURE

6. A slanted projection $\mathcal{S} : \Upsilon^3 \longrightarrow \Upsilon^2_P$ that projects vectors onto the plane P along a given line L, which intersects P in a point. INSERT PICTURE

Hint: Consider what such functions do to parallelograms and their diagonals. Keep in mind that we can use parallelograms to construct sums of vectors.

Test Your Comprehension 6.3.7

Let $\vec{u}_o$ be a non-null vector in Υ^3, and consider a function $\mathcal{F}$ on Υ^3 defined by

$$\mathcal{F}(\vec{v}) := \vec{v} + \vec{u}_o \ .$$

Argue that function $\mathcal{F}$ is NOT linear.

Comment 6.3.8

We can also consider a reverse construction. Start with a function $g : \mathbb{R}^3 \longrightarrow \mathbb{R}^3$ and use an analogous procedure to generate a corresponding function $\mathcal{G} : \Upsilon^3 \longrightarrow \Upsilon^3$, by interpreting elements of $\mathbb{R}^3$ as the C-addresses of vectors in Υ^3, and replacing each address with the corresponding vector.

Of course if we now apply our original maneuver (of replacing vectors with addresses) to $\mathcal{G}$, we will return to the function g.

In particular this shows that every matrix function f on $\mathbb{R}^3$ can be produced from exactly one linear function $\mathcal{F}$ on Υ^3, and vice versa.

Let us record this.

Induced correspondences between linear functions on Υ^3 and 3×3 matrices

Each Cartesian coordinate system on $\mathbb{E}^3$ induces a bijective correspondence between the linear functions on Υ^3 and 3×3 matrices.

This correspondence can be described by the formula

$$f = \varphi_C \circ \mathcal{F} \circ \varphi_C^{-1} ,$$

or by the statement that

$$f\left(\left[\vec{v}\right]_C\right) = \left[\mathcal{F}\left(\vec{v}\right)\right]_C , \quad \text{for all} \quad \vec{v} \in \Upsilon^3 .$$

The correspondence depends on the choice of the Cartesian coordinate system.

INSERT PICTURE

Observation 6.3.9

If we start with a liner function $\mathcal{F}$ on Υ^3, how do we find the 3×3 matrix f that corresponds to it? Comment 6.3.8 offers an answer. Recall that to find the columns of a matrix, we simply apply it to the standard basis tuples.

In the present case, we would like to find $f\begin{pmatrix}1\\0\\0\end{pmatrix}$, $f\begin{pmatrix}0\\1\\0\end{pmatrix}$ and $f\begin{pmatrix}0\\0\\1\end{pmatrix}$.

In other words we seek

$$f\left(\left[\vec{i}\right]_C\right), f\left(\left[\vec{j}\right]_C\right), \text{ and } f\left(\left[\vec{k}\right]_C\right) .$$

By the formula given in Comment 6.3.8, these tuples are equal to

$$\left[\mathcal{F}(\vec{i})\right]_C, \left[\mathcal{F}(\vec{j})\right]_C, \left[\mathcal{F}(\vec{k})\right]_C .$$

So,

$$f = \left[\left[\mathcal{F}(\vec{i})\right]_C \;\; \left[\mathcal{F}(\vec{j})\right]_C \;\; \left[\mathcal{F}(\vec{k})\right]_C\right] .$$

Example 6.3.10

Let us use calculus terminology and consider the following linear functions. Assume that a cartesian coordinate system C has been chosen.

1. A reflection function $\mathcal{H} : \Upsilon^3 \longrightarrow \Upsilon^3$ that reflects vectors with respect to the x-y-plane. INSERT PICTURE

2. A vertical projection $\mathcal{P} : \Upsilon^3 \longrightarrow \Upsilon^2_P$ that projects vectors vertically onto the x-y-plane. INSERT PICTURE

3. A rotation function $\mathcal{R} : \Upsilon^3 \longrightarrow \Upsilon^3$, that rotates vectors by 37 radians clockwise about the z-axis, where "clockwise" is determined by looking from a vantage point with the C-address $\begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}$. INSERT PICTURE

For each of these linear functions let us find the corresponding matrix using the formula derived in Observation 6.3.9.

1. $\mathcal{H}$ maps $\vec{\imath}$ to itself, and $\vec{\jmath}$ to itself. It maps $\vec{k}$ to $-\vec{k}$. Hence

$$\left[\mathcal{H}(\vec{\imath})\right]_C = \left[\vec{\imath}\right]_C \overset{\text{TYC 4.2.2}}{=} \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}.$$

Similarly

$$\left[\mathcal{H}(\vec{\jmath})\right]_C = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} \text{ and } \left[\mathcal{H}(\vec{k})\right]_C = \begin{pmatrix} 0 \\ 0 \\ -1 \end{pmatrix}.$$

Hence the corresponding matrix is

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

2. $\mathcal{P}$ maps $\vec{\imath}$ to itself, and $\vec{\jmath}$ to itself. It maps $\vec{k}$ to $\vec{o}$. Hence

$$\left[\mathcal{P}(\vec{\imath})\right]_C = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \left[\mathcal{P}(\vec{\jmath})\right]_C = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} \text{ and } \left[\mathcal{P}(\vec{k})\right]_C = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}.$$

Hence the corresponding matrix is

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

3. Standard trigonometric arguments show that $\mathcal{R}$ maps $\vec{\imath}$ to the vector with the address $\begin{pmatrix} \cos 37 \\ -sin 37 \\ 0 \end{pmatrix}$. So,

$$\left[\mathcal{R}(\vec{\imath})\right]_C = \begin{pmatrix} \cos 37 \\ -sin 37 \\ 0 \end{pmatrix}.$$

INSERT PICTURE

It maps $\vec{\jmath}$ to the vector with the address $\begin{pmatrix} \sin 37 \\ cos 37 \\ 0 \end{pmatrix}$, and it maps $\vec{k}$ to itself. So, the corresponding matrix is

$$\begin{bmatrix} \cos 37 & \sin 37 & 0 \\ -\sin 37 & \cos 37 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

Theorem 6.3.11 ☞ **Action on the standard unit vectors determines a linear function**

Given a Cartesian coordinate system C for $\mathbb{E}^3$, for any vectors $\vec{u}, \vec{v}, \vec{w}$ in Υ^3 there exists exactly one linear function $\mathcal{F}$ on Υ^3 such that

$$\mathcal{F}(\vec{i}) = \vec{u}, \quad \mathcal{F}(\vec{j}) = \vec{v}, \quad \text{and} \quad \mathcal{F}(\vec{k}) = \vec{w}\ .$$

Proof of Theorem 6.3.11. Let us say that

$$U := [\vec{u}]_C, \quad V := [\vec{v}]_C, \quad \text{and} \quad W := [\vec{w}]_C\ .$$

Consider the 3×3 matrix

$$\mathcal{M} := \begin{bmatrix} U & V & W \end{bmatrix}.$$

If a linear function $\mathcal{F}$ satisfies the stated conditions, its corresponding matrix is $\mathcal{M}$. Hence there can be at most one such linear function $\mathcal{F}$ (since the linear functions are bijectively matched with the matrices, per Comment 6.3.8).

On the other hand, $\mathcal{M}$ does correspond to some linear function $\mathcal{F}$ on Υ^3, and this $\mathcal{F}$ must satisfy the required conditions by the formula in Observation 6.3.9.

So there is exactly one such $\mathcal{F}$. ∎

It is clear that rotations of vectors about an axis and reflections of vectors with respect to a plane are examples of linear functions that do not alter length of the vectors and map perpendicular pairs of vectors to perpendicular pairs of vectors. Obviously compositions of such functions are again such functions.

As we shall show below, Theorem 6.3.11 tells us that in fact ANY such function can be expressed as a composition of two rotations, perhaps followed by a reflection in a plane.

In time we will improve this result and show that every such function is either a rotation, or is a rotation followed by a reflection in a plane.

Lemma 6.3.12

If a linear function $\mathcal{F}$ on Υ^3 does not alter lengths of vectors, then it maps any two perpendicular vectors to perpendicular vectors.

Proof of Lemma 6.3.12. The argument is based on the Real Polarization Identity (3.1). The same calculation that was used to establish this identity for $\mathbb{R}^n$ can be used to establish it for Υ^3.*

If $\vec{u}$ and $\vec{w}$ are orthogonal, then by the Polarization Identity for vectors we have

$$\left\|\vec{u}+\vec{w}\right\|^2-\left\|\vec{u}\right\|^2-\left\|\vec{w}\right\|^2=0\ .$$

Yet, by the same Polarization Identity we have

$$\begin{aligned}2\,\mathcal{F}\left(\vec{u}\right)\bullet\mathcal{F}\left(\vec{w}\right)&=\left\|\mathcal{F}\left(\vec{u}\right)+\mathcal{F}\left(\vec{w}\right)\right\|^2-\left\|\mathcal{F}\left(\vec{u}\right)\right\|^2-\left\|\mathcal{F}\left(\vec{w}\right)\right\|^2\\&=\left\|\mathcal{F}\left(\vec{u}+\vec{w}\right)\right\|^2-\left\|\mathcal{F}\left(\vec{u}\right)\right\|^2-\left\|\mathcal{F}\left(\vec{w}\right)\right\|^2\\&=\left\|\vec{u}+\vec{w}\right\|^2-\left\|\vec{u}\right\|^2-\left\|\vec{w}\right\|^2=0\ ,\end{aligned}$$

where we have used the fact that $\mathcal{F}$ does not alter lengths of vectors.

This shows that $\mathcal{F}$ maps any two perpendicular vectors to perpendicular vectors. ■

*Exercise 4.2.5 shows that the properties of the dot product on Υ^3 reflect those of the dot product on $\mathbb{R}^n$.

Exercise 6.3.13

Argue that a rotation function $\mathcal{R}:\Upsilon^2_P\longrightarrow\Upsilon^2_P$, that rotates vectors by 37 radians clockwise (where the meaning of “clockwise” needs to be established ahead of time), is a linear function. INSERT PICTURE

Find the 2×2 matrix that corresponds to this function.

Test Your Comprehension 6.3.14

What sort of a correspondence do coordinate systems generate for a line L and functions $\mathcal{F}:\Upsilon^1_L\longrightarrow\Upsilon^1_L$?

6.4 Matrix Jectivity

6.4.1 — Injectivity

Exercise 6.4.1

Verify the following claims.

1. A matrix with a null column is not injective.

2. If one of the generating tuples of a matrix $\mathcal{A}$ is a multiple of another, then $\mathcal{A}$ is not injective.

Hint: Use the linearity of matrices and Theorem 6.1.10.

Example 6.4.2

As the following example shows, a matrix may be not injective even if neither of the conditions in Exercise 6.4.1 holds. In other words, each of these conditions is sufficient but is not necessary to guarantee non-injectivity of a matrix. We will develop necessary and sufficient conditions later in the book.

Consider a matrix $\mathcal{A}$ generated by the list

$$\mathcal{A} = \begin{bmatrix} 1 & 3 & 5 \\ 2 & -4 & 0 \\ 3 & 1 & 7 \end{bmatrix}.$$

Clearly $\mathcal{A}$ satisfies neither of the two conditions in Example 6.4.1. Yet

$$\mathcal{A}(1, 2, -1) = 2 \cdot \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix} + \begin{pmatrix} 3 \\ -4 \\ 1 \end{pmatrix} - \begin{pmatrix} 5 \\ 0 \\ 7 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix} = \mathcal{A}(0, 0, 0),$$

which shows that $\mathcal{A}$ is not injective.

6.4.2 — Surjectivity

Theorem 6.4.3

1. A matrix with a null row is not surjective.

2. If one of the rows of $\mathcal{A}$ is a scalar multiple of another, then $\mathcal{A}$ is not surjective.

Observation 6.4.4

As the following example shows, a matrix may be non-surjective even if neither of the conditions in Theorem 6.4.3 holds. In other words, each of these conditions is sufficient but is not necessary to guarantee non-surjectivity of a matrix. We will develop necessary and sufficient conditions later in the book.

Consider the matrix

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

which satisfies neither condition in Theorem 6.4.3. Since

$$\mathcal{A}\begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} x \\ y \\ z \\ x+y+z \end{pmatrix},$$

it is clear that E_4 is not in the range of $\mathcal{A}$.

Proof of Theorem 6.4.3. We will make use of the formula (6.5).

1. If the fifth row of a matrix $\mathcal{A}$ is null, then the fifth entry of every output

of $\mathcal{A}$ is zero. In particular E_5 is not in the range of $\mathcal{A}$.

2. If the fifth row of a matrix $\mathcal{A}$ is α times the third row, then by (6.5) and a property of the dot product, the fifth entry of any output of $\mathcal{A}$ is α times the third entry of that output. So, E_5 is not in the range of $\mathcal{A}$, as $1 \neq \alpha \times 0$. ■

6.4.3 — Bijectivity

Let us recall that a function $\mathcal{F} : \mathbb{R}^n \longrightarrow \mathbb{R}^m$ is said to be **invertible** exactly when there exists a function $\mathcal{G} : \mathbb{R}^m \longrightarrow \mathbb{R}^n$ such that

$$\mathcal{F} \circ \mathcal{G} = id_{\mathbb{R}^m} \quad \text{and} \quad \mathcal{G} \circ \mathcal{F} = id_{\mathbb{R}^n} \ .$$

These conditions can be rewritten as follows:

$$\mathcal{F}\big(\mathcal{G}(Z)\big) = Z, \quad \text{for all} \quad Z \in \mathbb{R}^m \tag{6.7}$$

and

$$\mathcal{G}\big(\mathcal{F}(W)\big) = W, \quad \text{for all} \quad W \in \mathbb{R}^n \ . \tag{6.8}$$

In this sense $\mathcal{G}$ "cancels" $\mathcal{F}$ from either side.

A function $\mathcal{F} : \mathbb{R}^n \longrightarrow \mathbb{R}^m$ is invertible exactly when it is a bijection, and in that case just one $\mathcal{G}$ fits the bill: the *reverse* of $\mathcal{F}$. This $\mathcal{G}$ gains yet another name: it is called **the inverse** of $\mathcal{F}$ and is denoted by $\mathcal{F}^{-1}$.

It is easy to see that $\mathcal{F}^{-1}$ is also invertible and that

$$\left(\mathcal{F}^{-1}\right)^{-1} = \mathcal{F} \ .$$

Invertible/bijective matrices play a major role in linear algebra. Learning to discern invertibility (and injectivity/surjectivity) of matrices is a worthy goal.

This is not a frivolous question. When a function is invertible, its inverse may not enjoy the same properties.

For example, $g(x) = \sqrt[3]{x}$ is the inverse of $f(u) = u^3$. While f is a polynomial, and thus is infinitely differentiable on $\mathbb{R}$, g is neither a polynomial nor is differentiable at zero.

It is natural to ask whether M^{-1} is necessarily a matrix, when $\mathcal{M}$ is an bijective matrix.

The answer turns out to be affirmative.

Theorem 6.4.5

The inverse of a bijective matrix is a (bijective) matrix.

Proof of Theorem 6.4.5. Suppose that $\mathcal{F}$ is a bijective matrix. By Theorem 6.2.1 and Exercise 6.2.5, it shall be sufficient to demonstrate that $\mathcal{F}^{-1}$ satisfies the combined linearity condition. In other words, that

$$\mathcal{F}^{-1}(a \cdot X + Y) = a \cdot \mathcal{F}^{-1}(X) + \mathcal{F}^{-1}(Y) \ , \tag{6.9}$$

for all $a \in \mathbb{R}$ and X, Y in the initial space of $\mathcal{F}^{-1}$ (which is the final space of $\mathcal{F}$).

Given such an a, X and Y, let us write U and W for $\mathcal{F}^{-1}(X)$ and $\mathcal{F}^{-1}(Y)$ respectively. Then $\mathcal{F}(U) = X$ and $\mathcal{F}(W) = Y$.

In particular, by the linearity of $\mathcal{F}$,

$$\mathcal{F}(a \cdot U + W) = a \cdot \mathcal{F}(U) + \mathcal{F}(W) = a \cdot X + Y \ .$$

Since $\mathcal{F}$ maps $a \cdot U + W$ to $a \cdot X + Y$, $\mathcal{F}^{-1}$ maps $a \cdot X + Y$ back to $a \cdot U + W$. Therefore

$$\mathcal{F}^{-1}(a \cdot X + Y) = a \cdot U + W = a \cdot \mathcal{F}^{-1}(X) + \mathcal{F}^{-1}(Y) \ ,$$

which gives the desired equality (6.9). ■

While Theorem 6.4.5 equips us with the knowledge that inverses of bijective matrices are matrices, it does so without an explicit reference to the generating tuples or to the representing arrays of such inverses. In particular, it does not offer a method for constructing the array of $\mathcal{F}^{-1}$ from an array of $\mathcal{F}$. Such methods exist, and several will be presented later in the text.

Test Your Comprehension 6.4.6

Using the conditions (6.7) and (6.8), argue that $[a]_{1\times1}$ is invertible exactly when $a \neq 0$, and in that case

$$[a]^{-1} = \left[\frac{1}{a}\right]_{1\times1} .$$

Hint: By Exercise 6.4.1 and Theorem 6.4.3, a null matrix is neither injective nor surjective. It is easy to see this directly as well.

Exercise 6.4.7

Using the conditions (6.7) and (6.8), argue that a diagonal matrix is invertible exactly when all of its diagonal entries are non-zero, and in such a case

$$\begin{bmatrix} \alpha & 0 & 0 & 0 & 0 & 0 \\ 0 & \lambda & 0 & 0 & 0 & 0 \\ 0 & 0 & \delta & 0 & 0 & 0 \\ 0 & 0 & 0 & \omega & 0 & 0 \\ 0 & 0 & 0 & 0 & \epsilon & 0 \\ 0 & 0 & 0 & 0 & 0 & \beta \end{bmatrix}^{-1} = \begin{bmatrix} \frac{1}{\alpha} & 0 & 0 & 0 & 0 & 0 \\ 0 & \frac{1}{\lambda} & 0 & 0 & 0 & 0 \\ 0 & 0 & \frac{1}{\delta} & 0 & 0 & 0 \\ 0 & 0 & 0 & \frac{1}{\omega} & 0 & 0 \\ 0 & 0 & 0 & 0 & \frac{1}{\epsilon} & 0 \\ 0 & 0 & 0 & 0 & 0 & \frac{1}{\beta} \end{bmatrix} .$$

Hint: As we have observed in Exercise 6.4.1, a matrix with a null column is never injective.

Exercise 6.4.8

By considering the equalities (6.7) and (6.8), argue that matrices

$$\begin{bmatrix} 0 & \mathbf{1} & 0 & 0 & 0 & 0 \\ 0 & 0 & \mathbf{2} & 0 & 0 & 0 \\ 0 & 0 & 0 & \mathbf{3} & 0 & 0 \\ 0 & 0 & 0 & 0 & \mathbf{4} & 0 \\ 0 & 0 & 0 & 0 & 0 & \mathbf{5} \\ \mathbf{6} & 0 & 0 & 0 & 0 & 0 \end{bmatrix} \quad \text{and} \quad \begin{bmatrix} 0 & \frac{\mathbf{1}}{\mathbf{1}} & 0 & 0 & 0 & 0 \\ 0 & 0 & \frac{\mathbf{1}}{\mathbf{2}} & 0 & 0 & 0 \\ 0 & 0 & 0 & \frac{\mathbf{1}}{\mathbf{3}} & 0 & 0 \\ 0 & 0 & 0 & 0 & \frac{\mathbf{1}}{\mathbf{4}} & 0 \\ 0 & 0 & 0 & 0 & 0 & \frac{\mathbf{1}}{\mathbf{5}} \\ \frac{\mathbf{1}}{\mathbf{6}} & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

are NOT mutual inverse functions.

6.5 Appendix: Exiled Proofs

Proof of Theorem 6.3.2. The equivalence 2. $\Longleftrightarrow$ 3. is the subject of Exercise 6.3.4. We shall demonstrate the equivalence 1. $\Longleftrightarrow$ 3.

3. $\Longrightarrow$ 1. : Suppose that f satisfies the combined vector-linearity condition. Let us show that $\mathcal{F}$ satisfies the combined linearity condition. This will show that $\mathcal{F}$ is a matrix (Exc. 6.2.5).

Given X and Y in $\mathbb{R}^3$, as we know from Fact 4.2.1, there exist vectors $\vec{v}$ and $\vec{w}$ such that

$$X = \left[\vec{v}\right]_C \quad \text{and} \quad Y = \left[\vec{w}\right]_C .$$

Consequently

$$\alpha X + Y = \alpha \cdot \left[\vec{v}\right]_C + \left[\vec{w}\right]_C \overset{\text{Fact 4.2.1}}{=} \left[\alpha \cdot \vec{v} + \vec{w}\right]_C .$$

Therefore

$$\mathcal{F}\big(\alpha X + Y\big) = \mathcal{F}\Big(\left[\alpha \cdot \vec{v} + \vec{w}\right]_C\Big) \overset{\text{Exc. 6.3.4}}{=} \Big[f\big(\alpha \cdot \vec{v} + \vec{w}\big)\Big]_C$$

$$= \Big[\alpha \cdot f\big(\vec{v}\big) + f\big(\vec{w}\big)\Big]_C \overset{\text{Fact 4.2.1}}{=} \alpha \cdot \Big[f\big(\vec{v}\big)\Big]_C + \Big[f\big(\vec{w}\big)\Big]_C$$

$$\overset{\text{Exc. 6.3.4}}{=} \alpha \mathcal{F}(X) + \mathcal{F}(Y) .$$

1. $\Longrightarrow$ 3. : Suppose that $\mathcal{F}$ is a matrix, i.e. suppose it satisfies the combined linearity condition (Exc. 6.2.5). Let us show that f satisfies the combined vector-linearity condition. To this end it is sufficient to demonstrate that

$$\Big[f\big(\alpha \cdot \vec{v} + \vec{w}\big)\Big]_C = \Big[\alpha \cdot f(\vec{v}) + f(\vec{w})\Big]_C ,$$

because, by Fact 4.2.1, φ_C is a bijection.

The following calculation demonstrates the required equality.

$$\begin{aligned}\Big[f\big(\alpha\cdot\vec{v}+\vec{w}\big)\Big]_C &\overset{\text{Exc. 6.3.4}}{=} \mathcal{F}\Big(\big[\alpha\cdot\vec{v}+\vec{w}\big]_C\Big) \overset{\text{Fact 4.2.1}}{=} \mathcal{F}\Big(\alpha\cdot\big[\vec{v}\big]_C+\big[\vec{w}\big]_C\Big)\\ &= \alpha\cdot\mathcal{F}\Big(\big[\vec{v}\big]_C\Big)+\mathcal{F}\Big(\big[\vec{w}\big]_C\Big) \overset{\text{Exc. 6.3.4}}{=} \alpha\cdot\Big[f(\vec{v})\Big]_C+\Big[f(\vec{w})\Big]_C\\ &\overset{\text{Exc. 6.3.4}}{=} \Big[\alpha\cdot f(\vec{v})+f(\vec{w})\Big]_C\ .\end{aligned}$$

■

7. Simple Operations With Matrix Functions

Last modified on December 8, 2018

In this chapter we introduce some operations on matrices that allow us to treat matrices as algebraic objects which can be manipulated and combined using these operations, always producing matrix functions as a result. Algebra of matrices is a core tool of linear algebra.

7.1 Transposition

Definition 7.1.1

The **transpose** of a matrix $\mathcal{M} = \begin{bmatrix} V_1 & V_2 & V_3 & \dots & V_m \end{bmatrix}_{n\times m}$ is the matrix

$$\mathcal{M}^T \quad := \quad \begin{bmatrix} \longleftarrow & V_1 & \longrightarrow \\ \longleftarrow & V_2 & \longrightarrow \\ \longleftarrow & V_3 & \longrightarrow \\ & \vdots & \\ \longleftarrow & V_m & \longrightarrow \end{bmatrix}_{m\times n}$$

In other words, the columns of $\mathcal{M}$ are the rows of $\mathcal{M}^T$, in the same order.

Note that $\mathcal{F}$ and $\mathcal{F}^T$ act in the opposite directions: if $\mathcal{F} : \mathbb{R}^m \longrightarrow \mathbb{R}^n$ then $\mathcal{F}^T : \mathbb{R}^n \longrightarrow \mathbb{R}^m$.

Example 7.1.2

$$\begin{bmatrix} e & 4 \\ 3 & 5 \\ 0 & 0 \\ e & 4 \end{bmatrix}^T = \begin{bmatrix} e & 3 & 0 & e \\ 4 & 5 & 0 & 4 \end{bmatrix}$$

Test Your Comprehension 7.1.3

Verify that the transpose of a matrix can be obtained by "flipping" its array over with respect to the North-West-to-South-East diagonal of the rectangle.

Test Your Comprehension 7.1.4

Verify that the rows of $\mathcal{M}$ are the columns of $\mathcal{M}^T$.

Test Your Comprehension 7.1.5

Argue that

$$\left(\mathcal{M}^T\right)^T = \mathcal{M}\ .$$

Test Your Comprehension 7.1.6

Argue that

$$\mathcal{M}^T[\![i,j]\!] = \mathcal{M}[\![j,i]\!]$$

for all acceptable i, j.

Theorem 7.1.7 ☞ **A Fundamental Property of Transposition**

If $\mathcal{A}$ is a $n \times m$ matrix then

$$\mathcal{A}(X) \bullet Y = X \bullet \mathcal{A}^T(Y)$$

for all $X \in \mathbb{R}^m$ and $Y \in \mathbb{R}^n$.

So, a matrix function can be transferred across the dot product at a cost of a "flip", i.e. its transposition.

Proof of Theorem 7.1.7. Given an $\mathcal{A}$ as described, we can write

$$\mathcal{A} = [C_1 \quad C_2 \quad C_3 \quad \ldots \quad C_m],$$

for the appropriate n-tuples C_i. Then

$$\mathcal{A}^T = \begin{bmatrix} \longleftarrow & C_1 & \longrightarrow \\ \longleftarrow & C_2 & \longrightarrow \\ \longleftarrow & C_3 & \longrightarrow \\ & \vdots & \\ \longleftarrow & C_m & \longrightarrow \end{bmatrix}.$$

For any $X = \left(x_1, x_2, x_3, \ldots, x_m\right)$ we can evaluate $\mathcal{A}(X)$ in a column-centric way:

$$\mathcal{A}(X) = x_1 \cdot C_1 + x_2 \cdot C_2 + \ldots + x_m \cdot C_m\ .$$

For any $Y \in \mathbb{R}^n$ we shall evaluate $\mathcal{A}^T(Y)$ in a row-centric way:

$$\mathcal{A}^T(Y) = \begin{pmatrix} C_1 \bullet Y \\ C_2 \bullet Y \\ \vdots \\ C_m \bullet Y \end{pmatrix}.$$

Now,

$$\begin{aligned} \mathcal{A}(X) \bullet Y &= (x_1 \cdot C_1 + x_2 \cdot C_2 + \ldots + x_m \cdot C_m) \bullet Y \\ &\overset{\text{TYC 3.2.23}}{=} x_1 \cdot (C_1 \bullet Y) + x_2 \cdot (C_2 \bullet Y) + \ldots + x_m \cdot (C_m \bullet Y) \\ &= X \bullet \begin{pmatrix} C_1 \bullet Y \\ C_2 \bullet Y \\ \vdots \\ C_m \bullet Y \end{pmatrix} = X \bullet \mathcal{A}^T(Y) \end{aligned}$$

■

7.2 Scaling

Terminology 7.2.1

Given a function $\mathcal{F} : \mathbb{R}^m \longrightarrow \mathbb{R}^n$ and a scalar $\alpha \in \mathbb{R}$ we can form a new function $\mathcal{G} : \mathbb{R}^m \longrightarrow \mathbb{R}^n$ by declaring that

$$\mathcal{G}(X) := \alpha \cdot \mathcal{F}(X)$$

for all $X \in \mathbb{R}^m$. The function $\mathcal{G}$ is said to be **a (scalar) multiple of the function** $\mathcal{F}$, and is denoted by $\alpha \cdot \mathcal{F}$. So,

$$(\alpha \cdot \mathcal{F})(X) := \alpha \cdot \mathcal{F}(X)$$

Compare this to the construction of the function $3 \cdot \cos(x)$ in calculus.

In other words, $\alpha \cdot \mathcal{F}$ acts by performing $\mathcal{F}$ first, followed by the scaling of the output by α.

Example 7.2.2

If the function $\mathcal{F}$ is defined by:

$$\mathcal{F}\begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 2x-y+3z \\ y+2z \\ 5x+6y+5z \\ 8x-ez \end{pmatrix}$$

then the function $(-\pi) \cdot \mathcal{F}$ is given by:

$$(-\pi \cdot \mathcal{F})\begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} -2\pi x + \pi y - 3\pi z \\ -\pi y - 2\pi z \\ -5\pi x - 6\pi y - 5\pi z \\ -8\pi x + e\pi z \end{pmatrix}$$

Test Your Comprehension 7.2.3

Argue that for any $\mathcal{F} : \mathbb{R}^m \longrightarrow \mathbb{R}^n$ and $\alpha, \beta \in \mathbb{R}$,

$$\alpha \cdot (\beta \cdot \mathcal{F}) = (\alpha \cdot \beta) \cdot \mathcal{F} = (\beta \cdot \alpha) \cdot \mathcal{F} = \beta \cdot (\alpha \cdot \mathcal{F})$$

To show that two functions from $\mathbb{R}^m$ to $\mathbb{R}^n$ are equal it is enough to show that they produce exactly the same output for every choice of input.
Also recall that the operation of scaling on $\mathbb{R}^m$ has the following property:

$$\begin{aligned} \gamma \cdot (\delta \cdot W) &= (\gamma \cdot \delta) \cdot W \\ &= (\delta \cdot \gamma) \cdot W \\ &= \delta \cdot (\gamma \cdot W) \end{aligned}$$

Theorem 7.2.4 ☞ **Scaling a matrix produces another matrix (of the same size).**

If $\mathcal{F}$ is an $n \times m$ matrix, then so is $\alpha \cdot \mathcal{F}$. To obtain the array of $\alpha \cdot \mathcal{F}$, multiply the entries of the array of $\mathcal{F}$ by α.

Equivalently: scale each column of $\mathcal{F}$ by α.

In other words, if

$$\mathcal{F} = \begin{bmatrix} V_1 & V_2 & V_3 & \dots & V_m \end{bmatrix}$$

then

$$\alpha \cdot \mathcal{F} = \begin{bmatrix} \alpha \cdot V_1 & \alpha \cdot V_2 & \alpha \cdot V_3 & \dots & \alpha \cdot V_m \end{bmatrix}$$

We shall offer two proofs for the theorem. The first of these is "structural", and the second – "behavioral".

Proof of Theorem 7.2.4. A matrix function given by

$$\mathcal{F} = \begin{bmatrix} V_1 & V_2 & \dots & V_m \end{bmatrix}$$

acts according to the formula

$$\mathcal{F}\begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_m \end{pmatrix} = x_1 V_1 + x_2 V_2 + \cdots + x_m V_m \ .$$

Consequently $\alpha\mathcal{F}$ acts according to the formula

$$(\alpha\mathcal{F})\begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_m \end{pmatrix} = \alpha \cdot \left(\mathcal{F}\begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_m \end{pmatrix}\right)$$

$$= \alpha \cdot \big(x_1 V_1 + x_2 V_2 + \cdots + x_m V_m\big)$$

$$= \alpha x_1 V_1 + \alpha x_2 V_2 + \cdots + \alpha x_m V_m$$

$$= x_1 \alpha V_1 + x_2 \alpha V_2 + \cdots + x_m \alpha V_m$$

$$= \begin{bmatrix} \alpha V_1 & \alpha V_2 & \ldots & \alpha V_m \end{bmatrix}\begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_m \end{pmatrix} ,$$

which shows that

$$\alpha\mathcal{F} = \begin{bmatrix} \alpha V_1 & \alpha V_2 & \ldots & \alpha V_m \end{bmatrix} .$$

■

Proof of Theorem 7.2.4. To show that $\alpha \cdot \mathcal{F}$ is a matrix it is sufficient to verify that it satisfies the combined linearity condition. To that end, we know that $\mathcal{F}$ satisfies this condition, so that for any $X, Y \in \mathbb{R}^m$ and $b \in \mathbb{R}$:

$$\mathcal{F}(b \cdot X + Y) = b \cdot \mathcal{F}(X) + \mathcal{F}(Y) .$$

Multiply this equality through by α to arrive at

$$\alpha \cdot \mathcal{F}(b \cdot X + Y) = \alpha \cdot \big(b \cdot \mathcal{F}(X)\big) + \alpha \cdot \mathcal{F}(Y)$$

$$= b \cdot \big(\alpha \cdot \mathcal{F}(X)\big) + \alpha \cdot \mathcal{F}(Y) ,$$

where the second equality follows from TYC 7.2.3. Thus we have established the equality

$$\big(\alpha \cdot \mathcal{F}\big)(b \cdot X + Y) = b \cdot \big(\alpha \cdot \mathcal{F}\big)(X) + \big(\alpha \cdot \mathcal{F}\big)(Y) ,$$

for any $X, Y \in \mathbb{R}^m$ and $b \in \mathbb{R}$. So, $\alpha \cdot \mathcal{F}$ satisfies the combined linearity condition, as claimed.

It remains to note that the i-th column of $\alpha \cdot \mathcal{F}$ is the tuple $\big(\alpha \cdot \mathcal{F}\big)(E_i)$, which equals $\alpha \cdot \big(\mathcal{F}(E_i)\big)$. Hence the i-th column of $\alpha \cdot \mathcal{F}$ equals α times the i-th column of $\mathcal{F}$. ■

Example 7.2.5

$$3 \cdot \begin{bmatrix} -2 & 4 & 5 \\ 2 & 0 & \pi \end{bmatrix} = \begin{bmatrix} -6 & 12 & 15 \\ 6 & 0 & 3\pi \end{bmatrix}$$

Test Your Comprehension 7.2.6

Suppose that $\mathcal{M}$ is a *non-zero* matrix. Argue that

$$a \cdot \mathcal{M} = b \cdot \mathcal{M} \quad \Longleftrightarrow \quad a = b$$

Test Your Comprehension 7.2.7

Argue that the operations of scaling and transposition for matrices "**commute**" in the following sense: for any matrix $\mathcal{M}$ and a scalar γ:

$$(\gamma \cdot \mathcal{M})^{T} = \gamma \cdot \mathcal{M}^{T} .$$

In other words, one obtains the same result by scaling first and then transposing, as by transposing first and then scaling.

Test Your Comprehension 7.2.8

Give an example of a diagonal matrix that is not a scalar multiple of an identity matrix.

7.3 Addition

Terminology 7.3.1

This time we start with two functions $\mathcal{F} : \mathbb{R}^m \longrightarrow \mathbb{R}^n$ and $\mathcal{G} : \mathbb{R}^m \longrightarrow \mathbb{R}^n$, and form a new function $\mathcal{H} : \mathbb{R}^m \longrightarrow \mathbb{R}^n$ by declaring that

$$\mathcal{H}(X) := \mathcal{F}(X) + \mathcal{G}(X) ,$$

for all $X \in \mathbb{R}^m$.

This function $\mathcal{H}$ is said to be **the sum of functions $\mathcal{F}$ and $\mathcal{G}$**, and is denoted by $\mathcal{F} + \mathcal{G}$. So,

Compare this to the construction of the function $\cos(x) + \sin(x)$ in calculus.

$$\boxed{(\mathcal{F} + \mathcal{G})(X) := \mathcal{F}(X) + \mathcal{G}(X) .}$$

In other words, $\mathcal{F} + \mathcal{G}$ acts by applying $\mathcal{F}$ and $\mathcal{G}$ individually first (to the same given input), and then adding their outputs.

Example 7.3.2

If functions $\mathcal{F}$ and $\mathcal{G}$ are defined by

$$\mathcal{F}\begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 2x-y+3z \\ y+2z \\ 5x+6y+5z \\ 8x-ez \end{pmatrix}, \quad \text{and} \quad \mathcal{G}\begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 4y-z \\ x+5y \\ 0 \\ 4x+3y-\pi z \end{pmatrix},$$

then the function $\mathcal{F}+\mathcal{G}$ is given by the formula:

$$(\mathcal{F}+\mathcal{G})\begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 2x+3y+2z \\ x+6y+2z \\ 5x+6y+5z \\ 12x+3y-(e+\pi)z \end{pmatrix}.$$

Test Your Comprehension 7.3.3

Verify that for functions from $\mathbb{R}^m$ to $\mathbb{R}^n$ the operation of addition is commutative and associative. Furthermore, argue that the scaling of functions distributes over the addition of functions.

Recall that on $\mathbb{R}^k$ addition is commutative and associative, and that scaling distributes over addition.

Theorem 7.3.4

If $\mathcal{F}$ and $\mathcal{G}$ are $n \times m$ matrices, then so is $\mathcal{F}+\mathcal{G}$. To obtain the array of $\mathcal{F}+\mathcal{G}$, add the corresponding entries of the arrays of $\mathcal{F}$ and $\mathcal{G}$; i.e. add the two matrices "entry-by-entry". Equivalently: add the corresponding columns of $\mathcal{F}$ and $\mathcal{G}$.

In other words, if

$$\begin{cases} \mathcal{F} = \begin{bmatrix} V_1 & V_2 & V_3 & \dots & V_m \end{bmatrix} \\ \mathcal{G} = \begin{bmatrix} W_1 & W_2 & W_3 & \dots & W_m \end{bmatrix} \end{cases}$$

then

$$\mathcal{F}+\mathcal{G} = \begin{bmatrix} V_1+W_1 & V_2+W_2 & V_3+W_3 & \dots & V_m+W_m \end{bmatrix}.$$

Exercise 7.3.5

Give a proof of Theorem 7.3.4 by emulating either one of the proofs of Theorem 7.2.4.

Example 7.3.6

$$\begin{bmatrix} -6 & 12 & 15 \\ 6 & 0 & 3\pi \end{bmatrix} + \begin{bmatrix} 0 & 4 & 3 \\ e & -3 & 0 \end{bmatrix} = \begin{bmatrix} -6 & 16 & 18 \\ e+6 & -3 & 3\pi \end{bmatrix}.$$

On the other hand

$$\begin{bmatrix} -6 & 12 & 15 \\ 6 & 0 & 3\pi \end{bmatrix} + \begin{bmatrix} 0 & 4 \\ 3 & 3 \end{bmatrix} \text{ is undefined,}$$

because the matrices are not of the same size; the first is a function from $\mathbb{R}^3$ to $\mathbb{R}^2$, while the second is a function from $\mathbb{R}^2$ to $\mathbb{R}^2$.

Test Your Comprehension 7.3.7

Argue that the operations of addition and transposition for matrices "**commute**" in the following sense: for any $n \times m$ matrices $\mathcal{A}$ and $\mathcal{B}$:

$$(\mathcal{A} + \mathcal{B})^T = \mathcal{A}^T + \mathcal{B}^T .$$

In other words, one obtains the same result by adding first and then transposing, as by transposing first and then adding.

7.4 Linear Combination

Now that we have defined scaling and addition for matrices, we can also form linear combinations of matrices, and each such is again a matrix. Furthermore, the associativity of addition allows us to form linear combinations of more than two matrices at a time.

Compare this to the construction of the function $3\cos(x) + 5\sin(x) - \pi e^x$ in calculus.

Example 7.4.1

$$7 \cdot \begin{bmatrix} -6 & 12 & 15 \\ 6 & 0 & 3\pi \end{bmatrix} + 5 \cdot \begin{bmatrix} 0 & 4 & 3 \\ e & -3 & 0 \end{bmatrix} - \begin{bmatrix} 5 & -1 & \frac{3}{2} \\ 9 & 8 & 1 \end{bmatrix} = \begin{bmatrix} -47 & 105 & 118\frac{1}{2} \\ 33+5e & -23 & 21\pi-1 \end{bmatrix} .$$

Test Your Comprehension 7.4.2

Argue that the operations of linear combination and transposition for matrices "commute" in the following sense: for any $n \times m$ matrices $\mathcal{A}$ and $\mathcal{B}$, and scalars $a, b \in \mathbb{R}$:

$$(a \cdot \mathcal{A} + b \cdot \mathcal{B})^T = a \cdot \mathcal{A}^T + b \cdot \mathcal{B}^T .$$

In other words, one obtains the same result by forming a linear combination first and then transposing, as by transposing first and then forming the linear combination.

Exercise 7.4.3

Argue that the following are equivalent for matrix functions $\mathcal{F} : \mathbb{R}^m \longrightarrow \mathbb{R}^n$ and $\mathcal{G} : \mathbb{R}^m \longrightarrow \mathbb{R}^n$.

1. $\mathcal{F}(X) \bullet Y = \mathcal{G}(X) \bullet Y$ for all $X \in \mathbb{R}^m$, $Y \in \mathbb{R}^n$.
2. $\mathcal{F} = \mathcal{G}$.

Hint: Consider $\mathcal{F}(X) \bullet Y - \mathcal{G}(X) \bullet Y$. TYC 6.1.18 can be helpful here.

7.4.1 — : Linear Combinations Of Linear Functions On Vectors

As we have discussed in Section 6.3, each coordinate system on $\mathbb{E}^3$ induces a correspondence between linear functions on Υ^3 and 3×3 matrices. We can exploit this correspondence. For example, we have shown that a linear combination of $m \times n$ matrices is a matrix. Let us obtain a corresponding result for the geometric universe.

To initiate this procedure we need to introduce the operations of addition and scaling for the functions on Υ^3.

Terminology 7.4.4 ☞ **Scaling a function on Υ^3**

Given a function $f : \Upsilon^3 \longrightarrow \Upsilon^3$, and a scalar $\alpha \in \mathbb{R}$ we can form a new function $g : \Upsilon^3 \longrightarrow \Upsilon^3$ by declaring that

$$g(\vec{v}) := \alpha \cdot f(\vec{v}) ,$$

for all vectors $\vec{v}$. The function g is said to be **a scalar multiple of the function** f, and is denoted by $\alpha \cdot f$.

So

$$(\alpha \cdot f)(\vec{v}) := \alpha \cdot f(\vec{v}) .$$

In other words, $\alpha \cdot f$ acts by performing f first, followed by the scaling of the output by α.

Compare this to the construction presented in Terminology 7.2.1.

Test Your Comprehension 7.4.5

Argue that for any $f : \Upsilon^3 \longrightarrow \Upsilon^3$ and $\alpha, \beta \in \mathbb{R}$,

$$\alpha \cdot (\beta \cdot f) = (\alpha \cdot \beta) \cdot f = (\beta \cdot \alpha) \cdot f = \beta \cdot (\alpha \cdot f) .$$

Hint: Mimic the argument used for TYC 7.2.3.

Test Your Comprehension 7.4.6

Verify that for any $f : \Upsilon^3 \longrightarrow \Upsilon^3$,

$$1 \cdot f = f, \quad \text{and} \quad 0 \cdot f \text{ is the constantly } \vec{o} \text{ function.}$$

Terminology 7.4.7 ☞ **Addition of functions on Υ^3**

This time we start with two functions $f : \Upsilon^3 \longrightarrow \Upsilon^3$ and $g : \Upsilon^3 \longrightarrow \Upsilon^3$, and we form a new function $h : \Upsilon^3 \longrightarrow \Upsilon^3$ by declaring that

$$h(\vec{v}) := f(\vec{v}) + g(\vec{v}) \ ,$$

for all vectors $\vec{v}$.

This function h is said to be **the sum of functions** f **and** g, and is denoted by $f + g$. So,

$$\big(f + g\big)(\vec{v}) := f(\vec{v}) + g(\vec{v}) \ .$$

In other words, $f + g$ acts by applying f and g individually first (to the same given input vector), and then adding their outputs.

Compare this to the construction presented in Terminology 7.3.1 in the case of matrix functions.

Test Your Comprehension 7.4.8

For any $f : \Upsilon^3 \longrightarrow \Upsilon^3$,

$$\big(-1 \cdot f\big) + f \quad \text{is the constantly } \vec{o} \text{ function.}$$

Now we are ready for the promised theorem.

Theorem 7.4.9 ☞ **Linear combinations of linear functions on Υ^3**

A linear combination $\alpha \cdot f + \beta \cdot g$ of linear functions f, g on Υ^3 is again a linear function on Υ^3.

For any Cartesian coordinate system, the 3×3 matrix corresponding to the linear combination of f and g is the linear combination, with the same coefficients, of the matrices corresponding to f and g.

We shall offer two proofs of this theorem. The first involves a trip to the land of matrices and back, while the second amounts to verifying the combined linearity condition.

Proof of Theorem 7.4.9. Let us denote the matrices corresponding to f and g by $\mathcal{F}$ and $\mathcal{G}$ respectively. Then

$$\begin{aligned}
\Big(\alpha\cdot\mathcal{F}+\beta\cdot\mathcal{G}\Big)\left([\vec{v}]_C\right) &\overset{\text{Trm. 7.3.1}}{=} (\alpha\cdot\mathcal{F})\left([\vec{v}]_C\right)+(\beta\cdot\mathcal{G})\left([\vec{v}]_C\right)\\
&\overset{\text{Trm. 7.2.1}}{=} \alpha\cdot\Big(\mathcal{F}\big([\vec{v}]_C\big)\Big)+\beta\cdot\Big(\mathcal{G}\big([\vec{v}]_C\big)\Big)\\
&\overset{\text{Com. 6.3.8}}{=} \alpha\cdot\big[f(\vec{v})\big]_C+\beta\cdot\big[g(\vec{v})\big]_C\\
&\overset{\text{Fact 4.2.1}}{=} \big[\alpha\cdot f(\vec{v})+\beta\cdot g(\vec{v})\big]_C\\
&\overset{\text{Trms. 7.4.4 \& 7.4.7}}{=} \Big[\big(\alpha\cdot f+\beta\cdot g\big)(\vec{v})\Big]_C .
\end{aligned}$$

This shows that $\alpha\cdot f+\beta\cdot g$ corresponds to $\alpha\cdot\mathcal{F}+\beta\cdot\mathcal{G}$ (Com. 6.3.8), and since the latter is a matrix, $\alpha\cdot f+\beta\cdot g$ must be a linear function, per Theorem 6.3.2. ∎

Proof of Theorem 7.4.9. Let us do the calculations to verify that $\alpha\cdot f+\beta\cdot g$ satisfies the combined linearity condition. Of course, by the hypotheses, f and g do.

$$\begin{aligned}
\Big(\alpha\cdot f+\beta\cdot g\Big)(\gamma\cdot\vec{u}+\vec{w}) &= \Big(\alpha\cdot f\Big)(\gamma\cdot\vec{u}+\vec{w})+\Big(\beta\cdot g\Big)(\gamma\cdot\vec{u}+\vec{w})\\
&= \alpha\cdot\Big(f\big(\gamma\cdot\vec{u}+\vec{w}\big)\Big)+\beta\cdot\Big(g\big(\gamma\cdot\vec{u}+\vec{w}\big)\Big)\\
&= \alpha\cdot\Big(\gamma\cdot f(\vec{u})+f(\vec{w})\Big)+\beta\cdot\Big(\gamma\cdot g(\vec{u})+g(\vec{w})\Big)\\
&= \gamma\cdot\Big(\alpha\cdot f(\vec{u})+\beta\cdot g(\vec{u})\Big)+\Big(\alpha\cdot f(\vec{w})+\beta\cdot g(\vec{w})\Big)\\
&= \gamma\cdot\ \big(\alpha\cdot f+\beta\cdot g\big)(\vec{u})+\Big(\alpha\cdot f+\beta\cdot g\Big)(\vec{w}) .
\end{aligned}$$ ∎

8. Matrix Composition

Last modified on December 8, 2018

8.1 Composing Matrices

Terminology 8.1.1

In Chapter 2 we discussed the operation of composition for functions. *This operation is associative but is NOT generally commutative.*

Let us recall that if we start with two functions $\mathcal{F} : \mathbb{R}^m \longrightarrow \mathbb{R}^{n}$ and $\mathcal{G} : \mathbb{R}^{n} \longrightarrow \mathbb{R}^p$, we can form a new function $\mathcal{H} : \mathbb{R}^m \longrightarrow \mathbb{R}^p$ by declaring that

It is crucial here that the final space of $\mathcal{F}$ matches the initial space of $\mathcal{G}$.

$$\mathcal{H}(X) := \mathcal{G}\big(\mathcal{F}(X)\big) ,$$

for all $X \in \mathbb{R}^m$.

This function $\mathcal{H}$ is said to be **the composition of functions $\mathcal{F}$ and $\mathcal{G}$**, and is denoted by $\mathcal{G} \circ \mathcal{F}$. So,

$$(\mathcal{G} \circ \mathcal{F})(X) := \mathcal{G}\big(\mathcal{F}(X)\big) .$$

$\mathcal{G} \circ \mathcal{F}$ acts by applying $\mathcal{F}$ first (it is closer to the input X, since we list the inputs to the right of the function!), and then applies $\mathcal{G}$ to the output of $\mathcal{F}$. In other words $\mathcal{G} \circ \mathcal{F}$ applies $\mathcal{F}$ and $\mathcal{G}$ in sequence, with $\mathcal{F}$ going first.

Compare this to the construction of the function $\log(\cos(x))$ in calculus.

Observation 8.1.2

Recall that for any $\mathcal{F} : \mathbb{R}^{m} \longrightarrow \mathbb{R}^{n}$ we have

$$\mathcal{I}_{n} \circ \mathcal{F} \;=\; id_{R^{n}} \circ \mathcal{F} \;=\; \mathcal{F} \;=\; \mathcal{F} \circ id_{R^{m}} \;=\; \mathcal{F} \circ \mathcal{I}_{m} ,$$

so that a composition with the identity function, when it makes sense, returns the original function as a result. In that sense the identity functions act as a **neutral element** for the operation of composition.

Example 8.1.3

If functions $\mathcal{K}$ and $\mathcal{L}$ are defined by:

$$\mathcal{K}\begin{pmatrix} x\\ y\\ z\end{pmatrix} = \begin{pmatrix} 2x-y+3z\\ y+2z\\ 5x+6y+5z\\ 8x-ez\end{pmatrix}, \quad \text{and} \quad \mathcal{L}\begin{pmatrix} p\\ q\\ r\\ s\end{pmatrix} = \begin{pmatrix} 4q-2r+s\\ p+5q+7r+2s\end{pmatrix},$$

then $\mathcal{K}\circ\mathcal{L}$ is meaningless (do you see why?), while the function $\mathcal{L}\circ\mathcal{K}$ is given by:

$$\begin{aligned}(\mathcal{L}\circ\mathcal{K})\begin{pmatrix} a\\ b\\ c\end{pmatrix} &= \mathcal{L}\left(\mathcal{K}\begin{pmatrix} a\\ b\\ c\end{pmatrix}\right)\\ &= \mathcal{L}\begin{pmatrix} 2a-b+3c\\ b+2c\\ 5a+6b+5c\\ 8a-ec\end{pmatrix}\\ &= \begin{pmatrix} 4(b+2c)-2(5a+6b+5c)+(8a-ec)\\ (2a-b+3c)+5(b+2c)+7(5a+6b+5c)+2(8a-ec)\end{pmatrix}\\ &= \begin{pmatrix} -2a-8b-(2+e)c\\ 53a+46b+(48-2e)c\end{pmatrix}.\end{aligned}$$

Please keep in mind that the variable names used in a definition of a function are internal to that definition, and can be changed without altering the function.

Test Your Comprehension 8.1.4

Argue that composing a matrix with a null matrix of appropriate size produces a null matrix.

Hint: Keep in mind that matrices are linear functions and thus map a null tuple to a null tuple.

Test Your Comprehension 8.1.5

1. Fill in the missing details to make a valid statement.

   For matrices $\mathcal{A}\in\mathbb{M}_{m\times n}$ and $\mathcal{B}\in\mathbb{M}_{p\times q}$ we can form *both* compositions $\mathcal{A}\circ\mathcal{B}$ and $\mathcal{B}\circ\mathcal{A}$ exactly when ....and in such a case $\mathcal{A}\circ\mathcal{B}\in\mathbb{M}_{\dots}$ and $\mathcal{B}\circ\mathcal{A}\in\mathbb{M}_{\dots}$

2. Argue that the following are equivalent for a matrix $\mathcal{A}$.
   (a) $\mathcal{A}\circ\mathcal{A}$ makes sense;
   (b) $\mathcal{A}$ is a square matrix.

3. Argue that for any matrix $\mathcal{A}$, we can always form compositions

$$\mathcal{A}^T\circ\mathcal{A} \quad\text{and}\quad \mathcal{A}\circ\mathcal{A}^T.$$

Exercise 8.1.6 ☞ **Composition with a linear combination is a linear combination of compositions**

Argue that **composition of matrices distributes over linear combinations** (from either side).

Namely, for any $a, b \in \mathbb{R}$,

$$\mathcal{C} \circ \Big(a \cdot \mathcal{A} + b \cdot \mathcal{B} \Big) = a \cdot \big(\mathcal{C} \circ \mathcal{A} \big) + b \cdot \big(\mathcal{C} \circ \mathcal{B} \big)$$

and

$$\Big(a \cdot \mathcal{A} + b \cdot \mathcal{B} \Big) \circ \mathcal{C} = a \cdot \big(\mathcal{A} \circ \mathcal{C} \big) + b \cdot \big(\mathcal{B} \circ \mathcal{C} \big) \ ,$$

whenever these operations make sense for the matrices $\mathcal{A}, \mathcal{B}, \mathcal{C}$.

By taking $a = b = 1$, observe that composition of matrices distributes over addition (from either side).

By taking $\mathcal{B} = \mathcal{O}$ and exchanging the roles of $\mathcal{A}$ and $\mathcal{C}$ as needed, argue that

$$\mathcal{C} \circ \big(a \cdot \mathcal{A} \big) = a \cdot \big(\mathcal{C} \circ \mathcal{A} \big) = \big(a \cdot \mathcal{C} \big) \circ \mathcal{A} \ .$$

In other words, we can bring a scalar into a composition of matrices and attach it to any one of the matrices involved. Alternatively, we can pull scalar multiples out of matrix composition.

Since composition is NOT a commutative operation in general, one has to address its distributive properties from both the left side and the right side.

Hint: Keeping in mind that matrices are linear functions, and hence have the properties listed in Exercise 6.2.5.

Composing matrices, when this makes sense, produces a matrix. The columns of the resulting matrix are easy to describe.

Theorem 8.1.7 ☞ **To compose two matrices, apply the left one to the columns of the right one**

If $\mathcal{A} : \mathbb{R}^m \longrightarrow \mathbb{R}^n$ and $\mathcal{B} : \mathbb{R}^n \longrightarrow \mathbb{R}^p$ are matrices, then so is $\mathcal{B} \circ \mathcal{A}$. To obtain the columns of $\mathcal{B} \circ \mathcal{A}$, apply $\mathcal{B}$ to the columns of $\mathcal{A}$.

In other words, if

$$\mathcal{A} = \begin{bmatrix} V_1 & V_2 & V_3 & \dots & V_m \end{bmatrix}_{n \times m}$$

then

$$\mathcal{B} \circ \mathcal{A} = \begin{bmatrix} \mathcal{B}(V_1) & \mathcal{B}(V_2) & \mathcal{B}(V_3) & \dots & \mathcal{B}(V_m) \end{bmatrix}_{p \times m} \ .$$

For a composition $\mathcal{B} \circ \mathcal{A}$ of matrices to make sense, $\mathcal{B}$ must have as many columns as $\mathcal{A}$ has rows.
Here is a quick way to remember how the sizing of matrices works with composition:

$$\boxed{k \times r} \circ \boxed{r \times s} = \boxed{k \times s}$$

Compare this to the familiar formula: $\frac{k}{r} \cdot \frac{r}{s} = \frac{k}{s}$.

Proof of Theorem 8.1.7. Given $\mathcal{A}$ and $\mathcal{B}$ as described, and $X = \left(x_1, x_2, x_3, \ldots, x_m\right)$, we have

$$(\mathcal{B} \circ \mathcal{A})(X) = \mathcal{B}(\mathcal{A}(X)) = \mathcal{B}(x_1 \cdot V_1 + x_2 \cdot V_2 + x_3 \cdot V_3 + \ldots + x_m \cdot V_m)$$

$$= x_1 \cdot \mathcal{B}(V_1) + x_2 \cdot \mathcal{B}(V_2) + x_3 \cdot \mathcal{B}(V_3) + + \ldots + x_m \cdot \mathcal{B}(V_m)\ ,$$

For the last equality we used the fact that matrix functions are linear; see Exc. 6.2.5.

which gives the required result. ∎

As we have discussed in Section 6.3, each coordinate system on $\mathbb{E}^3$ induces a correspondence between linear functions on Υ^3 and 3×3 matrices. We can exploit this correspondence to transport a newly derived fact that a composition of matrices (when defined) is a matrix, to obtain a corresponding result in the geometric universe.

Theorem 8.1.8: Compositions of linear functions on Υ^3

A composition $f \circ g$ of two linear functions on Υ^3 is again a linear function on Υ^3.

For any Cartesian coordinate system, the 3×3 matrix corresponding to $f \circ g$ is the composition (in the same order) of the matrices corresponding to f and g.

Proof of Theorem 8.1.8. Let us denote matrices corresponding to f and g by $\mathcal{F}$ and $\mathcal{G}$ respectively. Then

$$\mathcal{F} \circ \mathcal{G} \overset{\text{Exc. 6.3.1}}{=} \varphi_C \circ f \circ \varphi_C^{-1} \circ \varphi_C \circ g \circ \varphi_C^{-1} = \cdots = \varphi_C \circ (f \circ g) \circ \varphi_C^{-1}\ .$$

This shows that $f \circ g$ corresponds to $\mathcal{F} \circ \mathcal{G}$, and since the latter is a matrix (Thm. 8.1.7), $f \circ g$ must be a linear function, per Theorem 6.3.2. ∎

Theorem 8.1.9

If a linear function f on Υ^3 does not alter lengths of vectors, then f can be expressed as a composition of two rotations, perhaps followed by a reflection in a plane.

Proof of Theorem 8.1.9. Will be presented in class. ■

Comment 8.1.10

Analogous constructions can be carried out with coordinate systems for a given plane P, and functions $f : \Upsilon^2_P \longrightarrow \Upsilon^2_P$. Here the correspondences will be between the linear functions and the 2×2 matrices.

Theorem 8.1.11 **Entry-by-entry calculation of matrix products**

If $\mathcal{B} : \mathbb{R}^m \longrightarrow \mathbb{R}^n$ and $\mathcal{A} : \mathbb{R}^n \longrightarrow \mathbb{R}^p$ are matrices, then

$$(\mathcal{A} \circ \mathcal{B})[\![i, j]\!] = R_i \bullet C_j$$

where R_i is the i-th row of $\mathcal{A}$ and C_j is the j-th row of $\mathcal{B}$.

In other words,

$$\begin{bmatrix} \longleftarrow & R_1 & \longrightarrow \\ \longleftarrow & R_2 & \longrightarrow \\ \longleftarrow & R_3 & \longrightarrow \\ & \vdots & \\ \longleftarrow & R_p & \longrightarrow \end{bmatrix}_{p\times n} \circ \begin{bmatrix} C_1 & C_2 & C_3 & \ldots & C_m \end{bmatrix}_{n\times m} = \begin{bmatrix} R_1\bullet C_1 & R_1\bullet C_2 & \ldots & R_1\bullet C_m \\ R_2\bullet C_1 & R_2\bullet C_2 & \ldots & R_2\bullet C_m \\ \vdots & \vdots & \ddots & \vdots \\ R_p\bullet C_1 & R_p\bullet C_2 & \ldots & R_p\bullet C_m \end{bmatrix}_{p\times m} .$$

Proof of Theorem 8.1.11. Simply note that by Theorem 8.1.7,

$$\mathcal{A} \circ \mathcal{B} = \begin{bmatrix} \mathcal{A}(C_1) & \mathcal{A}(C_2) & \mathcal{A}(C_3) & \ldots & \mathcal{A}(C_m) \end{bmatrix}_{p\times m} ,$$

and for each i the row-centric way (6.5) of evaluating $\mathcal{B}(C_i)$ gives

$$\mathcal{A}(C_i) = \begin{bmatrix} \longleftarrow & R_1 & \longrightarrow \\ \longleftarrow & R_2 & \longrightarrow \\ \longleftarrow & R_3 & \longrightarrow \\ & \vdots & \\ \longleftarrow & R_p & \longrightarrow \end{bmatrix} (C_i) = \begin{pmatrix} R_1\bullet C_i \\ R_2\bullet C_i \\ R_3\bullet C_i \\ \vdots \\ R_p\bullet C_i \end{pmatrix} .$$

■

Example 8.1.12

$$\begin{bmatrix} e & 4 \\ 3 & 3 \\ 0 & 0 \\ e & 4 \end{bmatrix} \circ \begin{bmatrix} -6 & 12 & 15 \\ 6 & 0 & 3\pi \end{bmatrix} = \begin{bmatrix} 24-6e & 12e & 15e+12\pi \\ 0 & 36 & 45+9\pi \\ 0 & 0 & 0 \\ 24-6e & 12e & 15e+12\pi \end{bmatrix},$$

whereas

$$\begin{bmatrix} -6 & 12 & 15 \\ 6 & 0 & 3\pi \end{bmatrix} \circ \begin{bmatrix} e & 4 \\ 3 & 3 \\ 0 & 0 \\ e & 4 \end{bmatrix} \quad \text{is undefined.}$$

Exercise 8.1.13

Argue that the last formula in Theorem 8.1.11 can be expressed as follows:

$$(\mathcal{B} \circ \mathcal{A})[\![i, j]\!] = \sum_{k=1}^{n} \mathcal{B}[\![i, k]\!] \cdot \mathcal{A}[\![k, j]\!] \,. \tag{8.1}$$

INSERT PICTURE

Note that this concise formula only involves just the entries of the two matrices (as opposed to the whole rows or columns).

Comment 8.1.14 ☞ **Matrix composition is NOT commutative**

Even when $\mathcal{A}$ and $\mathcal{B}$ are matrices such that $\mathcal{A} \circ \mathcal{B}$ and $\mathcal{B} \circ \mathcal{A}$ make sense, $\mathcal{A} \circ \mathcal{B}$ and $\mathcal{B} \circ \mathcal{A}$ may not be equal. This is not surprising since we already know that composition of function is generally not a commutative operation (i.e. order matters!).

For example, the reader should check that $\mathcal{A} \circ \mathcal{B} \neq \mathcal{B} \circ \mathcal{A}$ when $\mathcal{A} = \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}$ and $\mathcal{B} = \begin{bmatrix} -2 & 1 \\ 5 & -3 \end{bmatrix}$.

If it so happens that $\mathcal{A} \circ \mathcal{B} = \mathcal{B} \circ \mathcal{A}$, we say that matrices $\mathcal{A}$ and $\mathcal{B}$ **commute (with each other)**.

Exercise 8.1.15

Find, if such exist, 2×2 matrices $\mathcal{A}$ and $\mathcal{B}$ having only entries 0 or 1, such that

$$\mathcal{O}_{2\times 2} = A \circ B \neq B \circ A \,.$$

If such matrices do not exist, provide a rigorous argument supporting that claim.

Terminology 8.1.16

It is common to refer to matrix composition as **matrix multiplication** or **matrix product**.

Such terminology creates an association with the familiar operations on real numbers, reminding us that many of the same general features are present in the matrix setting. Many, but not all: matrix multiplication is NOT commutative!

Still, there is much benefit in associating a null matrix with zero, and an identity matrix with 1, as these are the neutral elements for the operations of addition and multiplication. Matrix inverses are akin to the reciprocals of numbers, but here again there will be a major difference: NOT ALL non-null matrices are invertible.

Notation 8.1.17

From now on, when there is no ambiguity, we shall commonly omit the symbol "$\circ$" and write $\mathcal{AB}$ instead of $\mathcal{A} \circ \mathcal{B}$, when $\mathcal{A}$ and $\mathcal{B}$ are matrices of appropriate size.

In a similar fashion, we shall drop off the symbol "$\cdot$" and write $\alpha\square$ in place of $\alpha \cdot \square$, when $\square$ is a matrix or a tuple, and $\alpha \in \mathbb{R}$.

Example 8.1.18

The reader should rely on context for a correct interpretation of the notation.

For example, $\left[\begin{smallmatrix} 1 & 2 \\ 3 & 4 \end{smallmatrix}\right]\left(7\left(\begin{smallmatrix} 5 \\ 6 \end{smallmatrix}\right)\right)$ is a tuple $\left(\begin{smallmatrix} 119 \\ 273 \end{smallmatrix}\right)$, whereas $\left[\begin{smallmatrix} 1 & 2 \\ 3 & 4 \end{smallmatrix}\right]\left(7\left[\begin{smallmatrix} 5 \\ 6 \end{smallmatrix}\right]\right)$ is a matrix $\left[\begin{smallmatrix} 119 \\ 273 \end{smallmatrix}\right]$. The first case involves applying a matrix to an input. The second – matrix multiplication.

In a similar vein, notation $\left(\begin{smallmatrix} 5 & 6 \end{smallmatrix}\right)\left(7\left[\begin{smallmatrix} 1 & 2 \\ 3 & 4 \end{smallmatrix}\right]\right)$ has not been assigned meaning, whereas $\left[\begin{smallmatrix} 5 & 6 \end{smallmatrix}\right]\left(7\left[\begin{smallmatrix} 1 & 2 \\ 3 & 4 \end{smallmatrix}\right]\right)$ gives the matrix $\left[\begin{smallmatrix} 161 & 238 \end{smallmatrix}\right]$.

8.1.1 — Matrix Powers

Notation 8.1.19 ☞ **Powers of a matrix**

When $\mathcal{A}$ is a square matrix in $\mathbb{M}_n$, then $\mathcal{A} \circ \mathcal{A}$, $\mathcal{A} \circ \mathcal{A} \circ \mathcal{A}$, $\mathcal{A} \circ \mathcal{A} \circ \mathcal{A} \circ \mathcal{A}$, etc. make sense and are matrices of the same size as $\mathcal{A}$. We shall denote these matrices by the symbols $\mathcal{A}^2$, $\mathcal{A}^3$, $\mathcal{A}^4$, etc., respectively, and refer to them as **the powers of** $\mathcal{A}$.

Let us also agree that $\mathcal{A}^1 = \mathcal{A}$ and $\mathcal{A}^0 = \mathcal{I}_n$.

It is now easy to see that

$$\boxed{\mathcal{A}^p \circ \mathcal{A}^q = \mathcal{A}^{p+q}\ .}$$

for all non-negative integers p, q.

Exercise 8.1.20

Consider a small web site that consists of 374 web pages, and sits off-line. So none of the pages link to or are linked to from anywhere beyond the web site. Still, any given page may link to or be linked to from another page or even itself. Let us denote the pages by $P_1, P_2, P_3, \ldots, P_{374}$.

Consider a matrix, which we will call $\mathcal{A}$, that has non-negative integer entries, and is defined as follows: $\mathcal{A}[\![i, j]\!]$ is the number of different links on page P_j that directly point to (i.e. take one to, when clicked) page P_i.

In other words, the j_o-th column of $\mathcal{A}$ can be considered to give an "out-linking" profile of P_{j_o} in the following sense: the i-th entry in that column tells us how many links on P_{j_o} will take us directly to page P_i.

1. What is a corresponding statement about the rows of $\mathcal{A}$?
2. Argue that the $[\![i, j]\!]$-th entry of $\mathcal{A} \circ \mathcal{A}$ is the number of different ways that one can get from page P_j to page P_i in exactly two steps, i.e. by hitting a link and then hitting some link again.
3. What do columns and rows of $\mathcal{A} \circ \mathcal{A}$ describe?
4. Argue that the $[\![i, j]\!]$-th entry of $\mathcal{A} \circ \mathcal{A} \circ \mathcal{A}$ is the number of different ways that one can get from page P_j to page P_i in exactly three steps.

We hope that at this point it is fairly clear to the reader that the $[\![i, j]\!]$-th entry of $\mathcal{A}^k$ is the number of different ways that one can get from page P_j to page P_i in exactly k steps. Of course a precise argument would be required to justify this claim fully.

Comment 8.1.21

It is natural to wonder which matrices have square roots. In other words, for which matrix $\mathcal{T}$ is there a matrix $\mathcal{A}$ such that $\mathcal{A}^2 = \mathcal{T}$? Similar questions can be asked about cube roots, etc.

For example, the reader can check that $\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$ has no matrix square roots at all, even though all of its entries are non-negative.

Characterizing matrices that have roots is not an easy task.

Terminology 8.1.22

When a square matrix $\mathcal{A}$ raised to some power produces a null matrix, we say that $\mathcal{A}$ is **nilpotent**.

A square matrix $\mathcal{A}$ is **idempotent** if it squares to itself: $\mathcal{A}^2 = \mathcal{A}$.

A square matrix $\mathcal{A}$ that squares to the identity matrix, i.e. such that $\mathcal{A}^2 = \mathcal{I}$, is said to be an **involution** matrix. These are exactly the matrices that are their own inverses.

Example 8.1.23

$\mathcal{O}_7$, $\begin{bmatrix} 1 & 2 \\ -2 & 1 \end{bmatrix}$ and $\begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{bmatrix}$ are examples of nilpotent matrices.

$\mathcal{O}_7$, $\mathcal{I}_4$, $\begin{bmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{bmatrix}$ and $\begin{bmatrix} 0 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 0 \end{bmatrix}$ are examples of idempotent matrices.

$\mathcal{I}_4$, $\begin{bmatrix} 0 & -1 \\ -1 & 0 \end{bmatrix}$, $\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$ and $\begin{bmatrix} 0 & -1 & 1 \\ -3 & 2 & -3 \\ -2 & 2 & -3 \end{bmatrix}$ are examples of involution matrices.

On the surface, matrix addition and multiplication follows some of the familiar principles of arithmetic in $\mathbb{R}$. Yet, as the examples above demonstrate, in the land of matrices we can encounter phenomena that are unlike any we have seen in $\mathbb{R}$. For example, a matrix with no zero entries can square to a null matrix. $\begin{bmatrix} 1 & 1 \\ -1 & -1 \end{bmatrix}$ is one such. A matrix with no zeros or ones as entries can square to itself (see Ex. 8.1.23). A matrix that is neither $\mathcal{I}$ nor is $-\mathcal{I}$ can square to $\mathcal{I}$.

It is this interplay between the familiar principles and wider possibilities that makes the theory of matrices so effective. A reader familiar with Complex numbers will appreciate a parallel. Complex numbers lack some of the properties that the Real numbers enjoy, but offer an enrichment of options via the existence of numbers with properties not present in $\mathbb{R}$. Of course, in a similar way, the Real numbers are an enrichment of the system of Rational numbers.

8.1.2 — Composition And Transposition

Test Your Comprehension 8.1.24 ☞ **The entries of $\mathcal{A}^T\mathcal{A}$ are the pairwise dot products of the columns of $\mathcal{A}$, and the entries of $\mathcal{A}\mathcal{A}^T$ are the pairwise dot products of the rows of $\mathcal{A}$.**

Verify that if $\mathcal{A} \in \mathbb{M}_{n\times m}$ then

$$\left(\mathcal{A}^T\mathcal{A}\right)[\![i,j]\!] = C_i \bullet C_j, \quad \text{and} \quad \left(\mathcal{A}\mathcal{A}^T\right)[\![i,j]\!] = R_i \bullet R_j\ ,$$

where $C_1, C_2, C_3 \ldots, C_m$ are the columns of $\mathcal{A}$, and $R_1, R_2, R_3, \ldots, R_n$ are the rows of $\mathcal{A}$.

Theorem 8.1.25 ☞ **Transpose of a product is the product of transposes in reversed order**

If $\mathcal{A}$ and $\mathcal{B}$ are matrices such that $\mathcal{AB}$ makes sense, then $\mathcal{B}^T\mathcal{A}^T$ also makes sense, and

$$(\mathcal{AB})^T = \mathcal{B}^T\mathcal{A}^T \ .$$

Proof of Theorem 8.1.25. For $\mathcal{A} \circ \mathcal{B}$ to make sense, $\mathcal{A}$ must have dimensions $n \times m$, and $\mathcal{B}$ – dimensions $m \times k$, for some n, m, k. In this case $\mathcal{B}^T \circ \mathcal{A}^T$ makes sense and has the same dimensions as $(\mathcal{A} \circ \mathcal{B})^T$:

Matrix	$\mathcal{A}$	$\mathcal{B}$	$\mathcal{B}^T$	$\mathcal{A}^T$	$\mathcal{A} \circ \mathcal{B}$	$(\mathcal{A} \circ \mathcal{B})^T$	$\mathcal{B}^T \circ \mathcal{A}^T$
Size	$n \times m$	$m \times k$	$k \times m$	$m \times n$	$n \times k$	$k \times n$	$k \times n$

Let us write

$$\mathcal{A} = \begin{bmatrix} \longleftarrow & R_1 & \longrightarrow \\ \longleftarrow & R_2 & \longrightarrow \\ \longleftarrow & R_3 & \longrightarrow \\ & \vdots & \\ \longleftarrow & R_n & \longrightarrow \end{bmatrix} \text{ and } \mathcal{B} = \begin{bmatrix} C_1 & C_2 & C_3 & \dots & C_k \end{bmatrix},$$

where R_i's and C_i's are m-tuples.

Then (for any appropriate i, j)

$$(\mathcal{A} \circ \mathcal{B})^T [\![i, j]\!] \overset{\text{TYC 7.1.6}}{=} (\mathcal{A} \circ \mathcal{B})[\![j, i]\!] \overset{\text{Thm. 8.1.11}}{=} R_j \bullet C_i \ .$$

Transposing $\mathcal{A}$ and $\mathcal{B}$ we arrive at

$$\mathcal{B}^T = \begin{bmatrix} \longleftarrow & C_1 & \longrightarrow \\ \longleftarrow & C_2 & \longrightarrow \\ \longleftarrow & C_3 & \longrightarrow \\ & \vdots & \\ \longleftarrow & C_k & \longrightarrow \end{bmatrix} \text{ and } \mathcal{A} = \begin{bmatrix} R_1 & R_2 & R_3 & \dots & R_n \end{bmatrix}.$$

Therefore

$$\left(\mathcal{B}^T \circ \mathcal{A}^T\right) [\![i, j]\!] \overset{\text{Thm. 8.1.11}}{=} C_i \bullet R_j = R_j \bullet C_i = (\mathcal{A} \circ \mathcal{B})^T [\![i, j]\!].$$

This shows that $\mathcal{B}^T \circ \mathcal{A}^T$ and $(\mathcal{A} \circ \mathcal{B})^T$ have identical entries, and hence are equal. ■

Theorem 8.1.26 ☞ **Transposition commutes with inversion**

The following statement are equivalent for a matrix $\mathcal{A}$.

1. $\mathcal{A}$ is invertible.
2. $\mathcal{A}^{T}$ is invertible.

When these hold true,

$$\left(\mathcal{A}^{T}\right)^{-1} = \left(\mathcal{A}^{-1}\right)^{T} . \tag{8.2}$$

Proof of Theorem 8.1.26.

[1. $\Longrightarrow$ 2.]: Suppose that $\mathcal{A}$ is invertible and *let $\mathcal{B}$ be the inverse of $\mathcal{A}$*. Then

$$\mathcal{A} \circ \mathcal{B} = \mathcal{I} = \mathcal{B} \circ \mathcal{A} .$$

Apply the transposition to arrive at

$$(\mathcal{A} \circ \mathcal{B})^{T} = \mathcal{I}^{T} = (\mathcal{B} \circ \mathcal{A})^{T} .$$

In other words, by Theorem 8.1.25,

$$\mathcal{B}^{T} \circ \mathcal{A}^{T} = \mathcal{I} = \mathcal{A}^{T} \circ \mathcal{B}^{T} .$$

This shows that $\mathcal{A}^{T}$ is invertible, and

$$\left(\mathcal{A}^{T}\right)^{-1} = \mathcal{B}^{T} = \left(\mathcal{A}^{-1}\right)^{T} .$$

[2. $\Longrightarrow$ 1.]: Suppose that $\mathcal{A}^{T}$ is invertible. Let us write $\mathfrak{A}$ for $\mathcal{A}^{T}$. Applying the (already established implication) [1. $\Longrightarrow$ 2.] to $\mathfrak{A}$, we can conclude that $\mathfrak{A}^{T}$ is invertible and

$$\left(\mathfrak{A}^{T}\right)^{-1} = \left(\mathfrak{A}^{-1}\right)^{T} .$$

Since

$$\mathfrak{A}^{T} = \left(\mathcal{A}^{T}\right)^{T} = \mathcal{A},$$

we see that $\mathcal{A}$ is invertible, and then the required formula (8.2) follows by the (already established implication) [1. $\Longrightarrow$ 2.] applied to $\mathcal{A}$.

Another proof of [2. $\Longrightarrow$ 1.]: Suppose that $\mathcal{A}^{T}$ is invertible and *let $\mathcal{C}$ be the inverse of $\mathcal{A}^{T}$*. Then

$$\mathcal{A}^{T} \circ \mathcal{C} = \mathcal{I} = \mathcal{C} \circ \mathcal{A}^{T} .$$

Apply transposition to arrive at

$$\left(\mathcal{A}^T \circ \mathcal{C}\right)^T = \mathcal{I}^T = \left(\mathcal{C} \circ \mathcal{A}^T\right)^T .$$

In other words, by Theorem 8.1.25,

$$\mathcal{C}^T \circ \mathcal{A} = \mathcal{I} = \mathcal{A} \circ \mathcal{C}^T .$$

This shows that $\mathcal{A}$ is invertible, and

$$\mathcal{A}^{-1} = \mathcal{C}^T = \left(\left(\mathcal{A}^T\right)^{-1}\right)^T .$$

Apply transposition to arrive at

$$\left(\mathcal{A}^{-1}\right)^T = \left(\mathcal{A}^T\right)^{-1} .$$ ■

8.1.3 — Compositions Involving Triangular Matrices

Exercise 8.1.27 ☞ **Compositions $\mathcal{A} \circ \mathcal{D}$ and $\mathcal{D} \circ \mathcal{A}$, where $\mathcal{D}$ is a diagonal matrix**

Verify that the effect of forming a composition $\mathcal{A} \circ \mathcal{D}$, where $\mathcal{D}$ is a diagonal matrix, is that of scaling the columns of $\mathcal{A}$:

$$\begin{bmatrix} C_1 & C_2 & C_3 & \dots & C_m \end{bmatrix}_{n\times m} \circ \begin{bmatrix} \lambda_1 & 0 & 0 & \dots & 0 \\ 0 & \lambda_2 & 0 & \dots & 0 \\ 0 & 0 & \lambda_3 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & \lambda_m \end{bmatrix}_{m\times m}$$

$$= \begin{bmatrix} \lambda_1 \cdot C_1 & \lambda_2 \cdot C_2 & \lambda_3 \cdot C_3 & \dots & \lambda_m \cdot C_m \end{bmatrix}_{n\times m} .$$

Argue that the effect of forming a composition $\mathcal{D} \circ \mathcal{A}$ is that of scaling the rows of $\mathcal{A}$:

$$\begin{bmatrix} \alpha_1 & 0 & 0 & \dots & 0 \\ 0 & \alpha_2 & 0 & \dots & 0 \\ 0 & 0 & \alpha_3 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & \alpha_n \end{bmatrix}_{n\times n} \circ \begin{bmatrix} \longleftarrow & R_1 & \longrightarrow \\ \longleftarrow & R_2 & \longrightarrow \\ \longleftarrow & R_3 & \longrightarrow \\ & \vdots & \\ \longleftarrow & R_n & \longrightarrow \end{bmatrix}_{n\times m} = \begin{bmatrix} \longleftarrow & \alpha_1 \cdot R_1 & \longrightarrow \\ \longleftarrow & \alpha_2 \cdot R_2 & \longrightarrow \\ \longleftarrow & \alpha_3 \cdot R_3 & \longrightarrow \\ & \vdots & \\ \longleftarrow & \alpha_n \cdot R_n & \longrightarrow \end{bmatrix}_{n\times m} .$$

Hint: To deal with the second claim apply transposition to the first claim.

Test Your Comprehension 8.1.28 ☞ **Diagonal ∘ diagonal = diagonal**

Argue that a composition of two $n \times n$ diagonal matrices is a diagonal matrix, and that it can be obtained by multiplying together the corresponding diagonal entries of the two matrices.

Consequently argue that any two $n \times n$ diagonal matrices commute with each other.

A corresponding result holds for a composition of any number of $n \times n$ diagonal matrices.

Theorem 8.1.29 ☞ **Lower-△ ∘ lower-△ = lower-△**

A composition of two $n \times n$ lower-triangular matrices is a lower-triangular matrix.

In fact, a composition of any number of lower-triangular matrices is a lower-triangular matrix.

Proof of Theorem 8.1.29. A matrix is lower-triangular exactly when its second column starts with a zero, its third column starts with two zeros, its fourth columns starts with three zeros, etc.

Say $\mathcal{A}$ and $\mathcal{B}$ are two $n \times n$ lower-triangular matrices. Let us argue that the fourth column of $\mathcal{A} \circ \mathcal{B}$ starts with three zeros (assuming $n \geq 4$). A general argument will follow the same steps, but will use a general notation.

The fourth column C of $\mathcal{A} \circ \mathcal{B}$ is the result of applying $\mathcal{A}$ to the fourth column of $\mathcal{B}$ (as in Theorem 8.1.7). Therefore C is a linear combination of the columns of $\mathcal{A}$ with the coefficients given by the entries of the fourth column of $\mathcal{B}$. Since the latter starts with three zeros, C is a linear combination of the 4-th and consequent columns of $\mathcal{A}$, all of which start with three zeros. Hence C starts with three zeros.

To deal with a composition of more than two $n \times n$ lower-triangular matrices, we appeal to the associativity of composition, and carry out the composition two matrices at a time. At each step the two matrices that are being multiplied yield (and are replaced by) a single lower-triangular matrix, and so the process continues, but with fewer matrices remaining at each step. The process will terminate exactly when we are left with a single (lower-triangular) matrix. ■

Test Your Comprehension 8.1.30 ☞ **Upper-△ ∘ upper-△ = upper-△**

Use of Theorems 8.1.29 and 8.1.25 to argue that a composition of $n \times n$ upper-triangular matrices is an upper-triangular matrix.

Exercise 8.1.31 ☞ **Diagonals of upper-△ matrices multiply in a composition; same with lower-△**

Suppose that $\mathcal{M}$ and $\mathcal{N}$ are $n \times n$ *upper-triangular* matrices.

1. Argue that
$$(\mathcal{M} \circ \mathcal{N})[\![i, i]\!] = \mathcal{M}[\![i, i]\!] \cdot \mathcal{N}[\![i, i]\!]$$
for every i.

   In other words, the diagonal entries of a composition of two upper-triangular matrices can be calculated by multiplying together the corresponding diagonal entries of the original matrices.

2. Explain why the result holds true for the lower-triangular matrices as well.

3. Give a concrete example to show that this result does NOT hold true for general matrices, even when $n = 2$.

8.2 Matrix Relations

Some relationships between matrices guarantee that the matrices share a number of important properties. Passing from a given matrix to a simpler one, without altering the property in question, is one of the common strategies of matrix theory, and is a theme of this book.

If the theory guarantees that related matrices share certain properties, and we develop an algorithm for passing from a given matrix to a much simpler related one, we are in a better position to solve a problem.

Let us introduce some of the most common relations of matrix theory. At this point the importance of these particular relations is not obvious. Furthermore, we are not ready to offer any concrete ways for evaluating whether two matrices are related in these ways. All of this will happen in due time.

The intent here is for the reader to get acquainted with the basic formal properties of the relations, and to get some practice in using what has been recently learned.

8.2.1 — Matrix Equivalence

Terminology 8.2.1

Matrix $\mathcal{B}$ is said to be **equivalent** to matrix $\mathcal{A}$, if by sandwiching $\mathcal{A}$ between some two invertible matrices in a composition, we can get $\mathcal{B}$. In other words, if $\mathcal{B}$ can be expressed as $\mathcal{S}\mathcal{A}\mathcal{T}$, for some invertible matrices $\mathcal{S}$ and $\mathcal{T}$.

When $\mathcal{B}$ is equivalent to $\mathcal{A}$, we write $\mathcal{B} \equiv \mathcal{A}$.

Exercise 8.2.2 ☞ $\equiv$ **is reflexive, symmetric and transitive**

Verify the following claims for matrices $\mathcal{A}$, $\mathcal{B}$ and $\mathcal{C}$.

(reflexivity) $\mathcal{A} \equiv \mathcal{A}$.

(symmetry) If $\mathcal{B} \equiv \mathcal{A}$ then $\mathcal{A} \equiv \mathcal{B}$.

(symmetry) $\mathcal{B} \equiv \mathcal{A}$ exactly when $\mathcal{A} \equiv \mathcal{B}$.

(transitivity) If $\mathcal{A} \equiv \mathcal{B}$ and $\mathcal{B} \equiv \mathcal{C}$ then $\mathcal{A} \equiv \mathcal{C}$.

The term "symmetric" being used here is distinct from that used to describe a matrix equal to its transpose.

Terminology 8.2.3

In view of the symmetry of $\equiv$, we can simply say that two **matrices are equivalent**, when one is equivalent to the other.

Test Your Comprehension 8.2.4

Argue that equivalent matrices have the same jectivity.

Hint: Thm. 2.5.14.

Exercise 8.2.5

Suppose that $\mathcal{A} \equiv \mathcal{B}$. Argue that

$$\mathcal{A}^T \equiv \mathcal{B}^T .$$

Hint: $\mathcal{B}^T = (\mathcal{SAM})^T = \cdots$

Test Your Comprehension 8.2.6

Argue that every invertible matrix is equivalent to the identity matrix. Deduce that any two invertible matrices are equivalent.

The remaining relations that we will discuss are particular kinds of equivalence. These are

right-equivalence, left-equivalence, similarity and congruence.

Later in the book we will also work with a particular kind of similarity that is a particular kind of congruence at the same time: a unitary similarity.

8.2.2 — Right/Left-Equivalence

Terminology 8.2.7

If a matrix $\mathcal{B}$ can be expressed as $\mathcal{S} \circ \mathcal{A}$, for some invertible matrix $\mathcal{S}$, we shall say that $\mathcal{B}$ is **left-equivalent** to $\mathcal{A}$, and we will write

$$\mathcal{B} \overset{\mathsf{L}}{\equiv} \mathcal{A} .$$

If a matrix $\mathcal{B}$ can be expressed as $\mathcal{A} \circ \mathcal{T}$, for some invertible matrix $\mathcal{T}$, we shall say that $\mathcal{B}$ is **right-equivalent** to $\mathcal{A}$, and we will write

$$\mathcal{B} \overset{\mathsf{R}}{\equiv} \mathcal{A} .$$

Test Your Comprehension 8.2.8 ☞ **$\overset{\mathsf{L}}{\equiv}$ and $\overset{\mathsf{R}}{\equiv}$ are reflexive, symmetric and transitive**

Verify that the replacement of all $\equiv$ by $\overset{\mathsf{L}}{\equiv}$ in Exercise 8.2.2 yields a valid theorem.

Similarly, argue that the replacement of all $\equiv$ by $\overset{\mathsf{R}}{\equiv}$ in Exercise 8.2.2 also yields a valid theorem.

Terminology 8.2.9

Since $\overset{\mathsf{L}}{\equiv}$ is a symmetric relation, we will simply say that two **matrices are left-equivalent** when one is left-equivalent to the other.

In a similar fashion we can say that two **matrices are right-equivalent** when one is right-equivalent to the other.

Equivalent matrices may be neither left-equivalent nor right-equivalent. The claims in Comment 8.2.13 can be used to construct counterexamples. For example, consider the equality

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

Since it is easy to check that $\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$ is an involution, i.e. is its own inverse, we can conclude that

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

Yet, these two matrices do not have the same range, and they do not annihilate exactly the same pairs of numbers. So, if Comment 8.2.13 is to be believed, these two matrices are neither left-equivalent, nor right-equivalent.

Test Your Comprehension 8.2.10 ☞ **Right/Left-equivalence implies equivalence**

Argue that left-equivalent matrices are equivalent, as are right-equivalent matrices.

Hint: Work with the equality $\mathcal{B} = \mathcal{B} \circ \mathcal{A}^{-1} \circ \mathcal{A}$ for the left-equivalence part.

Test Your Comprehension 8.2.11 ☞ **Right/Left-equivalence does not distinguish between invertible $n \times n$ matrices**

Argue that any two invertible $n \times n$ matrices are left-equivalent and are right-equivalent.

Test Your Comprehension 8.2.12 ☞ **Transposition switches one-sided equivalences**

Argue that the following claims are equivalent.

1. $\mathcal{A} \overset{\mathsf{L}}{\equiv} \mathcal{B}$.
2. $\mathcal{A}^T \overset{\mathsf{R}}{\equiv} \mathcal{B}^T$

Comment 8.2.13 ☞ **A peek into the future**

Eventually (in Sections 16.3 and 19.5) we will demonstrate that right-equivalence for matrices of the same size amounts to the equality of their ranges.

Left-equivalence for matrices of the same size turns out to be equivalent to the property that the two matrices "**annihilate**" exactly the same tuples. Here "annihilate" means "send to the null tuple".

8.2.3 — Similarity

Terminology 8.2.14

If a matrix $\mathcal{B}$ can be expressed as $\mathcal{S}^{-1}\mathcal{A}\mathcal{S}$, for some invertible matrix $\mathcal{S}$, we say that $\mathcal{B}$ is **similar** to $\mathcal{A}$, and we express this by writing

$$\mathcal{B} \sim \mathcal{A} .$$

Exercise 8.2.15 ☞ **$\sim$ is reflexive, symmetric and transitive**

Argue that the replacement of all $\equiv$ by $\sim$ in Exercise 8.2.2 yields a valid theorem.

Terminology 8.2.16

Since $\sim$ is a symmetric relation, we will simply say that two **matrices are similar** when one is similar to the other.

Test Your Comprehension 8.2.17

Argue that the only matrix similar to $\mathcal{I}_n$ is $\mathcal{I}_n$ itself.

Test Your Comprehension 8.2.18

Verify that similar matrices are equivalent.

Equivalent matrices may not be similar. Indeed, every invertible $n \times n$ matrix is equivalent to $\mathcal{I}_n$ (TYC 8.2.11), but the only matrix similar to $\mathcal{I}_n$ is $\mathcal{I}_n$ itself.

Exercise 8.2.19 ☞ **Similarity preserves powers and inverses**

Suppose that $\mathcal{S}$ is an invertible matrix, and $\mathcal{B} = \mathcal{S}^{-1}\mathcal{A}\mathcal{S}$. Argue that the following properties hold.

1. $\mathcal{B}^k = \mathcal{S}^{-1}\mathcal{A}^k\mathcal{S}$ for $k = 0, 1, 2, 3, \ldots$
2. If $\mathcal{A}$ is invertible, so is $\mathcal{B}$, and $\mathcal{B}^{-1} = \mathcal{S}^{-1}\mathcal{A}^{-1}\mathcal{S}$

In particular, the following claims are equivalent for invertible matrices $\mathcal{A}$ and $\mathcal{B}$.

1. $\mathcal{A} \sim \mathcal{B}$.
2. $\mathcal{A}^{-1} \sim \mathcal{B}^{-1}$.

Test Your Comprehension 8.2.20

Argue that the following statements are equivalent for matrices $\mathcal{A}$ and $\mathcal{B}$.

1. $\mathcal{A} \sim \mathcal{B}$.
2. $\mathcal{A}^T \sim \mathcal{B}^T$.

8.2.4 — Congruence

Terminology 8.2.21

If a matrix $\mathcal{B}$ can be expressed as $\mathcal{S}^T\mathcal{A}\mathcal{S}$, for some invertible matrix $\mathcal{S}$, we say that $\mathcal{B}$ is **congruent** to $\mathcal{A}$, and we express this by writing

$$\mathcal{B} \bowtie \mathcal{A} .$$

Exercise 8.2.22 ☞ **$\bowtie$ is reflexive, symmetric and transitive**

Argue that the replacement of all $\equiv$ by $\bowtie$ in Exercise 8.2.2 yields a valid theorem.

Terminology 8.2.23

Since $\bowtie$ is a symmetric relation, we will simply say that two **matrices are congruent** when one is congruent to the other.

Test Your Comprehension 8.2.24

Verify that congruent matrices are equivalent.

Equivalent matrices may not be congruent. Indeed, every invertible $n \times n$ matrix is equivalent to $\mathcal{I}_n$ (TYC 8.2.11), but all matrices congruent to $\mathcal{I}_n$ are symmetric; i.e. equal their own transpose (see TYC. 8.2.25).

Test Your Comprehension 8.2.25 ☞ **Congruence preserves transposes**

Suppose that $\mathcal{S}$ is an invertible matrix, and $\mathcal{B} = \mathcal{S}^T\mathcal{A}\mathcal{S}$. Verify that $\mathcal{B}^T = \mathcal{S}^T\mathcal{A}^T\mathcal{S}$.

In particular, the following statements are equivalent for matrices $\mathcal{A}$ and $\mathcal{B}$.

1. $\mathcal{A} \bowtie \mathcal{B}$.
2. $\mathcal{A}^T \bowtie \mathcal{B}^T$.

Hint: See Thm. 8.1.25.

Test Your Comprehension 8.2.26

Argue that the following claims are equivalent for *invertible* matrices $\mathcal{A}$ and $\mathcal{B}$.

1. $\mathcal{A} \bowtie \mathcal{B}$.
2. $\mathcal{A}^{-1} \bowtie \mathcal{B}^{-1}$.

8.3 Trace And Other Matrix Operations

8.3.1 — Tupling Matrices

Terminology 8.3.1

When we add matrix functions represented by arrays, the addition is an entry-wise operation. In this way it is similar to addition of the tuples in $\mathbb{R}^m$.

Let us associate to each $n \times m$ matrix $\mathcal{A} = \begin{bmatrix} C_1 & C_2 & \cdots & C_m \end{bmatrix}$ a tuple $\mathfrak{C}(\mathcal{A})$ obtained by stacking the columns of $\mathcal{A}$ as a tower, one on top of the next. We call $\mathfrak{C}(\mathcal{A})$ a **tupling** of $\mathcal{A}$.

We can express this using the notation for concatenation developed in Section 3.2.4:

$$\mathfrak{C}(\mathcal{A}) := C_1 \oplus C_2 \oplus \cdots \oplus C_m = \begin{pmatrix} C_1 \\ C_2 \\ C_3 \\ \vdots \\ C_m \end{pmatrix} \in \mathbb{R}^{mn} .$$

Example 8.3.2

if $\mathcal{A} = \begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{bmatrix}$ then $\mathfrak{C}(\mathcal{A}) = \begin{pmatrix} 1 \\ 4 \\ 2 \\ 5 \\ 3 \\ 6 \end{pmatrix}$.

Test Your Comprehension 8.3.3

Consider $\mathfrak{C}$ as a function from $\mathbb{M}_{n\times m}$ to $\mathbb{R}^{nm}$. Argue that $\mathfrak{C}$ is a bijection.

Test Your Comprehension 8.3.4

Consider $\mathfrak{C}$ as a function from $\mathbb{M}_{n\times m}$ to $\mathbb{R}^{nm}$. Argue that $\mathfrak{C}$ satisfies **the linearity conditions** in the following sense:

$$\begin{cases} \mathfrak{C}(\mathcal{A}+\mathcal{B}) = \mathfrak{C}(\mathcal{A})+\mathfrak{C}(\mathcal{B}) \\ \\ \mathfrak{C}(\alpha\cdot\mathcal{A}) = \alpha\cdot\mathfrak{C}(\mathcal{A}) \end{cases}.$$

Why are some operations symbol marked in red and others – in blue?

8.3.2 — Hadamard Product

Terminology 8.3.5 ☞ **Hadamard product**

Given two matrices $\mathcal{M}$ and $\mathcal{K}$ of the same size, we can form a new matrix $\mathcal{M}\bigstar\mathcal{K}$ by multiplying $\mathcal{M}$ and $\mathcal{K}$ together, entry-by-entry. In other words,

$$(\mathcal{M}\bigstar\mathcal{K})\,[\![i,j]\!] := \mathcal{M}[\![i,j]\!]\cdot\mathcal{K}[\![i,j]\!]\ .$$

$\mathcal{M}\bigstar\mathcal{K}$ is the **Hadamard product** of $\mathcal{M}$ and $\mathcal{K}$.

For example,

$$\begin{bmatrix} 6 & -5 & \pi \\ \sqrt{3} & 0 & \frac{1}{4} \end{bmatrix}\bigstar\begin{bmatrix} -1 & 2 & 0 \\ 5 & -3 & e \end{bmatrix} = \begin{bmatrix} -6 & -10 & 0 \\ 5\sqrt{3} & 0 & \frac{e}{4} \end{bmatrix}.$$

It is clear that

the sum of the entries of $\mathcal{A}\bigstar\mathcal{B}$ is exactly $\mathfrak{C}(\mathcal{A})\bullet\mathfrak{C}(\mathcal{B})$.

Test Your Comprehension 8.3.6

Verify that Hadamard product $\bigstar$ is an associative and commutative operation, and that it distributes over linear combinations.

Test Your Comprehension 8.3.7 ☞ **Transpose of a Hadamard product is the Hadamard product of transposes**

Argue that

$$\left(\mathcal{A}\bigstar\mathcal{B}\right)^{T} = \mathcal{A}^{T}\bigstar\mathcal{B}^{T} ,$$

for any matrices $\mathcal{A}$ and $\mathcal{B}$ of the same size.

Test Your Comprehension 8.3.8

Argue that

$$\mathfrak{C}(\mathcal{A}) \bullet \mathfrak{C}(\mathcal{B}) = \mathfrak{C}\left(\mathcal{A}^{T}\right) \bullet \mathfrak{C}\left(\mathcal{B}^{T}\right) ,$$

for any matrices $\mathcal{A}$ and $\mathcal{B}$ of the same size.

Hint: Use Trm. 8.3.5 and TYC 8.3.7.

8.3.3 — Trace

Definition 8.3.9

The **trace** of an $n \times n$ matrix $\mathcal{A}$ is the sum of its n diagonal entries. We denote this number by $\mathit{Trace}(\mathcal{A})$. So,

$$\mathit{Trace}(\mathcal{A}) := \sum_{i=1}^{n} \mathcal{A}[\![i,i]\!] .$$

Test Your Comprehension 8.3.10

Verify the following basic properties of trace. Here $\mathcal{A}, \mathcal{B} \in \mathbb{M}_n$ and $a, b \in \mathbb{R}$.

1. $\mathit{Trace}(a \cdot \mathcal{A} + b \cdot \mathcal{B}) = a \cdot \mathit{Trace}(\mathcal{A}) + b \cdot \mathit{Trace}(\mathcal{B})$.
2. $\mathit{Trace}(\mathcal{A}) = \mathit{Trace}\left(\mathcal{A}^{T}\right)$.

Exercise 8.3.11

Argue that

$$\mathit{Trace}\left(\mathcal{A}^{T}\mathcal{B}\right) = \mathfrak{C}(\mathcal{A}) \bullet \mathfrak{C}(\mathcal{B}) = \sum_{i=1,j=1}^{i=n,j=m} \left(\mathcal{A}[\![i,j]\!]\,\mathcal{B}[\![i,j]\!]\right) ,$$

for all $\mathcal{A}, \mathcal{B} \in \mathbb{M}_{n\times m}$.

In particular, $\mathit{Trace}\left(\mathcal{A}^{T}\mathcal{B}\right)$ is the sum of the entries of the Hadamard product $\mathcal{A}\bigstar\mathcal{B}$.

Hint: Write $\mathcal{A} = \begin{bmatrix} C_1 & C_2 & C_3 & \cdots & C_m \end{bmatrix}$ so that

$$\mathcal{A}^{T} = \begin{bmatrix} \longleftarrow & C_1 & \longrightarrow \\ \longleftarrow & C_2 & \longrightarrow \\ \longleftarrow & C_3 & \longrightarrow \\ & \vdots & \\ \longleftarrow & C_m & \longrightarrow \end{bmatrix} .$$

Write $\mathcal{B} = \begin{bmatrix} K_1 & K_2 & K_3 & \cdots & K_m \end{bmatrix}$. Show that

$$\left(\mathcal{A}^{T}\mathcal{B}\right)[\![i,i]\!] = C_i \bullet K_i .$$

In view of the result of Exercise 8.3.11, mathematicians often think of the construct $Trace\left(\mathcal{A}^T\mathcal{B}\right)$ as "a dot product for matrices".

Note that $\mathcal{AB} \in \mathbb{M}_n$, while $\mathcal{BA} \in \mathbb{M}_m$.

Theorem 8.3.12

For any $\mathcal{A} \in \mathbb{M}_{n\times m}$ and $\mathcal{B} \in \mathbb{M}_{m\times n}$,

$$Trace\left(\mathcal{AB}\right) = Trace\left(\mathcal{BA}\right) \ .$$

Proof of Theorem 8.3.12. We make use of the results of Exercises 8.3.11 and 8.3.8 in the following calculation:

$$\begin{aligned} Trace\left(\mathcal{AB}\right) &\overset{\text{Exc. 8.3.11}}{=} \mathfrak{C}\left(\mathcal{A}^T\right) \bullet \mathfrak{C}\left(\mathcal{B}\right) \overset{\text{Exc. 8.3.8}}{=} \mathfrak{C}\left(\mathcal{A}\right) \bullet \mathfrak{C}\left(\mathcal{B}^T\right) \\ &= \mathfrak{C}\left(\mathcal{B}^T\right) \bullet \mathfrak{C}\left(\mathcal{A}\right) \overset{\text{Exc. 8.3.11}}{=} Trace\left(\mathcal{BA}\right) \ . \end{aligned}$$

∎

Test Your Comprehension 8.3.13

Verify that the following identities hold for any matrix $\mathcal{A}$.

$$\begin{aligned} Trace\left(\mathcal{A}^T\mathcal{A}\right) = Trace\left(\mathcal{A}\mathcal{A}^T\right) \\ &= \mathfrak{C}(\mathcal{A}) \bullet \mathfrak{C}(\mathcal{A}) = \left\|\mathfrak{C}(\mathcal{A})\right\|^2 \\ &= \mathfrak{C}\left(\mathcal{A}^T\right) \bullet \mathfrak{C}\left(\mathcal{A}^T\right) = \left\|\mathfrak{C}\left(\mathcal{A}^T\right)\right\|^2 \\ &= \text{ the sum of the squares of the entries of } \mathcal{A} \ . \end{aligned}$$

Consequently argue that the following are equivalent.

1. $\mathcal{A}$ is null.
2. $Trace\left(\mathcal{A}^T\mathcal{A}\right) = 0$.
3. $Trace\left(\mathcal{A}\mathcal{A}^T\right) = 0$.

Comment 8.3.14

It would be INCORRECT to state that trace is completely insensitive to the order of composition. There are examples of (square) matrices A, B, C such that

$$\mathit{Trace}\,(\mathcal{CAB}) \neq \mathit{Trace}\,(\mathcal{BAC}) \ .$$

Still, the fact that $\mathcal{AB}$ and $\mathcal{BA}$, when both are defined, have the same trace, is the crucial property that makes the trace a useful tool for getting around the non-commutativity of matrix multiplication (see, for example, the proof of Theorem 33.1.23).

Exercise 8.3.15

Find 2×2 matrices A, B, C such that

$$\mathit{Trace}\,(\mathcal{CAB}) \neq \mathit{Trace}\,(\mathcal{BAC}) \ .$$

8.4 Symmetric And Anti-symmetric Matrices

8.4.1 — Symmetric Matrices

Terminology 8.4.1

A matrix that is equal to its own transpose is said to be **symmetric**. Such matrices enjoy special properties and play a central role in many applications. For example, covariance and correlation matrices in statistics are symmetric, as are adjacency and Laplacian matrices in graph theory.

Symmetric matrices must be square, and their entries do exhibit symmetry with respect to the main diagonal of the matrix: the $[\![i, j]\!]$-th entry of such a matrix equals its $[\![j, i]\!]$-th entry.

Test Your Comprehension 8.4.2

Argue that $\mathcal{A} + \mathcal{A}^{T}$ is a symmetric matrix for any square matrix $\mathcal{A}$.

Test Your Comprehension 8.4.3

Argue that for any (not necessarily square) matrix $\mathcal{A}$, matrices $\mathcal{A}^{T}\mathcal{A}$ and $\mathcal{A}\mathcal{A}^{T}$ are symmetric.

Test Your Comprehension 8.4.4

Argue that a linear combination of (a list of) symmetric matrices is a symmetric matrix.

Exercise 8.4.5

Argue that a matrix $\mathcal{A} \in \mathbb{M}_n$ is symmetric exactly when

$$\mathcal{A}(X) \bullet Y = X \bullet \mathcal{A}(Y) \, ,$$

for all $X, Y \in \mathbb{R}^n$.

Hint: TYC 6.1.17 can be useful here, along with a fundamental property of transposition (Thm. 7.1.7).

Exercise 8.4.6 ☞ **Polarization identity for symmetric matrices**

Verify that every *symmetric* matrix $\mathcal{A} \in \mathbb{M}_n$ satisfies the identity

$$4 \cdot \mathcal{A}(V) \bullet W = \Big(\mathcal{A}(V+W) \bullet (V+W)\Big) - \Big(\mathcal{A}(V-W) \bullet (V-W)\Big) \, ,$$

for all $V, W \in \mathbb{R}^n$.

Hint: Use the linearity of $\mathcal{A}$. Distribute the dot product over addition and perform cancellation.

Test Your Comprehension 8.4.7

Argue that the only *symmetric* matrix $\mathcal{F} : \mathbb{R}^n \longrightarrow \mathbb{R}^n$ such that

$$\mathcal{F}(X) \bullet X = 0 \quad \text{for all} \quad X \in \mathbb{R}^n$$

is the null matrix $\mathcal{O}_n$.

Hint: Exc. 8.4.6 and TYC 6.1.18.

8.4.2 — Anti-symmetric Matrices

Terminology 8.4.8

A matrix $\mathcal{A}$ is said to be **anti-symmetric** if

$$\mathcal{A}^{T} = -\mathcal{A}.$$

For example, $\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$ is anti-symmetric.

Test Your Comprehension 8.4.9

Verify the following claims.

1. All anti-symmetric matrices are square.
2. The diagonal entries of an anti-symmetric matrix are all zero.
3. $B - B^T$ is an anti-symmetric matrix for any square matrix $\mathcal{B}$.
4. A linear combination of (a list of) anti-symmetric matrices is an anti-symmetric matrix.

Theorem 8.4.10 ☞ **"Symmetric + anti-symmetric" decomposition**

Every square matrix can be expressed as a sum of a symmetric matrix and an anti-symmetric one in exactly one way.

Proof of Theorem 8.4.10. For every square matrix $\mathcal{A}$ we have the identity

$$\mathcal{A} = \frac{1}{2}\left(\mathcal{A} + \mathcal{A}^T\right) + \frac{1}{2}\left(\mathcal{A} - \mathcal{A}^T\right) .$$

The first summand on the right is a symmetric matrix (TYC's 8.4.2 and TYC2;19-08-18) and the second is an anti-symmetric one (TYC's 8.4.9 and 8.4.4).

We leave the claim of the uniqueness of the decomposition as an exercise for the reader (Exc. 8.4.11). ■

Exercise 8.4.11

Suppose that $A = B + C$, where B is a symmetric matrix, and C is an anti-symmetric one. Argue that

$$B = \frac{1}{2}\left(\mathcal{A} + \mathcal{A}^T\right) \text{ and } C = \frac{1}{2}\left(\mathcal{A} - \mathcal{A}^T\right) .$$

Hint: $A^T = (B + C)^T = \ldots$

Terminology 8.4.12

Based on the result of Exercise 8.4.11, $\frac{1}{2}\left(\mathcal{A}+\mathcal{A}^T\right)$ is said to be the **symmetric part** of a square matrix $\mathcal{A}$, and $\frac{1}{2}\left(\mathcal{A} - \mathcal{A}^T\right)$ is its **anti-symmetric part**.

Test Your Comprehension 8.4.13 ☞ **Congruence preserves (anti-)symmetry of matrices**

Suppose that matrices $\mathcal{A}$ and $\mathcal{B}$ are congruent. Argue that if one of these matrices is symmetric, then so is the other. Similarly, argue that if one is anti-symmetric, so is the other.

8.5 Additional Problems

Test Your Comprehension 8.5.1

Suppose that $\mathcal{A} \circ \mathcal{B} = \mathcal{C}$, and we remove the 7-th column from $\mathcal{B}$ and from $\mathcal{C}$ to produce smaller matrices $\mathcal{B}_o$ and $\mathcal{C}_0$. Argue that

$$\mathcal{A} \circ \mathcal{B}_o = \mathcal{C}_o \ .$$

Test Your Comprehension 8.5.2 ☞ **Null columns of the right-most matrix persist in a composition**

Argue that if the 13-th column of $\mathcal{B}$ is null, then the 13-th column of $\mathcal{A} \circ \mathcal{B}$ is also null.

Compare this with TYC 8.5.2.

Test Your Comprehension 8.5.3 ☞ **Null rows of the left-most matrix persist in a composition**

Argue that if the 8-th row of $\mathcal{A}$ is null then the 8-th row of $\mathcal{A} \circ \mathcal{B}$ is also null.

Hint: Apply TYC 8.5.2 and the fact that $\mathcal{B} = \mathcal{A}^{-1} \circ \left(\mathcal{A} \circ \mathcal{B}\right)$ to show that every null column of $\mathcal{A} \circ \mathcal{B}$ "yields" a null column of $\mathcal{B}$.

Exercise 8.5.4 ☞ **Multiplication by an invertible matrix on the left does not affect the positions of the null columns.**

Suppose that $\mathcal{A}$ is invertible. Argue that the null columns in matrices $\mathcal{A} \circ \mathcal{B}$ and $\mathcal{B}$ are in the same positions.

Test Your Comprehension 8.5.5 ☞ **Composing with a 1×1 matrix amounts to scaling**

Verify that for any $X \in \mathbb{R}^n$ and $\alpha \in \mathbb{R}$

$$\left[X\right]_{n\times 1} \circ \left[\alpha\right]_{1\times 1} = \left[\alpha \cdot X\right]_{n\times 1} = \alpha \cdot \left[X\right]_{n\times 1}$$

and

$$\left[\alpha\right]_{1\times 1} \circ \ \left[\leftarrow X \rightarrow\right]_{1\times n} = \left[\leftarrow \alpha \cdot X \rightarrow\right]_{1\times n} = \alpha \cdot \left[\leftarrow X \rightarrow\right]_{1\times n} \ .$$

Terminology 8.5.6

A **matrix unit** $\mathcal{M}_{i,j} \in \mathbb{M}_n$ is a matrix that has 1 as its (i,j)-th entry, and zeros elsewhere. In other words, all columns of $\mathcal{M}_{i,j}$ are null, except for the j-th column, and that one is E_i, the i-th standard basis tuple in $\mathbb{R}^n$.

INSERT PICTURE

Test Your Comprehension 8.5.7

Verify that

$$\left(\mathcal{M}_{i,j}\right)^T = \mathcal{M}_{j,i}.$$

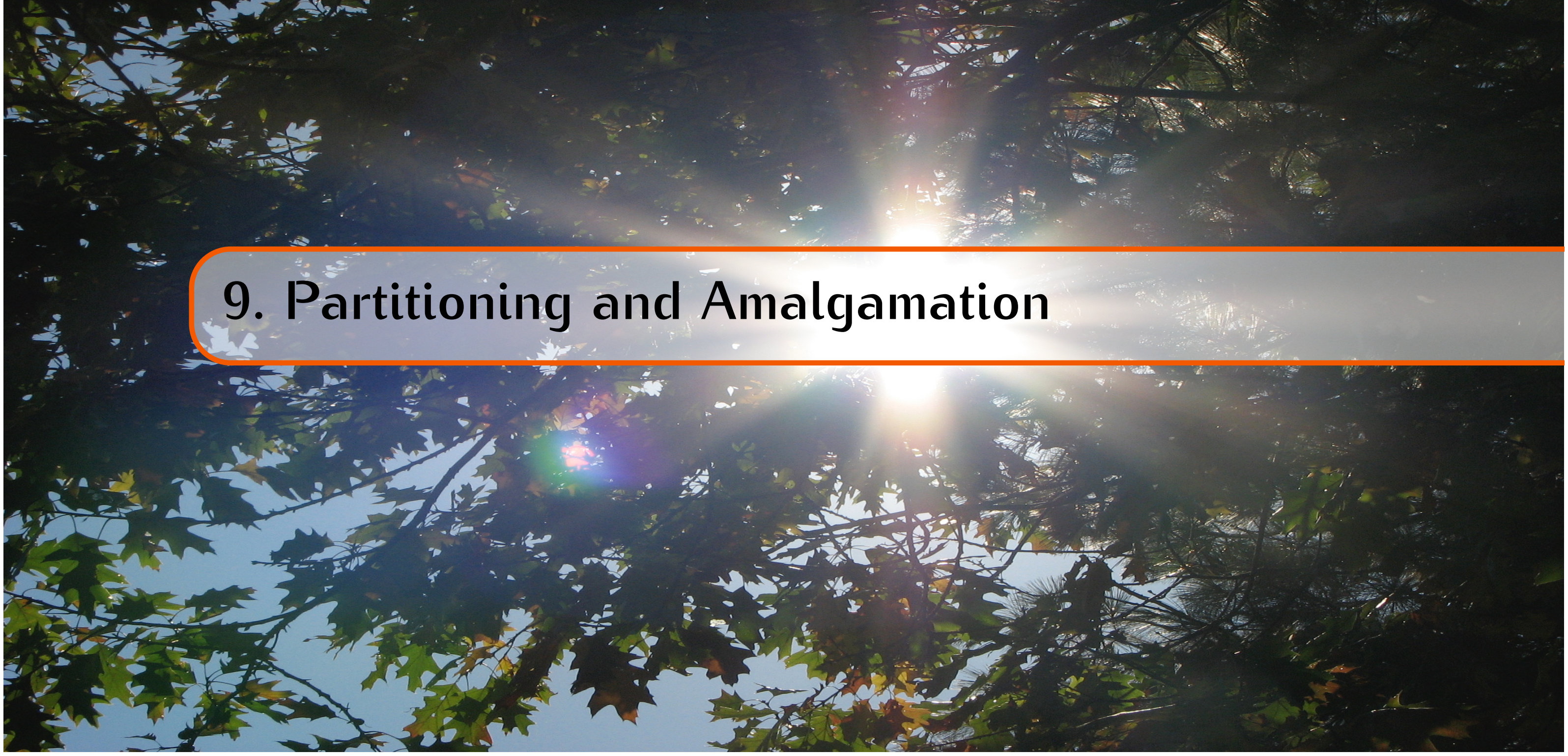
Exercise 8.5.8

Argue that in $\mathbb{M}_n$

$$\mathcal{M}_{i,j} \circ \mathcal{M}_{j,k} = \mathcal{M}_{i,k}\ , \quad \text{and} \quad \mathcal{M}_{i,j} \circ \mathcal{M}_{p,k} = \mathcal{O}\ , \ \text{if } j \neq p\ .$$

Exercise 8.5.9

1. Describe all 5×5 matrices that commute with the standard matrix unit $\mathcal{M}_{2,4}$.
2. Describe all 5×5 matrices that commute with the standard matrix unit $\mathcal{M}_{3,1}$.
3. Describe all 5×5 matrices that commute with the standard matrix unit $\mathcal{M}_{2,2}$.
4. Describe all 5×5 matrices that commute with all 25 standard matrix units $\mathcal{M}_{i,j}$.
5. Which 13×13 matrices commute with ALL other 13×13 matrices?



9. Partitioning and Amalgamation

Last modified on December 8, 2018

9.1 Partitioning a Matrix

Suppose that Pat asks for your help with multiplying two matrices:

$$M = \begin{bmatrix} A & B \\ C & D \end{bmatrix} \quad \text{and} \quad K = \begin{bmatrix} P & Q \\ R & S \end{bmatrix}, \tag{9.1}$$

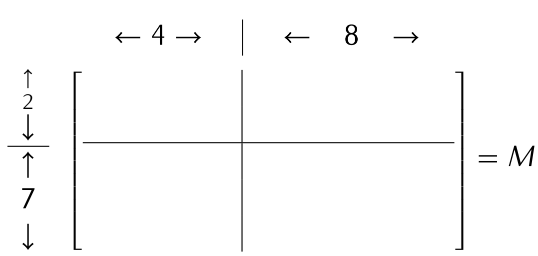
but before Pat can give you all of the details of the problem, Pat has to rush off to class. Eager to help, or to get it over with, you decide to carry out the calculation on your own.

Assessing M and K as 2×2 matrices you make the following calculation:

$$MK = \begin{bmatrix} AP+BR & AQ+BS \\ CP+DR & CQ+DS \end{bmatrix}. \tag{9.2}$$

Imagine your surprise when Pat returns and tells you that $A, B, \ldots, S$ in (9.1) are not numbers, and that M is not a 2×2 matrix, but is rather a 9×12 matrix! How can this be?

The story Pat tells is this: Pat started with a 9×12 matrix M of real numbers, and then drew a vertical line between the 4-th and the 5-th columns of the matrix. After that Pat drew a horizontal line between the 2-nd and the 3-rd rows. Here is the schematic of the lines drawn (not to scale!):



INSERT PICTURE

This way Pat has partitioned the original matrix M into four smaller matrices (**sub-matrices**), which Pat named A, B, C, D, as in (9.1). One can read off the dimensions of the sub-matrices A, B, C, D of M from the diagram. For example, B is a 2×8 matrix, and D is a 7×8 matrix.

Pat also partitioned matrix K into 4 matrices, which Pat named P, Q, R, S.

It may very well be that the actual size of K is such that $M \circ K$ is meaningless (and the same may or may not be true for $K \circ M$). As we know, $M \circ K$ is defined exactly when K has as many rows as M has columns (12 in our case).

Even if $M \circ K$ is defined, the sums of the compositions of the sub-matrices appearing in (9.2) (such as $C\ P + D\ R$, for example) may not be defined.

Terminology 9.1.1

The reader should consider horizontal and vertical partitioning of a matrix, as a form of an overlay. The matrix itself remains unchanged.

Let us think for a moment of cutting up a partitioned matrix according to the partitioning. Each piece we get can be considered a matrix in its own right. These matrices are said to be the **block-entries** of the original partitioned matrix. The block entries that are lined up horizontally form **block-rows** of the original partitioned matrix. **Block-columns** are defined similarly.

INSERT PICTURE

Notation 9.1.2

Stating that $\left[\begin{smallmatrix} \mathcal{A} & \mathcal{B} \\ \mathcal{C} & \mathcal{D} \end{smallmatrix}\right]$ is a $(9|32) \times (5|7)$ partitioned matrix indicates that the matrix is of size 41×12, and it has a $9|32$ **horizontal splitting**, and a $5|7$ **vertical splitting**. This will also be designated by the notation

$$\left[\begin{smallmatrix} \mathcal{A} & \mathcal{B} \\ \mathcal{C} & \mathcal{D} \end{smallmatrix}\right]_{(9|32)\times(5|7)} .$$

In the above example, $\mathcal{A}$ is a 9×5 matrix, and $\mathcal{B}$ is a 9×7 matrix.

We will also encounter partitioning with a single block-row or a single block-column. In such a case there is only one splitting: either a horizontal one or a vertical one. For example,

$$\left[\begin{smallmatrix} \mathcal{A} \\ \mathcal{C} \end{smallmatrix}\right]_{(9|32)\times 5} \text{and} \quad [\mathcal{A}\ \mathcal{B}]_{9\times(5|7)}$$

exhibit such partitioning.

We hope that the reader can now infer the meaning of a statement that a given matrix $\mathcal{A}$ is a $(3|5|1|2|3|5|5) \times (4|2|9)$ partitioned matrix. *Of course such an* $\mathcal{A}$ *is a* 24×15 *matrix, and the partitioning is just a grid overlaid on* $\mathcal{A}$*.*

INSERT PICTURE

Test Your Comprehension 9.1.3 ☞ **Linear combinations of partitioned matrices**

Keeping in mind that matrix scaling and addition are effectively entry-wise operations, as described in Theorems 7.2.4 and 7.3.4, argue that

$$\alpha\begin{bmatrix}\mathcal{A}_{11} & \mathcal{A}_{12} & \mathcal{A}_{13} & \mathcal{A}_{14}\\ \mathcal{A}_{21} & \mathcal{A}_{22} & \mathcal{A}_{23} & \mathcal{A}_{24}\\ \mathcal{A}_{31} & \mathcal{A}_{32} & \mathcal{A}_{33} & \mathcal{A}_{34}\end{bmatrix}_{(7|1|5)\times(5|1|5|3)} + \gamma\begin{bmatrix}\mathcal{C}_{11} & \mathcal{C}_{12} & \mathcal{C}_{13} & \mathcal{C}_{14}\\ \mathcal{C}_{21} & \mathcal{C}_{22} & \mathcal{C}_{23} & \mathcal{C}_{24}\\ \mathcal{C}_{31} & \mathcal{C}_{32} & \mathcal{C}_{33} & \mathcal{C}_{34}\end{bmatrix}_{(7|1|5)\times(5|1|5|3)}$$

$$= \begin{bmatrix}\alpha\mathcal{A}_{11}+\gamma\mathcal{C}_{11} & \alpha\mathcal{A}_{12}+\gamma\mathcal{C}_{12} & \alpha\mathcal{A}_{13}+\gamma\mathcal{C}_{13} & \alpha\mathcal{A}_{14}+\gamma\mathcal{C}_{14}\\ \alpha\mathcal{A}_{21}+\gamma\mathcal{C}_{21} & \alpha\mathcal{A}_{22}+\gamma\mathcal{C}_{22} & \alpha\mathcal{A}_{23}+\gamma\mathcal{C}_{23} & \alpha\mathcal{A}_{24}+\gamma\mathcal{C}_{24}\\ \alpha\mathcal{A}_{31}+\gamma\mathcal{C}_{31} & \alpha\mathcal{A}_{32}+\gamma\mathcal{C}_{32} & \alpha\mathcal{A}_{33}+\gamma\mathcal{C}_{33} & \alpha\mathcal{A}_{34}+\gamma\mathcal{C}_{34}\end{bmatrix}_{(7|1|5)\times(5|1|5|3)}.$$

Test Your Comprehension 9.1.4 ☞ **Transposition of Partitioned Matrices**

Use good diagrams to argue that the following is true, and is a concrete case of a true general formula. We suggest drawing in a representative individual column of the original matrix.

$$\begin{bmatrix}\mathcal{A}_{11} & \mathcal{A}_{12} & \mathcal{A}_{13} & \mathcal{A}_{14}\\ \mathcal{A}_{21} & \mathcal{A}_{22} & \mathcal{A}_{23} & \mathcal{A}_{24}\\ \mathcal{A}_{31} & \mathcal{A}_{32} & \mathcal{A}_{33} & \mathcal{A}_{34}\end{bmatrix}^T_{(7|1|5)\times(5|1|5|3)} = \begin{bmatrix}(\mathcal{A}_{11})^T & (\mathcal{A}_{21})^T & (\mathcal{A}_{31})^T\\ (\mathcal{A}_{12})^T & (\mathcal{A}_{22})^T & (\mathcal{A}_{32})^T\\ (\mathcal{A}_{13})^T & (\mathcal{A}_{23})^T & (\mathcal{A}_{33})^T\\ (\mathcal{A}_{14})^T & (\mathcal{A}_{24})^T & (\mathcal{A}_{34})^T\end{bmatrix}_{(5|1|5|3)\times(7|1|5)}$$

Terminology 9.1.5

A partitioned matrix

$$\begin{bmatrix}\square & \square & \square & \square & \square & \square\\ \mathcal{O} & \square & \square & \square & \square & \square\\ \mathcal{O} & \mathcal{O} & \square & \square & \square & \square\\ \mathcal{O} & \mathcal{O} & \mathcal{O} & \square & \square & \square\\ \mathcal{O} & \mathcal{O} & \mathcal{O} & \mathcal{O} & \square & \square\\ \mathcal{O} & \mathcal{O} & \mathcal{O} & \mathcal{O} & \mathcal{O} & \square\end{bmatrix},$$

with square colored blocks, is said to be in a **block-upper-triangular** form.[*] The square block-entries appearing in positions $\square$ are said to be the **diagonal blocks** [†] and they appear on the **block-diagonal**.

Block-lower-triangular partitioned matrices are defined similarly. A **block-triangular** partitioned matrix is one that is either block-upper-triangular or is block-lower-triangular (or both!). It should be obvious to the reader that a block-triangular partitioned matrix always has an equal number of block-rows and block-columns.

A partitioned matrix

$$\begin{bmatrix} \square & \mathcal{O} & \mathcal{O} & \mathcal{O} & \mathcal{O} & \mathcal{O} \\ \mathcal{O} & \square & \mathcal{O} & \mathcal{O} & \mathcal{O} & \mathcal{O} \\ \mathcal{O} & \mathcal{O} & \square & \mathcal{O} & \mathcal{O} & \mathcal{O} \\ \mathcal{O} & \mathcal{O} & \mathcal{O} & \square & \mathcal{O} & \mathcal{O} \\ \mathcal{O} & \mathcal{O} & \mathcal{O} & \mathcal{O} & \square & \mathcal{O} \\ \mathcal{O} & \mathcal{O} & \mathcal{O} & \mathcal{O} & \mathcal{O} & \square \end{bmatrix}$$

is said to be in a **block-diagonal** form.

---

*The block-entries in the boxes □ may or may not be null.
†... rather than "block-diagonal block-entries", which would be too cumbersome.

Test Your Comprehension 9.1.6 ☞ Square diagonal blocks

Argue that if every diagonal block of a partitioned matrix $\mathcal{A}$ is a square matrix then so is $\mathcal{A}$ itself. In particular, block-triangular matrices have to be square.

Test Your Comprehension 9.1.7

Argue that the following claims are equivalent for a block-upper-triangular matrix

$$\mathcal{M} = \begin{bmatrix} \mathcal{A} & \mathcal{B} \\ \mathcal{O} & \mathcal{D} \end{bmatrix}.$$

1. $\mathcal{M}$ is upper-triangular.

2. $\mathcal{A}$ and $\mathcal{D}$ are upper-triangular.

9.1.1 — Products of Partitioned Matrices

The next result is an important tool in the development of matrix theory. Applied to our encounter with Pat, it shows that our simple-minded calculation in (9.2) actually yields the correct answer in the appropriate circumstances.

As usual, we present a concrete case that captures all of the generality of the theorem and its proof, without the burden of a fully general notation.

Theorem 9.1.8 ☞ A fundamental formula for partitioned matrix products

If

$$\mathcal{A} = \begin{bmatrix} \mathcal{A}_{11} & \mathcal{A}_{12} & \mathcal{A}_{13} & \mathcal{A}_{14} \\ \mathcal{A}_{21} & \mathcal{A}_{22} & \mathcal{A}_{23} & \mathcal{A}_{24} \\ \mathcal{A}_{31} & \mathcal{A}_{32} & \mathcal{A}_{33} & \mathcal{A}_{34} \end{bmatrix}_{(7|1|5)\times(5|1|5|3)} \quad \text{and} \quad \mathcal{B} = \begin{bmatrix} \mathcal{B}_{11} & \mathcal{B}_{12} \\ \mathcal{B}_{21} & \mathcal{B}_{22} \\ \mathcal{B}_{31} & \mathcal{B}_{32} \\ \mathcal{B}_{41} & \mathcal{B}_{42} \end{bmatrix}_{(5|1|5|3)\times(9|28)},$$

then the product $\mathcal{AB}$ makes sense, and can be partitioned according to a $(7|1|5)\times(9|28)$ pattern. (Compare this to the margin note beside Theorem 8.1.7.)

More importantly, the (i, j)-th block-entry $\big(\mathcal{AB}\big)_{ij}$ of $\mathcal{AB}$ is given by the formula

$$\begin{aligned}\big(\mathcal{AB}\big)_{ij} &= \sum_{k=1}^{4} \mathcal{A}_{ik}\mathcal{B}_{kj} \\ &= \mathcal{A}_{i1}\mathcal{B}_{1j} + \mathcal{A}_{i2}\mathcal{B}_{2j} + \mathcal{A}_{i3}\mathcal{B}_{3j} + \mathcal{A}_{i4}\mathcal{B}_{4j} \\ &= \text{a formal } \bullet\text{-like product of the } i\text{-th block row of } \mathcal{A} \text{ and the } j\text{-th block-column of } \mathcal{B}: \\ &\qquad \begin{matrix} \mathcal{A}_{i1} & \mathcal{A}_{i2} & \mathcal{A}_{i3} & \mathcal{A}_{i4} \end{matrix} \quad \text{“}\bullet\text{”} \quad \begin{matrix} \mathcal{B}_{1j} \\ \mathcal{B}_{2j} \\ \mathcal{B}_{3j} \\ \mathcal{B}_{4j} \end{matrix}\,.\end{aligned}$$

(This formula should be compared to the row-centric formula (8.1) for the regular matrix multiplication.)

The gist of this fundamental theorem is that multiplication of partitioned matrices can be carried out in a way that is formally analogous to the regular row-centric matrix multiplication.

A proof of Theorem 9.1.8 is presented in the appendix to the chapter.

Test Your Comprehension 9.1.9

Verify the following formula.

$$\begin{bmatrix} \mathcal{A} & \mathcal{B} \\ \mathcal{O} & \mathcal{D} \end{bmatrix}_{(n|k)\times(n|k)} \begin{bmatrix} \mathcal{X} & \mathcal{Y} \\ \mathcal{O} & \mathcal{Z} \end{bmatrix}_{(k|m)\times(k|m)} = \begin{bmatrix} \mathcal{AX} & \mathcal{AY}+\mathcal{BZ} \\ \mathcal{O} & \mathcal{DZ} \end{bmatrix}_{(n|m)\times(n|m)}. \tag{9.3}$$

Theorem 9.1.10 ☞ **Invertibility of** $\begin{bmatrix} \mathcal{I} & \mathcal{B} \\ \mathcal{O} & \mathcal{I} \end{bmatrix}$

A square matrix of the form

$$\begin{bmatrix} \mathcal{I}_k & \mathcal{B} \\ \mathcal{O} & \mathcal{I}_m \end{bmatrix}_{(k|m)\times(k|m)}$$

is invertible for any $\mathcal{B} \in \mathbb{M}_{k\times m}$, and its inverse is

$$\begin{bmatrix} \mathcal{I}_k & -\mathcal{B} \\ \mathcal{O} & \mathcal{I}_m \end{bmatrix}_{(k|m)\times(k|m)}.$$

Proof of Theorem 9.1.10. It is sufficient to verify the identities

$$\begin{bmatrix} \mathcal{I}_k & \mathcal{B} \\ \mathcal{O} & \mathcal{I}_m \end{bmatrix}\begin{bmatrix} \mathcal{I}_k & -\mathcal{B} \\ \mathcal{O} & \mathcal{I}_m \end{bmatrix} = \mathcal{I} = \begin{bmatrix} \mathcal{I}_k & -\mathcal{B} \\ \mathcal{O} & \mathcal{I}_m \end{bmatrix}\begin{bmatrix} \mathcal{I}_k & \mathcal{B} \\ \mathcal{O} & \mathcal{I}_m . \end{bmatrix}.$$

These follow immediately from the formula (9.3). ■

In Theorem 8.1.29 we showed that a product of two lower-triangular matrices of the same size is again a lower-triangular matrix. TYC 8.1.30 offered the corresponding statement for the upper-triangular matrices. The fundamental formula for partitioned matrix multiplication allows us to generalize these results to block-triangular matrices.

Theorem 9.1.11 ☞ **Products of block-upper-△ are block-upper-△**

If two partitioned matrices have block-upper-triangular form, and are such that the fundamental formula (Thm. 9.1.8) applies to their product, then an application of the formula results in a block-upper-triangular partition of the product.

A proof of Theorem 9.1.11 is presented in the appendix to the chapter.

Exercise 9.1.12 ☞ **Products of block-lower-△ are block-lower-△**

Use Theorem 9.1.11 and TYC 9.1.4 to construct a short proof of the analogue of Theorem 9.1.11 for block-lower-triangular matrices.

Comment 9.1.13 ☞ **Partitioning into 1×1 matrices**

Clearly, we can partition every matrix into 1×1 blocks. $(1|1|1|1|1|1|1) \times (1|1|1)$ describes such a partitioning of a 7×3 matrix.

While $[3]_{1\times 1}$ is not the same object as the scalar 3, with the primer being a function from $\mathbb{R}^1$ to $\mathbb{R}^1$, and the latter being an element of $\mathbb{R}$ (see TYC 6.1.8), there are obvious parallels.

For example,

$$[3]_{1\times 1}^{T} = [3]_{1\times 1}\ , \quad [3]_{1\times 1} + [5]_{1\times 1} = [3+5]_{1\times 1}\ ,$$

and

$$[3]_{1\times 1} \circ [5]_{1\times 1} = [3 \cdot 5]_{1\times 1} = 3 \cdot [5]_{1\times 1} = 5 \cdot [3]_{1\times 1}\ .$$

Interpreting partitioning as an overlay, we can conclude that by applying general results about partitioned matrices to the case of partitioning into 1×1 block-entries, we can produce the corresponding results for non-partitioned matrices.

In this way the general results about block-upper-triangular matrices apply to upper-triangular matrices; etc.

9.1.2 — Matrixing Tuples

Terminology 9.1.14

For each tuple X, the **matrixation of** X is the matrix $[X]$ whose array has X as its single *column*.

In other words, the matrixation of a tuple $\left(x_1, x_2, x_3, \ldots, x_n\right)$ is $\begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ \vdots \\ x_n \end{bmatrix}$.

While we have given preference to a vertical orientation, we can always use transposition to arrive at a matrix whose array has X as its single row.

Obviously *two tuples are equal exactly when their matrixations are equal.* We shall make frequent use of this observation.

It is also immediate from our discussion of the operations of addition and scaling for matrices that

$$\left[\alpha \cdot X + \beta \cdot Y\right] = \alpha \cdot \left[X\right] + \beta \cdot \left[Y\right]$$

We have used color to indicate that even though the same symbols "+" and "$\cdot$" are being used on both sides of the equality, these symbols indicate operations in different contexts. What are the two distinct contexts?

In particular, the algebraic operations on matrices can re-capture the algebraic operations on the underlying spaces $\mathbb{R}^k$ of tuples.

Test Your Comprehension 9.1.15

Suppose that $\mathcal{A} \in \mathbb{M}_{n\times m}$ and $X \in \mathbb{R}^m$. Verify that

$$\mathcal{A} \circ \left[X\right]_{m\times 1} = \left[\mathcal{A}(X)\right]_{n\times 1} . \tag{9.4}$$

Here we see that the operation of matrix composition can recapture, through matrixation, the behavior of matrices as functions.

Observation 9.1.16

There is a counterpart to formula (9.4) for single-row matrices $\left[\leftarrow Y \rightarrow\right]_{1\times n}$.

$$\left[\leftarrow Y \rightarrow\right]_{1\times n} \circ \mathcal{A} = \left[Y\right]^T \circ \left(\mathcal{A}^T\right)^T \overset{\text{Thm. 8.1.25}}{=} \left(\mathcal{A}^T \circ \left[Y\right]\right)^T$$

$$\overset{(9.4)}{=} \left[\mathcal{A}^T(Y)\right]^T = \left[\leftarrow \mathcal{A}^T(Y) \rightarrow\right]_{1\times m} .$$

Let us record this.

$$\boxed{\left[\leftarrow Y \rightarrow\right]_{1\times n} \circ \mathcal{A} = \left[\leftarrow \mathcal{A}^T(Y) \rightarrow\right]_{1\times m} . \tag{9.5}}$$

Test Your Comprehension 9.1.17

Verify that

$$\left[\leftarrow Y \rightarrow\right] \circ \left[X\right] = \left[X \bullet Y\right]_{1\times 1} ,$$

for all $X, Y \in \mathbb{R}^n$.

9.1.3 — Actions of Partitioned Matrices

Theorem 9.1.18 ☞ **A fundamental formula for the action of a partitioned matrix**

If $\mathcal{A}$ is a $(7|1|5) \times (5|1|5|3)$ partitioned matrix (see below), and $X \oplus Y \oplus Z \oplus V \in \mathbb{R}^5 \oplus \mathbb{R}^1 \oplus \mathbb{R}^5 \oplus \mathbb{R}^3$, then

$$\begin{bmatrix} \mathcal{A}_{11} & \mathcal{A}_{12} & \mathcal{A}_{13} & \mathcal{A}_{14} \\ \mathcal{A}_{21} & \mathcal{A}_{22} & \mathcal{A}_{23} & \mathcal{A}_{24} \\ \mathcal{A}_{31} & \mathcal{A}_{32} & \mathcal{A}_{33} & \mathcal{A}_{34} \end{bmatrix} \begin{pmatrix} X \\ Y \\ Z \\ V \end{pmatrix} = \begin{pmatrix} \mathcal{A}_{11}(X) + \mathcal{A}_{12}(Y) + \mathcal{A}_{13}(Z) + \mathcal{A}_{14}(V) \\ \mathcal{A}_{21}(X) + \mathcal{A}_{22}(Y) + \mathcal{A}_{23}(Z) + \mathcal{A}_{24}(V) \\ \mathcal{A}_{31}(X) + \mathcal{A}_{32}(Y) + \mathcal{A}_{33}(Z) + \mathcal{A}_{34}(V) \end{pmatrix}.$$

It is clear that the rightmost tuple in the formula is in $\mathbb{R}^7 \oplus \mathbb{R}^1 \oplus \mathbb{R}^5$.

Notation 9.1.19

Based on Theorem 9.1.18, we shall occasionally write

$$\mathcal{A} : \mathbb{R}^5 \oplus \mathbb{R}^1 \oplus \mathbb{R}^5 \oplus \mathbb{R}^3 \longrightarrow \mathbb{R}^7 \oplus \mathbb{R}^1 \oplus \mathbb{R}^5$$

to declare that $\mathcal{A}$ is a $(7|1|5) \times (5|1|5|3)$ partitioned matrix.

Proof of Theorem 9.1.18. First of all,

$$\begin{pmatrix} X \\ Y \\ Z \\ V \end{pmatrix} = \begin{pmatrix} X \\ \mathbb{O} \\ \mathbb{O} \\ \mathbb{O} \end{pmatrix} + \begin{pmatrix} \mathbb{O} \\ Y \\ \mathbb{O} \\ \mathbb{O} \end{pmatrix} + \begin{pmatrix} \mathbb{O} \\ \mathbb{O} \\ Z \\ \mathbb{O} \end{pmatrix} + \begin{pmatrix} \mathbb{O} \\ \mathbb{O} \\ \mathbb{O} \\ V \end{pmatrix}.$$

Since matrices are linear functions, if we can demonstrate that

$$\mathcal{A}\begin{pmatrix} X \\ \mathbb{O} \\ \mathbb{O} \\ \mathbb{O} \end{pmatrix} = \begin{pmatrix} \mathcal{A}_{11}(X) \\ \mathcal{A}_{21}(X) \\ \mathcal{A}_{31}(X) \end{pmatrix}, \quad \mathcal{A}\begin{pmatrix} \mathbb{O} \\ Y \\ \mathbb{O} \\ \mathbb{O} \end{pmatrix} = \begin{pmatrix} \mathcal{A}_{12}(Y) \\ \mathcal{A}_{22}(Y) \\ \mathcal{A}_{32}(Y) \end{pmatrix}, \quad \dots, \quad \mathcal{A}\begin{pmatrix} \mathbb{O} \\ \mathbb{O} \\ \mathbb{O} \\ V \end{pmatrix} = \begin{pmatrix} \mathcal{A}_{14}(V) \\ \mathcal{A}_{24}(V) \\ \mathcal{A}_{34}(V) \end{pmatrix}, \tag{9.6}$$

the required result will follow.

The arguments demonstrating the validity of the four equalities (9.6) are very similar. We shall only verify the second equality, and leave the rest to the reader as an exercise.

To do so we apply the technique of matrixation, based on the formula (9.4) in TYC 9.1.15. The reader should pay close attention to the implicit use of tuple concatenation and matrix partitioning in the following derivation, which establishes the required equality.

$$\left[\mathcal{A}\begin{pmatrix}\mathbb{O}\\ Y\\ \mathbb{O}\\ \mathbb{O}\end{pmatrix}\right]_{13\times 1} \overset{(9.4)}{=} \mathcal{A}\circ\left[\begin{pmatrix}\mathbb{O}\\ Y\\ \mathbb{O}\\ \mathbb{O}\end{pmatrix}\right]_{14\times 1} = \mathcal{A}\circ\begin{bmatrix}\mathcal{O}\\ [Y]\\ \mathcal{O}\\ \mathcal{O}\end{bmatrix}_{(5|1|5|3)\times 1} \overset{\text{Thm. 9.1.8}}{=} \begin{bmatrix}\mathcal{A}_{12}\circ[Y]\\ \mathcal{A}_{22}\circ[Y]\\ \mathcal{A}_{32}\circ[Y]\end{bmatrix}_{(7|1|5)\times 1}$$

$$\overset{(9.4)}{=} \begin{bmatrix}[\mathcal{A}_{12}(Y)]\\ [\mathcal{A}_{22}(Y)]\\ [\mathcal{A}_{32}(Y)]\end{bmatrix}_{(7|1|5)\times 1} = \left[\begin{pmatrix}\mathcal{A}_{12}(Y)\\ \mathcal{A}_{22}(Y)\\ \mathcal{A}_{32}(Y)\end{pmatrix}\right]_{13\times 1}.$$

■

Theorem 9.1.20 ☞ **The jectivity of $\left[\begin{smallmatrix}\mathcal{A} & \mathcal{B}\\ \mathcal{O} & \mathcal{D}\end{smallmatrix}\right]$ and $\left[\begin{smallmatrix}\mathcal{X} & \mathcal{O}\\ \mathcal{Y} & \mathcal{Z}\end{smallmatrix}\right]$**

1. If $\left[\begin{smallmatrix}\mathcal{A} & \mathcal{B}\\ \mathcal{O} & \mathcal{D}\end{smallmatrix}\right]$ is injective then so is $\mathcal{A}$.
2. If $\left[\begin{smallmatrix}\mathcal{A} & \mathcal{B}\\ \mathcal{O} & \mathcal{D}\end{smallmatrix}\right]$ is surjective then so is $\mathcal{D}$.
3. If $\left[\begin{smallmatrix}\mathcal{X} & \mathcal{O}\\ \mathcal{Y} & \mathcal{Z}\end{smallmatrix}\right]$ is surjective then so is $\mathcal{X}$.
4. If $\left[\begin{smallmatrix}\mathcal{X} & \mathcal{O}\\ \mathcal{Y} & \mathcal{Z}\end{smallmatrix}\right]$ is injective then so is $\mathcal{Z}$.

Proof of Theorem 9.1.20. We shall verify the first two claims, and leave the last two to the reader (Exercise 9.1.21).

Let us assume that $\left[\begin{smallmatrix}\mathcal{A} & \mathcal{B}\\ \mathcal{O} & \mathcal{D}\end{smallmatrix}\right]$ is a partitioned $n\times m$ matrix, and $\mathcal{D}$ is a $k\times l$ matrix.

1. Suppose that $\left[\begin{smallmatrix}\mathcal{A} & \mathcal{B}\\ \mathcal{O} & \mathcal{D}\end{smallmatrix}\right]$ is injective. To show that $\mathcal{A}$ is injective, we will show that $\mathcal{A}(X)=\mathcal{A}(Y)$ can take place only if $X=Y$.
   If $\mathcal{A}(X)=\mathcal{A}(Y)$, then
   $$\left[\begin{smallmatrix}\mathcal{A} & \mathcal{B}\\ \mathcal{O} & \mathcal{D}\end{smallmatrix}\right]\left(\begin{smallmatrix}X\\ \mathbb{O}\end{smallmatrix}\right) \overset{\text{Thm. 9.1.18}}{=} \left(\begin{smallmatrix}\mathcal{A}(X)+\mathcal{B}(\mathbb{O})\\ \mathcal{O}(V)+\mathcal{D}(\mathbb{O})\end{smallmatrix}\right) = \left(\begin{smallmatrix}\mathcal{A}(X)\\ \mathbb{O}\end{smallmatrix}\right) = \left(\begin{smallmatrix}\mathcal{A}(Y)\\ \mathbb{O}\end{smallmatrix}\right) = \cdots = \left[\begin{smallmatrix}\mathcal{A} & \mathcal{B}\\ \mathcal{O} & \mathcal{D}\end{smallmatrix}\right]\left(\begin{smallmatrix}Y\\ \mathbb{O}\end{smallmatrix}\right).$$
   Since we are assuming that $\left[\begin{smallmatrix}\mathcal{A} & \mathcal{B}\\ \mathcal{O} & \mathcal{D}\end{smallmatrix}\right]$ is injective, it must be that
   $$\left(\begin{smallmatrix}X\\ \mathbb{O}\end{smallmatrix}\right) = \left(\begin{smallmatrix}Y\\ \mathbb{O}\end{smallmatrix}\right),$$
   and the equality of X and Y follows.

2. Suppose that $\left[\begin{smallmatrix}\mathcal{A} & \mathcal{B}\\ \mathcal{O} & \mathcal{D}\end{smallmatrix}\right]$ is a surjective, and consider an unspecified $W\in\mathbb{R}^k$. By showing that this W is necessarily in the range of $\mathcal{D}$ we will establish that $\mathcal{D}$ is surjective.
   Consider $\left(\begin{smallmatrix}\mathbb{O}\\ W\end{smallmatrix}\right)\in\mathbb{R}^{n-k}\oplus\mathbb{R}^k$. Since the range of $\left[\begin{smallmatrix}\mathcal{A} & \mathcal{B}\\ \mathcal{O} & \mathcal{D}\end{smallmatrix}\right]$ is all of $\mathbb{R}^n$, there

exists $\left(\begin{smallmatrix} P \\ Q \end{smallmatrix}\right)$ such that

$$\left(\begin{smallmatrix} \mathbb{O} \\ W \end{smallmatrix}\right) = \left[\begin{smallmatrix} \mathcal{A} & \mathcal{B} \\ \mathcal{O} & \mathcal{D} \end{smallmatrix}\right]\left(\begin{smallmatrix} P \\ Q \end{smallmatrix}\right) \overset{\text{Thm. 9.1.18}}{=} \left(\begin{smallmatrix} \mathcal{A}(P)+\mathcal{B}(Q) \\ \mathcal{D}(Q) \end{smallmatrix}\right) \in \mathbb{R}^{n-k} \oplus \mathbb{R}^{k} \,. \tag{9.7}$$

Hence $W = \mathcal{D}(Q)$, which shows that $W \in \mathit{Range}(\mathcal{D})$. ■

Exercise 9.1.21

Prove the last two claims of Theorem 9.1.20.

Hint: : An easy way to see this is to take all of the matrices not mentioned in the conclusion of each of the original implications to be null.

Test Your Comprehension 9.1.22

Argue that none of the converse implications of the implications in Theorem 9.1.20 hold true in general.

9.2 Direct Sums of Matrices

Notation 9.2.1

If we start with two matrices A and B of respective sizes $n \times m$ and $p \times q$ we can amalgamate these into a single matrix expressed as a partitioned matrix

$$\left[\begin{smallmatrix} A & \mathcal{O} \\ \mathcal{O} & B \end{smallmatrix}\right]_{(n|p)\times(m|q)} .$$

This matrix is said to be a **direct sum** of $\mathcal{A}$ and $\mathcal{B}$, and is denoted by

$$\mathcal{A} \boxplus \mathcal{B} \,.$$

Example 9.2.2

For example,

$$\begin{bmatrix} -3 & 5 \\ 1 & -2 \end{bmatrix} \boxplus \begin{bmatrix} 1 & -3 & 2 \\ 4 & 6 & 0 \end{bmatrix} = \begin{bmatrix} -3 & 5 & 0 & 0 & 0 \\ 1 & -2 & 0 & 0 & 0 \\ 0 & 0 & 1 & -3 & 2 \\ 0 & 0 & 4 & 6 & 0 \end{bmatrix} .$$

Test Your Comprehension 9.2.3

Argue that the operation $\boxplus$ is associative, but is NOT commutative. Don't forget that a partitioned matrix is just a matrix with an overlay.

Test Your Comprehension 9.2.4

Under what circumstances is the formula

$$\begin{bmatrix} \mathcal{A} & \mathcal{O} \\ \mathcal{O} & \mathcal{B} \end{bmatrix} \begin{pmatrix} X \\ Y \end{pmatrix} = \begin{pmatrix} \mathcal{A}(X) \\ \mathcal{B}(Y) \end{pmatrix}$$

valid? What about

$$\begin{bmatrix} \mathcal{A} & \mathcal{O} & \mathcal{O} \\ \mathcal{O} & \mathcal{B} & \mathcal{O} \\ \mathcal{O} & \mathcal{O} & \mathcal{C} \end{bmatrix} \begin{pmatrix} X \\ Y \\ Z \end{pmatrix} = \begin{pmatrix} \mathcal{A}(X) \\ \mathcal{B}(Y) \\ \mathcal{C}(Z) \end{pmatrix} \ ?$$

How would you express these formulas in "inline" notation using $\boxplus$ and $\oplus$?

Test Your Comprehension 9.2.5 ☞ **Operations with direct sums**

Argue that the following hold true when the sizes and the partitions of the matrices are appropriate (in each case).

1. $\alpha\,(\mathcal{A} \boxplus \mathcal{B} \boxplus \mathcal{C}) = (\alpha\mathcal{A}) \boxplus (\alpha\mathcal{B}) \boxplus (\alpha\mathcal{C})$.

2. $(\mathcal{A} \boxplus \mathcal{B} \boxplus \mathcal{C}) + (\mathcal{D} \boxplus \mathcal{P} \boxplus \mathcal{Q}) = (\mathcal{A} + \mathcal{D}) \boxplus (\mathcal{B} + \mathcal{P}) \boxplus (\mathcal{C} + \mathcal{Q})$.

3. $(\mathcal{A} \boxplus \mathcal{B} \boxplus \mathcal{C}) \circ (\mathcal{D} \boxplus \mathcal{P} \boxplus \mathcal{Q}) = (\mathcal{A} \circ \mathcal{D}) \boxplus (\mathcal{B} \circ \mathcal{P}) \boxplus (\mathcal{C} \circ \mathcal{Q})$.

4. $(\mathcal{A} \boxplus \mathcal{B} \boxplus \mathcal{C})^5 = \mathcal{A}^5 \boxplus \mathcal{B}^5 \boxplus \mathcal{C}^5$.

5. $(\mathcal{A} \boxplus \mathcal{B} \boxplus \mathcal{C})^T = \mathcal{A}^T \boxplus \mathcal{B}^T \boxplus \mathcal{C}^T$.

Hint: "Unwrap" the notation in each case and work with partitioned matrices of the form

$$\begin{bmatrix} \square & \mathcal{O} & \dots & \mathcal{O} \\ \mathcal{O} & \square & \dots & \mathcal{O} \\ \vdots & \vdots & \ddots & \vdots \\ \mathcal{O} & \mathcal{O} & \dots & \square \end{bmatrix}.$$

Exercise 9.2.6 ☞ **Jectivity of $\mathcal{A} \boxplus \mathcal{B}$**

Verify the following claims.

1. $\mathcal{A} \boxplus \mathcal{B}$ is injective exactly when $\mathcal{A}$ and $\mathcal{B}$ are injective.

2. $\mathcal{A} \boxplus \mathcal{B}$ is surjective exactly when $\mathcal{A}$ and $\mathcal{B}$ are surjective.

Once these claims are verified, it is clear that $\mathcal{A} \boxplus \mathcal{B}$ is invertible exactly when $\mathcal{A}$ and $\mathcal{B}$ are invertible. Show that in this case

$$(\mathcal{A} \boxplus \mathcal{B})^{-1} = \mathcal{A}^{-1} \boxplus \mathcal{B}^{-1}\ .$$

Theorem 9.2.7 ☞ **Jectivity and invertibility of direct sums**

1. $\mathcal{A} \boxplus \mathcal{B} \boxplus \mathcal{C}$ is injective exactly when $\mathcal{A}$, $\mathcal{B}$ and $\mathcal{C}$ are injective.

2. $\mathcal{A} \boxplus \mathcal{B} \boxplus \mathcal{C}$ is surjective exactly when $\mathcal{A}$, $\mathcal{B}$ and $\mathcal{C}$ are surjective.

Once these claims are verified, it is clear that

$\mathcal{A} \boxplus \mathcal{B} \boxplus \mathcal{C}$ is invertible exactly when $\mathcal{A}$, $\mathcal{B}$ and $\mathcal{C}$ are invertible.

Show that in this case

$$(\mathcal{A} \boxplus \mathcal{B} \boxplus \mathcal{C})^{-1} = \mathcal{A}^{-1} \boxplus \mathcal{B}^{-1} \boxplus \mathcal{C}^{-1} .$$

Proof of Theorem 9.2.7. We shall verify the first claim of the theorem, and leave the rest as an exercise to the reader (Exercise 9.2.8).

Let us write $\mathcal{D}$ for the matrix $\mathcal{B} \boxplus \mathcal{C}$. The reader can easily see that $\mathcal{A} \boxplus \mathcal{D}$ is exactly the same matrix as $\mathcal{A} \boxplus \mathcal{B} \boxplus \mathcal{C}$, but the partitioning of this matrix differs in the two cases.

Consequently the first two statements on the list below are equivalent. Starting with the second statement, each statement is equivalent to the next, by Exercise 9.2.6.

1. $\mathcal{A} \boxplus \mathcal{B} \boxplus \mathcal{C}$ is injective.

2. $\mathcal{A} \boxplus \mathcal{D}$ is injective.

3. $\mathcal{A}$ and $\mathcal{D}$ are injective.

4. $\mathcal{A}$ and $\mathcal{B}$ and $\mathcal{C}$ are injective. ■

Exercise 9.2.8

Prove the second and the third claims in Theorem 9.2.7.

It should now be fairly clear to the reader that Theorem 9.2.7 can be extended to the case of any number of direct summands, and is a generalization of the Exercise 6.4.7 which stated that a diagonal matrix is invertible exactly when when all of its diagonal entries are non-zero, and in that case the inverse is obtained by reciprocating the diagonal entries.

The fundamental formula for partitioned matrix multiplication can be used to generalize the results of Exercise 8.1.27 which dealt with the effects of multiplying a matrix by a diagonal matrix. In the following exercise we explore the effects of multiplying a partitioned matrix by a block-diagonal (partitioned) matrix.

Test Your Comprehension 9.2.9 ☞ **Multiplying by a block-diagonal matrix**

1. Verify that the following formula is valid for the appropriately partitioned matrices.

$$\begin{bmatrix} \mathcal{A}_1 & \mathcal{O} & \dots & \mathcal{O} \\ \mathcal{O} & \mathcal{A}_2 & \dots & \mathcal{O} \\ \vdots & \vdots & \ddots & \vdots \\ \mathcal{O} & \mathcal{O} & \dots & \mathcal{A}_n \end{bmatrix} \begin{bmatrix} \mathcal{B}_{11} & \mathcal{B}_{12} & \dots & \mathcal{B}_{1m} \\ \mathcal{B}_{21} & \mathcal{B}_{22} & \dots & \mathcal{B}_{2m} \\ \vdots & \vdots & \ddots & \vdots \\ \mathcal{B}_{n1} & \mathcal{B}_{n2} & \dots & \mathcal{B}_{nm} \end{bmatrix} = \begin{bmatrix} \mathcal{A}_1\mathcal{B}_{11} & \mathcal{A}_1\mathcal{B}_{12} & \dots & \mathcal{A}_1\mathcal{B}_{1m} \\ \mathcal{A}_2\mathcal{B}_{21} & \mathcal{A}_2\mathcal{B}_{22} & \dots & \mathcal{A}_2\mathcal{B}_{2m} \\ \vdots & \vdots & \ddots & \vdots \\ \mathcal{A}_n\mathcal{B}_{n1} & \mathcal{A}_n\mathcal{B}_{n2} & \dots & \mathcal{A}_n\mathcal{B}_{nm} \end{bmatrix}.$$

2. Verify that the following formula is valid for the appropriately partitioned matrices.

$$\begin{bmatrix} \mathcal{B}_{11} & \mathcal{B}_{12} & \dots & \mathcal{B}_{1m} \\ \mathcal{B}_{21} & \mathcal{B}_{22} & \dots & \mathcal{B}_{2m} \\ \vdots & \vdots & \ddots & \vdots \\ \mathcal{B}_{n1} & \mathcal{B}_{n2} & \dots & \mathcal{B}_{nm} \end{bmatrix} \begin{bmatrix} \mathcal{C}_1 & \mathcal{O} & \dots & \mathcal{O} \\ \mathcal{O} & \mathcal{C}_2 & \dots & \mathcal{O} \\ \vdots & \vdots & \ddots & \vdots \\ \mathcal{O} & \mathcal{O} & \dots & \mathcal{C}_n \end{bmatrix} = \begin{bmatrix} \mathcal{B}_{11}\mathcal{C}_1 & \mathcal{B}_{12}\mathcal{C}_2 & \dots & \mathcal{B}_{1m}\mathcal{C}_m \\ \mathcal{B}_{21}\mathcal{C}_1 & \mathcal{B}_{22}\mathcal{C}_2 & \dots & \mathcal{B}_{2m}\mathcal{C}_m \\ \vdots & \vdots & \ddots & \vdots \\ \mathcal{B}_{n1}\mathcal{C}_1 & \mathcal{B}_{n2}\mathcal{C}_2 & \dots & \mathcal{B}_{nm}\mathcal{C}_m \end{bmatrix}.$$

Exercise 9.2.10

Verify that the following formula is valid for the appropriately partitioned matrices with square blocks on the diagonal, under the assumption that $\mathcal{C}_1 \boxplus \mathcal{C}_2 \boxplus \cdots \boxplus \mathcal{C}_n$ is invertible.

$$\begin{bmatrix} \mathcal{C}_1 & \mathcal{O} & \dots & \mathcal{O} \\ \mathcal{O} & \mathcal{C}_2 & \dots & \mathcal{O} \\ \vdots & \vdots & \ddots & \vdots \\ \mathcal{O} & \mathcal{O} & \dots & \mathcal{C}_n \end{bmatrix}^{-1} \begin{bmatrix} \mathcal{A}_1 & \square & \dots & \square \\ \mathcal{O} & \mathcal{A}_2 & \dots & \square \\ \vdots & \vdots & \ddots & \vdots \\ \mathcal{O} & \mathcal{O} & \dots & \mathcal{A}_n \end{bmatrix} \begin{bmatrix} \mathcal{C}_1 & \mathcal{O} & \dots & \mathcal{O} \\ \mathcal{O} & \mathcal{C}_2 & \dots & \mathcal{O} \\ \vdots & \vdots & \ddots & \vdots \\ \mathcal{O} & \mathcal{O} & \dots & \mathcal{C}_n \end{bmatrix} = \begin{bmatrix} \mathcal{C}_1^{-1}\mathcal{A}_1\mathcal{C}_1 & \triangle & \dots & \triangle \\ \mathcal{O} & \mathcal{C}_2^{-1}\mathcal{A}_2\mathcal{C}_2 & \dots & \triangle \\ \vdots & \vdots & \ddots & \vdots \\ \mathcal{O} & \mathcal{O} & \dots & \mathcal{C}_n^{-1}\mathcal{A}_n\mathcal{C}_n \end{bmatrix}$$

Exercise 9.2.11

Suppose that a partitioned diagonal matrix $\mathcal{A} \in \mathbb{M}_n$ has the form

$$\begin{bmatrix} \alpha_1\mathcal{I}_{k_1} & \mathcal{O} & \dots & \mathcal{O} \\ \mathcal{O} & \alpha_2\mathcal{I}_{k_2} & \dots & \mathcal{O} \\ \vdots & \vdots & \ddots & \vdots \\ \mathcal{O} & \mathcal{O} & \dots & \alpha_l\mathcal{I}_{k_l} \end{bmatrix}, \quad \text{where } \alpha_1, \dots, \alpha_l \text{ are distinct}.$$

Argue that a matrix $\mathcal{B}$ commutes with $\mathcal{A}$ (i.e. $\mathcal{A}\mathcal{B} = \mathcal{B}\mathcal{A}$) exactly when $\mathcal{B}$ can be partitioned as

$$\begin{bmatrix} \mathcal{B}_1 & \mathcal{O} & \dots & \mathcal{O} \\ \mathcal{O} & \mathcal{B}_2 & \dots & \mathcal{O} \\ \vdots & \vdots & \ddots & \vdots \\ \mathcal{O} & \mathcal{O} & \dots & \mathcal{B}_l \end{bmatrix}, \quad \text{with } \mathcal{B}_i \in \mathbb{M}_{k_i}.$$

Hint: TYC 9.2.9 can be very helpful here. Do a test run first with $l = 4$ and $\alpha_1, \ldots, \alpha_l$ being $3, -2, 7, \pi$.

In other words, the only matrices that commute with an $n \times n$ diagonal matrix

$$\alpha_1 \mathcal{I}_{k_1} \boxplus \alpha_2 \mathcal{I}_{k_2} \boxplus \cdots \boxplus \alpha_l \mathcal{I}_{k_l} \text{ , with } \textit{distinct } \alpha_1, \ldots, \alpha_l \text{ ,}$$

are the $n \times n$ matrices of the form

$$\mathcal{B}_1 \boxplus \mathcal{B}_2 \boxplus \cdots \boxplus \mathcal{B}_l \text{ , with } \mathcal{B}_i \in \mathbb{M}_{k_i} \text{ .}$$

Comment 9.2.12

The condition that $\alpha_1, \ldots, \alpha_l$ are *distinct* is essential in Exercise 9.2.11. For example, in the extreme case that all of the α's are equal, $\mathcal{A}$ is a scalar multiple of $\mathcal{I}_n$ and thus commutes with ALL $n \times n$ matrices.

Test Your Comprehension 9.2.13

Verify that the 4×4 diagonal matrices are the only matrices that commute with the matrix

$$\begin{bmatrix} 3 & 0 & 0 & 0 \\ 0 & -2 & 0 & 0 \\ 0 & 0 & \frac{4}{7} & 0 \\ 0 & 0 & 0 & \pi \end{bmatrix}.$$

9.3 Appendix: Exiled Proofs

Proof of Theorem 9.1.8. As part of the hypothesis the vertical partitioning of $\mathcal{A}$ coincides with the horizontal partitioning of $\mathcal{B}$, and this has been indicated through the use of colors.

Let us not forget that $\mathcal{A}$ is just a 13×14 matrix (partitioned in a $(7|1|5) \times (5|1|5|3)$ pattern). $\mathcal{B}$ is a 14×28 matrix. So $\mathcal{AB}$ certainly makes sense, and is a 13×28 matrix.

In particular $\mathcal{AB}$ can be partitioned according to a pattern $(7|1|5) \times (9|28)$, and in that case $\mathcal{AB}$ and $\mathcal{B}$ have identical vertical partitioning. Similarly $\mathcal{AB}$ and $\mathcal{A}$ have identical horizontal partitioning.

The rest of the proof should be done via an illustration (INSERT PICTURE) ...

■

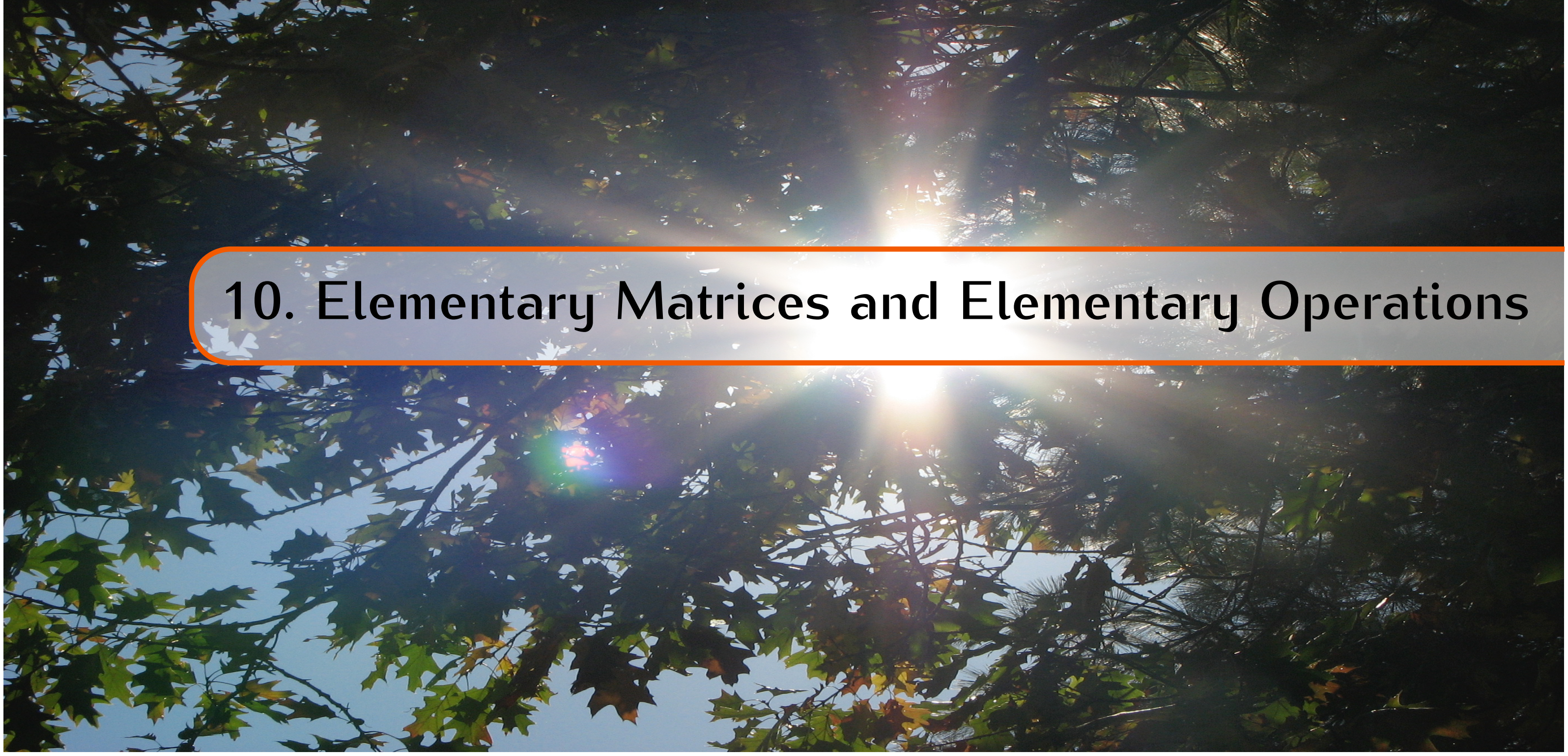
Proof of Theorem 9.1.11. One feature of the ever-so-useful strategy of partitioning matrices is that we are frequently able to "boost" a result about partitioned matrices with just 2 block-rows and 2 block-columns to more general partitioned matrices with very little effort.

This is the case in the present setting, and shall be a common feature of our approach in what follows. The claim of the theorem in the case when each of the two partitioned matrices in question has 2 block-rows and 2 block-columns has been established already in TYC 9.1.9.

Next we consider a case of the partitioned matrices $\mathcal{M}$ and $\mathcal{N}$ with k block-rows and k block-columns, where $k > 2$.

■

III Row And Column Reduction



10. Elementary Matrices and Elementary Operations

Last modified on December 8, 2018

10.1 Elementary Matrices

Notation 10.1.1

There are three types of **elementary matrices**, and we have encountered all three in Exercise 6.1.9. We will use the letter $\mathcal{E}$ in our notation for the elementary matrices.

The reason these three types gained prominence is that they are essential to Gauss-Jordan Elimination Scheme which we shall present in a later chapter.

10.1.1 — Swaps

Terminology 10.1.2

For $i \neq j$, a **swap** $\overset{[i]\leftrightarrow[j]}{\mathcal{E}}$ is a function that acts by swapping the i-th and the j-th entries of an input, and leaving all other entries as they were. For example,

$$\overset{[4]\leftrightarrow[2]}{\mathcal{E}} \begin{pmatrix} x \\ y \\ z \\ u \\ v \\ w \end{pmatrix} = \begin{pmatrix} x \\ u \\ z \\ y \\ v \\ w \end{pmatrix} .$$

It is easy to check that swaps have the property (6.4) and thus are matrices.

A swap $\overset{[2]\leftrightarrow[5]}{\mathcal{E}}$ sends the second standard basis tuple to the fifth, the fifth – to the second, and all other standard basis tuples – to themselves. So

$$\overset{[2]\leftrightarrow[5]}{\mathcal{E}} = \left[E_1 \;\; E_5 \;\; E_3 \;\; E_4 \;\; E_2 \;\; \cdots \right] .$$

Since

$$\mathcal{I} = \left[E_1 \;\; E_2 \;\; E_3 \;\; E_4 \;\; E_5 \;\; \cdots \right] ,$$

this establishes the following result.

Theorem 10.1.3 ☞ **Constructing $\overset{[2]\leftrightarrow[5]}{\mathcal{E}}$ from $\mathcal{I}$**

$\overset{[2]\leftrightarrow[5]}{\mathcal{E}}$ is obtained from the identity matrix by swapping the second and the fifth columns.

Of course this generalizes to all swaps $\overset{[i]\leftrightarrow[j]}{\mathcal{E}}$.

Example 10.1.4

For example, in the 6×6 setting,

$$\overset{[2]\leftrightarrow[5]}{\mathcal{E}} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & \mathbf{0} & 0 & 0 & \mathbf{1} & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & \mathbf{1} & 0 & 0 & \mathbf{0} & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}.$$

10.1.2 — Partial Scalings

Terminology 10.1.5

A **partial scaling** $\overset{\alpha\cdot[i]}{\mathcal{E}}$ **(with a *<u>non-zero</u>* weight α)** is a function which acts by multiplying the i-th entry of an input by α, and leaving all other entries alone.

For example,

$$\overset{\sqrt{3}\cdot[2]}{\mathcal{E}} \begin{pmatrix} x \\ y \\ z \\ u \\ v \end{pmatrix} = \begin{pmatrix} x \\ \sqrt{3}\, y \\ z \\ u \\ v \end{pmatrix}$$

It is easy to see that partial scalings satisfy the identity (6.4) and thus are matrices.

A partial scaling $\overset{-\pi\cdot[3]}{\mathcal{E}}$ sends E_3 to $-\pi \cdot E_3$, and sends all other standard basis tuples to themselves. So,

$$\overset{-\pi\cdot[3]}{\mathcal{E}} = \begin{bmatrix} E_1 & E_2 & (-\pi \cdot E_3) & E_4 & \cdots \end{bmatrix},$$

and in particular we have the following result.

Theorem 10.1.6 ☞ **Constructing $\overset{-\pi\cdot[3]}{\mathcal{E}}$ from $\mathcal{I}$**

$\overset{-\pi\cdot[3]}{\mathcal{E}}$ is obtained from the identity matrix by scaling the third column by $-\pi$, or equivalently by replacing the third diagonal entry of the identity matrix by $-\pi$.

This generalizes to all partial scalings $\overset{\alpha\cdot[i]}{\mathcal{E}}$.

Example 10.1.7

For example, in the 6×6 setting,

$$\overset{\alpha\cdot[4]}{\mathcal{E}} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & \alpha & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}.$$

10.1.3 — Shears

Terminology 10.1.8

For $i \neq j$, a **shear** $\overset{[j]\leftarrow\!+\,\alpha\cdot[i]}{\mathcal{E}}$ **(with a *non-zero* weight α)** is a function that acts by adding to the j-th entry of an input, α times the i-th entry, while leaving all entries (beside the j-th) as they were.

For example,

$$\overset{[5]\leftarrow\!+\,\frac{1}{2}\cdot[3]}{\mathcal{E}} \begin{pmatrix} x \\ y \\ z \\ u \\ v \end{pmatrix} = \begin{pmatrix} x \\ y \\ z \\ u \\ v+\frac{1}{2}z \end{pmatrix}.$$

Shears satisfy the identity (6.4) and thus are matrices.

A shear $\overset{[5]\leftarrow\!+\,\frac{1}{2}\cdot[3]}{\mathcal{E}}$ sends E_3 to $E_3 + \frac{1}{2}E_5$, and sends all other standard basis tuples to themselves (note a reversal of indices here). So,

$$\overset{[5]\leftarrow\!+\,\frac{1}{2}\cdot[3]}{\mathcal{E}} = \begin{bmatrix} E_1 & E_2 & \left(E_3 + \dfrac{1}{2}E_5\right) & E_4 & E_5 & \cdots \end{bmatrix}.$$

This leads to the following result.

Theorem 10.1.9 ☞ **Constructing $\overset{[5]\leftarrow+\frac{1}{2}\cdot[3]}{\mathcal{E}}$ from $\mathcal{I}$**

$\overset{[5]\leftarrow+\frac{1}{2}\cdot[3]}{\mathcal{E}}$ is obtained from $\mathcal{I}$ by adding to the 3-rd column the 5-th column scaled by $\frac{1}{2}$. All other columns, apart from the 3-rd, are left alone. (*Note the index reversal!*)

Equivalently, $\overset{[5]\leftarrow+\frac{1}{2}\cdot[3]}{\mathcal{E}}$ is obtained from $\mathcal{I}$ by replacing the zero in the $[\![5,3]\!]$ position with $\frac{1}{2}$.

General shears $\overset{[j]\leftarrow+\alpha\cdot[i]}{\mathcal{E}}$ can be obtained in a similar fashion.

Example 10.1.10

For example, in the 6×6 setting,

$$\overset{[3]\leftarrow+\alpha\cdot[1]}{\mathcal{E}} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ \alpha & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}.$$

Test Your Comprehension 10.1.11

Demonstrate that $\overset{[4]\leftarrow+\alpha\cdot[7]}{\mathcal{E}} = \mathcal{I} + \alpha\mathcal{M}_{4,7}$, where $\mathcal{M}_{4,7}$ is a matrix unit (Trm. 8.5.6).

10.1.4 — Basic Properties Of Elementary Matrices

Test Your Comprehension 10.1.12

Argue that an identity function is an elementary matrix.

Test Your Comprehension 10.1.13 ☞ **Constructing elementary matrices from $\mathcal{I}$ via row operations**

Verify the following claims.

1. $\overset{[2]\leftrightarrow[5]}{\mathcal{E}}$ can be also obtained from $\mathcal{I}$ by swapping the second and the fifth ROWS.

2. $\overset{-\pi\cdot[3]}{\mathcal{E}}$ can be also obtained from the identity matrix by scaling the third ROW by $-\pi$.

3. $\overset{[5] \leftarrow+ \frac{1}{2}\cdot[3]}{\mathcal{E}}$ can also be obtained from $\mathcal{I}$ by adding to the 5-th ROW the 3-rd ROW scaled by $\frac{1}{2}$. All other ROWS, apart from the 5-th, are left alone.

Test Your Comprehension 10.1.14 ☞ **Transposes of elementary matrices are elementary**

Verify that the following identities hold in every appropriate $n \times m$ matrix setting.

1. $\left(\overset{[2]\leftrightarrow[5]}{\mathcal{E}}\right)^T = \overset{[2]\leftrightarrow[5]}{\mathcal{E}}$.

2. $\left(\overset{-\pi\cdot[3]}{\mathcal{E}}\right)^T = \overset{-\pi\cdot[3]}{\mathcal{E}}$.

3. $\left(\overset{[5] \leftarrow+ \frac{1}{2}\cdot[3]}{\mathcal{E}}\right)^T = \overset{[3] \leftarrow+ \frac{1}{2}\cdot[5]}{\mathcal{E}}$.

In particular, the transpose of an elementary matrix is an elementary matrix of the same type.

Exercise 10.1.15 ☞ **All elementary matrices are invertible**

Argue that the following identities hold.

1. $\overset{[2]\leftrightarrow[5]}{\mathcal{E}} \circ \overset{[2]\leftrightarrow[5]}{\mathcal{E}} = \mathcal{I}$.

2. $\overset{-\pi\cdot[3]}{\mathcal{E}} \circ \overset{\frac{1}{-\pi}\cdot[3]}{\mathcal{E}} = \overset{\frac{1}{-\pi}\cdot[3]}{\mathcal{E}} \circ \overset{-\pi\cdot[3]}{\mathcal{E}} = \mathcal{I}$.

3. $\overset{[5] \leftarrow+ \frac{1}{2}\cdot[3]}{\mathcal{E}} \circ \overset{[5] \leftarrow+ \frac{-1}{2}\cdot[3]}{\mathcal{E}} = \overset{[5] \leftarrow+ \frac{-1}{2}\cdot[3]}{\mathcal{E}} \circ \overset{[5] \leftarrow+ \frac{1}{2}\cdot[3]}{\mathcal{E}} = \mathcal{I}$.

Similarly one can verify the general formulas (the reader is encouraged but is NOT required to do so):

1. $\left(\overset{[i]\leftrightarrow[j]}{\mathcal{E}}\right)^{-1} = \overset{[i]\leftrightarrow[j]}{\mathcal{E}}$;

2. $\left(\overset{\alpha\cdot[i]}{\mathcal{E}}\right)^{-1} = \overset{\frac{1}{\alpha}\cdot[i]}{\mathcal{E}}$;

3. $\left(\overset{[j]\leftarrow+\alpha\cdot[i]}{\mathcal{E}}\right)^{-1} = \overset{[j]\leftarrow+-\alpha\cdot[i]}{\mathcal{E}}$.

In particular, these formulas show the inverse of an elementary matrix is an elementary matrix of the same type.

Exercise 10.1.16 ☞ **Products of partial scalings**

Argue that a product of partial scalings is a diagonal matrix, and that every diagonal matrix can be expressed as a product of partial scalings.

In other words, the diagonal matrices are exactly the matrices that can be expressed as products of partial scalings.

Exercise 10.1.17 ☞ **Products of swaps**

Suppose that a matrix $\mathcal{A}$ can be expressed a product of a number of swaps. Argue that $\mathcal{A}$ is invertible, and that

$$\mathcal{A}^{-1} = \mathcal{A}^{T}.$$

Hint: How does the inverse of a swap relate to its transpose?

Later on we will characterize the matrices that can be expressed as products of just swaps. These are said to be *the permutation matrices*.

We shall also show that matrices which can be expressed as products of just shears are exactly the matrices with *determinant* 1.

Of course the discussion of these concepts is yet to come.

Theorem 10.1.18 ☞ **Transforming tuples into E_1**

If Z is a non-null n-tuple, then there exist elementary matrices $\mathcal{E}_1, \mathcal{E}_2, \ldots, \mathcal{E}_n \in \mathbb{M}_n$ such that

$$\mathcal{E}_n \cdots \mathcal{E}_2\mathcal{E}_1(Z) = \begin{pmatrix} 1 \\ 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix} = E_1.$$

In other words, we can transform any non-null n-tuple into E_1 through an application of (at most) n elementary matrices in sequence.

A proof of Theorem 10.1.18 is presented in the appendix to the chapter.

10.2 Elementary Operations

10.2.1 — Elementary Row Operations

In this portion of the chapter we explore the effect of multiplying a matrix $\mathcal{A}$ by an elementary matrix $\mathcal{E}$ from the left. Let us say

$$\mathcal{A} = [C_1 \quad C_2 \quad C_3 \quad \ldots \quad C_m].$$

Then

$$\mathcal{E}\mathcal{A} = \left[\mathcal{E}\left(C_1\right) \quad \mathcal{E}\left(C_2\right) \quad \mathcal{E}\left(C_3\right) \quad \ldots \quad \mathcal{E}\left(C_m\right)\right].$$

Case 1: $\mathcal{E} = \overset{[i]\leftrightarrow[j]}{\mathcal{E}}$.

Here $\mathcal{E}\left(C_k\right)$ is obtained from C_k by swapping the i-th and the j-th entries of the latter. In other words, the columns of $\mathcal{E}\mathcal{A}$ are obtained from the columns of $\mathcal{A}$ by swapping their i-th and the j-th entries.

If we color the i-th entry of each column green, and the j-th entry – blue, we have colored the whole i-th row of $\mathcal{A}$ green, and the j-th – blue. Performing the swapping of the green and blue entries within each column amounts to swapping the green and the blue rows of $\mathcal{A}$.

Let us record this.

> $\overset{[i]\leftrightarrow[j]}{\mathcal{E}}\mathcal{A}$ is obtained from $\mathcal{A}$ by swapping the i-th and the j-th rows of $\mathcal{A}$, and leaving all other rows as they were.

Case 2: $\mathcal{E} = \overset{\alpha\cdot[i]}{\mathcal{E}}$.

In this case $\mathcal{E}\left(C_k\right)$ is obtained from C_k by multiplying the i-th entry of the latter by α. If we color the i-th entry of each column green, we have colored the whole i-th row of $\mathcal{A}$ green. Multiplying the i-th entry of each column by α amounts to scaling the whole i-th row of $\mathcal{A}$ by α.

> $\overset{\alpha\cdot[i]}{\mathcal{E}}\mathcal{A}$ is obtained from $\mathcal{A}$ by scaling the i-th row of $\mathcal{A}$ by α.

Case 3: $\mathcal{E} = \overset{[j]+\alpha\cdot[i]}{\mathcal{E}}$.

Now $\mathcal{E}\left(C_k\right)$ is obtained from C_k by adding to the j-th entry of the latter α times the i-th entry. Again imagine coloring the i-th entry of each column green, and the j-th entry – blue, thus coloring the whole i-th row of $\mathcal{A}$ green, and the j-th – blue. Performing the described operation within each column amounts to adding to the blue row of $\mathcal{A}$, α times the green row.

> $\overset{[j]+\alpha\cdot[i]}{\mathcal{E}}\mathcal{A}$ is obtained from $\mathcal{A}$ by adding to the j-th row of $\mathcal{A}$, α times the i-th row.

Terminology 10.2.1

Based on these results we introduce the concept of **(elementary) row operations** on matrices. There are three types of row operations.

Swap Two Rows: Swap two rows of a matrix, leaving all other rows as they were.

Scale a Row: Scale a row of a matrix by a NON-ZERO scalar.

Adjust a Row: Add to a given row of a matrix a NON-ZERO multiple of another row.

Let us summarize.

Theorem 10.2.2 ☞ **Row operations amount to a multiplication by an elementary matrix from the left**

Performing an elementary row operation on a matrix $\mathcal{A}$ is equivalent to multiplying $\mathcal{A}$ by a corresponding elementary matrix $\mathcal{E}$ on the left.

Observation 10.2.3 ☞ **Elementary row operations do not affect the jectivity**

Performing an elementary row operation on a matrix $\mathcal{A}$ produces a matrix equivalent to $\mathcal{A}$, and hence does not alter the jectivity of a matrix (TYC 8.2.4).

Hint: Make use of TYC 8.5.2 and Thm. 10.2.2.

Test Your Comprehension 10.2.4 ☞ **Row operations preserve null columns**

Argue that if the j-th column of a matrix is null, and we perform a row operation on the matrix, the resulting matrix still has a null j-th column.

10.2.2 — Elementary Column Operations

As we have observed, multiplying a matrix $\mathcal{A}$ by an elementary matrix $\mathcal{E}$ from the left amounts to performing an elementary row operation on $\mathcal{A}$. It is now natural to consider the effects of the multiplication by an elementary matrix $\mathcal{E}$ from the right. The reader should not be surprised to see that this involves elementary column operations on $\mathcal{A}$.

Terminology 10.2.5

There are three types of **elementary column operations** on matrices .

Swap Two Columns: Swap two columns of a matrix, leaving all other columns as they were.

Scale a Column: Scale a column of a matrix by a NON-ZERO scalar.

Adjust a Column: Add to a given column a NON-ZERO multiple of another column of the matrix.

Test Your Comprehension 10.2.6 ☞ **Column operations via row operations and the transpose**

Argue that performing an elementary column operation on a matrix $\mathcal{A}$ is equivalent to the following procedure:

1. Transpose $\mathcal{A}$.

2. Perform the corresponding elementary *row* operation on $\mathcal{A}^{T}$, and arrive at a matrix $\mathcal{B}$.

3. Transpose $\mathcal{B}$.

Since we have already established that performing an elementary row operation on a matrix amounts to multiplying it from the left by an appropriate elementary matrix (Theorem 10.2.2), we can leverage this via TYC 10.2.6 into a result about elementary column operations.

$$\Downarrow$$

Theorem 10.2.7 ☞ **Column operations amount to a multiplication by an elementary matrix from the right**

Performing an elementary column operation on a matrix amounts to multiplying it from the right by an appropriate elementary matrix.

Here are the details:

1. To swap the i-th and the j-th columns of $\mathcal{A}$: form $\mathcal{A}\overset{[i]\leftrightarrow[j]}{\mathcal{E}}$.

2. To scale the j-th column of $\mathcal{A}$ by $\alpha \neq 0$: form $\mathcal{A}\overset{\alpha\cdot[j]}{\mathcal{E}}$.

3. To adjust the j-th column of $\mathcal{A}$ by adding to it α times the i-th column: form $\mathcal{A}\overset{[i]\leftarrow\!\!+\,\alpha\cdot[j]}{\mathcal{E}}$. (Note the index reversal.)

Proof of Theorem 10.2.7. By TYC 10.2.6 and Theorem 10.2.2, swapping i-th and j-th columns of $\mathcal{A}$ transforms $\mathcal{A}$ into

$$\left(\overset{[i]\leftrightarrow[j]}{\mathcal{E}}\mathcal{A}^{T}\right)^{T}.$$

The latter matrix is equal to $\left(\mathcal{A}^{T}\right)^{T}\left(\overset{[i]\leftrightarrow[j]}{\mathcal{E}}\right)^{T}$, which in turn equals

$$\mathcal{A}\overset{[i]\leftrightarrow[j]}{\mathcal{E}}.$$

This establishes the validity of the first claim.

The justification of the other two claims follows exactly the same path, and we leave it to the reader as an exercise (TYC 10.2.8). ■

Test Your Comprehension 10.2.8

Establish the remaining two claims of Theorem 10.2.7.

Test Your Comprehension 10.2.9 ☞ **Elementary column operations do not affect the jectivity**

Argue that performing an elementary column operation on a matrix $\mathcal{A}$ produces a matrix equivalent to $\mathcal{A}$, and hence does not alter the jectivity of a matrix (TYC 8.2.4).

Test Your Comprehension 10.2.10 ☞ **Elementary column operations do not affect the range**

Argue that performing an elementary column operation on a matrix $\mathcal{A}$ produces a matrix with the same range as $\mathcal{A}$.

In particular, rearranging the order in which the columns of a matrix appear has no bearing on the range of the matrix.

Hint: Performing a column operation on $\mathcal{A}$ amounts to multiplying $\mathcal{A}$ by an elementary matrix from the right. Elementary matrices are bijective. Exc. 2.3.10 can be useful here.

Comment 10.2.11 ☞ **Elementary *row* operations may alter the range**

For example, matrix $\begin{bmatrix} 0 & 0 \\ 1 & 1 \end{bmatrix}$ is obtained from a matrix $\begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix}$ via a row swap, yet these two matrices have different ranges. For example, $\begin{pmatrix} 0 \\ 1 \end{pmatrix}$ is in the range of the former, but is not in the range of the latter.

Exercise 10.2.12 ☞ **SWAP DIAG SWAP sandwich**

Suppose that $\mathcal{D} \in \mathbb{M}_n$ is a diagonal matrix. Argue that $\overset{[i]\leftrightarrow[j]}{\mathcal{E}} \; \mathcal{D} \; \overset{[i]\leftrightarrow[j]}{\mathcal{E}}$ is the diagonal matrix obtained from $\mathcal{D}$ by swapping the diagonal entries appearing in the $[\![i, i]\!]$ and $[\![j, j]\!]$ positions.

Theorem 10.2.13 **Inverse formula for 2×2 matrices**

Matrix $\left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right]$ is invertible exactly when $ad - bc \neq 0$, and in that case

$$\left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right]^{-1} = \tfrac{1}{ad-bc}\left[\begin{smallmatrix} d & -b \\ -c & a \end{smallmatrix}\right].$$

Proof of Theorem 10.2.13. It is a straight forward exercise on matrix multiplication to verify that

$$\left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right] \circ \left(\tfrac{1}{ad-bc}\left[\begin{smallmatrix} d & -b \\ -c & a \end{smallmatrix}\right]\right) = \left[\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right] = \tfrac{1}{ad-bc}\left[\begin{smallmatrix} d & -b \\ -c & a \end{smallmatrix}\right] \circ \left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right], \tag{10.1}$$

whenever $ad - bc \neq 0$.

What remains to be shown is that the invertibility of $\left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right]$ entails $ad - bc \neq 0$.

Let us consider the two possibilities: $a \neq 0$ and $a = 0$.

<u>Case 1</u>: $\left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right]$ is invertible and $a \neq 0$.

We will carry out a number of elementary row and column operations on our matrix $\left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right]$ to produce simpler matrices. Keep in mind that these operations do not affect the jectivity (Obs. 10.2.3 and 10.2.9).

1. Scale the first row of $\left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right]$ by $\frac{1}{a}$ to arrive at $\left[\begin{smallmatrix} 1 & \frac{b}{a} \\ c & d \end{smallmatrix}\right]$.
2. Adjust the second row of $\left[\begin{smallmatrix} 1 & \frac{b}{a} \\ c & d \end{smallmatrix}\right]$ by subtracting from it c times the first row. This produces the matrix $\left[\begin{smallmatrix} 1 & \frac{b}{a} \\ 0 & d-\frac{bc}{a} \end{smallmatrix}\right]$.
3. Adjust the second column of $\left[\begin{smallmatrix} 1 & \frac{b}{a} \\ 0 & d-\frac{bc}{a} \end{smallmatrix}\right]$ by subtracting from it $\frac{b}{a}$ times the first column. The resulting matrix is $\left[\begin{smallmatrix} 1 & 0 \\ 0 & d-\frac{bc}{a} \end{smallmatrix}\right]$.

Since $\left[\begin{smallmatrix} 1 & 0 \\ 0 & d-\frac{bc}{a} \end{smallmatrix}\right]$ must be invertible, none of its diagonal entries are zero (Exc. 6.4.7). So $d - \frac{bc}{a} \neq 0$, or equivalently, $ad - bc \neq 0$.

We have established that $ad - bc \neq 0$ whenever $\left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right]$ is invertible and $a \neq 0$.

<u>Case 2</u>: $\left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right]$ is invertible and $a = 0$.

In this case it must be that $c \neq 0$ (otherwise $\left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right]$ would have a null column, and so would not be injective by Exercise 6.4.1).

Swap the rows of $\left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right]$ to arrive at an invertible matrix $\left[\begin{smallmatrix} c & d \\ 0 & b \end{smallmatrix}\right]$ which we will denote by $\mathcal{B}$. $\mathcal{B}$ falls under our Case 1, since its north-west entry (c) is not zero. Hence it must be that $cb - 0d \neq 0$. In our case this is exactly the inequality $ad - bc \neq 0$, and so we are done. ■

Terminology 10.2.14

The tell-tale quantity $ad - bc$ appearing in Theorem 10.2.13 is said to be **the determinant** of $\left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right]$. It determines the invertibility of the matrix.

The matrix $\left[\begin{smallmatrix} d & -b \\ -c & a \end{smallmatrix}\right]$ is said to be **the classical adjoint** of $\left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right]$. It is the inverse of $\left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right]$ scaled by the determinant, whenever the latter is not zero.

These concepts will be generalized to apply to square matrices of all sizes later in the book.

10.3 Fitting Polynomials To Data; Revisited

Let us recall the problem of fitting polynomial to data that we discussed in Section 5.4.

Given any seven pairs $(a_1, b_1), \dots, (a_7, b_7)$ of real numbers, where $a_1, a_2, \dots, a_7$ are distinct, we seek a polynomial p such that

$$p(a_i) = b_i?$$

Using Cartesian coordinates for a plane, one can associate to each pair of numbers a point on the plane, so that, geometrically speaking, the task is to find a polynomial whose graph goes through all of the marked points.

Test Your Comprehension 10.3.1

Why are we imposing a condition that all a_i's are distinct?

We shall demonstrate that there is exactly one polynomial of degree at most 6 which fits the bill. Later (see TYC 12.1.8) we shall show that there are always infinitely many polynomials of any degree higher than 6 which can also do the job.

Test Your Comprehension 10.3.2

By emulating the steps of a concrete case presented in Section 5.4, reduce the problem to that of finding scalars $c_0, c_1, c_2, \dots, c_6$ such that

$$\begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_7 \end{pmatrix} = c_0 \begin{pmatrix} 1 \\ 1 \\ \vdots \\ 1 \end{pmatrix} + c_1 \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_7 \end{pmatrix} + c_2 \begin{pmatrix} a_1^2 \\ a_2^2 \\ \vdots \\ a_7^2 \end{pmatrix} + \cdots + c_6 \begin{pmatrix} a_1^7 \\ a_2^7 \\ \vdots \\ a_7^7 \end{pmatrix}.$$

So, we are trying to find a 7-tuple $C := \begin{pmatrix} c_0 \\ c_1 \\ \vdots \\ c_6 \end{pmatrix}$ such that

$$\begin{bmatrix} 1 & a_1 & a_1^2 & \dots & a_1^6 \\ 1 & a_2 & a_2^2 & \dots & a_2^6 \\ 1 & a_3 & a_3^2 & \dots & a_3^6 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & a_7 & a_7^2 & \dots & a_7^6 \end{bmatrix}_{7\times 7} (C) = \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_7 \end{pmatrix}.$$

In other words, we are looking for an input into a 7×7 matrix that produces a given output. If we can demonstrate that our 7×7 matrix is invertible, then we would know that there is a unique input 7-tuple that produces any given output 7-tuple.

The matrix we are dealing with depends only on the scalars $a_1, a_2, \dots, a_7$, and has a very particular form.

Terminology 10.3.3

A matrix of the form

$$\begin{bmatrix} 1 & a & a^2 & \dots & a^k \\ 1 & b & b^2 & \dots & b^k \\ 1 & c & c^2 & \dots & c^k \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \zeta & \zeta^2 & \dots & \zeta^k \end{bmatrix}_{(k+1)\times(k+1)}$$

is called a **Vandermonde matrix** and is denoted by the symbol $\mathcal{V}_{k+1}(a, b, c, \dots, \zeta)$.

Each row of this matrix is a geometric progression.

Test Your Comprehension 10.3.4 ☞ **A Vandermonde matrix with repeated rows is NOT invertible**

Verify that a Vandermonde matrix $\mathcal{V}_{k+1}(a, b, c, \dots, \zeta)$ is not invertible when two of the values $a, b, c, \dots, \zeta$ are equal.

Theorem 10.3.5 ☞ **A Vandermonde matrix with distinct rows is invertible**

$\mathcal{V}_{k+1}(a, b, c, \dots, \zeta)$ is invertible exactly when $a, b, c, \dots, \zeta$ are all distinct.

Our eventual proof of Theorem 10.3.5 will rely on the following auxiliary result.

Lemma 10.3.6 ☞ **Vandermonde descent**

The following statements are equivalent for *distinct* scalars $a, b, c, \ldots, \zeta$.

1. $\mathcal{V}_{k+1}(a, b, c, \ldots, \zeta)$ is invertible.

2. $\mathcal{V}_{k}(b, c, \ldots, \zeta)$ is invertible.

Let us show how this lemma furnishes a proof of Theorem 10.3.5.

Proof of Theorem 10.3.5. We shall carry out the argument in the case we presented at the start of this section: i.e. that of $\mathcal{V}_7\left(a_1, a_2, \ldots, a_7\right)$. A general argument shall become apparent in the process.

By Lemma 10.3.6, each of the following statements is equivalent to its neighbour statements, and so all of these statements are equivalent to each other.

1. $\mathcal{V}_7\left(a_1, a_2, \ldots, a_7\right)$ is invertible.
2. $\mathcal{V}_6\left(a_2, a_3, \ldots, a_7\right)$ is invertible.
3. $\mathcal{V}_5\left(a_3, a_4, \ldots, a_7\right)$ is invertible.
4. $\mathcal{V}_4\left(a_4, a_5, \ldots, a_7\right)$ is invertible.
5. $\vdots$
6. $\mathcal{V}_2\left(a_6, a_7\right)$ is invertible.

Now,

$$\mathcal{V}_2\left(a_6, a_7\right) = \begin{bmatrix} 1 & a_6 \\ 1 & a_7 \end{bmatrix},$$

and so has a non-zero determinant $a_7 - a_6$, which indicates that $\mathcal{V}_2\left(a_6, a_7\right)$ is invertible (Thm. 10.2.13).

Hence the last statement on our list is true, and so all the others, including the first one, are true. ■

We shall lead the reader through a proof of Lemma 10.3.6 in the case of $\mathcal{V}_7\left(a_1, a_2, \ldots, a_7\right)$ and $\mathcal{V}_6\left(a_2, a_3, \ldots, a_7\right)$. A general argument follows exactly the same steps.

Exercise 10.3.7 ☞ **Proof of Lemma 10.3.6**

1. Adjust the last column of $\mathcal{V}_7\left(a_1, a_2, \ldots, a_7\right)$ by subtracting from it a_1 times the sixth column, thus arriving at a matrix we shall call $\mathcal{T}_7$.

2. Adjust the sixth column of $\mathcal{T}_7$ by subtracting from it a_1 times the fifth column, thus arriving at a matrix we shall call $\mathcal{T}_6$.

3. Adjust the fifth column of $\mathcal{T}_6$ by subtracting from it a_1 times the fourth column, thus arriving at a matrix $\mathcal{T}_5$.

4. Proceed this way until you arrive at $\mathcal{T}_2$.

5. Adjust the second row of $\mathcal{T}_2$ by subtracting from it the first row, thus arriving at a matrix we shall call $\mathcal{Q}_2$.

6. Adjust the third row of $\mathcal{Q}_2$ by subtracting from it the first row, thus arriving at a matrix we shall call $\mathcal{Q}_3$.

7. Proceed this way until you arrive at $\mathcal{Q}_7$ which has a partitioned form
$$\begin{bmatrix} 1 & O \\ O & \mathcal{M} \end{bmatrix}_{(1|6)\times(1|6)} .$$

8. Apply an appropriate sequence of partial scalings of the rows of $\mathcal{Q}_7$ to produce a matrix
$$\begin{bmatrix} 1 & O \\ O & \mathcal{V}_6(a_2, a_3, \ldots, a_7) \end{bmatrix} .$$

9. Argue that $\mathcal{V}_7\left(a_1, a_2, \ldots, a_7\right)$ is invertible exactly when $\mathcal{V}_6\left(a_2, a_3, \ldots, a_7\right)$ is invertible.

Hint: Observations 10.2.3 and 10.2.9, and Exc. 9.2.6.

10.4 Appendix: Exiled Proofs

Proof of Theorem 10.1.18.

Case 1: The first entry α of Z is not zero.

In this case the first entry of $Z_1 := \overset{\frac{1}{\alpha}\cdot[1]}{\mathcal{E}}(Z)$ is 1. So, by applying an elementary matrix (perhaps $\mathcal{I}$) to Z we arrive at an n-tuple of the form
$$Z_1 = \begin{pmatrix} 1 \\ a_2 \\ a_3 \\ \vdots \\ a_n \end{pmatrix} .$$

If $a_2 = 0$, let $Z_2 := Z_1 = \mathcal{I}\left(Z_1\right)$. If $a_2 \neq 0$, let $Z_2 := \overset{[2]\leftarrow -a_2\cdot[1]}{\mathcal{E}}\left(Z_1\right)$.

In either case, Z_2 has the form
$$\begin{pmatrix} 1 \\ 0 \\ a_3 \\ \vdots \\ a_n \end{pmatrix} .$$

If $a_3 = 0$, let $Z_3 := Z_2 = \mathcal{I}\left(Z_2\right)$. If $a_3 \neq 0$, let $Z_3 := \overset{[3]\leftarrow -a_3\cdot[1]}{\mathcal{E}}\left(Z_2\right)$.

In either case, Z_3 has the form

$$\begin{pmatrix} 1 \\ 0 \\ 0 \\ a_4 \\ \vdots \\ a_n \end{pmatrix}.$$

Proceed this way to arrive (eventually) at

$$Z_n = \begin{pmatrix} 1 \\ 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}.$$

In this case, by applying n elementary matrices in sequence, we transformed Z into E_1.

Note that we used the identity matrix every time we encountered a zero entry a_i. These identity matrices can be removed from the process without changing the outcome. Hence, in the present case, if Z has k zero entries ($0 \leq k < n$), by applying $n - k$ elementary matrices in sequence, we transformed Z into E_1.

Case 2: The first entry of Z is zero.

If the first entry of Z is zero, and say, the fourth is not, then the first entry of $\overset{[1]\leftrightarrow[4]}{\mathcal{E}}(Z)$ is not zero. So, after applying a swap to Z we arrive at an n-tuple Z_o with a non-zero first entry *and at least one zero entry*.

Given the observation made at the end of Case 1, by applying $n-1$ elementary matrices in sequence, we can transform Z_o into E_1. Therefore we can transform Z into E_1 by applying n elementary matrices in sequence. ■

Additional Commentary on the Proof of Theorem 10.2.13. The first part of our proof of Theorem 10.2.13 was based on the verification of the identity (10.1). This is effective but is not educationally satisfying, as is often the case. The matrix $\frac{1}{ad-bc}\begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$ was proverbially "pulled out of a hat", and no indication has been given as to its genesis.

To see a path to the formula, let us consider the setting of our Case 1. The reader should observe that

$$\mathcal{C} = \overset{[2]\leftarrow + -c\cdot[1]}{\mathcal{E}} \; \overset{\frac{1}{a}\cdot[1]}{\mathcal{E}} \; \mathcal{A} \; \overset{[1]\leftarrow + -\frac{b}{a}\cdot[2]}{\mathcal{E}}. \tag{10.2}$$

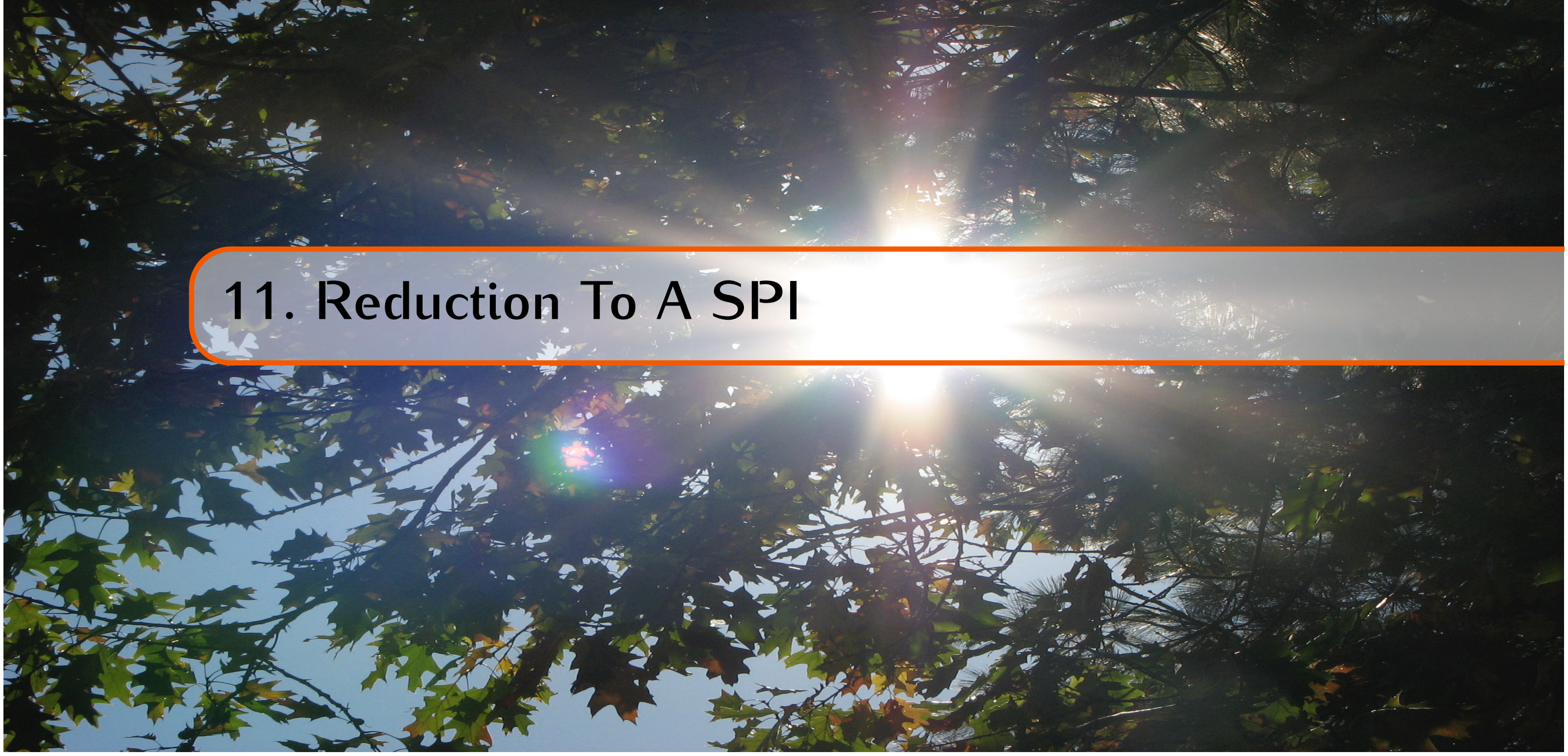
By using TYC 10.1.15 we can move the elementary matrices in (10.2) over to the left side of the equation via inversion, and rewrite the equation as

$$\mathcal{A} = \overset{[2] \leftarrow\!+\, c\cdot[1]}{\mathcal{E}} \; \overset{a\cdot[1]}{\mathcal{E}} \, \mathcal{C} \; \overset{[1] \leftarrow\!+\, \frac{b}{a}\cdot[2]}{\mathcal{E}} \; .$$

Then

$$\mathcal{A}^{-1} = \overset{[1] \leftarrow\!+\, -\frac{b}{a}\cdot[2]}{\mathcal{E}} \, \mathcal{C}^{-1} \; \overset{\frac{1}{a}\cdot[1]}{\mathcal{E}} \; \overset{[2] \leftarrow\!+\, -c\cdot[1]}{\mathcal{E}} \; . \tag{10.3}$$

Now the required formula for $\mathcal{A}^{-1}$ can be obtained by multiplying together the four matrices on the right side of (10.3). Keep in mind that the inverse of the diagonal matrix $\mathcal{C}$ is obtained by reciprocating its diagonal entries. ■



11. Reduction To A SPI

Last modified on December 8, 2018

11.1 Reduction To A SPI

By performing a sequence of elementary row and column operations it is always possible to convert a given non-null matrix to a matrix of just zeros and ones, with the 1's marching down diagonally (for a while) starting from the North-West corner of the matrix.

We develop the strategy for doing so in a number of steps.

Test Your Comprehension 11.1.1

Suppose that $\mathcal{A}$ is a non-null matrix. Argue that by performing at most one column swap, at most one row swap and at most one scaling, we can transform $\mathcal{A}$ into a matrix $\mathcal{B}$ such that $\mathcal{B}[\![1,1]\!] = 1$.

Test Your Comprehension 11.1.2

Suppose that $\mathcal{B}$ is an $n \times m$ matrix such that $\mathcal{B}[\![1,1]\!] = 1$. Argue that by performing at most $n+m-2$ row and column adjustments, we can transform $\mathcal{B}$ into a matrix $\mathcal{C}$ of the form

$$\begin{bmatrix} 1 & 0 & \cdots & 0 & 0 \\ 0 & \square & \cdots & \square & \square \\ 0 & \square & \cdots & \square & \square \\ \vdots & \vdots & & \vdots & \vdots \\ 0 & \square & \cdots & \square & \square \end{bmatrix}_{n \times m},$$

where we include the possibility that this matrix has just one column, or just one row, or both, in which case the picture has to be adjusted accordingly.

Of course we can express $\mathcal{C}$ more concisely as a partitioned matrix

$$\begin{bmatrix} 1 & \mathcal{O} \\ \mathcal{O} & \mathcal{M} \end{bmatrix}_{(1|n-1)\times(1|m-1)}. \tag{11.1}$$

Test Your Comprehension 11.1.3

Suppose that we have a matrix $\mathcal{C}$ of the form (11.1).

1. Verify that when $n > 1$, elementary row operations *which do not involve the first row*, will not alter the zeros in the first column, and amount to the corresponding row operations performed on the matrix $\mathcal{M}$.

2. Verify that when $m > 1$, a similar statement holds with regards to performing elementary column operations *that do not involve the first column*.

Test Your Comprehension 11.1.4

Suppose that we have a matrix $\mathcal{C}$ of the form (11.1), where m and n are bigger than 1, and $\mathcal{M}$ is not null.

Use the results of TYC's 11.1.1, 11.1.2 and 11.1.3 to argue that by performing at most $n + m - 1$ elementary row and column operations we can transform $\mathcal{C}$ into a matrix of the form

$$\begin{bmatrix} 1 & 0 & 0 & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & \diamond & \cdots & \diamond \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & \diamond & \cdots & \diamond \end{bmatrix}_{n \times m},$$

which can be expressed as a partitioned matrix

$$\begin{bmatrix} \mathcal{I}_2 & \mathcal{O} \\ \mathcal{O} & \mathcal{K} \end{bmatrix}_{(2|n-2)\times(2|m-2)}. \tag{11.2}$$

Test Your Comprehension 11.1.5 **Reduction to a SPI**

By iterating the procedure laid out in TYC's 11.1.1, 11.1.2, 11.1.3, and Exercise 11.1.4, verify that elementary row and column operations can be used to transform every non-null matrix into a matrix in one of the following forms.

I: $\begin{bmatrix} \mathcal{I} & \mathcal{O} \\ \mathcal{O} & \mathcal{O} \end{bmatrix}$

II: $\begin{bmatrix} \mathcal{I} \\ \mathcal{O} \end{bmatrix}$

III: $[\mathcal{I} \ \ \mathcal{O}]$

IV: $\mathcal{I}$

As is the case with most algebraically intensive and time-consuming algorithms, one should resort to machines to carry out the procedure in all cases that are not trivial.

Exercise 11.1.6

Argue that the process described in TYC 11.1.5 can be carried out using no more than
$$\min(n, m) \cdot \Big(\max(n, m) + 2 \Big) - 1$$
elementary row and column operations.

Terminology 11.1.7

Matrices of the four forms listed in TYC 11.1.5 are said to be **standard partial isometries (SPI's for short)**.

The 1's in a SPI are said to be its **pivots**, and the number of 1's is said to its **rank**.

A SPI is completely determined by its size and its rank.

It turns out to be notationally convenient to *declare a null matrix to be a SPI of rank* 0, even though a null matrix is NOT an isometry (a term that we will define in due time).

We shall introduce the meaning of the terms involved in the nomenclature "standard partial isometry" later in the text. For now the reader should treat these three words as a single term.

Example 11.1.8

Here are some SPI's:

$$\begin{bmatrix} 1&0&0&0\\0&1&0&0\\0&0&0&0 \end{bmatrix}, \quad \begin{bmatrix} 1&0&0&0\\0&1&0&0\\0&0&1&0 \end{bmatrix}, \quad \begin{bmatrix} 1&0&0\\0&0&0\\0&0&0 \end{bmatrix}, \quad \begin{bmatrix} 1&0&0\\0&1&0\\0&0&1 \end{bmatrix}, \quad \begin{bmatrix} 1&0&0\\0&1&0\\0&0&1\\0&0&0 \end{bmatrix}, \quad \begin{bmatrix} 1&0&0\\0&0&0\\0&0&0\\0&0&0 \end{bmatrix}, \quad \begin{bmatrix} 0&0&0\\0&0&0\\0&0&0\\0&0&0 \end{bmatrix},$$

and the ranks of these SPI's are $2, 3, 1, 3, 3, 1, 0$ respectively.

Performing elementary operations amounts to multiplying the matrix by an elementary matrix from an appropriate side. Therefore we can interpret the result of Exercise 11.1.5 as follows.

$$\Downarrow$$

Theorem 11.1.9

For any matrix $\mathcal{A}$ there exist elementary matrices $\mathcal{E}_i$ and $\mathcal{F}_j$ such that
$$\mathcal{E}_t\,\mathcal{E}_{t-1}\ldots\mathcal{E}_2\,\mathcal{E}_1\,\mathcal{A}\,\mathcal{F}_1\,\mathcal{F}_2\ldots\mathcal{F}_{s-1}\,\mathcal{F}_s$$
is a SPI.

Of course here the $\mathcal{E}_i$'s correspond to the row operations and $\mathcal{F}_j$'s – to the column operations.

Test Your Comprehension 11.1.10

Argue that every matrix is equivalent to a SPI.

Exercise 11.1.11

Suppose that students are given a list of row operations and a list of column operations to be performed (in their respective orders) on a matrix $\mathcal{A}$. Yet the instructions omit any directive on alternating between the row operations and the column operations.

One student decides to perform the list of all row operations first, followed by the list of all column operations.

Another student does the opposite: all column operations first and then all row operations.

Another student decides to alternate row and column operations for as long as possible.

Another student does a few column operations, then a few row operations, etc.

Will all of these students, on the same matrix $\mathcal{A}$, necessarily arrive at the same matrix in the end?

Justify your answer.

11.2 SPI's, Jectivity And Transposition

Exercise 11.2.1

Argue that

1. SPI's of type **I** are non-jective;
2. SPI's of type **II** are injective but are not surjective;
3. SPI's of type **III** are surjective but are not injective;
4. $\mathcal{I}$ is the only invertible SPI.

In particular, argue that for a square SPI's other than the 1×1 null matrix, its "all or nothing": either it is $\mathcal{I}$ or it is non-jective.

As we already know (Observations 10.2.3 and 10.2.9), elementary row and column operations do not alter the size or the jectivity of a matrix. Since every matrix can be reduced to a SPI via elementary row and column operations, we are now able to discern the jectivity of a matrix by examining a SPI it can be reduced to.

Test Your Comprehension 11.2.2 **Affect of a matrix's shape on its possible jectivity**

Argue that the following claims are valid.

1. Strictly portrait-shaped matrices are never surjective.
2. Strictly landscape-shaped matrices are never injective.
3. Only square matrices may be invertible.

Test Your Comprehension 11.2.3

Argue that equivalent matrices must be of the same size.

Hint: TYC 11.2.2.

Test Your Comprehension 11.2.4 **The jectivity of square matrices**

Argue that for a square matrix $\mathcal{A}$ the following statements are equivalent.

1. $\mathcal{A}$ is bijective.
2. $\mathcal{A}$ is injective.
3. $\mathcal{A}$ is surjective.

Theorem 11.2.5 **Equivalent SPI's are equal**

Distinct SPI's are not (matrix-)equivalent.

A proof of Theorem 11.2.5 is presented in the appendix to the chapter.

Test Your Comprehension 11.2.6

Argue that a matrix cannot be equivalent to two distinct SPI's.

Hint: Use Thm. 11.2.5 and the transitivity of matrix equivalence relation.

Putting TYC 11.1.10 and Theorem 11.2.5 together we arrive at the following conclusion.

Theorem 11.2.7 **Uniqueness of SPI's**

Every matrix $\mathcal{A}$ is equivalent to exactly one SPI, which we shall denote by $\mathrm{SPI}(\mathcal{A})$, and refer to as **the SPI of $\mathcal{A}$**.

Even though for each $\mathcal{A}$, $\mathrm{SPI}(\mathcal{A})$ is the only SPI equivalent to $\mathcal{A}$, there are *always infinitely many different pairs* of invertible matrices $\mathcal{T}$ and $\mathcal{S}$ such that $\mathcal{T}\mathcal{A}\mathcal{S} = \mathrm{SPI}(\mathcal{A})$.

Notation 11.2.8

The **rank of a matrix** $\mathcal{A}$ is defined to be the rank of SPI($\mathcal{A}$), and is denoted by $Rank(\mathcal{A})$.

As we shall see, this notion of rank is equivalent to several others, and it turns out that the rank of a matrix is a measure of the size for its range. Furthermore, the rank of a matrix is intimately related to a measure of the size of its nullspace as well. All of this shall be explored later in the text.

Exercise 11.2.9

Argue that the following statements are equivalent for $n \times m$ matrices $\mathcal{A}$ and $\mathcal{C}$.

1. $\mathcal{A} \equiv \mathcal{C}$.
2. SPI($\mathcal{A}$) = SPI($\mathcal{C}$) .
3. $Rank(\mathcal{A}) = Rank(\mathcal{C})$.

Hint: Use Thm. 11.2.7 and the transitivity of matrix equivalence. Recall that a SPI is completely determined by its size and rank.

In due time we will be able to characterize left-equivalence and right-equivalence of matrices in somewhat similar terms.

The result of Exercise 11.2.9 offers an easy test for matrix equivalence: simply check if the matrices have the same SPI's.

Test Your Comprehension 11.2.10 ☞ **Jectivity and transposition for SPI's**

Validate the following claims.

1. A transpose of a SPI is a SPI of the same rank.
2. The following are equivalent for a SPI $\mathcal{A}$:
   (a) $\mathcal{A}$ is injective;
   (b) $\mathcal{A}^T$ is surjective.
3. The following are equivalent for a SPI $\mathcal{A}$:
   (a) $\mathcal{A}$ is surjective;
   (b) $\mathcal{A}^T$ is injective.

We shall say that transposition interchanges injectivity and surjectivity of SPI's, or **flips the jectivity** of SPI's, for short.

Performing row operations on a matrix is clearly related to performing column operations on its transpose. The same goes for column operations. In this sense performing row and column operations on a matrix is related to performing column and row operations on its transpose.

If some row and column operations transform a matrix $\mathcal{A}$ into its SPI, then the corresponding column and row operations on $\mathcal{A}^T$ should transform it into the transpose of SPI($\mathcal{A}$), which is still a SPI. So the transpose of SPI($\mathcal{A}$) should be SPI$\left(\mathcal{A}^T\right)$. This is indeed the case.

Theorem 11.2.11

$$\mathrm{SPI}\left(\mathcal{A}^T\right) = \left(\mathrm{SPI}(\mathcal{A})\right)^T .$$

Proof of Theorem 11.2.11. By Theorem 11.2.7, every matrix is equivalent to exactly one SPI. Hence it shall be sufficient to show that $\left(\mathrm{SPI}(\mathcal{A})\right)^T$ is a SPI equivalent to $\mathcal{A}^T$.

We have already observed that a transpose of a SPI is a SPI of the same rank (TYC 11.2.10).

The proof will be complete as soon as we show that $\left(\mathrm{SPI}(\mathcal{A})\right)^T$ is equivalent to $\mathcal{A}^T$. Yet we know that $\mathcal{A}$ is equivalent to SPI($\mathcal{A}$), and so the required result follows by Exercise 8.2.5. ∎

Test Your Comprehension 11.2.12 ☞ **Transposition does not change rank**

Argue that

$$\mathit{Rank}(\mathcal{A}) = \mathit{Rank}\left(\mathcal{A}^T\right) ,$$

for any matrix $\mathcal{A}$.

Test Your Comprehension 11.2.13

Argue that every *square* matrix is equivalent to its transpose.

(The claim makes no sense for non-square matrices.)

Hint: Exc. 11.2.9 and TYC 11.2.12.

Since equivalent matrices have the same jectivity, and every matrix is equivalent to its SPI, Theorem 11.2.11 can be used to extend the result of TYC 11.2.10 to all matrices.

Theorem 11.2.14 ☞ **Transposition switches the jectivity**

The following statements are equivalent for a matrix $\mathcal{A}$.

1. $\mathcal{A}$ is injective.
2. $\mathcal{A}^{T}$ is surjective.

Similarly the following statements are equivalent.

1. $\mathcal{A}$ is surjective.
2. $\mathcal{A}^{T}$ is injective.

We express this by saying that transposition interchanges injectivity and surjectivity of a matrix; i.e. flips the jectivity.

Proof of Theorem 11.2.14. Each of the following statements is equivalent to its neighbors. We are making use of Theorem 11.2.11 and TYC 11.2.10.

1. $\mathcal{A}$ is injective.
2. $\mathrm{SPI}(\mathcal{A})$ is injective.
3. $\left(\mathrm{SPI}(\mathcal{A})\right)^{T}$ is surjective.
4. $\mathrm{SPI}\left(\mathcal{A}^{T}\right)$ is surjective.
5. $\mathcal{A}^{T}$ is surjective.

To establish the equivalence of the last two claims of the theorem, we make use of the already established equivalence of the first two: each of the following statements is equivalent to its neighbors.

1. $\mathcal{A}$ is surjective.
2. $\left(\mathcal{A}^{T}\right)^{T}$ is surjective.
3. $\mathcal{A}^{T}$ is injective. ■

11.3 Implementing Equivalence And Finding Inverses

If $\mathcal{A}$ and $\mathcal{C}$ do have the same SPI's and are therefore equivalent, how would one find invertible $\mathcal{S}$ and $\mathcal{T}$ such that

$$\mathcal{S}\mathcal{A}\mathcal{T} = \mathcal{C}?$$

When one starts with a matrix $\mathcal{A}$ and applies a sequence of elementary row operations, arriving in the end at a matrix $\mathcal{B}$, one has

$$\mathcal{E}_{k}\mathcal{E}_{k-1}\cdots\mathcal{E}_{1}\mathcal{A} = \mathcal{B}\ ,$$

where $\mathcal{E}_i$ is the correct elementary matrix corresponding to the i-th elementary row operation being performed. So,

$$\mathcal{S}\mathcal{A} = \mathcal{B} \, ,$$

where

$$\mathcal{S} = \mathcal{E}_k \mathcal{E}_{k-1} \cdots \mathcal{E}_1 \, .$$

The following theorem gives a simple algorithm for finding $\mathcal{S}$.

Theorem 11.3.1

Suppose that one starts with a matrix $\mathcal{A}$ and applies a sequence of elementary row operations, arriving in the end at a matrix $\mathcal{B}$.

If one performs the very same sequence of elementary row operations on a (partitioned) matrix $[\mathcal{A} \;\; \mathcal{I}]$, one will arrive at the matrix $[\mathcal{B} \;\; \mathcal{S}]$, where $\mathcal{S}$ is an invertible matrix such that

$$\mathcal{S}\mathcal{A} = \mathcal{B} \, .$$

Proof of Theorem 11.3.1. As we have observed already,

$$\mathcal{S}\mathcal{A} = \mathcal{B} \, ,$$

where

$$\mathcal{S} = \mathcal{E}_k \mathcal{E}_{k-1} \cdots \mathcal{E}_1 \, ,$$

and $\mathcal{E}_i$ is the correct elementary matrix corresponding to the i-th elementary row operation being performed.

Now we simply note that

$$\begin{aligned}
\mathcal{E}_k \mathcal{E}_{k-1} \cdots \mathcal{E}_1 \, [\mathcal{A} \;\; \mathcal{I}] &= \left[\mathcal{E}_k \mathcal{E}_{k-1} \cdots \mathcal{E}_1 \mathcal{A} \quad \mathcal{E}_k \mathcal{E}_{k-1} \cdots \mathcal{E}_1 \mathcal{I} \right] \\
&= \left[\mathcal{B} \quad \mathcal{E}_k \mathcal{E}_{k-1} \cdots \mathcal{E}_1 \right] \\
&= [\mathcal{B} \;\; \mathcal{S}] \, ,
\end{aligned}$$

which demonstrates the validity of our claim. ∎

Test Your Comprehension 11.3.2

Suppose that one starts with a matrix $\mathcal{A}$ and applies a sequence of elementary column operations, arriving in the end at a matrix $\mathcal{B}$.

Argue that if one performs the very same sequence of elementary column operations on a (partitioned) matrix $\left[\begin{smallmatrix} \mathcal{A} \\ \mathcal{I} \end{smallmatrix}\right]$, one will arrive at the matrix $\left[\begin{smallmatrix} \mathcal{B} \\ \mathcal{T} \end{smallmatrix}\right]$, where $\mathcal{T}$ is an invertible matrix such that

$$\mathcal{A}\mathcal{T} = \mathcal{B}\,.$$

Exercise 11.3.3

Suppose that by applying a given sequence of elementary row operations and a given sequence of elementary column operations on a matrix $\mathcal{A} \in \mathbb{M}_{n\times m}$ one arrives at a matrix $\mathcal{B}$. Then one can write

$$\mathcal{S}\mathcal{A}\mathcal{T} = \mathcal{B}\,,$$

for the invertible matrices $\mathcal{S}$ and $\mathcal{T}$, such that $\mathcal{S}$ is a product of the elementary matrices corresponding to the row operations that have been performed, and $\mathcal{T}$ is a product of the elementary matrices corresponding to the column operations that have been performed.

Design an algorithm based on Theorem 11.3.1 for finding $\mathcal{S}$ and $\mathcal{T}$.

Hint: Consider the matrix $\begin{bmatrix} \mathcal{A} & \mathcal{I}_n \\ \mathcal{I}_m & \mathcal{O} \end{bmatrix}$, or work with two matrices: $[\mathcal{A} \;\; \mathcal{I}_n]$ and $\begin{bmatrix} \mathcal{A} \\ \mathcal{I}_m \end{bmatrix}$.

Algorithm 11.3.4 ☞ **An algorithm for constructing a matrix inverse**

Obviously, given an $\mathcal{A}$, Exercise 11.3.3 deals with an algorithm for producing matrices

$$\mathcal{S} := \mathcal{E}_t\,\mathcal{E}_{t-1}\ldots\mathcal{E}_2\,\mathcal{E}_1 \quad \text{and} \quad \mathcal{T} := \mathcal{F}_1\,\mathcal{F}_2\ldots\mathcal{F}_{s-1}\,\mathcal{F}_s$$

described in Theorem 11.1.9, based on the reduction to a SPI described in Exercise 11.1.5.

Since the only invertible SPI's are the identity matrices, if $\mathcal{A}$ is invertible, its SPI is the identity, and so we have an equation

$$\mathcal{S}\mathcal{A}\mathcal{T} = \mathcal{I}\,,$$

from where we get

$$\mathcal{A}\mathcal{T} = \mathcal{S}^{-1}\mathcal{I} = \mathcal{S}^{-1}\,,$$

and then

$$\mathcal{A}\big(\mathcal{T}\mathcal{S}\big) = \mathcal{I}\,. \tag{11.3}$$

Similarly

$$\mathcal{S}\mathcal{A} = \mathcal{I}\mathcal{T}^{-1} = \mathcal{T}^{-1}\,,$$

so that

$$\big(\mathcal{T}\mathcal{S}\big)\mathcal{A} = \mathcal{I}\,. \tag{11.4}$$

Therefore, by (11.3) and (11.4), $\mathcal{T}\mathcal{S}$ is the inverse of $\mathcal{A}$.

Since $\mathcal{S}$ and $\mathcal{T}$ can be constructed via Exercise 11.3.3, we have formulated *an algorithm for constructing matrix inverses via a process of reduction to a SPI.*

Later (Obs. 16.1.21) we will be able to improve this algorithm.

11.4 Smith Factorization

Theorem 11.4.1 **Smith Factorization**

Every matrix $\mathcal{A}$ can be expressed as a product $\mathcal{KBL}$, where $\mathcal{K}$ and $\mathcal{L}$ are invertible square matrices that are products of elementary matrices, and $\mathcal{B}$ is a SPI of the same size and jectivity as $\mathcal{A}$.

Proof of Theorem 11.4.1. Given an $\mathcal{A}$, by Theorem 11.1.9 there exist elementary matrices $\mathcal{E}_i$ and $\mathcal{F}_j$ such that

$$\mathcal{E}_t\,\mathcal{E}_{t-1}\ldots\mathcal{E}_2\,\mathcal{E}_1\,\mathcal{A}\,\mathcal{F}_1\,\mathcal{F}_2\ldots\mathcal{F}_{s-1}\,\mathcal{F}_s$$

is a SPI, which we denote by $\mathcal{B}$.

Let us write

$$\mathcal{T} := \mathcal{E}_t\,\mathcal{E}_{t-1}\cdots\mathcal{E}_2\,\mathcal{E}_1 \quad \text{and} \quad \mathcal{S} := \mathcal{F}_1\,\mathcal{F}_2\cdots\mathcal{F}_{s-1}\,\mathcal{F}_s\ ,$$

so that

$$\mathcal{B} = \mathcal{TAS}\ .$$

Since elementary matrices are invertible, and a product of invertible matrices is invertible, $\mathcal{S}$ and $\mathcal{T}$ are invertible. Therefore,

$$\mathcal{T}^{-1}\mathcal{B}\mathcal{S}^{-1} = \mathcal{T}^{-1}(\mathcal{TAS})\mathcal{S}^{-1} = \mathcal{A}\ .$$

Denote $\mathcal{T}^{-1}$ by $\mathcal{K}$, and $\mathcal{S}^{-1}$ by $\mathcal{L}$. Then

$$\mathcal{A} = \mathcal{KBL}\ ,$$

and

$$\mathcal{K} = \mathcal{T}^{-1} = \left(\mathcal{E}_t\,\mathcal{E}_{t-1}\cdots\mathcal{E}_2\,\mathcal{E}_1\right)^{-1} = \mathcal{E}_1^{-1}\,\mathcal{E}_2^{-1}\cdots\mathcal{E}_{t-1}^{-1}\,\mathcal{E}_t^{-1}\ .$$

The inverse of an elementary matrix is an elementary matrix (of the same type), and therefore $\mathcal{K}$ is a product of elementary matrices. By a similar argument, so is $\mathcal{L}$. ∎

Theorem 11.4.2 **Invertible matrices are the products of the elementary ones**

A matrix is invertible exactly when it can be expressed as a product of elementary matrices.

Proof of Theorem 11.4.2. Since elementary matrices are invertible, so are their products. The non-trivial part of the theorem is that every invertible matrix factors out as a product of elementary matrices.

If $\mathcal{A}$ is an invertible matrix, it is square (TYC 11.2.2), and has Smith factorization $\mathcal{A} = \mathcal{K}\mathcal{B}\mathcal{L}$ (Thm. 11.4.1), where $\mathcal{K}$ and $\mathcal{L}$ are products of elementary matrices, and $\mathcal{B}$ is an invertible SPI. The only invertible SPI's are the identity matrices (TYC 11.2.10), and therefore

$$\mathcal{A} = \mathcal{K}\mathcal{B}\mathcal{L} = \mathcal{K}\mathcal{L} = \text{ a product of elementary matrices .} \qquad \blacksquare$$

Theorem 11.4.3 ☞ **Left-equivalence and row operations**

Two matrices are left-equivalent exactly when there is a sequence of elementary row operations that transforms one matrix into the other.

Proof of Theorem 11.4.3. Saying that $\mathcal{A}$ and $\mathcal{B}$ are left-equivalent means that there exists an invertible matrix $\mathcal{S}$ such that

$$\mathcal{B} = \mathcal{S}\mathcal{A}.$$

In view of Theorem 11.4.2 this iequivalent to stating that

$$\mathcal{B} = \mathcal{E}_k\mathcal{E}_{k-1}\cdots\mathcal{E}_1\mathcal{A}\ ,$$

for some elementary matrices $\mathcal{E}_i$. Multiplying a matrix by an elementary matrix from the left amounts to performing a corresponding elementary row operation on the matrix (see Section 10.2). $\blacksquare$

Test Your Comprehension 11.4.4 ☞ **Right-equivalence and column operations**

Argue that two matrices are right-equivalent exactly when there is a sequence of elementary column operations that transforms one matrix into the other.

11.5 Appendix: Exiled Proofs

Proof of Theorem 11.2.5. It is quite obvious that equal matrices are equivalent (Exc. 8.2.2), but two matrices can generally be equivalent without being equal. Our task is to show that SPI's do not have this option. We will argue that if SPI's $\mathcal{P}$ and $\mathcal{Q}$ are equivalent then they have to be equal.

Since equivalent matrices have the same size, it is sufficient to show that equivalent SPI's have the same rank. SPI's of the same shape and of equal rank are automatically identical. Since non-null matrix cannot be equivalent to a null matrix, we can focus on the case of non-null $\mathcal{P}$ and $\mathcal{Q}$.

If SPI's $\mathcal{P}$ and $\mathcal{Q}$ in $\mathbb{M}_{n\times m}$ are equivalent, then there exist invertible matrices $\mathcal{S} \in \mathbb{M}_m$ and $\mathcal{R} \in \mathbb{M}_n$ such that

$$\mathcal{P} = \mathcal{R}\mathcal{Q}\mathcal{S}. \tag{11.5}$$

Let us denote $\mathcal{R}^{-1}$ by $\mathcal{T}$ to simplify the notation. We have

$$\mathcal{T}\mathcal{P} = \mathcal{Q}\mathcal{S}. \tag{11.6}$$

Let us say that $\mathcal{P}$ has rank k (> 0) and $\mathcal{Q}$ has rank l (> 0). In particular, l and k exceed neither m nor n. We aim to show that $k = l$.

We can partition our SPI's and write

$$\mathcal{P} = \begin{bmatrix} \mathcal{I}_k & \mathcal{O} \\ \mathcal{O} & \mathcal{O} \end{bmatrix}_{n\times m} \quad \text{and} \quad \mathcal{Q} = \begin{bmatrix} \mathcal{I}_l & \mathcal{O} \\ \mathcal{O} & \mathcal{O} \end{bmatrix}_{n\times m},$$

with the understanding that some of the null matrices may be absent (which happens if either k or l equals either m or n).

Partition $\mathcal{T}$ as $\begin{bmatrix} \mathcal{A} & \mathcal{B} \\ \mathcal{C} & \mathcal{D} \end{bmatrix}$, using the partitioning $(l|n\text{-}l)\times(k|n\text{-}k)$. In particular the vertical partitioning of $\mathcal{T}$ matches the horizontal partitioning of $\mathcal{P}$, and we can use the fundamental formula for partitioned matrix multiplication (Theorem 9.1.8) to calculate the product $\mathcal{T}\mathcal{P}$.

Similarly, partition $\mathcal{S}$ as $\begin{bmatrix} \mathcal{X} & \mathcal{Y} \\ \mathcal{Z} & \mathcal{W} \end{bmatrix}$, using the partitioning $(l|m\text{-}l)\times(k|m\text{-}k)$. Here the vertical partitioning of $\mathcal{Q}$ matches the horizontal partitioning of $\mathcal{S}$. This allows the use of the fundamental formula for partitioned matrix multiplication in calculating $\mathcal{Q}\mathcal{S}$.

Recall that our goal is to show the equality of k and l. Since $\mathcal{A} \in \mathbb{M}_{l\times k}$, this amounts to showing that $\mathcal{A}$ is a square matrix. If we can show that $\mathcal{A}$ is invertible, then $\mathcal{A}$ is automatically square (TYC 11.2.2). This shall be our approach.

Equation (11.6) can be rewritten as

$$\begin{bmatrix} \mathcal{A} & \mathcal{B} \\ \mathcal{C} & \mathcal{D} \end{bmatrix}\begin{bmatrix} \mathcal{I}_k & \mathcal{O} \\ \mathcal{O} & \mathcal{O} \end{bmatrix} = \begin{bmatrix} \mathcal{I}_l & \mathcal{O} \\ \mathcal{O} & \mathcal{O} \end{bmatrix}\begin{bmatrix} \mathcal{X} & \mathcal{Y} \\ \mathcal{Z} & \mathcal{W} \end{bmatrix}. \tag{11.7}$$

After carrying out the multiplication in (11.7) via the fundamental formula for partitioned matrix multiplication, we arrive at

$$\begin{bmatrix} \mathcal{A} & \mathcal{O} \\ \mathcal{C} & \mathcal{O} \end{bmatrix}_{n\times m} = \begin{bmatrix} \mathcal{X} & \mathcal{Y} \\ \mathcal{O} & \mathcal{O} \end{bmatrix}_{n\times m}. \tag{11.8}$$

The reader should check that the two partitioned matrices in (11.8) have identical partitioning.

It follows that $\mathcal{C} = \mathcal{O}$, $\mathcal{Y} = \mathcal{O}$, and $\mathcal{A} = \mathcal{X}$, so that

$$\mathcal{T} = \begin{bmatrix} \mathcal{A} & \mathcal{B} \\ \mathcal{O} & \mathcal{D} \end{bmatrix} \quad \text{and} \quad \mathcal{S} = \begin{bmatrix} \mathcal{A} & \mathcal{O} \\ \mathcal{Z} & \mathcal{W} \end{bmatrix}.$$

Now we can apply Theorem 9.1.20 to our block-triangular matrices $\mathcal{T}$ and $\mathcal{S}$. By this theorem, $\mathcal{A}$ is injective because $\mathcal{T}$ is injective, and $\mathcal{A}$ is surjective because $\mathcal{S}$ is surjective. Thus $\mathcal{A}$ is a bijection, and we are done. ■

IV Matrix Nullspaces And Ranges

12. Matrix Nullspaces And Linear Independence

Last modified on December 8, 2018

12.1 Matrix Nullspaces

Terminology 12.1.1

A matrix **annihilates** a given tuple if it sends it to the null tuple.

The set of all tuples nullified/annihilated by a matrix $\mathcal{A}$ is said to be **the kernel** or **the nullspace** of $\mathcal{A}$. In other words, for $\mathcal{A} \in \mathbb{M}_{n\times m}$,

$$\mathit{Nullspace}\,(\mathcal{A}) := \{\ X \in \mathbb{R}^m \mid \mathcal{A}(X) = \mathbb{0}_n\ \}.$$

Since matrices map null tuples to null tuples, the nullspace of a matrix always contains a null tuple.

Test Your Comprehension 12.1.2

Argue that an $n \times m$ matrix is null exactly when its nullspace is all of $\mathbb{R}^m$.

Test Your Comprehension 12.1.3 ☞ **Nullspaces are subspaces**

Verify the following claims.

1. Every matrix annihilates the null tuple in its domain.
2. If $\mathcal{A}$ annihilates X then $\mathcal{A}$ annihilates every scalar multiple of X.
3. If $\mathcal{A}$ annihilates X and $\mathcal{A}$ annihilates Y then A annihilates $X + Y$.
4. If $\mathcal{A}$ annihilates X and $\mathcal{A}$ annihilates Y then A annihilates every linear combination of X and Y.

In particular, a nullspace of an $n \times m$ matrix is a subspace of $\mathbb{R}^m$, and as such is either a singleton set whose sole element is the null tuple, or is an infinite set. In the primer case we say that the nullspace is **trivial**, and in the latter – **non-trivial**.

Test Your Comprehension 12.1.4

Argue that a matrix A has a null column exactly when its nullspace contains a standard basis tuple.

12.1.1 — Nullspaces And Injectivity

Test Your Comprehension 12.1.5

Argue that an injective matrix annihilates only the null tuple; i.e. its nullspace is $\{\mathbb{0}\}$.

Hint: Matrices map null tuples to null tuples.

If a matrix annihilates two distinct tuples, it is not injective, as it sends both tuples to the same output: the null tuple. In other words, if the nullspace of a matrix is not a singleton set, then the matrix is not injective. The nullspaces of injective matrices are trivial (TYC 12.1.5). The converse is true as well. This establishes a fundamental connection between the nullspaces and the injectivity for matrices.

Theorem 12.1.6

The following statements are equivalent for a matrix $\mathcal{A}$.

1. $\mathcal{A}$ is injective.
2. $\mathit{Nullspace}(\mathcal{A})$ is trivial; i.e. $\mathcal{A}$ annihilates only the null tuple.

Proof of Theorem 12.1.6. We have already explained above why the first statement implies the second. Let us verify the reverse implication.

Suppose that $\mathcal{A}$ annihilates only the null tuple.

If U and W are distinct tuples in the initial space of $\mathcal{A}$, then $U - W \neq \mathbb{0}$. Therefore

$$\mathcal{A}(U) - \mathcal{A}(W) = \mathcal{A}(U - W) \neq \mathbb{0}.$$

Hence $\mathcal{A}(U) \neq \mathcal{A}(W)$, and this shows that $\mathcal{A}$ is injective. ∎

12.1.2 — Non-injective Matrices Are Non-injective In A Big Way

A function is not injective if it sends a pair of different inputs to the same output. Not all outputs have to have more than one "progenitor", at least not in the case of general functions.

For example, $f(x) = x^2 + 1$ describes a non-injective function $f : \mathbb{R} \longrightarrow \mathbb{R}$, and yet 1 has a single f-progenitor: 0.

If one does not insist on continuity, then examples can be given where there is a single output that has multiple progenitor inputs, with all other outputs coming from a single input each.

Matrix functions are not only continuous (something that we do not explore address in the course) but are always very structured by their linearity. It turns out that when matrix functions are not injective, every output has infinitely many progenitors, and that this infinitude has very much to do with the (non-trivial, and hence infinite) nullspace of the matrix. As the reader surely remembers, when a subspace of $\mathbb{R}^n$ is not trivial, it has to be infinite.

Let us do some work and establish the bold claims we have just made.

Theorem 12.1.7 ☞ **Non-Injective Matrices Are Very Much So**

Suppose that $\mathcal{A}$ is a matrix, and $\mathcal{A}(X_o) = Y_o$.

Then

$$\{ \ X \mid \mathcal{A}(X) = Y_o \ \} = \left\{ X_o + Z \ \middle| \ Z \in \mathit{Nullspace}\,(\mathcal{A}) \right\} .$$

Hence, once we have one input X_o that produces the output Y_o via $\mathcal{A}$, by perturbing X_o by all possible elements of the nullspace of $\mathcal{A}$, we obtain ALL inputs that produce the output Y_o.

If $\mathcal{A}$ is NOT injective, then $\mathit{Nullspace}\,(\mathcal{A})$ is an infinite set, and so there are infinitely many different choices for Z. In that case $\{ \ X \mid \mathcal{A}(X) = Y_o \ \}$ is infinite.

Proof of Theorem 12.1.7.

$$\begin{aligned}
\mathcal{A}(X) = Y_o \iff & \mathcal{A}(X) = \mathcal{A}(X_o) \\
\iff & \mathcal{A}(X - X_o) = \mathcal{A}(X) - \mathcal{A}(X_o) = \mathbb{0} \\
\iff & X - X_o \in \mathit{Nullspace}\,(\mathcal{A}) \\
\iff & X = X_o + Z, \quad \text{for some } Z \in \mathit{Nullspace}\,(\mathcal{A}) \ .
\end{aligned}$$

■

In section 10.3 we argued that for any seven pairs $(a_1, b_1), \ldots, (a_7, b_7)$ of real numbers, where $a_1, a_2, \ldots, a_7$ are distinct, there is exactly one polynomial p of degree at most 6 such that

$$p(a_i) = b_i \quad \text{for all} \quad i\,. \tag{12.1}$$

We also made a claim that there are infinitely many such polynomials of any degree greater than 6. Let us justify this latter claim.

Exercise 12.1.8

Recall that the problem of finding polynomials p of degree 13 satisfying the conditions (12.1) reduces to the problem of finding 13-tuples $C := (\,c_0 \;\, c_1 \;\, \cdots \;\, c_{13}\,)$ such that

$$\begin{bmatrix} 1 & a_1 & a_1^2 & \dots & a_1^{13} \\ 1 & a_2 & a_2^2 & \dots & a_2^{13} \\ 1 & a_3 & a_3^2 & \dots & a_3^{13} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & a_7 & a_7^2 & \dots & a_7^{13} \end{bmatrix}_{7\times 14} (C) = \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_7 \end{pmatrix}. \tag{12.2}$$

1. Argue that equation (12.2) has solutions C. (Hint: see section 10.3.)
2. Argue that the matrix in (12.2) is surjective.
3. Argue that the matrix in (12.2) is not injective. (Hint: What is its shape?)
4. Argue that the equation (12.2) has infinitely many solutions C. (Hint: Thm. 12.1.7.)

12.1.3 — Nullspaces And Transposition

Lemma 12.1.9

The nullspace of a matrix $\mathcal{A}^T$ consists exactly of the tuples that are orthogonal to the columns of $\mathcal{A}$.

Proof of Theorem 12.1.9. Let us write

$$\mathcal{A} = [C_1 \;\; C_2 \;\; \cdots \;\; C_m]\,.$$

Then

$$\mathcal{A}^T = \begin{bmatrix} \longleftarrow & C_1 & \longrightarrow \\ \longleftarrow & C_2 & \longrightarrow \\ & \vdots & \\ \longleftarrow & C_m & \longrightarrow \end{bmatrix}, \quad \text{and} \quad \mathcal{A}^T(X) = \begin{pmatrix} C_1 \bullet X \\ C_2 \bullet X \\ \vdots \\ C_m \bullet X \end{pmatrix}$$

It is now clear that

$$\mathcal{A}^{T}(X) = \mathbb{0} \iff C_i \bullet X = 0 \text{ for all } i\,. \qquad \blacksquare$$

Test Your Comprehension 12.1.10 ☞ **Nullspace of $\mathcal{A}^{T}$**

Argue that for any matrix $\mathcal{A}$:

$$\mathit{Nullspace}\left(\mathcal{A}^{T}\right) = \left(\mathit{Range}\,(\mathcal{A})\right)^{\perp}.$$

Hint: Recall, as a stating point, that the dot product distributes over linear combinations. This can be used to argue that a tuple is orthogonal to all linear combinations of V, W, X, Y and Z, whenever it is orthogonal to V, W, X, Y, Z. Follow this up by an application of Lemma 12.1.9.

Test Your Comprehension 12.1.11

Non-null tuples in the nullspace of $\mathcal{A}^{T}$ cannot belong to the range of $\mathcal{A}$.

Hint: TYC 3.5.12

In general, inserting additional rows into a matrix can produce a matrix with a smaller nullspace. With more rows in play, fewer tuples will be orthogonal to ALL of the rows. Some, which may have been orthogonal to all original rows, may not be orthogonal to the inserted rows.

Of course, if the rows that were inserted are all null, these will not introduce any new restrictions, and whatever tuples were orthogonal to all of the original rows, are still orthogonal to all rows.

$\Downarrow$

Theorem 12.1.12 ☞ **Inserting or deleting null rows does not alter the nullspace**

A matrix produced from a matrix $\mathcal{A}$ by inserting or deleting null rows has the same nullspace as $\mathcal{A}$.

Proof of Theorem 12.1.12. Let us show that for any matrix $\mathcal{B}$,

$$\mathit{Nullspace}\begin{bmatrix}\mathcal{B}\\ \mathcal{O}\end{bmatrix} = \mathit{Nullspace}\,(\mathcal{B})\,.$$

To this end, observe that

$$X \in \mathit{Nullspace}\begin{bmatrix}\mathcal{B}\\ \mathcal{O}\end{bmatrix} \iff \begin{bmatrix}\mathcal{B}\\ \mathcal{O}\end{bmatrix}(X)=\mathbb{0} \overset{\text{Thm. 9.1.18}}{\iff} \begin{pmatrix}\mathcal{B}(X)\\ \mathbb{0}\end{pmatrix} = \mathbb{0}$$

$$\iff \mathcal{B}(X) = \mathbb{0} \iff X \in \mathit{Nullspace}\,(\mathcal{B})\,. \qquad \blacksquare$$

12.1.4 — Nullspaces And Composition

Test Your Comprehension 12.1.13 ☞ **Nullspace of a composition**

Validate the formula

$$\mathit{Nullspace}\,(\mathcal{B}) \subseteq \mathit{Nullspace}\,(\mathcal{A}\,\mathcal{B}) \ .$$

It states that X is annihilated by $\mathcal{A}\,\mathcal{B}$ whenever it is annihilated by $\mathcal{B}$.

Test Your Comprehension 12.1.14

Demonstrate that the inclusion in TYC 12.1.13 may be strict.

Exc. 8.1.15.

So, it may happen that a tuple "gets past" $\mathcal{B}$ unharmed only to be annihilated by $\mathcal{A}$.

Theorem 12.1.15

If $\mathcal{A}$ is *injective* and $\mathcal{A}\,\mathcal{B}$ makes sense, then

$$\mathit{Nullspace}\,(\mathcal{B}) = \mathit{Nullspace}\,(\mathcal{A}\,\mathcal{B}) \ .$$

The intuitive idea here is that injective matrices only annihilate the null tuples (TYC 12.1.5) and so are of little help in the business of annihilation.

Proof of Theorem 12.1.15. In view of TYC 12.1.13 we only need to verify the inclusion $\mathit{Nullspace}\,(\mathcal{A}\,\mathcal{B}) \subseteq \mathit{Nullspace}\,(\mathcal{B})$. To this end we argue that if $\mathcal{A}\,\mathcal{B}$ annihilates X, then so does $\mathcal{B}$.

If X is annihilated by $\mathcal{A}\,\mathcal{B}$, then $\mathcal{A}$ annihilates $\mathcal{B}(X)$. Yet $\mathcal{A}$ is injective, and so annihilates only the null tuple. Hence $\mathcal{B}(X) = \mathbb{0}$; i.e. $\mathcal{B}$ annihilates X. ■

Test Your Comprehension 12.1.16 ☞ **Left-equivalent matrices have equal nullspaces**

Argue that left-equivalent matrices have identical nullspaces.

In other words, argue that elementary *row* operations transform a matrix into a matrix with the same nullspace.

Comment 12.1.17 ☞ **Performing elementary column operations may alter the nullspace.**

For example, $\left(\begin{smallmatrix} 1 \\ -1 \end{smallmatrix}\right)$ is annihilated by $\left[\begin{smallmatrix} 1 & 1 \\ 1 & 1 \end{smallmatrix}\right]$, but not by $\left[\begin{smallmatrix} 1 & 0 \\ 1 & 0 \end{smallmatrix}\right]$.

Similarly, $\left(\begin{smallmatrix} -2 \\ 1 \end{smallmatrix}\right)$ is annihilated by $\left[\begin{smallmatrix} 1 & 2 \\ 0 & 0 \end{smallmatrix}\right]$, but not by $\left[\begin{smallmatrix} 2 & 1 \\ 0 & 0 \end{smallmatrix}\right]$.

For every matrix $\mathcal{A}$, the symmetric matrices $\mathcal{A}^{T}\mathcal{A}$ and $\mathcal{A}\mathcal{A}^{T}$ (commonly of different size) capture many attributes of $\mathcal{A}$ and $\mathcal{A}^{T}$, and serve as bridging quantities between $\mathcal{A}$ and $\mathcal{A}^{T}$.

Since the theory of symmetric matrices is particularly nice, the constructs $\mathcal{A}^{T}\mathcal{A}$ and $\mathcal{A}\mathcal{A}^{T}$ play an important role in the development of matrix algebra.

Theorem 12.1.18

For any matrix $\mathcal{A}$,

1. $\mathit{Nullspace}\left(\mathcal{A}^{T}\mathcal{A}\right) = \mathit{Nullspace}(\mathcal{A})$;
2. $\mathit{Nullspace}\left(\mathcal{A}\mathcal{A}^{T}\right) = \mathit{Nullspace}\left(\mathcal{A}^{T}\right)$.

Proof of Theorem 12.1.18. The second equality follows from the first via a replacement of $\mathcal{A}$ by $\mathcal{A}^{T}$. Let us focus on the first equality.

By TYC 12.1.13, $\mathit{Nullspace}(\mathcal{A}) \subset \mathit{Nullspace}\left(\mathcal{A}^{T}\mathcal{A}\right)$. If we can show the reverse inclusion as well, then the two sets are equal.

So, we aim to verify that every X annihilated by $\mathcal{A}^{T}\mathcal{A}$ is also annihilated by $\mathcal{A}$.

If X annihilated by $\mathcal{A}^{T}\mathcal{A}$, then $\mathcal{A}^{T}\mathcal{A}(X) = \mathbb{O}$, and therefore $\mathcal{A}^{T}\mathcal{A}(X) \bullet X = 0$. Hence

$$0 = \mathcal{A}^{T}\mathcal{A}(X) \bullet X = \mathcal{A}(X) \bullet \mathcal{A}(X) = \left\|\mathcal{A}(X)\right\|^{2}.$$

Since $\mathcal{A}(X)$ has zero length, it must be a null tuple. This shows that $\mathcal{A}$ annihilates X. ∎

Test Your Comprehension 12.1.19

1. Argue that the following statements are equivalent for a matrix $\mathcal{A}$.

   (a) $\mathcal{A}$ is injective.

   (b) $\mathcal{A}^{T}\mathcal{A}$ is invertible.

2. Argue that the following statements are also equivalent to each other.

   (a) $\mathcal{A}$ is surjective.

   (b) $\mathcal{A}\mathcal{A}^{T}$ is invertible.

Hint: Use Thms. 12.1.18 and 11.2.14. What is the shape of $\mathcal{A}^{T}\mathcal{A}$ and $\mathcal{A}\mathcal{A}^{T}$?

12.2 Injectivity And Linear Independence Of Columns

Theorem 12.1.6 helps us to express the injectivity of a matrix in terms of its generating tuples. This will be done in several steps.

[We will have to wait a bit longer before we can do this for the surjectivity as well.]

Terminology 12.2.1

If a *non-trivial* linear combination of tuples $V_1, V_2, V_3, \ldots, V_k$ equals a null tuple, then the tuples $V_1, V_2, V_3, \ldots, V_k$ are said to be **linearly (inter)dependent**.

If the only linear combination of tuples $V_1, V_2, V_3, \ldots, V_k$ that equals a null tuple is the trivial linear combination, then the tuples $V_1, V_2, V_3, \ldots, V_k$ are said to be **linearly independent**.

Exercise 12.2.2 ☞ **A reason for the terminology**

Verify that the following statements about tuples are equivalent.

1. $V_1, V_2, V_3, \ldots, V_k$ are linearly (inter)dependent.
2. Either $k = 1$ and V_1 is null, or $k > 1$ and one of the V_i's is a linear combination of (some of) the others.

Theorem 12.2.3

The following statements are equivalent for a matrix A.

1. A is injective.
2. The columns of $\mathcal{A}$ are linearly independent.

Proof of Theorem 12.2.3. If $\mathcal{A} = \begin{bmatrix} C_1 & C_2 & C_3 & \ldots & C_m \end{bmatrix}$, then

$$\alpha_1 C_1 + \alpha_2 C_2 + \cdots + \alpha_m C_m = \mathcal{A} \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_m \end{pmatrix}.$$

Now we can see that the following are equivalent.

1. $\mathcal{A}$ annihilates only the null tuple.
2. The only linear combination of $C_1, C_2, \ldots, C_m$ that equals the null tuple is the trivial linear combination.

The primer is the claim that $\mathcal{A}$ is injective (Theorem 12.1.6); the latter – that the columns of $\mathcal{A}$ are linearly independent. ∎

Test Your Comprehension 12.2.4

Argue that a single-column matrix $\left[X\right]$ is injective exactly when X is not null.

Theorem 12.2.5

The following statements are equivalent for a matrix $\mathcal{A}$.

1. $\mathcal{A}$ is NOT injective.
2. Either $\mathcal{A} = \left[\mathbb{O}_k\right]$ or $\mathcal{A}$ has a column that is a linear combination of some other columns of $\mathcal{A}$.
3. Either the first column of $\mathcal{A}$ is null, or $\mathcal{A}$ has a column that is a linear combination of the *preceding* columns of $\mathcal{A}$.

A proof of Theorem 12.2.5 is presented in the appendix to the chapter.

Exercise 12.2.6 ☞ **Matrices cannot create linear independence**

If $\mathcal{A} \in \mathbb{M}_{n\times m}$ and $X_1, X_2, X_3, \ldots, X_{14}$ is a list of m-tuples such that

$$\mathcal{A}\left(X_1\right), \mathcal{A}\left(X_2\right), \mathcal{A}\left(X_3\right), \ldots, \mathcal{A}\left(X_{14}\right) \text{ are linearly independent,}$$

then

$$X_1, X_2, X_3, \ldots, X_{14} \text{ are linearly independent.}$$

Hint: Infer from the hypothesis that $\mathcal{A} \circ \left[X_1 \;\; X_2 \;\; X_3 \;\; \ldots \;\; X_{14}\right]$ is injective. Then apply Theorem 2.4.2.

Synopsis 12.2.7 ☞ **Conditions equivalent to *injectivity***

Let us collect the *conditions that are equivalent to the injectivity* of a matrix $\mathcal{A}$. The reader should take the time to see why these conditions are indeed equivalent to each other.

Injectivity: $\mathcal{A}$ does not send distinct inputs to identical outputs.

Trivial Nullspace: $\mathit{Nullspace}\left(\mathcal{A}\right) = \left\{\mathbb{O}\right\}$.

Non-Agression: $\mathcal{A}$ annihilates only the null tuple.

Linear Independence of Columns: The only linear combination of the columns of A that equals the null tuple is the trivial linear combination.

No Column is a Linear Combination of Other Columns, and . . . : *$\mathcal{A}$ is not a null matrix and* no column of $\mathcal{A}$ is a linear combination of some other columns.

No Column is a Linear Combination of the Preceding Columns, and . . . : *The first column of $\mathcal{A}$ is not null, and* no column of $\mathcal{A}$ is a linear combination of the preceding columns.

12.3 Additional Problems

Terminology 12.3.1

A tuple X is said to be **fixed** by a matrix $\mathcal{A}$, if

$$\mathcal{A}(X) = X \ .$$

For example, $\begin{pmatrix} -1 \\ 2 \end{pmatrix}$ is fixed by the matrix $\begin{bmatrix} 3 & 1 \\ 2 & 2 \end{bmatrix}$.

It is common to refer to fixed tuples as "**fixed points**".

Test Your Comprehension 12.3.2 ☞ **Fixed points of a matrix**

Verify that for any square matrix $\mathcal{A}$,

$$\begin{aligned} \mathit{Nullspace}\,(\mathcal{I} - \mathcal{A}) &= \{ \ W \mid \mathcal{A}(W) = W \ \} \\ &= \text{the set of all fixed tuples of } \mathcal{A} \ . \end{aligned}$$

12.4 Appendix: Exiled Proofs

Proof of Theorem 12.2.5. We shall verify the implications [3. $\Longrightarrow$ 2.], [2. $\Longrightarrow$ 1.] and [1. $\Longrightarrow$ 3.] to complete the proof.

[**3.** $\Longrightarrow$ **2.**]: Suppose that condition 3. holds for $\mathcal{A}$. Let us deal with the two possibilities in turn.

- If one of the columns of $\mathcal{A}$ is a linear combination of the preceding columns of $\mathcal{A}$, then $\mathcal{A}$ satisfies condition 2. trivially.

- If the first column of $\mathcal{A}$ is null, and $\mathcal{A}$ has a single column, then $\mathcal{A} = \begin{bmatrix} \mathbb{O}_k \end{bmatrix}$. If $\mathcal{A}$ has more than one column, then the first column of $\mathcal{A}$, being null, is the trivial linear combination of the other columns of $\mathcal{A}$. In either case, $\mathcal{A}$ satisfies condition 2.

[**3.** $\Longrightarrow$ **2.**]: Now suppose that $\mathcal{A}$ satisfies condition 2.. Since null matrices are not injective (TYC 12.1.2), let us focus on the scenario in which a column C of $\mathcal{A}$ is a linear combination of some other columns of $\mathcal{A}$.

By employing zero coefficients, as necessary, we can express C as a linear combination of ALL other columns of $\mathcal{A}$. Let us denote these other columns by $K_1, K_2, \ldots, K_p$, and say

$$C = \alpha_1 K_1 + \cdot + \alpha_p K_p \ .$$

Then

$$\mathbb{0} = (-1)C + \alpha_1 K_1 + \cdot + \alpha_p K_p \ ,$$

which shows that a non-trivial linear combination of the columns of $\mathcal{A}$ equals a null tuple. Hence $\mathcal{A}$ is not injective by Theorem 12.2.3.

[**1.** $\Longrightarrow$ **3.**]: Suppose that $\mathcal{A}$ is not injective. If the first column of $\mathcal{A}$ happens to be null, then $\mathcal{A}$ satisfies condition 3. Let us now focus on the case that the first column of $\mathcal{A}$ is not null. In particular, by TYC 12.2.4, $\mathcal{A}$ must have more than one column.

Since $\mathcal{A}$ is not injective, it annihilates some non-null tuple, and hence also all scalar multiples of this tuple (TYC 12.1.3). Among the multiples of this tuple there is one whose *last* non-zero entry is -1.

Let us call this tuple Z and assume that $Z[\![i]\!]$ is its last non-zero entry.

Note that i cannot be 1. If it were, Z would be $-E_1$, and $\mathcal{A}(Z)$ would be $-\mathcal{A}(E_1)$; i.e. the negative of the first column of $\mathcal{A}$. Since the latter is not null, neither would be $\mathcal{A}(Z)$, contradicting our choice of Z.

$\mathcal{A}(Z)$ is a linear combination of the columns of $\mathcal{A}$ with the coefficients given by the entries of Z. Hence

A linear combination of several tuples can be considered to be a sum of a linear combination of the first few and a linear combination of the rest.

$$\begin{aligned}\mathbb{0} = \mathcal{A}(Z) = (&\text{a linear combination of the first } i\text{-}1 \text{ columns of } \mathcal{A}) \\ &+ (-1)\cdot(\text{the } i\text{-th column of } \mathcal{A}).\end{aligned}$$

INSERT PICTURE

Therefore

$$\text{the } i\text{-th column of } \mathcal{A} = \text{a linear combination of the first } i\text{-}1 \text{ columns of } \mathcal{A} \ .$$

This shows that $\mathcal{A}$ satisfies condition 3. ∎

13. Matrix Ranges And Invertibility

Last modified on December 8, 2018

13.1 Matrix Ranges

13.1.1 — Range Inclusion Factorization

As we have seen early in the text, the inclusion

$$Range\,(f \circ g) \subseteq Range\,(f) \tag{13.1}$$

holds for functions in general, and if g is surjective, we have the equality (Thm. 2.4.2).

In Theorem 13.1.2 we will present a form of the converse of this result in the setting of matrix functions.

Test Your Comprehension 13.1.1 ☞ **Right-equivalent matrices have equal ranges**

Argue that right-equivalent matrices have identical ranges.

In other words, argue that elementary *column* operations transform a matrix into a matrix with the same range.

Theorem 13.1.2 ☞ **Range inclusion factorization**

The following statements are equivalent for matrices $\mathcal{A} \in \mathbb{M}_{n\times m}$ and $\mathcal{B} \in \mathbb{M}_{n\times k}$.

1. $Range\,(\mathcal{A}) \subseteq Range\,(\mathcal{B})$.
2. $\mathcal{A} = \mathcal{B}\mathcal{C}$, for some $\mathcal{C} \in \mathbb{M}_{k\times m}$.

Tuples X_i are solutions to equations $Z_i = \mathcal{B}(X)$, which can be interpreted as systems of linear equations. Later in the text we shall develop an algorithm for discerning if such solutions exist, and if so, for finding them. As usual, such algorithms are best carried out by a computer.
It is important to note that one of the equations $Z_i = \mathcal{B}(X)$ not having a solution is equivalent to the range of $\mathcal{A}$ NOT being a subset of the range of $\mathcal{B}$. So the above-mentioned algorithms can be used to discern range inclusion/non-inclusion in concrete situations.

Proof of Theorem 13.1.2. The validity of the implication 2. $\Longrightarrow$ 1. follows from (13.1). Let us verify the implication 1. $\Longrightarrow$ 2.

Suppose that $Range(\mathcal{A}) \subseteq Range(\mathcal{B})$. Let us write $\mathcal{A} = \begin{bmatrix} Z_1 & \dots & Z_m \end{bmatrix}$. Every column Z_i of $\mathcal{A}$ is in the range of $\mathcal{A}$, and hence is in the range of $\mathcal{B}$. Thus, for every i, there exists a tuple X_i such that $Z_i = \mathcal{B}(X_i)$. This shows that

$$\mathcal{A} = \begin{bmatrix} Z_1 & \dots & Z_m \end{bmatrix} = \begin{bmatrix} \mathcal{B}(X_1) & \dots & \mathcal{B}(X_m) \end{bmatrix} \overset{\text{Thm. 8.1.7}}{=} \mathcal{B} \circ \begin{bmatrix} X_1 & \dots & X_m \end{bmatrix} .$$

Therefore $\mathcal{A} = \mathcal{B}\mathcal{C}$, where $\mathcal{C} = \begin{bmatrix} X_1 & \dots & X_m \end{bmatrix}$. ■

Observation 13.1.3

By Exercise 2.3.10, if $\mathcal{A} = \mathcal{B}\mathcal{C}$, and $\mathcal{C}$ is surjective, then

$$Range(\mathcal{A}) = Range(\mathcal{B}) \ .$$

One may conjecture that the converse implication is true as well; i.e. that the equality $Range(\mathcal{A}) = Range(\mathcal{B})$ holds for $\mathcal{A} \in \mathbb{M}_{n\times m}$ and $\mathcal{B} \in \mathbb{M}_{n\times k}$ exactly when there is a surjective $\mathcal{C} \in \mathbb{M}_{k\times m}$ such that $\mathcal{A} = \mathcal{B}\mathcal{C}$. Unfortunately *this is NOT the case.*

Let $\mathcal{A} = \left[\begin{smallmatrix} 1 \\ 1 \end{smallmatrix}\right]$ and $\mathcal{B} = \left[\begin{smallmatrix} 1 & 1 \\ 1 & 1 \end{smallmatrix}\right]$. As the reader should verify, both of these matrices have the range $\left\{ \left(\begin{smallmatrix} t \\ t \end{smallmatrix}\right) \;\middle|\; t \in \mathbb{R} \right\}$. (This verification can be done directly, or by using Exercise 14.1.1 and TYC 10.2.10.)

Yet, there does NOT exist a surjective matrix $\mathcal{C}$ such that

$$\mathcal{A}_{2\times 1} = \mathcal{B}_{2\times 2}\,\mathcal{C}_{2\times 1} \ , \tag{13.2}$$

because strictly portrait-shaped matrices are never surjective (TYC 11.2.2).

The correct result, which we shall develop a bit later, is the following.

[A peek into the future; see section 16.3]

The equality $Range(\mathcal{A}) = Range(\mathcal{B})$ happens exactly when either there is a surjective $\mathcal{C}$ such that $\mathcal{A} = \mathcal{B}\mathcal{C}$, or there is a surjective $\mathcal{G}$ such that $\mathcal{B} = \mathcal{A}\mathcal{G}$.

When $\mathcal{A}$ and $\mathcal{B}$ have the same size, the following are equivalent.

1. $Range(\mathcal{A}) = Range(\mathcal{B})$.
2. $\mathcal{A} = \mathcal{B}\mathcal{C}$, for some invertible $\mathcal{C}$.

13.2 Matrix Invertibility

13.2.1 — One-Sided Invertibility

When we explored the anatomy of functions, we observed that for general functions left-invertibility is equivalent to injectivity, and right invertibility is equivalent to surjectivity (Axiom of Choice). It is worth keeping in mind that a function may have many one-sided inverses, but never more than one (two-sided) inverse.

Theorem 6.4.5 established that inverse functions of bijective matrices are also matrices. The following theorem is an analogue of this result for the one-sided invertibility.

Theorem 13.2.1 ☞ **The jectivity and one-sided invertibility**

The following statements about a matrix $\mathcal{A}$ are equivalent.

1. $\mathcal{A}$ is surjective.
2. $\mathcal{A}$ is right-invertible (as a function).
3. $\mathcal{A}$ has a right inverse that is a matrix.

The same goes for the following statements.

1. $\mathcal{A}$ is injective.
2. $\mathcal{A}$ is left-invertible (as a function).
3. $\mathcal{A}$ has a left inverse that is a matrix.

Proof of Theorem 13.2.1. Let us deal with the first three statements. We already know that the first two of these are equivalent, and that the third implies the first.

To complete the proof we show that every surjective matrix $\mathcal{A}$ has a right inverse that is also a matrix. If $\mathcal{A} \in \mathbb{M}_{n\times m}$ is surjective, then

$$Range\,(\mathcal{I}_n) = Range\,(\mathcal{A}) \enspace ,$$

and therefore by range inclusion factorization there exists a matrix $\mathcal{C} \in \mathbb{M}_n$ such that $\mathcal{I}_n = \mathcal{A}\,\mathcal{C}$ (Theorem 13.1.2). This $\mathcal{C}$ is a right inverse of $\mathcal{A}$.

Let us establish the mutual equivalence of the second batch of statements. Again, what remains to be shown is the implication 1. $\Longrightarrow$ 3.

Suppose that $\mathcal{A}$ is injective. Since transposition flips the jectivity (Thm. 11.2.14), $\mathcal{A}^T$ is surjective. By the argument above, $\mathcal{A}^T$ has a right inverse that is a matrix, which we denote by $\mathcal{M}$. Then

$$\mathcal{A}^T\mathcal{M} = \mathcal{I}\ ,$$

and therefore

$$\mathcal{I} = \mathcal{I}^T = \left(\mathcal{A}^T\mathcal{M}\right)^T = \mathcal{M}^T\mathcal{A}.$$

This shows that $\mathcal{M}^T$ is a left inverse of $\mathcal{A}$, and the proof is complete. ■

Test Your Comprehension 13.2.2 ☞ **One-sided inversion switches the jectivity**

Hint: TYC 2.4.3.

Argue that a left inverse of an injective matrix is automatically surjective, and that a right inverse of a surjective matrix is automatically injective.

Example 13.2.3

A matrix that has a partitioned form $\begin{bmatrix}\mathcal{I}\\ \mathcal{A}\end{bmatrix}$ is injective, because it is left-invertible. Indeed,

$$[\mathcal{I}\ \mathcal{O}]\begin{bmatrix}\mathcal{I}\\ \mathcal{A}\end{bmatrix} = \mathcal{I}\ .$$

Since

$$[\mathcal{O}\ \mathcal{I}]\begin{bmatrix}\mathcal{A}\\ \mathcal{I}\end{bmatrix} = \mathcal{I}\ ,$$

every matrix with a partitioned form $\begin{bmatrix}\mathcal{A}\\ \mathcal{I}\end{bmatrix}$ is injective as well.

Identities

$$[\mathcal{A}\ \mathcal{I}]\begin{bmatrix}\mathcal{O}\\ \mathcal{I}\end{bmatrix} = \mathcal{I} \text{ and } [\mathcal{I}\ \mathcal{A}]\begin{bmatrix}\mathcal{I}\\ \mathcal{O}\end{bmatrix} = \mathcal{I}$$

show that matrices of partitioned forms $[\mathcal{A}\ \mathcal{I}]$ and $[\mathcal{I}\ \mathcal{A}]$ are always right-invertible, and hence surjective.

We can generalize this to (partitioned) matrices of the form $\begin{bmatrix}\mathcal{A}\\ \mathcal{B}\end{bmatrix}$ and $[\mathcal{A}\ \mathcal{B}]$, where either $\mathcal{A}$ or $\mathcal{B}$ is invertible.

For example, if $\mathcal{A}$ is invertible, then

$$[\mathcal{A}\ \mathcal{B}]\begin{bmatrix}\mathcal{A}^{-1}\\ \mathcal{O}\end{bmatrix} = \mathcal{I}\ ,$$

which shows that $[\mathcal{A}\ \mathcal{B}]$ is right-invertible, and hence – surjective.

Test Your Comprehension 13.2.4

Argue that $\begin{bmatrix}\mathcal{A}\\ \mathcal{B}\end{bmatrix}$ is injective and $[\mathcal{A}\ \mathcal{B}]$ is surjective, whenever either $\mathcal{A}$ or $\mathcal{B}$ is invertible.

Observation 13.2.5

Matrices $\left[\begin{smallmatrix}\mathcal{A}\\ \mathcal{B}\end{smallmatrix}\right]$, where either $\mathcal{A}$ or $\mathcal{B}$ is invertible, have the property that by removing some rows we can arrive at an invertible matrix.

Matrices $[\mathcal{A}\ \mathcal{B}]$, where either $\mathcal{A}$ or $\mathcal{B}$ is invertible, have the property that by removing some columns we can arrive at an invertible matrix.

As we shall show on the next few pages, these properties turn out to be equivalent to the respective injectivity/surjectivity of the matrices.

13.2.2 — Invertibility Of Products Of Square Matrices

Lemma 13.2.6

A product $\mathcal{AB}$ of *square* matrices $\mathcal{A}$ and $\mathcal{B}$ is invertible exactly when $\mathcal{A}$ and $\mathcal{B}$ are both invertible.

Proof of Lemma 13.2.6. Let $\mathcal{C} = \mathcal{AB}$. If $\mathcal{C}$ is invertible, it is bijective, in which case $\mathcal{A}$ must be surjective, and $\mathcal{B}$ must be injective by TYC 2.4.3. For square matrices all jectivities are equivalent to invertibility (TYC 11.2.4). ■

Test Your Comprehension 13.2.7

Demonstrate that the claim of Corollary 13.2.6 would be false without the assumption that at least one of A and B is a square matrix.

Corollary 13.2.8 ☞ **Square factorizations of the identity**

If $\mathcal{A}$ and $\mathcal{B}$ are *square* matrices such that

$$\mathcal{AB} = \mathcal{I},$$

then $\mathcal{A}$ and $\mathcal{B}$ are invertible and are mutual (two-sided) inverses. In particular

$$\mathcal{AB} = \mathcal{I} = \mathcal{BA}.$$

The hypothesis that $\mathcal{A}$ and $\mathcal{B}$ are square is essential.

Proof of Theorem 13.2.8. If $\mathcal{AB} = \mathcal{I}$ then $\mathcal{A}$ and $\mathcal{B}$ are invertible by Lemma 13.2.6. Thus

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

If either $\mathcal{A}$ or $\mathcal{B}$ is not square, then either $\mathcal{AB} = \mathcal{I}$ or $\mathcal{BA} = \mathcal{I}$ fails by TYC 13.2.9. ■

Hint: Theorem 13.2.1.

Test Your Comprehension 13.2.9

Argue that the identity matrix $\mathcal{I}$ *cannot* be expressed as a product $\mathcal{AB}$ where $\mathcal{A}$ is strictly portrait-shaped.

Similarly, argue that it *cannot* be expressed as a product $\mathcal{AB}$ where $\mathcal{B}$ is strictly landscape-shaped.

Hint: In fact we can always find such $\mathcal{A}$ and $\mathcal{B}$ that are SPI's. Clearly $\mathcal{A}$ has to be surjective, and $\mathcal{B}$ has to be injective.

Test Your Comprehension 13.2.10

Argue that it is always possible to express $\mathcal{I}$ as a product $\mathcal{AB}$ where $\mathcal{A}$ is strictly landscape-shaped and $\mathcal{B}$ is strictly portrait-shaped.

Theorem 13.2.11 ☞ **Invertibility of products of square matrices**

A product $\mathcal{A}_1\mathcal{A}_2\cdots\mathcal{A}_k$ of *square* matrices is invertible if and only if each $\mathcal{A}_i$ is invertible.

Proof of Theorem 13.2.11. Since we already know that a composition of invertible functions is invertible, what remains to be shown is that for *square* matrices the invertibility of the product implies the invertibility of the individual matrices.

By Lemma 13.2.6, this implication holds true when $k = 2$. If it were not true in general, there would be a first k for which the implication fails, and such k would be at least 3. For the simplicity of notation let us say that the first such k is 173.

So, we would have that the invertibility of a product of at most 172 square matrices entails invertibility of the factors, but there would be an invertible product of 173 square matrices at least one of which is not invertible:

$$\mathcal{A}_1\mathcal{A}_2\cdots\mathcal{A}_{173}\ .$$

Express this product as a product of just two matrices:

$$(\mathcal{A}_1)\circ(\mathcal{A}_2\mathcal{A}_3\cdots\mathcal{A}_{173})\ .$$

Apply Lemma 13.2.6 and conclude that $\mathcal{A}_1$ is invertible, and that $\mathcal{A}_2\mathcal{A}_3\cdots\mathcal{A}_{173}$ is invertible.

Since the latter is the product of 172 square matrices, and the implication we are working with holds true for products of at most 172, it must be that $\mathcal{A}_2, \mathcal{A}_3, \ldots, \mathcal{A}_{173}$ are invertible.

Now we have that all $\mathcal{A}_1, \mathcal{A}_2, \ldots, \mathcal{A}_{173}$ are invertible, contrary to the initial assumption that not all of these matrices are.

The only feasible conclusion is that no counterexamples exist, and the implication holds universally. ∎

13.2.3 — Invertibility Of Block-Triangular Matrices

We can now improve on the last part of Exercise 9.2.6 which dealt with the invertibility of direct sums of matrices. Please note that at the time the exercise was given, we had not yet established that invertible matrices must be square.

Theorem 13.2.12

A block-upper-triangular matrix $\left[\begin{smallmatrix} \mathcal{A} & \mathcal{B} \\ \mathcal{O} & \mathcal{D} \end{smallmatrix}\right]$ is invertible exactly when $\mathcal{A}$ and $\mathcal{D}$ are invertible.

When these conditions hold, we have the formula

$$\left[\begin{smallmatrix} \mathcal{A} & \mathcal{B} \\ \mathcal{O} & \mathcal{D} \end{smallmatrix}\right]^{-1} = \begin{bmatrix} \mathcal{A}^{-1} & -\mathcal{A}^{-1}\mathcal{B}\mathcal{D}^{-1} \\ \mathcal{O} & \mathcal{D}^{-1} \end{bmatrix}.$$

While this may be surprising at first, $\mathcal{B}$ has no effect on the invertibility of our matrix.

Please recall that our definition of the term "block-upper-triangular" incorporates the requirement that the diagonal blocks are all square-shaped.

Proof of Theorem 13.2.12. If $\left[\begin{smallmatrix} \mathcal{A} & \mathcal{B} \\ \mathcal{O} & \mathcal{D} \end{smallmatrix}\right]$ is bijective, then $\mathcal{A}$ is injective and $\mathcal{D}$ is surjective (Theorem 9.1.20). Since $\mathcal{A}$ and $\mathcal{D}$ are square matrices, any form of the jectivity is equivalent to bijectivity for these matrices (TYC 11.2.4). Hence $\mathcal{A}$ and $\mathcal{D}$ are bijective, and we have verified the implication in the forward direction.

Next we assume that $\mathcal{A}$ and $\mathcal{D}$ are invertible, and argue that $\left[\begin{smallmatrix} \mathcal{A} & \mathcal{B} \\ \mathcal{O} & \mathcal{D} \end{smallmatrix}\right]$ is invertible as well. This can be accomplished by verifying the identity

$$\left[\begin{smallmatrix} \mathcal{A} & \mathcal{B} \\ \mathcal{O} & \mathcal{D} \end{smallmatrix}\right]\begin{bmatrix} \mathcal{A}^{-1} & -\mathcal{A}^{-1}\mathcal{B}\mathcal{D}^{-1} \\ \mathcal{O} & \mathcal{D}^{-1} \end{bmatrix} = \mathcal{I}\ , \tag{13.3}$$

and then applying Theorem 13.2.8, which tells us that there is no need to test the product of these *square* matrices in reversed order.

We leave the verification of the identity (13.3) to the reader (TYC 13.2.13), as it is a straight forward application of the fundamental formula for partitioned matrix multiplication (Theorem 9.1.8). Of course, the reader should verify that the partitioning involved is appropriate for the application of the fundamental formula. ∎

Test Your Comprehension 13.2.13

Verify the validity of the identity (13.3).

An Additional Commentary on the Proof of Theorem 13.2.12. Our proof of Theorem 13.2.12 was based on the verification of the identity (13.3). It is effective but is not educationally satisfying, as is often the case. The matrix $\begin{bmatrix} \mathcal{A}^{-1} & -\mathcal{A}^{-1}\mathcal{B}\mathcal{D}^{-1} \\ \mathcal{O} & \mathcal{D}^{-1} \end{bmatrix}$ was proverbially "pulled out of a hat", and no indication has been given as to its genesis. To alleviate this shortcoming we offer an additional explanation here.

1. Theorem 9.1.10 tells us that a square matrix of the form

$$\begin{bmatrix} \mathcal{I}_k & \mathcal{B} \\ \mathcal{O} & \mathcal{I}_m \end{bmatrix}_{(k|m)\times(k|m)}$$

is invertible for any $\mathcal{B} \in \mathbb{M}_{k\times m}$, and its inverse is

$$\begin{bmatrix} \mathcal{I}_k & -\mathcal{B} \\ \mathcal{O} & \mathcal{I}_m \end{bmatrix}_{(k|m)\times(k|m)} .$$

2. In Exercise 8.1.27 we explored the effect of multiplying a given matrix by a diagonal matrix. Later the fundamental formula for partitioned matrix multiplication was used to verify a generalization of this for partitioned matrices (TYC. 9.2.9).

Thus, when $\mathcal{A}$ is invertible, we are led to the identity

$$\begin{bmatrix} \mathcal{A} & \mathcal{B} \\ \mathcal{O} & \mathcal{D} \end{bmatrix} = \begin{bmatrix} \mathcal{A} & \mathcal{O} \\ \mathcal{O} & \mathcal{D} \end{bmatrix}\begin{bmatrix} \mathcal{I} & \mathcal{A}^{-1}\mathcal{B} \\ \mathcal{O} & \mathcal{I} \end{bmatrix}. \tag{13.4}$$

3. When both $\mathcal{A}$ and $\mathcal{D}$ are invertible, so is $\mathcal{A} \oplus \mathcal{D}$, and

$$\begin{bmatrix} \mathcal{A} & \mathcal{O} \\ \mathcal{O} & \mathcal{D} \end{bmatrix}^{-1} = \begin{bmatrix} \mathcal{A}^{-1} & \mathcal{O} \\ \mathcal{O} & \mathcal{D}^{-1} \end{bmatrix}$$

(Exc. 9.2.6). In such a case, we have the following equalities that lead to the formula "pulled out from a hat" in Theorem 13.2.12:

$$\begin{bmatrix} \mathcal{A} & \mathcal{B} \\ \mathcal{O} & \mathcal{D} \end{bmatrix}^{-1} \overset{(13.4)}{=} \left(\begin{bmatrix} \mathcal{A} & \mathcal{O} \\ \mathcal{O} & \mathcal{D} \end{bmatrix}\begin{bmatrix} \mathcal{I} & \mathcal{A}^{-1}\mathcal{B} \\ \mathcal{O} & \mathcal{I} \end{bmatrix}\right)^{-1} = \begin{bmatrix} \mathcal{I} & \mathcal{A}^{-1}\mathcal{B} \\ \mathcal{O} & \mathcal{I} \end{bmatrix}^{-1}\begin{bmatrix} \mathcal{A} & \mathcal{O} \\ \mathcal{O} & \mathcal{D} \end{bmatrix}^{-1}$$

$$\overset{\text{Thm. 13.2.12 \& Exc. 9.2.6}}{=} \begin{bmatrix} \mathcal{I} & -\mathcal{A}^{-1}\mathcal{B} \\ \mathcal{O} & \mathcal{I} \end{bmatrix}\begin{bmatrix} \mathcal{A}^{-1} & \mathcal{O} \\ \mathcal{O} & \mathcal{D}^{-1} \end{bmatrix}$$

$$\overset{\text{TYC. 9.2.9}}{=} \begin{bmatrix} \mathcal{A}^{-1} & -\mathcal{A}^{-1}\mathcal{B}\mathcal{D}^{-1} \\ \mathcal{O} & \mathcal{D}^{-1} \end{bmatrix}.$$

■

Test Your Comprehension 13.2.14

Demonstrate that Theorem 13.2.12 would be false without the assumption that both $\mathcal{A}$ and $\mathcal{D}$ are square. Do this by partitioning the identity matrix

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

Test Your Comprehension 13.2.15

Use transposition to prove the analogue of Theorem 13.2.12 for the block-lower-triangular case.

One advantage of partitioning matrices is that we are frequently able to generalize a result about partitioned matrices with just 2 block-rows and 2 block-columns to more general partitioned matrices. Using this approach we shall be able to prove the following extension of Theorem 13.2.12 with relative ease.

Theorem 13.2.16

If $\mathcal{A}$ is a block-upper-triangular matrix, then $\mathcal{A}$ is invertible exactly when every one of its block-diagonal entries is invertible.

(Alas, there is no simple formula for the inverse of $\mathcal{A}$ in this general case.)

Proof of Theorem 13.2.16.

INSERT PICTURE ■

Test Your Comprehension 13.2.17

Use transposition to prove the analogue of Theorem 13.2.16 for the block-lower-triangular case.

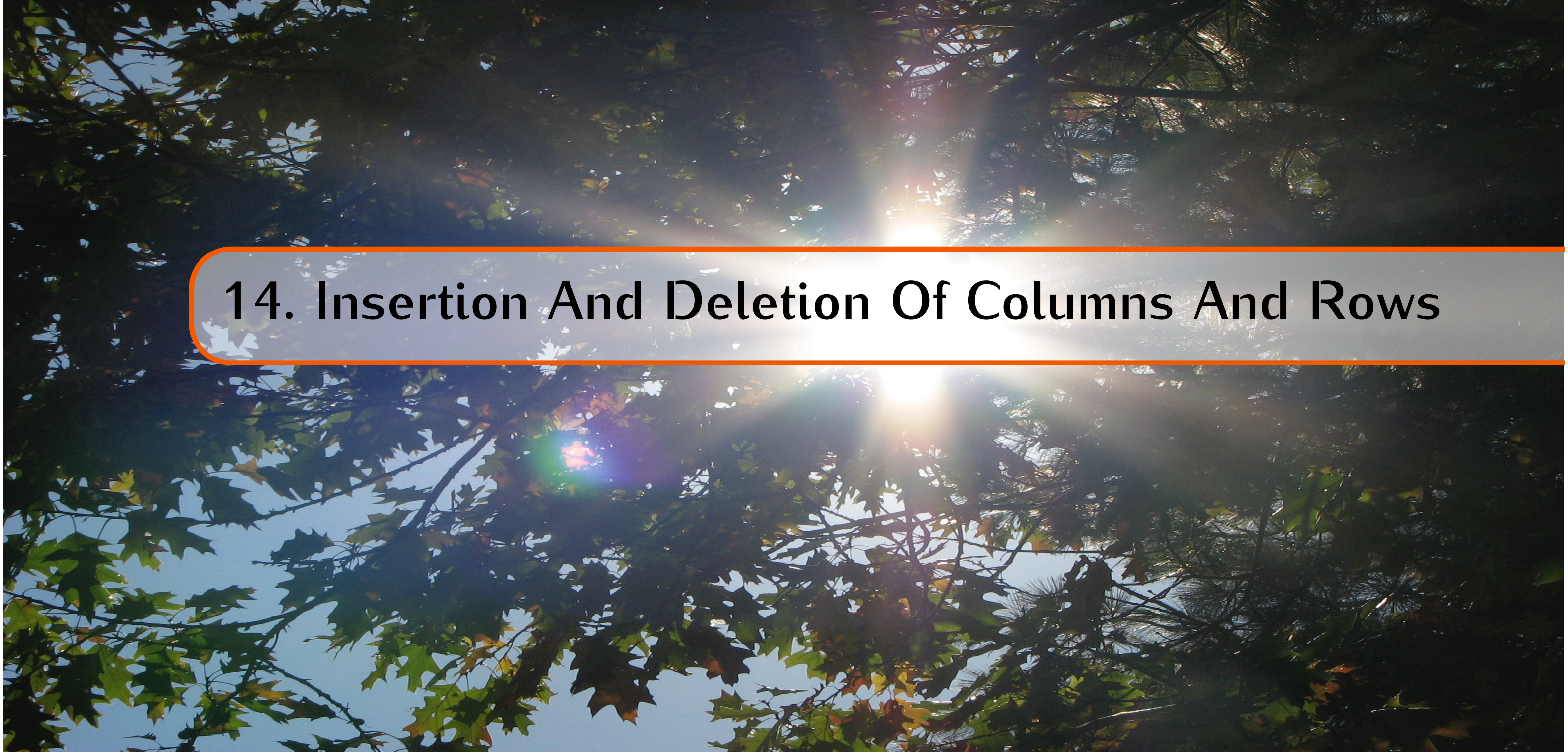
Corollary 13.2.18

An upper-triangular matrix is invertible exactly when none of its diagonal entries are zero.

The same goes for lower-triangular matrices.

It is natural to ask for a similarly simple way of deciding when a more general (partitioned) matrix is invertible. There is a method in a non-partitioned case, but its mechanism is not what one might call simple. This shall be a focus in our discussion of “determinant” later on. We have already dealt with the 2×2 setting in Theorem 10.2.13. No easy analogue of the method is available in the general partitioned matrix case, even though much can be said in some restricted cases.

13.2.4 — Schur Complements



14. Insertion And Deletion Of Columns And Rows

Last modified on December 8, 2018

14.1 Column Deletion And Jectivity

14.1.1 — Column Deletion And The Range

Exercise 14.1.1 ☞ **Inserting or deleting null columns does not alter the range**

Argue that a matrix produced from a matrix $\mathcal{A}$ by inserting or deleting null columns has the same range as $\mathcal{A}$.

Hint: The range of a matrix is the set of all linear combinations of its columns.

Theorem 14.1.2 ☞ **Creating null columns via column operations**

If a column of a matrix $\mathcal{A}$ is a linear combination of some of the other columns of $\mathcal{A}$, then by performing a sequence of column adjustments we can turn that column into a null tuple.

Proof of Theorem 14.1.2. As usual, we shall avoid the use of fully general subscripts in order to simplify the notation without any detriment to the crux of the argument. In the same vein we assume that it is the last column of our $\mathcal{A}$ that is a linear combination of some of the previous columns.

Let us say $\mathcal{A} = \begin{bmatrix} C_1 & C_2 & \dots & C_{27} & C_{28} \end{bmatrix}$, where

$$\alpha_7 C_7 + \alpha_3 C_3 + \alpha_{23} C_{23} + \cdots + \alpha_{15} C_{15} = C_{28} \ .$$

Adjust the 28-th column C_{28} of $\mathcal{A}$ by subtracting from it $\alpha_7 C_7$. This produces a matrix

$$\mathcal{A}' \coloneqq \begin{bmatrix} C_1 & C_2 & \dots & C_{27} & C'_{28} \end{bmatrix} ,$$

where $\alpha_3 C_3 + \alpha_{23} C_{23} + \cdots + \alpha_{15} C_{15} = C'_{28}$.

Adjust the 28-th column C'_{28} of $\mathcal{A}'$ by subtracting from it $\alpha_3 C_3$. This produces a matrix

$$\mathcal{A}'' := \begin{bmatrix} C_1 & C_2 & \ldots & C_{27} & C''_{28} \end{bmatrix},$$

where $\alpha_{23} C_{23} + \cdots + \alpha_{15} C_{15} = C''_{28}$.

Proceeding this way, we eventually arrive at a matrix

$$\mathcal{A}^* := \begin{bmatrix} C_1 & C_2 & \ldots & C_{27} & C^*_{28} \end{bmatrix},$$

where $\alpha_{15} C_{15} = C^*_{28}$.

Adjust the 28-th column C^*_{28} of $\mathcal{A}^*$ by subtracting from it $\alpha_{15} C_{15}$. This produces a matrix

$$\mathcal{A}^{**} := \begin{bmatrix} C_1 & C_2 & \ldots & C_{27} & \mathbb{0} \end{bmatrix}.$$

■

Corollary 14.1.3 ☞ **Deleting columns without changing the range**

Suppose that a matrix $\mathcal{B}$ is obtained from a matrix $\mathcal{A}$ via a deletion of some of the columns. Then the following statements are equivalent.

1. *Range* $(\mathcal{B})$ = *Range* $(\mathcal{A})$.

2. All of the deleted columns were in the range of $\mathcal{B}$; i.e. were linear combinations of the remaining columns.

Proof of Corollary 14.1.3.

1. $\implies$ 2.: Columns of a matrix are always in its range. Thus, all columns of $\mathcal{A}$, including the ones being deleted, are in the range of $\mathcal{A}$, and so in the range of $\mathcal{B}$, when the two ranges are equal.

2. $\implies$ 1.: Elementary column operations do not affect the range of a matrix (TYC 10.2.10) and neither does a deletion of null columns (Exc. 14.1.1). Hence the claimed implication follows immediately from Theorem 14.1.2. ■

Theorem 14.1.4 ☞ **Slimming down to an injective matrix with the same range**

Given a non-null matrix $\mathcal{A}$, by deleting some (may be none) of the columns of $\mathcal{A}$ it is always possible to arrive at an *injective* matrix that has the same range as $\mathcal{A}$.

Proof of Corollary 14.1.4. Begin by deleting all of the null columns of $\mathcal{A}$. By Exercise 14.1.1 this does not alter the range. If one of the remaining columns is a linear combination of the others, remove it. By Theorem 14.1.3 this does not alter the range either. If one of the remaining columns is a linear combination of the others, remove it. Keep going until no remaining column is a linear combination of the others.

This procedure does terminate, since there are only finitely many columns to start with. After the procedure terminates we are left with a matrix $\mathcal{B}$ that has the same range as $\mathcal{A}$ (since no step in the procedure altered the range). In particular $\mathcal{B} \neq \mathcal{O}$. Furthermore, no column of $\mathcal{B}$ is a linear combination of the other columns of $\mathcal{B}$. This means that $\mathcal{B}$ is injective (Theorem 12.2.5). ■

Synopsis 14.1.5 ☞ **Operations preserving *the range***

Composition with a surjection on the right.

Elementary column operations.

Reordering (the list of) the columns.

Insertion or deletion of null columns.

Removal of a column that is a linear combination of other columns.

Insertion of a column that is a linear combination of the existing columns.

Test Your Comprehension 14.1.6 ☞ **Every surjective matrix can be slimmed down to an invertible one**

Argue that if $\mathcal{A}$ is a surjective matrix then by deleting some of the columns of $\mathcal{A}$ it is possible to arrive at an invertible matrix.

Hint: Thm. 14.1.4.

Comment 14.1.7

As we have shown, by deleting some of the columns of a non-null $\mathcal{A}$ it is always possible to produce an injective matrix with the same range. Our argument relied on the deletion, one by one, of the columns that are linear combinations of the other columns. How does one discern which of the columns of a matrix have this property?

Deciding whether a tuple is a linear combination of some given tuples amounts to figuring out whether a certain system of linear equations has solutions. We shall develop algorithms for this later in the book. Hence, in principle, one can consider the columns one at a time, and in each case analyze the associated linear system.

It is natural to ask whether the removal of the columns can be done in a "whole sale" fashion via a reasonably simple algorithm. The answer is affirmative, and we shall introduce such a procedure (Thm. 19.6.1) after we explore Gauss-Jordan Elimination Scheme.

Hint: Think about deleting one column at a time. Thm. 12.2.5 can be useful here. The same goes for Thm. 12.2.3.

Exercise 14.1.8 ☞ Column deletion cannot destroy injectivity

Argue that deleting some (but not all) columns from an injective matrix (with more than one column) produces another injective matrix.

14.2 Column Insertion And Jectivity

14.2.1 — Surjectivity And Column Insertion

Exercise 14.2.1 ☞ Inserting columns without changing the range

Suppose that a matrix $\mathcal{B}$ is obtained from a matrix $\mathcal{A}$ via an insertion of some additional columns. Argue that the following statements are equivalent.

Hint: Cor. 14.1.3.

1. $\mathit{Range}(\mathcal{B}) = \mathit{Range}(\mathcal{A})$.
2. All of the inserted columns came from the range of $\mathcal{A}$.

Test Your Comprehension 14.2.2 ☞ Column insertion cannot destroy surjectivity

Hint: Exc. 14.2.1.

Argue that inserting columns into a surjective matrix produces a surjective matrix.

By putting TYC's 14.2.2 and 14.1.6 together, we deduce that surjective matrices are exactly those that can be obtained from invertible matrices by inserting columns; i.e. by "widening" them.

Test Your Comprehension 14.2.3 ☞ Surjective = a widened invertible

Argue that the following are equivalent for a matrix $\mathcal{A}$.

Comment 14.1.7 is relevant in this context as well.

1. $\mathcal{A}$ is surjective.
2. $\mathcal{A}$ can be obtained by inserting some additional columns into an invertible matrix.
3. By deleting some of the columns of $\mathcal{A}$ it is possible to arrive at an invertible matrix.

Given a surjective matrix, how does one discern which columns of it can be removed to reveal an invertible matrix promised by TYC 14.2.3? Theorem 19.6.1 will furnish an efficient answer to this question.

14.2.2 — Injectivity And Column Insertion

Theorem 14.2.4 **Inserting columns without creating/destroying injectivity**

If Y is a tuple of an appropriate size that is not in the range of a matrix $\mathcal{A}$, then inserting Y into $\mathcal{A}$ as an additional column does not create or destroy injectivity.

In other words, the new matrix is injective if and only if $\mathcal{A}$ is injective.

Synopsis of the proof: When a tuple Y is not in the range of a matrix $\mathcal{A}$, it is not a linear combination of the columns of $\mathcal{A}$. If we insert Y into $\mathcal{A}$ as an additional column in the last position, thus creating a new matrix $\mathcal{B}$, then the injectivity of $\mathcal{B}$ is determined by the answers to the following two questions.

- Is the first column of $\mathcal{B}$ is null?
- Is any of the columns of $\mathcal{B}$ a linear combination of the previous columns?

Since the last column of $\mathcal{B}$ is Y and it is NOT a linear combination of the previous columns (those from $\mathcal{A}$), the questions we stated have exactly the same answers as the questions

- Is the first column of $\mathcal{A}$ is null?
- Is any of the columns of $\mathcal{A}$ a linear combination of the previous columns?

This shows that the injectivity of $\mathcal{A}$ is equivalent to the injectivity of $\mathcal{B}$.

Proof of Theorem 14.2.4.

Let $\mathcal{B}$ be a matrix obtained from $\mathcal{A}$ by inserting Y as an additional column. Since column swaps do not affect the jectivity of a matrix, it is sufficient to focus on the case of Y being the last column of $\mathcal{B}$; (otherwise we can always make it so through swaps).

Let us write $\mathcal{A} = \begin{bmatrix} C_1 & C_2 & \cdots & C_m \end{bmatrix}$, so that $\mathcal{B} = \begin{bmatrix} C_1 & C_2 & \cdots & C_m & Y \end{bmatrix}$.

If $\mathcal{A}$ is not injective, then either $\mathcal{A} = \begin{bmatrix} \mathbb{O}_n \end{bmatrix}$ or a column of $\mathcal{A}$ is a linear combination of other columns of $\mathcal{A}$ (Thm. 12.2.5). Thus either $\mathcal{B}$ has a null column or one of its columns is a linear combination of its other columns. In either case $\mathcal{B}$ is not injective.

If $\mathcal{A}$ is injective then C_1 is not null and no C_j is a linear combination of the preceding C_i's (Thm. 12.2.5). Thus the first column of $\mathcal{B}$ is not null, and the only column of $\mathcal{B}$ that is possibly a linear combination of the preceding columns is Y.

Yet Y is not in the range of $\mathcal{A}$, and so is not a linear combination of $C_1, C_2, \ldots, C_m$. Thus no column of $\mathcal{B}$ is a linear combination of the preceding columns of $\mathcal{B}$. Hence $\mathcal{B}$ is injective. ■

Test Your Comprehension 14.2.5

Argue that inserting additional columns into a matrix ALWAYS changes its nullspace. Why does this not contradict Theorem 14.2.4?

Hint: What happens to the domain of the matrix when one inserts additional columns?

Injective matrices are half-way to being invertible. They are of course exactly the left-invertible matrices, but this is not what we mean in this instance. Invertible matrices are exactly those with the smallest possible nullspace and the largest possible range. The injective matrices have a trivial subspace, but may be lacking in the fullness of the range.

The next result shows that it is always possible to add a few columns to an injective matrix to fill out the range without increasing the nullspace, thus creating an invertible matrix. In fact this characterizes the injective matrices as exactly those that can be obtained from invertible matrices by deleting columns; i.e. by "narrowing" them.

As usual, "some" includes the possibility of "none".

Theorem 14.2.6 ☞ Injective = a narrowed invertible

The following statements are equivalent for a matrix $\mathcal{A}$.

1. $\mathcal{A}$ is injective.
2. By inserting some columns into $\mathcal{A}$ it is possible to arrive at an invertible matrix. (Where the columns are inserted is immaterial.*)
3. $\mathcal{A}$ can be obtained by deleting some columns from an invertible matrix.

*Rearranging the order in which the columns appear amounts to performing a number of column swaps, and thus does not affect the jectivity (Obs. 10.2.9).

Proof of Theorem 14.2.6.

[**1.** $\Longrightarrow$ **2.**]: The proof is based on Theorem 14.2.4, which tells us that inserting an n-tuple, which is outside of the range of an $n \times m$ matrix $\mathcal{A}$, into $\mathcal{A}$ as an additional column does not create or destroy injectivity.

Injective non-invertible matrices are strictly portrait-shaped (TYC's 11.2.2 and 11.2.4). If $\mathcal{A} \in \mathbb{M}_{n\times m}$ is one such then it is not surjective and so there is an n-tuple Y outside of its range.

Inserting this Y into $\mathcal{A}$ as an additional column does not destroy injectivity (Thm. 14.2.4). If the resulting injective matrix is square, it is invertible (TYC 11.2.4), and we are done.

In the alternative case, the resulting injective matrix is again strictly portrait-shaped, and we can add one more column to it without destroying injectivity. We proceed this way, adding one column at a time, without destroying injectivity, until we arrive at an injective square matrix, and that matrix is invertible by TYC 11.2.4.

[**3.** $\Longrightarrow$ **1.**]: TYC 14.1.8.

Since the equivalence 2. $\Longleftrightarrow$ 3. is clear, we are done. ■

Comment 14.2.7

Let us note that while Theorem 14.2.6 tells us that certain things are possible, it does not offer a practical way (i.e. an algorithm) for carrying out the process. How do we actually find the appropriate columns for insertion/deletion that will let us arrive at an invertible matrix? Such algorithms do exists, and we will present one as Algorithm 16.2.34.

14.3 Row Insertion/Deletion And Jectivity

The fact that transposition reverses the jectivity (Thm. 11.2.14) can be used to convert the jectivity results dealing with the insertion/deletion of columns into the results dealing with the insertion/deletion of rows.

14.3.1 — Row Deletion And Jectivity

For example, the fact that a deletion of some (but not all) columns from an injective matrix produces an injective matrix (TYC 14.1.8), yields the following result.

Test Your Comprehension 14.3.1 ☞ **Row deletion does not destroy surjectivity**

Argue that a deletion of some (but not all) rows from a surjective matrix produces a surjective matrix.

Hint: Thms. 14.2.3 and 11.2.14.

As usual, "some" includes the possibility of "none".

Test Your Comprehension 14.3.2 ☞ **Injective = a heightened invertible**

Argue that the following are equivalent for a matrix $\mathcal{A}$.

1. $\mathcal{A}$ is injective.
2. By deleting some of the rows of $\mathcal{A}$ it is possible to arrive at an invertible matrix.
3. $\mathcal{A}$ can be obtained by inserting some additional rows into an invertible matrix.

14.3.2 — Row Insertion And Jectivity

Since an insertion of columns into a surjective matrix produces a surjective matrix (TYC 14.2.2), we also have the following.

Test Your Comprehension 14.3.3 ☞ **Row insertion does not destroy injectivity**

Argue that an insertion of additional rows into an injective matrix produces an injective matrix.

Test Your Comprehension 14.3.4 ☞ **Surjective = a shortened invertible**

Argue that the following are equivalent for a matrix $\mathcal{A}$.

1. $\mathcal{A}$ is surjective.
2. By inserting some rows into $\mathcal{A}$ it is possible to arrive at an invertible matrix.
3. $\mathcal{A}$ can be obtained by deleting some rows from an invertible matrix.

14.4 Synopsi

Synopsis 14.4.1 ☞ **Producing injective/surjective matrices from the invertible ones**

A widening or a narrowing of an invertible matrix always produces a matrix possessing the only jectivity possible for its shape.

This does not apply to a simultaneous change in both width and height: see TYC 14.4.2 below.

Test Your Comprehension 14.4.2

1. Give a concrete example to show that by deleting some rows *and* some columns from an invertible matrix one can arrive at a matrix that is neither injective nor surjective.

2. Similarly, give a concrete example to show that by inserting some rows *and* some columns into an invertible matrix one can arrive at a matrix that is neither injective nor surjective.

Synopsis 14.4.3 ☞ **Producing the invertible matrices from the injective/surjective ones**

A matrix that is either injective or surjective may be converted to an invertible matrix by either a change in width or in height (in a way that produces a square shape).

Such changes are NOT arbitrary and have to be carried out in a particular way to achieve the stated result.

Synopsis 14.4.4 ☞ **Operations on matrices that do not destroy *injectivity***

Composition with an injective matrix.

Elementary row/column operations.

Reordering of the columns and of the rows.

Deletion of some columns.

Insertion of a column that is NOT a linear combination of the existing columns.

Deletion of a row that is a linear combination of other rows.

Insertion of some rows.

It is understood that we are only considering operations that produce matrices. For example, deleting the only column of a matrix does not qualify.

Synopsis 14.4.5 ☞ Operations on matrices that do not destroy *surjectivity*

Composition with a surjective matrix.

Elementary row/column operations.

Reordering of the columns and of the rows.

Deletion of some rows.

Insertion of a row that is NOT a linear combination of the existing rows.

Deletion of a column that is a linear combination of other columns.

Insertion of some columns.

Synopsis 14.4.6 ☞ Conditions equivalent to *injectivity*

This enlarges Synopsis 12.2.7 for a matrix $\mathcal{A}$.

$\mathcal{A}$ has a trivial nullspace: $\mathit{Nullspace}(\mathcal{A}) = \{\mathbb{O}\}$.

Columns of $\mathcal{A}$ are linearly independent: The only linear combination of the columns of A that equals the null tuple is the trivial linear combination.

No column of $\mathcal{A}$ is a linear combination of other columns, . . . : *$\mathcal{A}$ is not a null matrix and* no column of $\mathcal{A}$ is a linear combination of some other columns.

No column of $\mathcal{A}$ is a linear combination of the preceding columns, . . . : *The first column of $\mathcal{A}$ is not null, and* no column of $\mathcal{A}$ is a linear combination of the preceding columns.

$\mathcal{A}^T\mathcal{A}$ is invertible.

$\mathcal{A}$ is obtained by inserting some rows into an invertible matrix.

$\mathcal{A}$ is obtained by deleting some columns from an invertible matrix.

$\mathcal{A}$ is left-invertible (as a function).

$\mathcal{A}$ has a left inverse that is a matrix.

A^T is surjective.

One obtains the corresponding equivalent conditions for surjectivity via the transposition.

15. Rank One Matrices And Full Rank Factorization

Last modified on December 8, 2018

15.1 Full Rank Factorization

Test Your Comprehension 15.1.1 ☞ **Factoring out a SPI**

Every $n \times m$ SPI $\mathcal{S}$ of a positive rank k can be expressed as a product of two SPI's of a particular form:

$$\mathcal{S} = \begin{bmatrix} \mathcal{I}_k \\ \mathcal{O} \end{bmatrix}_{n\times k} \begin{bmatrix} \mathcal{I}_k & \mathcal{O} \end{bmatrix}_{k\times m} = \begin{bmatrix} 1 & 0 & 0 & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}_{n\times k} \begin{bmatrix} 1 & 0 & 0 & \dots & 0 & \cdots & 0 \\ 0 & 1 & 0 & \dots & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \dots & \vdots \\ 0 & 0 & 0 & \dots & 1 & \cdots & 0 \end{bmatrix}_{k\times m}$$

$$= \begin{bmatrix} E_1 & E_2 & \dots & E_k \end{bmatrix}_{n\times k} \circ \begin{bmatrix} \longleftarrow & E_1 & \longrightarrow \\ \longleftarrow & E_2 & \longrightarrow \\ & \vdots & \\ \longleftarrow & E_k & \longrightarrow \end{bmatrix}_{k\times m} .$$

Theorem 15.1.2 ☞ **Inj∘Surj Factorization (a.k.a. Full Rank Factorization)**

Every non-null matrix $\mathcal{A} \in \mathbb{M}_{n\times m}$ can be expressed as a product $\mathcal{B}\mathcal{C}$, where $\mathcal{B}$ is injective and $\mathcal{C}$ is surjective.

Furthermore:

1. In every such factorization $\mathcal{B}$ is an $n \times \boldsymbol{k}$ matrix and $\mathcal{C}$ is a $\boldsymbol{k} \times m$ matrix, and $\boldsymbol{k}$ is the rank of $\mathcal{A}$.

2. In every such factorization

$$\mathit{Range}(\mathcal{B}) = \mathit{Range}(\mathcal{A}) \quad \text{and} \quad \mathit{Nullspace}(\mathcal{C}) = \mathit{Nullspace}(\mathcal{A}) \ .$$

3. If $\mathcal{B}\mathcal{C}$ and $\hat{\mathcal{B}}\hat{\mathcal{C}}$ are two such factorizations of $\mathcal{A}$, then there is an invertible matrix $\mathcal{S}$ such that

$$\hat{\mathcal{B}} = \mathcal{B}\mathcal{S} \quad \text{and} \quad \hat{\mathcal{C}} = \mathcal{S}^{-1}\mathcal{C} \ .$$

A proof of Theorem 15.1.2 is presented in the appendix to the chapter.

Exercise 15.1.3

Which matrices can be expressed as "Surj ∘ Inj", i.e. as a composition $\mathcal{A} \circ \mathcal{B}$, where $\mathcal{A}$ is a surjective matrix, and $\mathcal{B}$ is an injective matrix? Give a complete characterization.

15.2 Rank One Matrices

Exercise 15.2.1

An $n \times m$ matrix $\mathcal{A}$ has rank 1 exactly when it can be expressed as

$$\mathcal{A} = \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix} \begin{bmatrix} y_1 & y_2 & \cdots & y_m \end{bmatrix} = \begin{bmatrix} x_1 y_1 & x_1 y_2 & \cdots & x_1 y_m \\ x_2 y_1 & x_2 y_2 & \cdots & x_2 y_m \\ \vdots & \vdots & \ddots & \vdots \\ x_n y_1 & x_n y_2 & \cdots & x_n y_m \end{bmatrix} = \big[X\big]_{n\times 1} \big[\leftarrow Y \rightarrow\big]_{1\times m} = [X][Y]^T,$$

for some *non-null* $X \in \mathbb{R}^n$ and $Y \in \mathbb{R}^m$.

Hint: Thm. 15.1.2.

Notation 15.2.2

For $X \in \mathbb{R}^n$, $Y \in \mathbb{R}^m$ we write

$$X \boxtimes Y \quad := \quad [X][Y]^T \ ,$$

and say that the $n \times m$ matrix $X \boxtimes Y$ is **the tensor product matrix of tuples X and Y.**

Test Your Comprehension 15.2.3

Since

$$\begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ \vdots \\ x_n \end{pmatrix} \boxtimes \begin{pmatrix} y_1 \\ y_2 \\ y_3 \\ \vdots \\ y_m \end{pmatrix} := \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ \vdots \\ x_n \end{bmatrix} \circ \begin{bmatrix} y_1 & y_2 & y_3 & \cdots & y_m \end{bmatrix} = \begin{bmatrix} x_1 y_1 & x_1 y_2 & \cdots & x_1 y_m \\ x_2 y_1 & x_2 y_2 & \cdots & x_2 y_m \\ \vdots & \vdots & \ddots & \vdots \\ x_n y_1 & x_n y_2 & \cdots & x_n y_m \end{bmatrix},$$

we have

$$(X \boxtimes Y)\llbracket i, j \rrbracket = X\llbracket i \rrbracket \, Y\llbracket j \rrbracket \, .$$

Comment 15.2.4

As we have seen in Exercise 15.2.1, rank one matrices are exactly those that can be expressed as $X \boxtimes Y$, for some non-null tuples X and Y.

Please note that such a representation is not unique. For example,

$$\begin{pmatrix} 1 \\ 2 \end{pmatrix} \boxtimes \begin{pmatrix} 9 \\ 3 \end{pmatrix} = \begin{bmatrix} 9 & 3 \\ 18 & 6 \end{bmatrix} = \begin{pmatrix} 3 \\ 6 \end{pmatrix} \boxtimes \begin{pmatrix} 3 \\ 1 \end{pmatrix} .$$

We shall say more about this in Theorem 15.2.12, where we show that the representation is somewhat unique.

Test Your Comprehension 15.2.5 **Basic properties of $\boxtimes$**

The following hold for any $X \in \mathbb{R}^n$, $Y \in \mathbb{R}^m$.

1. $(X \boxtimes Y)^T = Y \boxtimes X$;
2. The j-th column of $X \boxtimes Y$ is $Y\llbracket j \rrbracket \cdot X$;
3. The i-th row of $X \boxtimes Y$ is $X\llbracket i \rrbracket \cdot Y$;
4. $X \boxtimes Y$ is null exactly when either X or Y is a null tuple;
5. $\left(\beta \cdot X\right) \boxtimes \left(\frac{1}{\beta} \cdot Y\right) = X \boxtimes Y$, for any non-zero β.

Please remember that in mathematics "either-or" generally includes the possibility of "and".

Test Your Comprehension 15.2.6 **$\boxtimes$ and $\bullet$**

If $X, Y \in \mathbb{R}^n$ then $\mathit{Trace}\,(X \boxtimes Y) = X \bullet Y$.

Exercise 15.2.7 **Action and range of $X \boxtimes Y$**

For any $X \in \mathbb{R}^n$ and $Y, Z \in \mathbb{R}^m$,

$$\big(X \boxtimes Y\big)(Z) = (Y \bullet Z) \cdot X \, .$$

Consequently, when $Y \neq \mathcal{O}_m$, the range of $X \boxtimes Y$ is the set of *all* scalar multiples of X.

Exercise 15.2.8

1. Find X and Y such that $X \boxtimes Y = \begin{bmatrix} 1 & -1 & 0 \\ -1 & 1 & 0 \end{bmatrix}$.

2. For which values of δ can one find X and Y such that

$$X \boxtimes Y = \begin{bmatrix} 0 & 1 & 2 \\ 0 & \delta & 3 \\ 0 & 0 & 0 \end{bmatrix} ?$$

Exercise 15.2.9

Every elementary matrix has the form $\mathcal{I} + X \boxtimes Y$, for some tuples X, Y.

Test Your Comprehension 15.2.10 **$\boxtimes$ distributes over linear combinations**

Verify that each of the following formulas is a particular case of a general rule you studied in Exercise 8.1.6.

1. $(\alpha \cdot X + \beta \cdot Y) \boxtimes Z = \alpha \cdot (X \boxtimes Z) + \beta \cdot (Y \boxtimes Z)$.

2. $Z \boxtimes (\alpha \cdot X + \beta \cdot Y) = \alpha \cdot (Z \boxtimes X) + \beta \cdot (Z \boxtimes Y)$.

Please note that one can take $\alpha = \beta = 1$ in the above formulas to see that $\boxtimes$ distributes over addition. Similarly, taking $\beta = 0$ shows how scalars can be moved in and out of the tensor product.

Exercise 15.2.11 **$\boxtimes$ and composition**

Use the results of *Section* 8.3.1 to verify each of the following claims in the appropriate circumstances.

1. $A \circ (X \boxtimes Y) = A(X) \boxtimes Y$.

2. $(X \boxtimes Y) \circ B = X \boxtimes \left(B^{T}(Y)\right)$.

3. $(X \boxtimes Y) \circ (U \boxtimes W) = (Y \bullet U) \cdot (X \boxtimes W)$.

ILLUSTRATION TO HELP REMEMBER THESE

Earlier you have observed the following identity:

$$\left(\beta \cdot X\right) \boxtimes \left(\frac{1}{\beta} \cdot Y\right) = X \boxtimes Y .$$

It is natural to wonder whether this is the only way of expressing a rank one matrix in two different ways as a tensor product of tuples. In the non-zero case, it is. This describes the extent to which a representation of a rank one matrix as a tensor product is almost unique.

Theorem 15.2.12 **$X \boxtimes Y$ representation is unique up to scalar multiples**

For *non-null* tuples X, Y, U, W, the equality

$$X \boxtimes Y = U \boxtimes W$$

takes place exactly when there is a non-zero scalar β such that

$$U = \beta \cdot X \quad \text{and} \quad W = \frac{1}{\beta} \cdot Y\ .$$

Proof of Theorem 15.2.12. In view of TYC 15.2.5, what remains to be shown is that the equality $X \boxtimes Y = U \boxtimes W$ leads to the existence of a β satisfying the described conditions. To this end it is enough to show that $U = \alpha \cdot X$ and $W = \gamma \cdot Y$ where $\alpha\gamma = 1$.

In fact, the last bit ($\alpha\gamma = 1$) is automatic in our case: if $U = \alpha \cdot X$ and $W = \gamma \cdot Y$ then

$$(\alpha\gamma) \cdot \big(X \boxtimes Y\big) \overset{\text{TYC 15.2.10}}{=} (\alpha \cdot X) \boxtimes (\gamma \cdot Y) = U \boxtimes W = X \boxtimes Y\ .$$

Therefore $\alpha\gamma = 1$ by TYC 7.2.6.

So, all we have to do is show that U is a scalar multiple of X, and W is a scalar multiple of Y.

Since $X \boxtimes Y = U \boxtimes W$,

$$\|W\|^2 \cdot U \overset{\text{Exc. 15.2.7}}{=} \big(U \boxtimes W\big)(W) = \big(X \boxtimes Y\big)(W) \overset{\text{Exc. 15.2.7}}{=} (Y \bullet W) \cdot X\ .$$

Therefore

$$U = \left(\frac{Y \bullet W}{\|W\|^2}\right) \cdot X\ .$$

By TYC 15.2.5, $X \boxtimes Y = U \boxtimes W$ leads to $Y \boxtimes X = W \boxtimes U$ via transposition. Thus a similar argument yields

$$W = \left(\frac{X \bullet U}{\|U\|^2}\right) \cdot Y\ . \qquad \blacksquare$$

15.3 Matrix Rank And Sums Of Rank One Matrices

Here we present yet one more equivalent characterization of matrix rank. So far we have seen that the number of pivots in its SPI, RREF or RCEF equals the dimension of its range, and this number is its rank. In the present section we shall show that rank of non-null matrix $\mathcal{A}$ is the smallest natural number k such that $\mathcal{A}$ can be expressed as a sum of k matrices of the form $X \boxtimes Y$.

We begin with a wonderful formula for expressing a composition of two matrices as a sum of associated rank one matrices.

Exercise 15.3.1 ☞ **Composition as a sum of rank one matrices**

Suppose that

$$\mathcal{A} = \begin{bmatrix} C_1 & C_2 & C_3 & \cdots & C_k \end{bmatrix}_{n\times k} \quad \text{and} \quad \mathcal{B} = \begin{bmatrix} \longleftarrow & R_1 & \longrightarrow \\ \longleftarrow & R_2 & \longrightarrow \\ \longleftarrow & R_3 & \longrightarrow \\ & \vdots & \\ \longleftarrow & R_k & \longrightarrow \end{bmatrix}_{k\times m} .$$

Define auxiliary matrices

$$\mathcal{A}_j := \begin{bmatrix} \mathbb{O}_n & \cdots & C_j & \cdots & \mathbb{O}_n \end{bmatrix}_{n\times k} \quad \text{and} \quad \mathcal{B}_i := \begin{bmatrix} \longleftarrow & \mathbb{O}_m & \longrightarrow \\ & \vdots & \\ \longleftarrow & R_i & \longrightarrow \\ & \vdots & \\ \longleftarrow & \mathbb{O}_m & \longrightarrow \end{bmatrix}_{k\times m} .$$

Then the following claims hold true.

1. $$\mathcal{A} = \mathcal{A}_1 + \mathcal{A}_2 + \cdots + \mathcal{A}_k, \qquad \mathcal{B} = \mathcal{B}_1 + \mathcal{B}_2 + \cdots + \mathcal{B}_k .$$

2. $$\mathcal{A}_j\mathcal{B}_i = \begin{cases} \mathcal{O}, & \text{if } j \neq i \\ C_j \boxtimes R_i, & \text{if } j = i \end{cases} .$$

3. $$\begin{aligned} \mathcal{A}\,\mathcal{B} &= \mathcal{A}_1\mathcal{B}_1 + \mathcal{A}_2\mathcal{B}_2 + \cdots + \mathcal{A}_k\mathcal{B}_k \\ &= C_1 \boxtimes R_1 + C_2 \boxtimes R_2 + \cdots + C_k \boxtimes R_k . \end{aligned}$$

Since we can express every non-null matrix as a product of an injection and a surjection (Theorem 15.1.2), we can apply the result of Exercise 15.3.1 to derive yet another equivalent definition of the concept of matrix rank.

Theorem 15.3.2 ☞ **Rank via sums of rank one matrices**

A matrix of positive rank k can be expressed as a sum of k rank one matrices, and cannot be expressed as a sum of any fewer than that.

Proof. Every rank one matrix has the form $X \boxtimes Y$ (Exc. 15.2.1). Let us show that a sum of p rank one matrices has rank at most p. This will establish the fact that a matrix of rank k cannot be expressed as a sum of fewer than k rank one matrices.

We demonstrate the argument in the case $p = 3$ for the simplicity of notation. A general proof is completely analogous.

$$\big(U \boxtimes V + W \boxtimes X + Y \boxtimes Z\big)(C) \overset{\text{Exc. 15.2.7}}{=} (V \bullet C) \cdot U + (X \bullet C) \cdot W + (Z \bullet C) \cdot Y \ .$$

This shows that every output of $U \boxtimes V + W \boxtimes X + Y \boxtimes Z$ is a linear combination of tuples U, W and Y.

It follows that the range of $U \boxtimes V + W \boxtimes X + Y \boxtimes Z$ sits inside the range of $\begin{bmatrix} U & W & Y \end{bmatrix}_{n\times 3}$. By Rank-Nullity theorem, the rank (i.e. the dimension of the range) of $\begin{bmatrix} U & W & Y \end{bmatrix}_{n\times 3}$ is at most 3. Hence the dimension of the range of $U \boxtimes V + W \boxtimes X + Y \boxtimes Z$ cannot be any bigger than that (Theorem 18.3.26).

To complete the proof let us verify that a matrix $\mathcal{A} \in \mathbb{M}_{n\times m}$ of positive rank k can be expressed as a sum of k rank one matrices. It is sufficient to show that $\mathcal{A}$ can be expressed as a sum of k matrices of the form $X \boxtimes Y$, as none of these can be null by the argument in the first part of the proof.

Give an $\mathcal{A}$ as described, using the Inj∘Surj factorization we can write $\mathcal{A} = \mathcal{B}_{n\times k}\mathcal{C}_{k\times m}$, for some injective $\mathcal{B}$ and surjective $\mathcal{C}$ (Theorem 15.1.2). By applying the result of Exercise 15.3.1 to $\mathcal{BC}$, we see that $\mathcal{A}$ can be expressed as a sum of k matrices of the form $X \boxtimes Y$. ■

15.4 Appendix: Exiled Proofs

Proof of Theorem 15.1.2. Suppose that $\mathcal{A} \in \mathbb{M}_{n\times m}$ has a positive rank $\boldsymbol{k}$. By Smith factorization we can express $\mathcal{A}$ as $\mathcal{KSL}$, where $\mathcal{K}_{n\times n}$ and $\mathcal{L}_{m\times m}$ are invertible matrices, and $\mathcal{S}_{n\times m}$ is a SPI of rank $\boldsymbol{k}$.

By Exercise 15.1.1,

$$\mathcal{S} = \begin{bmatrix} \mathcal{I}_{\boldsymbol{k}} \\ \mathcal{O} \end{bmatrix}_{n\times \boldsymbol{k}} [\mathcal{I}_{\boldsymbol{k}} \ \mathcal{O}]_{\boldsymbol{k}\times m} \ ,$$

and so

$$\mathcal{A} = \left(\mathcal{K} \begin{bmatrix} \mathcal{I}_{\boldsymbol{k}} \\ \mathcal{O} \end{bmatrix}_{n\times \boldsymbol{k}}\right)_{n\times \boldsymbol{k}} \big([\mathcal{I}_{\boldsymbol{k}} \ \mathcal{O}]_{\boldsymbol{k}\times m}\mathcal{L}\big)_{\boldsymbol{k}\times m} \ .$$

Let

$$\mathcal{B} := \mathcal{K} \begin{bmatrix} \mathcal{I}_{\boldsymbol{k}} \\ \mathcal{O} \end{bmatrix}_{n\times \boldsymbol{k}} \quad \text{and} \quad \mathcal{C} := [\mathcal{I}_{\boldsymbol{k}} \ \mathcal{O}]_{\boldsymbol{k}\times m}\mathcal{L} \ .$$

Since $\begin{bmatrix} \mathcal{I}_{\boldsymbol{k}} \\ \mathcal{O} \end{bmatrix}$ is injective (Theorem ??), and $\mathcal{K}$ is bijective, $\mathcal{B}$ is injective (composing with a bijection does not alter the jectivity (Thm. 2.5.14)). Similarly, since $[\mathcal{I}_{\boldsymbol{k}}\ \mathcal{O}]$ is surjective (Theorem ??) and $\mathcal{L}$ is bijective, $\mathcal{C}$ is surjective.

Next we shall verify the other three claims of the theorem, but in different order.

Claim 3: Let us say

$$\mathcal{A} = \mathcal{B}_{n\times p}\mathcal{C}_{p\times m} = \mathcal{B}'_{n\times q}\mathcal{C}'_{q\times m}\ , \tag{15.1}$$

where $\mathcal{B}$ and $\mathcal{B}'$ are injections, and $\mathcal{C}$ and $\mathcal{C}'$ are surjections.

Let us show that $p = q$. If we demonstrate that $p \geq q$, then by symmetry we would also have $q \geq p$, since the roles of $\mathcal{B}, \mathcal{C}$ and of $\mathcal{B}', \mathcal{C}'$ can be interchanged.

Being a surjection, $\mathcal{C}'_{q\times m}$ has a right inverse matrix $\mathcal{G}_{m\times q}$ (Theorem 13.2.1). We use $\mathcal{G}$ to cancel $\mathcal{C}'$ from the left in (15.1):

$$\mathcal{B}_{n\times p}\mathcal{C}_{p\times m}\mathcal{G}_{m\times q} = \mathcal{B}'_{n\times q}\mathcal{C}'_{q\times m}\mathcal{G}_{m\times q} = \mathcal{B}'_{n\times q}\mathcal{I}_q = \mathcal{B}'_{n\times q}\ . \tag{15.2}$$

Since

$$Nullspace\,(\mathcal{C}\,\mathcal{G}) \overset{\text{TYC 12.1.13}}{\subseteq} Nullspace\,(\mathcal{B}\,\mathcal{C}\,\mathcal{G}) = Nullspace\left(\mathcal{B}'\right) = \{\mathbb{O}_q\}\ ,$$

$\mathcal{C}\,\mathcal{G}$ is a $(p \times q)$ injection, and thus is a portrait-shaped matrix (TYC 11.2.2). So $p \geq q$, and consequently $p = q$.

In particular, $\mathcal{C}\,\mathcal{G}$ is a $p \times p$ injection, and hence is an invertible matrix (TYC 11.2.4). Let us write $\mathcal{S}$ for $\mathcal{C}\,\mathcal{G}$, so that $\mathcal{B}' = \mathcal{B}\,\mathcal{S}$. Let us show that $\mathcal{C}' = \mathcal{S}^{-1}\mathcal{C}$. We have

$$\mathcal{B}\,\mathcal{C} = \mathcal{B}'\,\mathcal{C}' = \mathcal{B}\,\mathcal{S}\,\mathcal{C}'\ . \tag{15.3}$$

Since $\mathcal{B}$ is injective, it has a left inverse $\mathcal{T}$ that is a matrix (Theorem 13.2.1). We use $\mathcal{T}$ to cancel $\mathcal{B}$ from the left in (15.3):

$$\mathcal{C} = \mathcal{T}\,\mathcal{B}\,\mathcal{C} = \mathcal{T}\,\mathcal{B}\,\mathcal{S}\,\mathcal{C}' = \mathcal{S}\,\mathcal{C}'\ .$$

Hence $\mathcal{S}^{-1}\mathcal{C} = \mathcal{C}'$.

Claim 1: In the first portion of the proof we have demonstrated that an $n \times m$ matrix $\mathcal{A}$ of positive rank $\boldsymbol{k}$ can be expressed as $\mathcal{B}_{n\times\boldsymbol{k}}\mathcal{C}_{\boldsymbol{k}\times m}$, where $\mathcal{B}$ is an injection and $\mathcal{C}$ is a surjection.

In proving Claim 3. we had established that for every "injection $\circ$ surjection" factorization of $\mathcal{A}$ as $\mathcal{B}'\mathcal{C}'$, the size of $\mathcal{B}'$ has to be the same as that of $\mathcal{B}$, and similarly – for $\mathcal{C}'$ and $\mathcal{C}$. This establishes the required result.

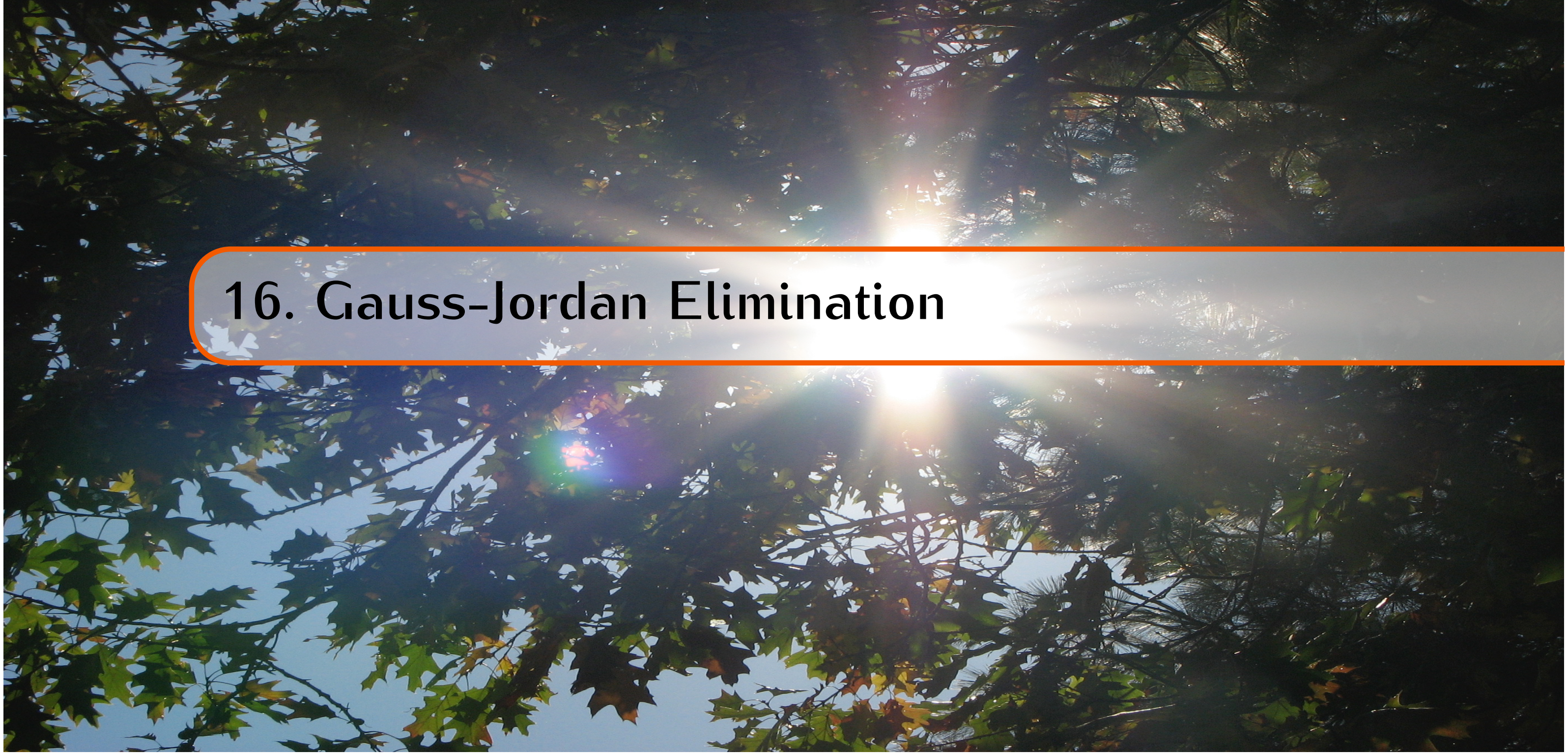
Claim 2: Since $\mathcal{C}$ is a surjection,

$$\mathit{Range}(\mathcal{A}) = \mathit{Range}(\mathcal{B}\mathcal{C}) \overset{\text{Thm. 2.4.2}}{=} \mathit{Range}(\mathcal{B}) \ .$$

Similarly,

$$\mathit{Nullspace}(\mathcal{A}) = \mathit{Nullspace}(\mathcal{B}\mathcal{C}) \overset{\text{Thm. 12.1.15}}{=} \mathit{Nullspace}(\mathcal{C}) \ . \qquad \blacksquare$$

V Gauss-Jordan Elimination And Linear Systems



16. Gauss-Jordan Elimination

Last modified on December 8, 2018

16.1 Gauss-Jordan Elimination Scheme

The origins of linear algebra lie in the methods devised by Gauss and Jordan to solve systems of linear equations. Translated into the language of matrices, these methods rely on simplifying a given matrix by performing a sequence of elementary row operations on it. Column operations are NOT to be involved.

Were we allowed to use column operations as well, every matrix can be turned into a SPI. How much simplification can be achieved with row operations only?

Let us note right away, that the corresponding question about a simplification via elementary column operations need not be treated separately, since transposition can be used to translate the results involving rows into the results involving columns, and vice versa.

In this chapter we present an algorithm for simplifying a given matrix by performing a sequence of elementary row operations on it (or equivalently, through multiplying it on the left by a sequence of elementary matrices).

We will then leverage this algorithm into a method for solving general linear systems.

As usual, we will describe the algorithm and explain why it achieves the desired results, but we shall not ask the reader to execute such an algorithm by hand.

The algorithm has two stages: Gaussian elimination and Jordan's reduction.

16.1.1 — Gaussian Elimination And REF

The ideas in this part of the algorithm are similar to those in the reduction to a SPI (Section 11.1).

Test Your Comprehension 16.1.1

Suppose that $\mathcal{A}$ is a non-null $n \times m$ matrix. Argue that by performing at most n elementary row operations in sequence, we can convert $\mathcal{A}$ into a matrix whose *first non-null column* equals E_1.

In other words, we can multiply $\mathcal{A}$ on the left by a product of at most n elementary matrices to produce a matrix whose *first non-null column* equals E_1.

> Do you see why we canNOT always produce a matrix whose *first column* is E_1?

> Hint: Multiplying $\mathcal{A}$ on the left by $\mathcal{B}$ amounts to applying $\mathcal{B}$ to all of the columns of $\mathcal{A}$. Thm. 10.1.18 and TYC 10.2.4 can be useful here.

Exercise 16.1.2

Let $\mathcal{A} = \begin{bmatrix} 0 & 0 & 3 & 2 \\ 0 & 0 & -1 & 4 \\ 0 & 0 & 5 & 6 \\ 0 & 0 & 9 & 2 \end{bmatrix}$.

Find a matrix $\mathcal{B}$ that is a product of elementary matrices, such that the first non-null column of $\mathcal{B}\mathcal{A}$ is E_1.

> Hint: Thm. 11.3.1.

Let $\mathcal{A}$ be a non-null $n \times m$ matrix. TYC 16.1.1 tells us that by performing at most n elementary row operations in sequence, we can convert $\mathcal{A}$ into a matrix $\mathcal{A}_1$ whose *first non-null column* equals E_1. This means that

$$\mathcal{A}_1 = \begin{bmatrix} 0 & \cdots & 0 & 1 & \diamond & \cdots & \diamond \\ 0 & \cdots & 0 & 0 & \square & \cdots & \square \\ 0 & \cdots & 0 & 0 & \square & \cdots & \square \\ \vdots & & \vdots & \vdots & \vdots & & \vdots \\ 0 & \cdots & 0 & 0 & \square & \cdots & \square \end{bmatrix}_{n \times m},$$

where the leading zero columns may be absent. Depending on the size of the matrix, the columns following E_1 and/or rows following the first row may be absent as well. The reader should adjust the schematic appropriately, based on the size of the matrix.

When $n > 1$, the argument involved in TYC 11.1.3 tells us that elementary row operations *which do not involve the first row of* $\mathcal{A}_1$

- will not alter the zeros in the leading columns up to an including E_1, and
- will amount to the corresponding row operations on the matrix

$$\begin{bmatrix} \square & \cdots & \square \\ \square & \cdots & \square \\ \vdots & & \vdots \\ \square & \cdots & \square \end{bmatrix}.$$

If this latter matrix is not null, we can perform at most $n-1$ elementary row operations that do not involve the first row of $\mathcal{A}_1$ to transform

$$\begin{bmatrix} \square & \cdots & \square \\ \square & \cdots & \square \\ \vdots & & \vdots \\ \square & \cdots & \square \end{bmatrix}$$

into a matrix whose first non-zero column is (a smaller) E_1. This way we transform A_1 into a matrix $\mathcal{A}_2$ of the form

$$\begin{bmatrix} 0 & \cdots & 0 & 1 & \diamond & \cdots & \diamond & \diamond & \diamond & \cdots & \diamond \\ 0 & \cdots & 0 & 0 & 0 & \cdots & 0 & 1 & \square & \cdots & \square \\ 0 & \cdots & 0 & 0 & 0 & \cdots & 0 & 0 & \triangle & \cdots & \triangle \\ \vdots & & \vdots & \vdots & \vdots & & \vdots & \vdots & \vdots & & \vdots \\ 0 & \cdots & 0 & 0 & 0 & \cdots & 0 & 0 & \triangle & \cdots & \triangle \end{bmatrix}.$$

Proceeding in this fashion, one eventually arrives at an $n \times m$ matrix $\mathcal{B}$ with the following features.

- The first non-null column of $\mathcal{B}$ is E_1.
- For each feasible k, let $\mathcal{B}_k$ stand for the matrix obtained from $\mathcal{B}$ by erasing the first k rows. If $\mathcal{B}_k$ is not null, then the first non-null column of $\mathcal{B}_k$ is E_1 (of appropriate size).

A non-null matrix $\mathcal{B}$ that has these properties is said to be in a **Row Echelon Form (REF)**.

We shall also agree that a null matrix is in a REF.

Test Your Comprehension 16.1.3

Argue that a matrix $\mathcal{C}$ is in a REF exactly when it has the following properties.

- The zero rows of $\mathcal{C}$ are at the bottom.
- The first non-zero entry in each non-null row of $\mathcal{C}$ is a 1. These leading 1's are said to be **the pivots** of $\mathcal{C}$, and they occur in the **pivot columns** of $\mathcal{C}$
- A pivot in a lower row is always more eastern than the pivot in a higher row; in other words, the pivots move eastward as one descends the rows.

Example 16.1.4

Test Your Comprehension 16.1.5

Which of the following matrices are in REF?

$$\begin{bmatrix} 1 & 2 & 0 & -5 & 9 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 6 & 4 & 0 \\ 0 & 0 & 0 & 0 & 1 & 3 \\ 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 & -5 & 9 & 0 \\ 0 & 2 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 4 & 0 \\ 0 & 0 & 0 & 0 & 6 & 3 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 3 & 0 & -5 & 9 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 4 & 0 \\ 0 & 0 & 1 & 2 & 6 & 3 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 & 4 & 0 & 0 \\ 0 & 0 & 0 & 0 & 3 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 4 & 0 & 0 \\ 0 & 0 & 0 & 3 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}.$$

Test Your Comprehension 16.1.6

Argue that if a matrix $\mathcal{A}$ is in REF and has a null column, then removing the null column produces another matrix in REF.

Exercise 16.1.7

Hint: Thm. 12.2.5.

Argue that the pivot columns of a non-null matrix in REF form a linearly independent list.

Exercise 16.1.8

Argue that if a partitioned matrix $\left[\begin{smallmatrix} \mathcal{A} & \mathcal{B} \\ \mathcal{O} & \mathcal{D} \end{smallmatrix}\right]$ is in REF, then $\mathcal{A}$ and $\mathcal{D}$ are also in REF. Furthermore, every pivot of $\mathcal{A}$ and of $\mathcal{D}$ is a pivot of $\left[\begin{smallmatrix} \mathcal{A} & \mathcal{B} \\ \mathcal{O} & \mathcal{D} \end{smallmatrix}\right]$.

Exercise 16.1.9

Argue that every $n \times m$ matrix can be transformed into a matrix in a REF through an application of a sequence of at most $\frac{n(n+1)}{2}$ elementary row operations.

16.1.2 — Jordan's Reduction To A RREF

Terminology 16.1.10

A non-null matrix in a REF is said to be in a **Reduced Row Echelon Form (RREF)** if the pivot is the only non-zero entry in each of its pivot columns. Equivalently, if its first pivot column is E_1, its second (if there is such) – is E_2, its third (if there is such) – is E_3, etc.

We shall also agree that the null matrix is in an RREF.

Test Your Comprehension 16.1.11

1. Which of the following matrices are in an RREF?

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

2. For each of the following matrices, is it possible to fill in the missing entries so that the resulting matrix is in an RREF?

$$\begin{bmatrix} \square & \square & \square & \square & \square \\ \square & \square & 1 & \square & \square \\ \square & 1 & \square & \square & \square \\ \square & \square & \square & \square & 1 \\ \square & \square & \square & \square & \square \\ \square & \square & \square & \square & \square \end{bmatrix}, \begin{bmatrix} \square & \square & 1 & \square & \square \\ \square & 1 & \square & \square & \square \\ \square & \square & \square & \square & 1 \\ \square & \square & \square & \square & \square \\ \square & \square & \square & \square & \square \\ \square & \square & \square & \square & \square \end{bmatrix}, \begin{bmatrix} \square & \square & \square & \square & \square \\ \square & \square & \square & \square & \square \\ \square & \square & \square & \square & 1 \\ \square & 1 & \square & \square & \square \\ \square & \square & \square & 1 & \square \\ \square & \square & \square & \square & \square \end{bmatrix}, \begin{bmatrix} \square & \square & \square & \square & \square & 1 \\ \square & \square & \square & 1 & \square & \square \\ \square & \square & 1 & \square & \square & \square \\ \square & \square & \square & \square & \square & \square \\ \square & \square & \square & \square & \square & 1 \end{bmatrix}, \begin{bmatrix} \square & \square & \square & \square & \square & 1 \\ \square & \square & \square & 1 & \square & \square \\ \square & \square & \square & \square & \square & \square \\ \square & \square & \square & 1 & \square & \square \\ \square & \square & \square & \square & \square & 1 \end{bmatrix}.$$

Test Your Comprehension 16.1.12

Argue that if a matrix $\mathcal{A}$ is in an RREF and has a null column, then removing the null column produces another matrix in an RREF.

Test Your Comprehension 16.1.13

Argue that every column of a matrix in an RREF is a linear combination of its pivot columns.

Test Your Comprehension 16.1.14

Argue that if a partitioned matrix $\begin{bmatrix} \mathcal{A} & \mathcal{B} \\ \mathcal{O} & \mathcal{D} \end{bmatrix}$ is in an RREF, then $\mathcal{A}$ and $\mathcal{D}$ are also in an RREF.

Hint: Exercise 16.1.8.

Algorithm 16.1.15 ☞ **Jordan's Reduction**

Putting Gaussian Elimination and Jordan's reduction together we arrive at the following result.

Theorem 16.1.16 ☞ **Gauss-Jordan Elimination: reduction to RREF**

Every matrix can be transformed into a matrix in an RREF through an application of a sequence of elementary row operations.

Equivalently, every matrix $\mathcal{A}$ is left-equivalent to a matrix in an RREF.

Performing a sequence of elementary row operations on $\mathcal{A}$ amounts to multiplying $\mathcal{A}$ on the left by a product of elementary matrices. Products of elementary matrices are invertible.

Observation 16.1.17

Theorem 11.3.1 offers an algorithm for finding a matrix $\mathcal{S}$ such that $\mathcal{S}\mathcal{A}$ is in an RREF.

Suppose that one starts with a matrix $\mathcal{A}$ and applies a sequence of elementary row operations, arriving in the end at a matrix $\mathcal{B}$ in an RREF.

Theorem 11.3.1 tells us that by performing the very same sequence of elementary row operations on a (partitioned) matrix $[\mathcal{A} \;\; \mathcal{I}]$, we will arrive at the matrix $[\mathcal{B} \;\; \mathcal{S}]$, where $\mathcal{S}$ is an invertible matrix such that

$$\mathcal{S}\mathcal{A} = \mathcal{B}\,.$$

Exercise 16.1.18

1. How many elementary row operations are needed to transform an $n \times m$ matrix in REF with k pivots into a matrix in an RREF using Jordan's reduction? Give a good upper bound.

2. How many elementary row operations are needed to transform an $n \times m$ matrix into a matrix in an RREF with k pivots using Gauss-Jordan's elimination?

16.1.3 — Invertibility And RREF

Test Your Comprehension 16.1.19 ☞ **Invertible matrices in an RREF**

Argue that the only invertible matrices in an RREF are the identity matrices.

Test Your Comprehension 16.1.20

Argue that if $\mathcal{A}$ is an invertible matrix and $\mathcal{S}$ is a matrix such that $\mathcal{S}\mathcal{A}$ is in an RREF, then

$$\mathcal{S} = \mathcal{A}^{-1}.$$

Hint: TYC 16.1.19.

Observation 16.1.21 ☞ **A better algorithm for discerning invertibility and finding the inverses of matrices**

By combining Observation 16.1.17 with TYC 16.1.20, we arrive at an improved algorithm for deciding whether a matrix is invertible and if it is, finding its inverse.*

Given an $n \times n$ matrix $\mathcal{A}$, perform Gauss-Jordan elimination on the partitioned matrix $\begin{bmatrix}\mathcal{A} & \mathcal{I}_n\end{bmatrix}$ to arrive at $\begin{bmatrix}\mathcal{B} & \mathcal{S}\end{bmatrix}$, where $\mathcal{B}$ is in an RREF.

$\mathcal{A}$ is invertible exactly when $\mathcal{B} = \mathcal{I}_n$, and in that case

$$\mathcal{S} = \mathcal{A}^{-1}.$$

*Compare this to our previous algorithm in Obs. 11.3.4.

Comment 16.1.22

Modern computing systems can execute an algorithm for finding an inverse of a matrix very quickly, when asked properly. We are not suggesting by any means that the algorithm presented in Observation 16.1.21 is optimized for speed, or that it should be implemented by hand.

When the student is asked to find an inverse of a concrete matrix, we expect that a computing system is to be used for that purpose.

Exercise 16.1.23

As we have observed in Theorem 10.3.5, a Vandermonde matrix with distinct rows is invertible. Hence the unique solution for a linear system $\mathcal{V}(X) = B$ with such a (Vandermonde) coefficient matrix $\mathcal{V}$ has a unique solution

$$X = \mathcal{V}^{-1}(B).$$

Use the development presented in Section 10.3 to find the unique polynomial of degree at most 5 that fits the data points given in the following table.

input:	output:
1	0
2	7
-3	-8
π	π
$\frac{4}{7}$	7
$-e$	π

16.2 Properties of RREF/RCEF

16.2.1 — The Uniqueness Of The RREF

In this section we shall argue that for any $n \times m$ matrix $\mathcal{A}$ there is exactly one matrix $\mathcal{B}$ in an RREF that can be produced from $\mathcal{A}$ via a sequence of elementary row operations.

Observation 16.2.1

It is important to notice that the corresponding result does NOT hold for REF. Namely, it is usually possible to produce a variety of matrices in REF from given matrix $\mathcal{A}$ via a sequence of elementary row operations.

This is not hard to see. By performing Gaussian elimination on $\mathcal{A}$ we produce a matrix in REF, and by applying Jordan's reduction to that matrix we commonly produce a different matrix in an RREF, which is still in REF, of course.

In fact, after every step in Jordan's reduction we arrive at a different matrix in REF (obtained from $\mathcal{A}$ via a sequence of elementary row operations).

Theorem 16.2.2 Distinct matrices in an RREF cannot be left-equivalent

If two matrices in an RREF are left-equivalent, then they are equal.

In other words, one canNOT turn a matrix in an RREF into a *different* matrix in an RREF by performing row operations.

A proof of Theorem 16.2.2 is presented in the appendix to the chapter.

Exercise 16.2.3

Verify that the theorem holds when either $n = 1$ or $m = 1$ or $\mathcal{A}$ is null.

Don't forget that our default "or" is inclusive.

Corollary 16.2.4 ☞ **The uniqueness of RREF**

Every matrix $\mathcal{A}$ is left-equivalent to exactly one matrix in an RREF. This matrix is denoted by RREF($\mathcal{A}$) and is referred to as **the RREF of** $\mathcal{A}$.

Test Your Comprehension 16.2.5

For every matrix $\mathcal{A}$ there is exactly one matrix in an RREF that can be produced from $\mathcal{A}$ via a sequence of elementary row operations.

Test Your Comprehension 16.2.6

Argue that $\mathcal{A}$ and RREF($\mathcal{A}$) have the same jectivity.

Proof of Corollary 16.2.4. We have already demonstrated an algorithm for producing a matrix in an RREF via a sequence of elementary row operations applied to a matrix $\mathcal{A}$. What remains to be shown is that one cannot produce two distinct matrices in an RREF by applying a sequence of elementary row operations to $\mathcal{A}$.

Suppose that we produced matrices $\mathcal{B}$ and $\mathcal{C}$ in an RREF by applying two sequences of elementary row operations to $\mathcal{A}$. Since all elementary row operations are reversible, we can perform a sequence of elementary row operations on $\mathcal{B}$ to produce $\mathcal{A}$, and then perform consequent elementary row operations to arrive at $\mathcal{C}$. This shows that by applying a sequence of elementary row operations to $\mathcal{B}$ we can arrive at $\mathcal{C}$.

Since applying an elementary row operation to a matrix amounts to multiplying it on the left by an elementary matrix, we can write

$$\mathcal{C} = \mathcal{E}_1\, \mathcal{E}_2\, \cdots\, \mathcal{E}_k \mathcal{B}\,,$$

for some elementary matrices $\mathcal{E}_i$. Elementary matrices are invertible, and so are their products. This shows that

$$\mathcal{C} = \mathcal{T}\mathcal{B}\,,$$

for an invertible matrix $\mathcal{T}$.

We now appeal to Theorem 16.2.2 and conclude that $\mathcal{B} = \mathcal{C}$, as required. ■

Comment 16.2.7

We know that $\mathcal{A}$ and RREF($\mathcal{A}$) are left-equivalent. How does one find matrices invertible $\mathcal{S}$ and $\mathcal{T}$ such that

$$\mathcal{A} = \mathcal{T} \circ \mathrm{RREF}(\mathcal{A}) \quad \text{and} \quad \mathrm{RREF}(\mathcal{A}) = \mathcal{S}\mathcal{A}?$$

By applying the algorithm of Theorem 11.3.1 to $\mathcal{A}$, we can construct $\mathcal{S}$. The $\mathcal{S}^{-1}$ can serve as $\mathcal{T}$ (Exc. 2.5.13), and it can be constructed by applying the algorithm of Observation 11.3.4 to $\mathcal{S}$.

Test Your Comprehension 16.2.8

Argue that
$$Nullspace(\mathcal{A}) = Nullspace\big(\mathrm{RREF}(\mathcal{A})\big) ,$$
for every matrix $\mathcal{A}$.

Hint: See TYC 12.1.16.

Theorem 16.2.9 ☞ **Two matrices are left-equivalent exactly when they have the same RREF**

The following are equivalent for matrices $\mathcal{A}$ and $\mathcal{B}$.

1. $\mathcal{A} \overset{\mathsf{L}}{\equiv} \mathcal{B}$.

2. $\mathrm{RREF}(\mathcal{A}) = \mathrm{RREF}(\mathcal{B})$.

Proof of Theorem 16.2.9.

$[\mathbf{2.} \Longrightarrow \mathbf{1.}]$ **:** Suppose that $\mathrm{RREF}(\mathcal{A}) = \mathrm{RREF}(\mathcal{B})$. Since $\mathcal{A}$ is left-equivalent to $\mathrm{RREF}(\mathcal{A})$, and $\mathcal{B}$ is left-equivalent to $\mathrm{RREF}(\mathcal{B})$ (Cor. 16.2.4), i.e. to $\mathrm{RREF}(\mathcal{A})$, $\mathcal{A}$ is left-equivalent to $\mathcal{B}$ by the transitivity of the relation $\overset{\mathsf{L}}{\equiv}$ (TYC 8.2.8).

$[\mathbf{1.} \Longrightarrow \mathbf{2.}]$ **:** Suppose that $\mathcal{A} \overset{\mathsf{L}}{\equiv} \mathcal{B}$. Then
$$\mathrm{RREF}(\mathcal{A}) \overset{\mathsf{L}}{\equiv} \mathcal{A} \overset{\mathsf{L}}{\equiv} \mathcal{B} \overset{\mathsf{L}}{\equiv} \mathrm{RREF}(\mathcal{B}) ,$$
by Corollary 16.2.4. Since the relation $\overset{\mathsf{L}}{\equiv}$ is transitive (TYC 8.2.8), we can conclude that $\mathrm{RREF}(\mathcal{A})$ is left-equivalent to $\mathrm{RREF}(\mathcal{B})$. Left-equivalence means equality for matrices in an RREF (Thm. 16.2.2). Therefore
$$\mathrm{RREF}(\mathcal{A}) = \mathrm{RREF}(\mathcal{B}) .$$
■

16.2.2 — RCEF

Terminology 16.2.10

One can devise a Gauss-Jordan elimination scheme for column operations by mimicking that for row operations or by performing the original scheme on the transpose of a matrix.

This leads to the concepts of **Column Echelon Form (CEF)** and **Reduced Column Echelon Form (RCEF)** .

Test Your Comprehension 16.2.11

Argue that a matrix $\mathcal{A}$ is in CEF (respectively, RCEF) if and only if $\mathcal{A}^T$ is in REF (respectively, RREF).

Comment 16.2.12

Loosely speaking, matrix $\mathcal{A}$ is in CEF when $\mathcal{A}$ has a descending staircase pattern delineated by the pivot 1's, with potentially different drops in hight between the steps. The zero columns are at the far right. When $\mathcal{A}$ is not null, the first pivot is in the $[\![1, 1]\!]$ position.

Here is a more precise description.

- The null columns of $\mathcal{A}$ are at the far right.

- Pivots:

  - The first non-zero entry in each non-null column of $\mathcal{A}$ is a 1. These leading 1's are said to be **the pivots** of $\mathcal{A}$, and they occur in the **pivot rows** of $\mathcal{A}$.

  - A pivot in a more eastern column is always lower than the pivot in a more western column; in other words, the pivots "descend" as one moves eastward.

Test Your Comprehension 16.2.13

Argue that a non-null matrix in a CEF is in an RCEF if the pivot is the only non-zero entry in each of its pivot rows.

In other words, if its first *pivot row* is E_1, its second *pivot row* (if there is such) is E_2, its third *pivot row* (if there is such) is E_3, etc.

Test Your Comprehension 16.2.14

Find the following examples, if they exists.

1. A matrix in CEF that is not in an RCEF.

2. A matrix in CEF that is also in REF.

3. A matrix in an RCEF whose transpose in NOT in REF.

Test Your Comprehension 16.2.15

Argue that if a matrix $\mathcal{A}$ is in an RCEF and has a null row, then removing the null row produces another matrix in an RCEF.

Test Your Comprehension 16.2.16

Argue that if a partitioned matrix $\left[\begin{smallmatrix} \mathcal{A} & \mathcal{O} \\ \mathcal{C} & \mathcal{D} \end{smallmatrix}\right]$ is in an RCEF, then $\mathcal{A}$ and $\mathcal{D}$ are also in an RCEF.

Test Your Comprehension 16.2.17

Argue that every matrix is right-equivalent to a matrix in an RCEF.

In other words, argue that every matrix can be transformed into a matrix in an RCEF through an application of a sequence of elementary column operations.

Test Your Comprehension 16.2.18 ☞ **Distinct matrices in an RCEF cannot be right-equivalent**

If two matrices in an RCEF are right-equivalent, then they are equal.

In other words, one canNOT turn a matrix in an RCEF into a *different* matrix in an RCEF by performing column operations.

Test Your Comprehension 16.2.19 ☞ **The uniqueness of RCEF**

Argue that every matrix $\mathcal{A}$ is right-equivalent to exactly one matrix in an RCEF. This matrix is referred to as RCEF($\mathcal{A}$) or as **the RCEF of** $\mathcal{A}$.

In other words, argue that for any $n \times m$ matrix $\mathcal{A}$ there is exactly one matrix in an RCEF that can be produced from $\mathcal{A}$ via a sequence of elementary column operations.

Test Your Comprehension 16.2.20 ☞ **Two matrices are right-equivalent exactly when they have the same RCEF**

The following are equivalent for matrices $\mathcal{A}$ and $\mathcal{B}$.

1. $\mathcal{A} \overset{\mathrm{R}}{\equiv} \mathcal{B}$.

2. $\mathrm{RCEF}(\mathcal{A}) = \mathrm{RCEF}(\mathcal{B})$.

Test Your Comprehension 16.2.21

Given a matrix $\mathcal{A}$, how does one find matrices $\mathcal{S}$ and $\mathcal{T}$ such that

$$\mathcal{A} = \mathrm{RCEF}(\mathcal{A}) \circ \mathcal{T} \quad \text{and} \quad \mathrm{RCEF}(\mathcal{A}) = \mathcal{A}\mathcal{S}?$$

Test Your Comprehension 16.2.22

Argue that

$$\mathit{Range}\,(\mathcal{A}) = \mathit{Range}\big(\mathrm{RCEF}(\mathcal{A})\,\big)\,,$$

for every matrix $\mathcal{A}$.

Hint: See TYC 13.1.1.

Theorem 16.2.23

Removing all of the null columns from a non-null matrix in an RCEF produces an injective matrix (with the same range).

Proof of Theorem 18.1.3. The non-null columns of a non-null matrix $\mathcal{A}$ in an RCEF are exactly the pivot columns. Let us remove the null columns and argue that the resulting matrix $\mathcal{B}$ is injective. Removing null columns does not alter the range (Exc. 14.1.1). By performing elementary row operations (swaps) we can transform $\mathcal{B}$ into a matrix of the form $\left[\begin{smallmatrix}\mathcal{I}\\ \mathcal{O}\end{smallmatrix}\right]$, (where $\mathcal{O}$ may be absent). Matrices of this form are injective (Example 13.2.3), and since the elementary operations do not alter the jectivity, $\mathcal{B}$ is injective. ■

The reader should compare Theorem 18.1.3 to Theorem 14.1.4. Both indicate that a range of a non-null matrix can be expressed as a range of an injective matrix. Theorem 14.1.4 offers a concrete procedure for constructing the said injective matrix. Later (Thm. 19.6.1) we shall develop an algorithm to implement a wholesale removal of the columns discussed in Comment 14.1.7.

16.2.3 — Relating RREF($\mathcal{A}$), RCEF($\mathcal{A}$) and SPI($\mathcal{A}$)

To carry out Gauss-Jordan elimination on the columns of $\mathcal{A}$, we can transpose $\mathcal{A}$, so that its columns become the rows, perform Gauss-Jordan elimination on the rows of $\mathcal{A}^{T}$, and then transpose the result to get us back to the original orientation. This leads us to the following conclusion.

Theorem 16.2.24 ☞ **Relating RCEF and RREF**

$$\mathrm{RCEF}(\mathcal{A}) = \mathrm{Transpose}\Big(\mathrm{RREF}\big(\mathrm{Transpose}(\mathcal{A})\big)\Big). \tag{16.1}$$

Proof of Theorem 16.2.24. First of all, $\text{Transpose}\Big(\text{RREF}\big(\text{Transpose}(\mathcal{A})\big)\Big)$, being a transpose of a matrix in an RREF, is in an RCEF (TYC 16.2.11). Therefore, by the uniqueness of RCEF (TYC 16.2.19), it is sufficient to demonstrate that $\text{Transpose}\Big(\text{RREF}\big(\text{Transpose}(\mathcal{A})\big)\Big)$ is right-equivalent to $\mathcal{A}$.

By TYC 8.2.12, this amounts to showing that $\text{RREF}\left(\mathcal{A}^T\right)$ is left-equivalent to $\mathcal{A}^T$, and the validity of this last claim is guaranteed by Theorem 16.1.16. ■

Comment 16.2.25

Some computational systems have obvious methods for finding an RREF of a matrix, but no such methods for finding the RCEF. Formula (16.1) shows that this is an insignificant shortcoming.

Theorem 16.2.26 ☞ **RREF($\mathcal{A}$) $\rightsquigarrow$ SPI($\mathcal{A}$), via column operations**

One can transform RREF($\mathcal{A}$) into SPI($\mathcal{A}$) via a sequence of elementary column operations. Furthermore, this can be done is such a way that the pivots of RREF($\mathcal{A}$) become the pivots in SPI($\mathcal{A}$).

In particular,

- the number of pivots in RREF($\mathcal{A}$) is the same as the number of pivots in SPI($\mathcal{A}$);
- SPI($\mathcal{A}$) and RREF($\mathcal{A}$) are right-equivalent.

Proof of Theorem 16.2.26. By TYC 16.1.13, every non-pivot column in RREF($\mathcal{A}$) is a linear combination of the pivot columns, which are $E_1, \ldots, E_k$. Theorem 14.1.2 tells us that by performing a sequence of column adjustments we can turn these columns into null columns. The resulting matrix has the same size as $\mathcal{A}$, and has non-null columns $E_1, \ldots, E_k$. Hence by applying a sequence of column swaps we will arrive at a SPI matrix $\mathcal{S}$.

Since we can produce RREF($\mathcal{A}$) from $\mathcal{A}$ by performing a sequence of elementary row operations, and we can produce $\mathcal{S}$ from RREF($\mathcal{A}$) by performing a sequence of elementary column operations, we can produce $\mathcal{S}$ from $\mathcal{A}$ by performing a sequence of elementary row and column operations. In particular $\mathcal{S}$ and $\mathcal{A}$ are equivalent matrices. Thus $\mathcal{S} = \text{SPI}(\mathcal{A})$ (Thm. 11.2.7).

The last claim of the theorem holds true because performing a sequence of elementary column operations on RREF($\mathcal{A}$) amounts to multiplying RREF($\mathcal{A}$) by a product of (invertible) elementary matrices from the right. ■

Test Your Comprehension 16.2.27 ☞ **RCEF($\mathcal{A}$) $\rightsquigarrow$ SPI($\mathcal{A}$), via row operations**

Argue that one can transform RCEF($\mathcal{A}$) into SPI($\mathcal{A}$) via a sequence of elementary row operations. Furthermore, this can be done is such a way that the pivots of RCEF($\mathcal{A}$) become the pivots in SPI($\mathcal{A}$).

In particular,

- the number of pivots in RCEF($\mathcal{A}$) is the same as the number of pivots in SPI($\mathcal{A}$);
- SPI($\mathcal{A}$) and RCEF($\mathcal{A}$) are left-equivalent.

Hint: Thms. 11.2.11 and 16.2.24.

Exercise 16.2.28 ☞ **Calculating SPI's using RREF and Transpostion**

Verify the following identity.

$$\mathrm{SPI}(\mathcal{A}) = \mathrm{RCEF}\Big(\mathrm{RREF}(\mathcal{A})\Big) = \mathrm{RREF}\Big(\mathrm{RCEF}(\mathcal{A})\Big)$$

This result shows how one can employ computing software to calculate SPI's even when the software is only programmed to do row-reduction and transposition.

Consequently, argue that

$$\begin{aligned}\mathrm{SPI}(\mathcal{A}) &= \mathrm{RREF}\Big(\mathrm{Transpose}\big(\mathrm{RREF}\left(\mathrm{Transpose}(\mathcal{A})\right)\big)\Big)\\ &= \mathrm{Transpose}\Big(\mathrm{RREF}\big(\mathrm{Transpose}\left(\mathrm{RREF}(\mathcal{A})\right)\big)\Big).\end{aligned}$$

Hint: RREF($\mathcal{A}$) and SPI($\mathcal{A}$) are right-equivalent, and SPI($\mathcal{A}$) is in an RCEF. Make use of the uniqueness of an RCEF. Emulate this method to get the other equality.

RREF/RCEF And Jectivity

We have a firm understanding of the jectivity of SPI's (Exc. 11.2.1), which is completely determined by the size of the matrix and the number of pivots.

Since equivalent matrices have the same jectivity, we can determine the jectivity of a matrix by finding the number of pivots in its SPI, i.e. its rank.

By Theorem 16.2.26, this can be achieved by finding the RREF($\mathcal{A}$), since RREF($\mathcal{A}$) has the same number of pivots as SPI($\mathcal{A}$). In other words, one can read off SPI($\mathcal{A}$) from RREF($\mathcal{A}$) without making any further calculations.

By TYC 16.2.27, RCEF($\mathcal{A}$) can be used instead of RREF($\mathcal{A}$) for this purpose. Let us summarize.

Test Your Comprehension 16.2.29 ☞ **Injectivity and RREF/RCEF**

Argue that the following claims are equivalent for a *strictly portrait-shaped* matrix $\mathcal{A}$.

1. $\mathcal{A}$ is injective.
2. RCEF($\mathcal{A}$) has a pivot in every column.
3. RCEF($\mathcal{A}$) has no null columns.
4. RREF($\mathcal{A}$) $= \begin{bmatrix} \mathcal{I} \\ \mathcal{O} \end{bmatrix}$.

Test Your Comprehension 16.2.30 ☞ **Surjectivity and RREF/RCEF**

Argue that the following claims are equivalent for a *strictly landscape-shaped* matrix $\mathcal{A}$.

1. $\mathcal{A}$ is surjective.
2. RREF($\mathcal{A}$) has a pivot in every row.
3. RREF($\mathcal{A}$) has no null rows.
4. RCEF($\mathcal{A}$) $= [\,\mathcal{I} \;\; \mathcal{O}\,]$.

Hint: Formula (16.1).

Test Your Comprehension 16.2.31 ☞ **Invertibility and RREF/RCEF**

Argue that the following claims are equivalent for a *square* matrix $\mathcal{A}$.

- $\mathcal{A}$ is invertible.
- RREF($\mathcal{A}$) $= \mathcal{I}$.
- RCEF($\mathcal{A}$) $= \mathcal{I}$.
- SPI($\mathcal{A}$) $= \mathcal{I}$.

Comment 16.2.32

Soon (see Comment 16.3.4) we shall demonstrate that RREF($\mathcal{A}$) and RCEF($\mathcal{A}$) capture more information about $\mathcal{A}$ than just its rank. In fact they are repositories of the *Nullspace* ($\mathcal{A}$) and the *Range* ($\mathcal{A}$) respectively.

As an application of these results we shall offer another proof of Theorem 14.2.6, and this time the proof will lead us to an algorithm promised in Comment 14.2.7.

Terminology 16.2.33 ☞ **Matrix widening**

We say that an $n \times p$ matrix $\mathcal{M}$ is a **widening** of an $n \times m$ matrix $\mathcal{A}$ when $\mathcal{M} = \begin{bmatrix}\mathcal{A} & \mathcal{B}\end{bmatrix}$, for some matrix $\mathcal{B}$, which may be absent altogether; (in that case $\mathcal{M} = \mathcal{A}$). Another way to express this is to say that $\mathcal{M}$ can be produced from $\mathcal{A}$ by inserting some additional columns into $\mathcal{A}$ from the right.

It is clear that $\mathcal{M} \in \mathbb{M}_{n\times p}$ is a widening of $\mathcal{A} \in \mathbb{M}_{n\times m}$ exactly when

$$\mathcal{A} = \mathcal{M} \circ \begin{bmatrix}\mathcal{I}_m \\ \mathcal{O}\end{bmatrix}.$$

Algorithm 16.2.34 ☞ **Widening injective matrices to invertible matrices**

Theorem 14.2.6 tells us that by attaching additional columns to an injective (non-invertible) matrix it is always possible to arrive at an invertible matrix.

Let us start with an alternate proof of Theorem 14.2.6.

> *Proof of Theorem 14.2.6.* Suppose that $\mathcal{A}$ is an injective non-invertible matrix. Then $\mathrm{RREF}(\mathcal{A}) = \begin{bmatrix}\mathcal{I} \\ \mathcal{O}\end{bmatrix}$, where $\mathcal{O}$ is NOT absent (TYC 16.2.29). Hence (Com. 16.2.7) there is an invertible matrix $\mathcal{T}$ such that
>
> $$\mathcal{A} = \mathcal{T} \circ \mathrm{RREF}(\mathcal{A}) = \mathcal{T}\begin{bmatrix}\mathcal{I} \\ \mathcal{O}\end{bmatrix}.$$
>
> It follows that the invertible matrix $\mathcal{T}$ is a widening of $\mathcal{A}$ (Trm. 16.2.33), and the proof is complete. ■

The proof shows that any invertible matrix $\mathcal{T}$ such that

$$\mathcal{A} = \mathcal{T} \circ \mathrm{RREF}(\mathcal{A})$$

is an invertible widening of $\mathcal{A}$.

Observation 16.1.17 describes an algorithm for constructing an invertible matrix $\mathcal{S}$ such that

$$\mathcal{S}\mathcal{A} = \mathrm{RREF}(\mathcal{A}).$$

Since for such an $\mathcal{S}$ we have

$$\mathcal{A} = \mathcal{S}^{-1} \circ \mathrm{RREF}(\mathcal{A}),$$

$\mathcal{S}^{-1}$ is an invertible widening of $\mathcal{A}$.

Observation 16.1.21 describes an algorithm for constructing $\mathcal{S}^{-1}$, and putting this together with an algorithm for constructing $\mathcal{S}$, we arrive at an algorithm for widening any injective matrix to an invertible matrix.

So let us summarize this into a single procedure.

If $\mathcal{A}$ is an injective matrix, begin with a matrix $[\mathcal{A} \;\; \mathcal{I}]$ and perform row operations to convert this matrix into a matrix of the form $[\mathcal{B} \;\; \mathcal{C}]$, where $\mathcal{B}$ is in an RREF (which means that $\mathcal{B} = \mathrm{RREF}(\mathcal{A})$). Then the matrix $\mathcal{C}$ is invertible, and is a widening of $\mathcal{A}$.

Test Your Comprehension 16.2.35

Hint: Exc. 16.2.29 can be relevant here.

Algorithm 16.2.34 does not apply to non-injective matrices. Suppose that one starts with a matrix $\mathcal{A}$ that may or may not be injective. What would be a simple adjustment to Algorithm 16.2.34 that will result in the inclusion of a built-in test for the injectivity of $\mathcal{A}$?

Exercise 16.2.36

Decide whether the following matrix is injective, and if it is, find an invertible widening of it. Use of computing software is strongly recommended.

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

16.3 Range Equality Theorems

We are now ready to establish a theorem (Thm. 16.3.2) that we stated in Example 13.1.3 as "a peek into the future". This extends TYC 16.2.20 as well.

Lemma 16.3.1 ☞ **Range equality gives equality for $n \times m$ matrices in an RCEF**

If two $n \times m$ matrices in an RCEF have equal ranges, then these matrices are equal.

Proof of Lemma 16.3.1. Let the matrices in question be $\mathcal{A}$ and $\mathcal{B}$.

A removal of null columns from a matrix in an RCEF produces another matrix in an RCEF with the same range (Exc. 14.1.1). By removing null columns (from the right), one at a time, simultaneously from both matrices, we can arrive at two $n \times k$ matrices $\mathcal{A}'$ and $\mathcal{B}'$ still in an RCEF which have equal ranges, with (at least) one of the two matrices, say $\mathcal{A}'$, having no null columns.

Then $\mathcal{A}'$ is injective (Thm. 18.1.3), and by the range inclusion factorization

(Thm. 13.1.2),

$$\underset{m\times k}{\mathcal{A}'} = \underset{m\times k}{\mathcal{B}'}\mathcal{C} \ ,$$

for some matrix $\mathcal{C}$, which has to have the size $k \times k$. Since $\mathcal{A}'$ is injective, $\mathcal{B}'\mathcal{C}$ is injective, and so $\mathcal{C}$ is as well (Thm. 2.4.2). Yet $\mathcal{C}$ is a square matrix, and thus $\mathcal{C}$ is invertible (TYC 11.2.4). This shows that $\mathcal{A}'$ and $\mathcal{B}'$ are right-equivalent, and hence are equal (TYC 16.2.18).

Since $\mathcal{A}$ and $\mathcal{B}$ are obtained from $\mathcal{A}'$ and $\mathcal{B}'$ by inserting the same number of null columns from the right, these matrices are equal as well. ■

Theorem 16.3.2 ☞ **Range Equality For Matrices Of The Same Size**

When matrices $\mathcal{A}$ and $\mathcal{B}$ have the same size, the following are equivalent.

1. $\mathit{Range}(\mathcal{A}) = \mathit{Range}(\mathcal{B})$.
2. $\mathcal{A} \overset{\text{R}}{\equiv} \mathcal{B}$ (i.e. $\mathcal{A}$ and $\mathcal{B}$ are right-equivalent).
3. $\mathcal{A}$ can be turned into $\mathcal{B}$ (and vice versa) through an application of a sequence of elementary column operations.
4. $\text{RCEF}(\mathcal{A}) = \text{RCEF}(\mathcal{B})$.

Proof of Theorem 16.3.2. The equivalence of the last three claims has been established in TYC's 11.4.4 and 16.2.20.

The implication 2. $\Longrightarrow$ 1. is the subject of TYC 13.1.1.

We will complete the proof by establishing the implication 1. $\Longrightarrow$ 4. Let us suppose that $\mathit{Range}(\mathcal{A}) = \mathit{Range}(\mathcal{B})$, where $\mathcal{A}, \mathcal{B} \in \mathbb{M}_{n\times m}$. Then $\text{RCEF}(\mathcal{A})$ and $\text{RCEF}(\mathcal{B})$ have the same range (TYC 16.2.22). Hence

$$\text{RCEF}(\mathcal{A}) = \text{RCEF}(\mathcal{B}) \ ,$$

by Lemma 16.3.1. ■

Comment 16.3.3

Since we have an algorithm for calculating an RCEF of any matrix, the last criterion in Theorem 16.3.2 allows us to discern the equality of ranges of any two matrices of the same size through the use of computing software.

A similar observation can be made with regards to testing the equality of matrices of different sizes via Corollary 16.3.5 below.

Comment 16.3.4

We have observed already that for a given matrix $\mathcal{A}$, SPI($\mathcal{A}$) determines which matrices are equivalent to $\mathcal{A}$. Of course, SPI($\mathcal{A}$) is itself completely determined by the size of $\mathcal{A}$ and the rank (or equivalently, by Rank-Nullity formula, the nullity) of $\mathcal{A}$.

In this way,

> SPI($\mathcal{A}$) can be interpreted as a repository of rank/nullity of $\mathcal{A}$, and we can associate matrix equivalence with the equality of rank/nullity.

Theorem 16.3.2 offers us a similar insight into RCEF($\mathcal{A}$). It indicates that

> RCEF($\mathcal{A}$) can be interpreted as a repository of the range of $\mathcal{A}$, and we can associate right-equivalence with the equality of ranges.

Later on we shall argue that

> $\big[$**a peek into the future; see Theorem 19.5.1**$\big]$
>
> RREF($\mathcal{A}$) can be interpreted as a repository of the nullspace of $\mathcal{A}$, and we can associate left-equivalence with the equality of nullspaces.

Corollary 16.3.5 ☞ **Range Equality For Matrices Of Different Size**

Given matrices $\mathcal{A} \in \mathbb{M}_{n\times 21}$ and $\mathcal{B} \in \mathbb{M}_{n\times 328}$, the following are equivalent.

1. *Range* $(\mathcal{A})$ = *Range* $(\mathcal{B})$.
2. $\mathcal{B} = \mathcal{A}\mathcal{G}$, for some *surjective* $\mathcal{G} \in \mathbb{M}_{21\times 328}$.
3. $\mathrm{RCEF}\left(\begin{bmatrix}\mathcal{A} & \mathcal{O}\end{bmatrix}_{n\times(21|307)}\right) = \mathrm{RCEF}(\mathcal{B})$. *

*Note that $\begin{bmatrix}\mathcal{A} & \mathcal{O}\end{bmatrix}_{n\times(21|307)}$ is created by inserting enough null columns into $\mathcal{A}$ to produce a matrix of the same size as $\mathcal{B}$.

Proof of Corollary 16.3.5. Let $\mathcal{A}_o := \begin{bmatrix}\mathcal{A} & \mathcal{O}\end{bmatrix}_{n\times(21|307)}$. Then $\mathcal{A}_o$ has the same range as $\mathcal{A}$ (Exc. 14.1.1). By Theorem 16.3.2, the following are equivalent.

1. *Range* $(\mathcal{A})$ = *Range* $(\mathcal{B})$.
2. $\mathcal{B} = \mathcal{A}_o\mathcal{D}$, for some invertible $\mathcal{D}$.
3. $\mathrm{RCEF}(\mathcal{A}_o) = \mathrm{RCEF}(\mathcal{B})$.

Let us write

$$\mathcal{D} = \begin{bmatrix} \mathcal{G} \\ \mathcal{H} \end{bmatrix}_{(21|307)\times 328} .$$

Then

$$\mathcal{B} = \mathcal{A}_o \mathcal{D} \overset{\text{Thm. 9.1.8}}{=} \mathcal{AG} .$$

Hence we have the following equivalent statements.

1. *Range* $(\mathcal{A})$ = *Range* $(\mathcal{B})$.

2. $\mathcal{B} = \mathcal{AG}$, for some $\mathcal{G}$ that can be produced by removing rows from an invertible matrix.

3. RCEF$(\mathcal{A}_o)$ = RCEF$(\mathcal{B})$.

Since matrices that can be produced by removing rows from an invertible matrix are exactly the surjective matrices (TYC 14.3.4), the proof is complete. ■

Exercise 16.3.6

Among the following matrices match those that have equal ranges.

$$\begin{bmatrix} 37 & 265 & 359 & -206 & -64 & -274 \\ -42 & -201 & -312 & 169 & -41 & 198 \\ -554 & -476 & -418 & 106 & 284 & 602 \\ -189 & -285 & -354 & 203 & 100 & 318 \\ -225 & -133 & -125 & -22 & -22 & 172 \end{bmatrix}, \quad \begin{bmatrix} 12 & 4 & -19 & 10 & 4 & -1 \\ 0 & -4 & 4 & 11 & -4 & -3 \\ 15 & 18 & -25 & -25 & -19 & -6 \\ -17 & -19 & 24 & -2 & 14 & 6 \\ -6 & 18 & 10 & -4 & -6 & 10 \\ 10 & 1 & 2 & -20 & 9 & 17 \end{bmatrix},$$

$$\begin{bmatrix} 1 & 4 & 6 & 2 & 50 & 10 & -17 \\ 0 & -7 & 4 & -2 & -25 & -19 & 27 \\ 4 & -8 & -6 & 8 & -40 & 46 & 82 \\ 9 & -2 & 0 & -9 & -37 & -2 & 37 \\ -3 & -10 & 8 & 10 & 12 & 10 & 47 \end{bmatrix}, \quad \begin{bmatrix} 33 & 26 & -149 & 1 & 26 \\ 17 & 31 & -139 & 24 & -3 \\ 6 & 26 & -143 & 70 & -58 \\ -70 & -57 & 271 & -1 & 39 \\ 109 & 126 & -622 & 79 & -42 \end{bmatrix}.$$

Test Your Comprehension 16.3.7

Given the set up of Corollary 16.3.5, explain why it can NEVER happen that there is a surjective $\mathcal{C}$ such that $\mathcal{A} = \mathcal{BC}$.

Hint: What would be the size of such a $\mathcal{C}$?

Comment 16.3.8

Since we know how to use computing systems to find RREF$(\mathcal{A})$ and thus RCEF$(\mathcal{A})$ (Thm. 16.2.24) for any concrete matrix $\mathcal{A}$ of a reasonable size, Theorem 16.3.2 and Corollary 16.3.5 offer a way for determining whether the ranges of two given matrices are the same.

Of course if the matrices do not share the same final space, their ranges cannot be identical. So, for example, a $35 \times k$ matrix can never have the same range as a $54 \times p$ matrix.

16.4 Nullspaces As Ranges

In this section we introduce an algorithm for expressing a nullspace of a non-injective matrix as a range of an injective matrix.

Later on, in TYC 18.3.19, we shall claim that every subspace of $\mathbb{R}^n$ is a range of an injective matrix.

Since the nullspace of $\mathcal{O}$ is the range of $\mathcal{I}$, we shall focus on non-null matrices only.

As we know from TYC 16.2.8,

$$\mathit{Nullspace}\,(\mathcal{A}) = \mathit{Nullspace}\left(\text{RREF}(\mathcal{A})\right) .$$

Hence it shall be sufficient to assume that we are starting with a (non-null, non-injective) matrix in an RREF. By Theorem 12.1.12, removing null rows from a matrix does not alter its nullspace, and so

we shall concentrate on matrices in an RREF that have no null rows.

Our strategy will rely on the fact that the required process is quite simple for a matrix of the form $[\mathcal{I}_n\ \mathcal{B}]$ (Lem. 16.4.2), and that every non-injective matrix in an RREF with no null rows can be transformed into a matrix of this form via a sequence of column swaps (TYC 16.4.1).

Of course, we already know (Comment 12.1.17) that performing elementary column operations may alter the nullspace of a matrix. Keeping track of these changes and reversing them in the end is the crux of our method.

Test Your Comprehension 16.4.1

Argue that a non-injective non-null matrix $\mathcal{A}$ in an RREF can be transformed into a matrix of the form $\begin{bmatrix} \mathcal{I}_n & \mathcal{B} \\ \mathcal{O} & \mathcal{O} \end{bmatrix}$ (where the $\mathcal{O}$'s may be absent) through a sequence of column swaps. The process does not alter the number of pivot/non-pivot columns.

Lemma 16.4.2

For any $\mathcal{B} \in \mathbb{M}_{n\times m}$,

$$\mathit{Nullspace}\begin{bmatrix} \mathcal{I}_n & \mathcal{B} \\ \mathcal{O} & \mathcal{O} \end{bmatrix} = \mathit{Range}\begin{bmatrix} -\mathcal{B} \\ \mathcal{I}_m \end{bmatrix} .$$

Proof of Lemma 16.4.2.

$$Nullspace \begin{bmatrix} \mathcal{I}_n & \mathcal{B} \\ \mathcal{O} & \mathcal{O} \end{bmatrix} = \left\{ \begin{pmatrix} X \\ Y \end{pmatrix} \;\middle|\; \begin{bmatrix} \mathcal{I}_n & \mathcal{B} \\ \mathcal{O} & \mathcal{O} \end{bmatrix}\begin{pmatrix} X \\ Y \end{pmatrix} = \begin{pmatrix} \mathbb{0} \\ \mathbb{0} \end{pmatrix},\ {\scriptstyle X\in\mathbb{R}^n, Y\in\mathbb{R}^m} \right\}$$

$$\overset{\text{Thm. 9.1.18}}{=} \left\{ \begin{pmatrix} X \\ Y \end{pmatrix} \;\middle|\; X + \mathcal{B}(Y) = \mathbb{0},\ {\scriptstyle X\in\mathbb{R}^n, Y\in\mathbb{R}^m} \right\}$$

$$= \left\{ \begin{pmatrix} X \\ Y \end{pmatrix} \;\middle|\; X = -\mathcal{B}(Y),\ {\scriptstyle X\in\mathbb{R}^n, Y\in\mathbb{R}^m} \right\}$$

$$= \left\{ \begin{pmatrix} -\mathcal{B}(Y) \\ Y \end{pmatrix} \;\middle|\; Y \in \mathbb{R}^m \right\}$$

$$= Range \begin{bmatrix} -\mathcal{B} \\ \mathcal{I}_m \end{bmatrix}. \qquad \blacksquare$$

Test Your Comprehension 16.4.3

Argue that matrix $\begin{bmatrix} -\mathcal{B} \\ \mathcal{I}_m \end{bmatrix}$ is injective, for any $\mathcal{B} \in \mathbb{M}_{n\times m}$.

Hint: Note that $[\mathcal{O}\ \mathcal{I}_m]\begin{bmatrix} -\mathcal{B} \\ \mathcal{I}_m \end{bmatrix} = \mathcal{I}_m$. Thm. 13.2.1 can be useful here. See also Example 13.2.3.

Algorithm 16.4.4 ☞ Expressing a nullspace of a non-injective non-null $n \times m$ matrix $\mathcal{A}$ in an RREF as a range of an injective $n \times k$ matrix $\mathcal{M}$, where k is the number of non-pivot columns in $\mathcal{A}$

Given a matrix $\mathcal{A}$ as described, by TYC 16.4.1, by applying a sequence of column swaps we can transform $\mathcal{A}$ into a matrix of the form

$$\begin{bmatrix} \mathcal{I} & \mathcal{B} \\ \mathcal{O} & \mathcal{O} \end{bmatrix}. \tag{16.2}$$

In other words, there is a product $\mathcal{P}$ of swaps (elementary matrices) such that $\mathcal{AP}$ has the form presented in (16.2).

By TYC 11.3.2, the same sequence of column swaps will transform matrix $\begin{bmatrix} \mathcal{A} \\ \mathcal{I} \end{bmatrix}$ into the matrix $\begin{bmatrix} \mathcal{AP} \\ \mathcal{P} \end{bmatrix}$, from whence we can discern both $\mathcal{AP}$ and $\mathcal{P}$.

By Lemma 16.4.2,

$$Nullspace\,(\mathcal{AP}) = Nullspace \begin{bmatrix} \mathcal{I} & \mathcal{B} \\ \mathcal{O} & \mathcal{O} \end{bmatrix} = Range \begin{bmatrix} -\mathcal{B} \\ \mathcal{I} \end{bmatrix}.$$

Consequently,

$$
\begin{aligned}
X \in \mathit{Nullspace}\,(\mathcal{A}) \iff \mathcal{A}(X) = \mathbb{0} \iff \mathcal{A}\mathcal{P}\mathcal{P}^{-1}(X) = \mathbb{0} \\
&\iff \mathcal{P}^{-1}(X) \in \mathit{Nullspace}\,(\mathcal{A}\mathcal{P}) \\
&\iff \mathcal{P}^{-1}(X) \in \mathit{Range}\left[\begin{smallmatrix}-\mathcal{B}\\ \mathcal{I}\end{smallmatrix}\right] \\
&\iff \mathcal{P}^{-1}(X) = \left[\begin{smallmatrix}-\mathcal{B}\\ \mathcal{I}\end{smallmatrix}\right](Z), \quad \text{for some } \; Z \\
&\iff X = \mathcal{P}\left[\begin{smallmatrix}-\mathcal{B}\\ \mathcal{I}\end{smallmatrix}\right](Z), \quad \text{for some } \; Z \\
&\iff X \in \mathit{Range}\left(\mathcal{P}\left[\begin{smallmatrix}-\mathcal{B}\\ \mathcal{I}\end{smallmatrix}\right]\right) .
\end{aligned}
$$

This shows that

$$\mathit{Nullspace}\,(\mathcal{A}) = \mathit{Range}\left(\mathcal{P}\left[\begin{smallmatrix}-\mathcal{B}\\ \mathcal{I}\end{smallmatrix}\right]\right) .$$

Since $\mathcal{P}$ and $\mathcal{B}$ have been constructed at the outset, we know how to construct the product $\mathcal{P}\left[\begin{smallmatrix}-\mathcal{B}\\ \mathcal{I}\end{smallmatrix}\right]$. Furthermore, since $\mathcal{P}$ is bijective and $\left[\begin{smallmatrix}-\mathcal{B}\\ \mathcal{I}\end{smallmatrix}\right]$ is injective (TYC 16.4.3), their product is an injection, as required.

Test Your Comprehension 16.4.5

Don't forget to deal with null matrices.

Argue that the nullspace of a non-injective non-null $n \times m$ matrix $\mathcal{A}$ can be expressed as the range of an injective $m \times (m - r)$ matrix, where r is the rank of $\mathcal{A}$.

Comment 16.4.6 ☞ **A peek into the future: all subspaces are nullspaces**

The reader may be curious as to whether all ranges are nullspaces. If that were the case, then the future TYC 18.3.19, which claims that all subspaces are ranges, would show that all subspaces are nullspaces. This is indeed the case, as we shall show in Theorem 24.2.2.

16.5 Appendix: Exiled Proofs

Terminology 16.5.1

We shall say that $n + m$ is **the girth** of an $n \times m$ matrix. For example, the girth of a 3×5 matrix is 8.

Proof of Theorem 16.2.2. We aim to show that if a matrix $\mathcal{A}$ is in an RREF, and $\mathcal{S}$ is an invertible matrix such that $\mathcal{SA}$ is also in an RREF, then

$$\mathcal{SA} = \mathcal{A}.$$

Synopsis of the proof: We will show that there are no counterexamples to the theorem. We will suppose otherwise, and consider a minimal counterexample in terms of girth. Exercise 16.2.3 tells us that a counterexample would have to have at least two rows and two columns, and not be null.

The minimality of girth will tell us that the counterexample $\mathcal{A}$ cannot have zero columns, as these can always be removed to create a less girthy counterexample. The $\mathcal{SA}$ cannot have null columns either.

When matrices in an RREF have no null columns, their first column is the first standard basis tuple. So they have a partitioned form $\begin{bmatrix} 1 & V \\ \mathbb{0} & \mathcal{D} \end{bmatrix}$, where $\mathcal{D}$ is in an RREF.

This will force the first column of our $\mathcal{S}$ to be E_1 as well, and the South-East corner of $\mathcal{S}$ is invertible.

The South-East corners of the matrices in play have smaller girth and so satisfy the claim of the theorem. From this we deduce that the South-East corners of $\mathcal{A}$ and of $\mathcal{SA}$ must be identical.

This brings us to focus on the one-row-thick North-East corners, and the proof is completed by showing that these must be identical as well, negating the possibility of a counterexample.

In view of Exercise 16.2.3, we shall concentrate on the case of a non-null matrix and $n, m > 1$.

If the theorem were not true in general, there would exist an $n_o \times m_o$ counterexample $\mathcal{A}_o$ of the smallest girth. In other words, for this $\mathcal{A}_o$ (in an RREF) there would exists an invertible $\mathcal{S}$ such that

- $\mathcal{SA}_o$ is in an RREF, and
- $\mathcal{SA}_o \neq \mathcal{A}_o$.

Yet there would not exist such an $\mathcal{S}$ for any $\mathcal{A}$ (in an RREF) having a smaller girth.

By Exercise 16.2.3 we know that $\mathcal{A}_o$ is not null, and $n_o, m_o > 1$.

By Exercise 8.5.4, we know that $\mathcal{SA}_o$ and $\mathcal{A}_o$ have exactly the same null columns. Let matrix $\mathcal{A}_1$ be obtained from $\mathcal{A}_o$ by removing all of the null columns. Then $\mathcal{A}_1$ is in an RREF (TYC 16.1.12), and $\mathcal{SA}_1$ is produced from

$\mathcal{S}\mathcal{A}_o$ by removing its null columns (Exc. 8.5.4 and TYC 8.5.1), so that $\mathcal{S}\mathcal{A}_1$ is also in an RREF (TYC 16.1.12). This means that $\mathcal{A}_1$ is a counterexample to the theorem as well, and hence cannot have a smaller girth than $\mathcal{A}_o$.

Yet, $\mathcal{A}_1$ is obtained from $\mathcal{A}_o$ by removing all of the null columns. Therefore it must be that $\mathcal{A}_o$ has no null columns, and so neither does $\mathcal{S}\mathcal{A}_o$ (Exc. 8.5.4).

It follows that the first column of $\mathcal{A}_o$ and of $\mathcal{S}\mathcal{A}_o$ is E_1, and so $\mathcal{A}_o$ and $\mathcal{S}\mathcal{A}_o$ can be expressed as

$$\mathcal{A}_o = \begin{bmatrix} 1 & X \\ \mathbb{0} & \mathcal{B} \end{bmatrix}_{(1|n-1)\times(1|m-1)} \quad \text{and} \quad \mathcal{S}\mathcal{A}_o = \begin{bmatrix} 1 & Y \\ \mathbb{0} & \mathcal{C} \end{bmatrix}_{(1|n-1)\times(1|m-1)} .$$

By TYC 16.1.14, $\mathcal{B}$ and $\mathcal{C}$ are in an RREF.

Since the first column of $\mathcal{S}\mathcal{A}_o$ is obtained by applying $\mathcal{S}$ to the first column of $\mathcal{A}_o$, we have

$$\mathcal{S}(E_1) = E_1 .$$

This shows that the first column of $\mathcal{S}$ is also E_1, and so $\mathcal{S}$ has a partitioned form

$$\begin{bmatrix} 1 & Z \\ \mathbb{0} & \mathcal{T} \end{bmatrix}_{(1|n-1)\times(1|n-1)} .$$

In particular,

$$\begin{bmatrix} 1 & Y \\ \mathbb{0} & \mathcal{C} \end{bmatrix} = \mathcal{S}\mathcal{A}_o = \begin{bmatrix} 1 & Z \\ \mathbb{0} & \mathcal{T} \end{bmatrix}\begin{bmatrix} 1 & X \\ \mathbb{0} & \mathcal{B} \end{bmatrix} , \tag{16.3}$$

so that $\mathcal{C} = \mathcal{T}\mathcal{B}$ by formula (9.3).

Since

$$\mathcal{A}_o = \mathcal{S}^{-1}\left(\mathcal{S}\mathcal{A}_o\right) ,$$

a similar argument shows that the first column of $\mathcal{S}^{-1}$ is also E_1, and so $\mathcal{S}^{-1}$ has a partitioned form

$$\begin{bmatrix} 1 & W \\ \mathbb{0} & \mathcal{Q} \end{bmatrix}_{(1|n-1)\times(1|n-1)} .$$

The equality $\mathcal{S}\mathcal{S}^{-1} = \mathcal{S}^{-1}\mathcal{S} = \mathcal{I}$ yields

$$\begin{bmatrix} 1 & Z \\ \mathbb{0} & \mathcal{T} \end{bmatrix}\begin{bmatrix} 1 & W \\ \mathbb{0} & \mathcal{Q} \end{bmatrix} = \mathcal{I} = \begin{bmatrix} 1 & W \\ \mathbb{0} & \mathcal{Q} \end{bmatrix}\begin{bmatrix} 1 & Z \\ \mathbb{0} & \mathcal{T} \end{bmatrix} .$$

By formula (9.3), we conclude that

$$\mathcal{T}\mathcal{Q} = \mathcal{I} = \mathcal{Q}\mathcal{T} ,$$

so that $\mathcal{T}$ and $\mathcal{Q}$ are invertible matrices that are inverses of each other.

Let us summarize:

- $\mathcal{B}$ has girth smaller than that of $\mathcal{A}_o$;
- $\mathcal{B}$ is in an RREF;
- $\mathcal{T}\mathcal{B}$ $(= \mathcal{C})$ is in an RREF;
- $\mathcal{T}$ is invertible.

It follows that $\mathcal{B} = \mathcal{T}\mathcal{B}$ $(= \mathcal{C})$, by our choice of $\mathcal{A}_o$. So

$$\mathcal{A}_o = \begin{bmatrix} 1 & X \\ \mathbb{0} & \mathcal{B} \end{bmatrix} \text{ and } \mathcal{S}\mathcal{A}_o = \begin{bmatrix} 1 & Y \\ \mathbb{0} & \mathcal{B} \end{bmatrix}.$$

Since $\mathcal{S}\mathcal{A}_o \neq \mathcal{A}_o$, it must be that $X \neq Y$. Let us write $Z = \left(z_1, z_2, z_3, \ldots, z_{n-1}\right)$.

Since $\mathcal{B}$ is in an RREF, all of its zero rows are at the bottom. Let us say that $R_1, R_2, \ldots, R_k$ are the non-zero rows of $\mathcal{B}$ listed in order. Note that in each of these rows the first non-zero entry is a pivot 1. If this pivot 1 is the $\star$-th entry of R_i, then the $\star$-th entry of every other R_j and of X and of Y must be zero. This is because

$$\begin{bmatrix} 1 & X \\ \mathbb{0} & \mathcal{B} \end{bmatrix} \text{ and } \begin{bmatrix} 1 & Y \\ \mathbb{0} & \mathcal{B} \end{bmatrix}$$

are in an RREF. This shows that no R_i is a linear combination of the other R_j's, X and Y (TYC 3.2.11).

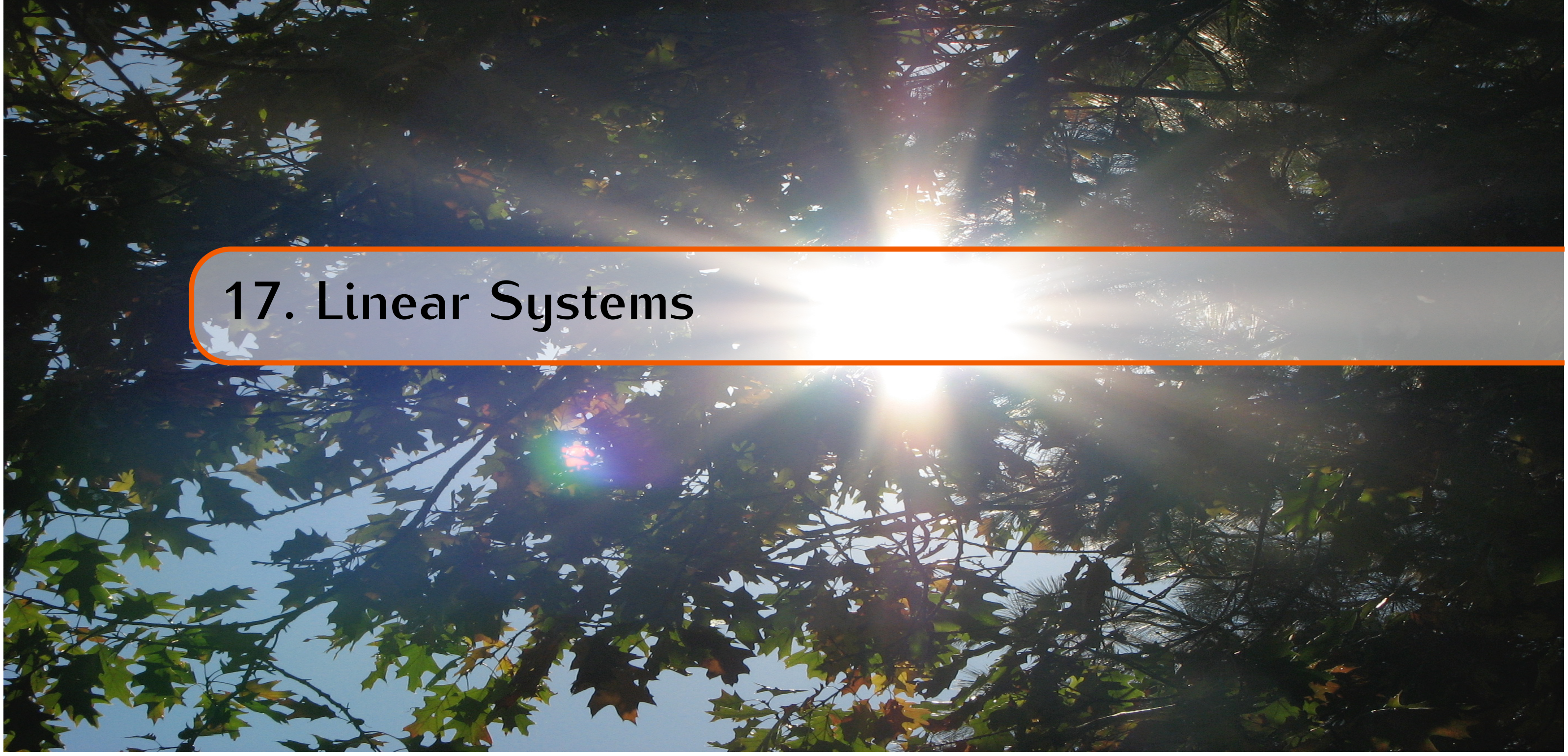
Yet from the equation (16.3), we conclude (via formula (9.3)) that

$$Y = X + z_1 R_1 + \cdots + z_k R_k \ . \tag{16.4}$$

It it were the case that some z_i is non-zero, then equality (16.4) can be rewritten to show that the corresponding R_i is a linear combination of the other R_j's, X and Y, which cannot be.

Hence every z_i is zero, and consequently $X = Y$, which cannot be true either.

This shows that the assumption of an existence of a counterexample to the theorem inevitably leads to a falsehood, and therefore, no such counterexample can exist. In other words, the theorem's claim is true. ■



17. Linear Systems

Last modified on December 8, 2018

17.1 Linear Equations

Terminology 17.1.1

An equation of the form

$$3x + \pi y - 7z - \alpha t + \frac{e}{4}s = -12 \tag{17.1}$$

is said to be **a linear equation in variables** x, y, z, t, s **with respective coefficients** $3, \pi, -7, -\alpha, \frac{e}{4}$ **and the right hand side** -12.

In a sense, the left hand side of equation (17.1) is a "linear combination of the variables", and the right hand side – a scalar.

We often have to rely on the context to discern which symbols or letters denote the variables and which – the coefficients, especially when the coefficients of the equation may vary, as is the case above, with α being unspecified, or when some of the coefficients are zero.

The convention is to *declare the variables first, and to identify their coefficients thereafter*. For example, if one declares the equation

$$pr + tq + vw = 7 \tag{17.2}$$

to be an equation in variables p, q, v, u, then this equation can be considered to be a linear equation in these variables with the corresponding coefficients $r, t, w, 0$.

The variable u is not appearing explicitly, as it is common to omit variables whose coefficients are zero. Nonetheless, such a variable, once declared, is very much present in the equation.

A **solution** to an equation (17.1) is a pentuple r_1, r_2, r_3, r_4, r_5 of numbers, such that assigning these to be the values of x, y, z, t, s respectively (i.e. replacing x, y, z, t, s by these numbers) turns (17.1) into a true equality.

In other words, $(x, y, z, t, s) = \left(r_1, r_2, r_3, r_4, r_5\right)$ gives a solution to (17.1) exactly when the equality

$$3r_1 + \pi r_2 - 7r_3 - \alpha r_4 + \frac{e}{4} r_5 = -12$$

holds.

For example, $(x, y, z, t, s) = (-4, 0, 0, 0, 0)$ describes a solution of (17.1), as does $(x, y, z, t, s) = (0, \frac{-5}{\pi}, 1, 0, 0)$, while $(x, y, z, t, s) = (0, 1, 0, 2, 0)$ does not.

Note that in describing a solution for (17.2) one has to assign a value to u as well as to p, q, v.

Notation 17.1.2

We shall adopt a matricial notation and express equations (17.1) and (17.2) as

$$\begin{bmatrix} 3 & \pi & -7 & -\alpha & \frac{e}{4} \end{bmatrix} \begin{pmatrix} x \\ y \\ z \\ t \\ s \end{pmatrix} = -12 ,$$

and

$$\begin{bmatrix} r & t & w & 0 \end{bmatrix} \begin{pmatrix} p \\ q \\ v \\ u \end{pmatrix} = 7 ,$$

respectively.

With this in mind, one can see that solving equation (17.1) amounts to finding all inputs for the matrix $\begin{bmatrix} 3 & \pi & -7 & -\alpha & \frac{e}{4} \end{bmatrix}$ that produce the output of -12.

The matrix $\begin{bmatrix} 3 & \pi & -7 & -\alpha & \frac{e}{4} \end{bmatrix}$ is said to be **the coefficient matrix of the equation** (17.1). The vector $\begin{pmatrix} x \\ y \\ z \\ t \\ s \end{pmatrix}$ is **the variable tuple, or a tuple of the variables**.

Example 17.1.3

Each of the following is a linear equation in variables x, y, γ:

1. $2x - 5y + 6\gamma = 9$.
2. $2x - 5y = 9$.
3. $5y + 6\gamma = 9$.
4. $2x = 9$.

The following are NOT linear equations in variables x, y, γ:

1. $2x^2 - 5y + 6\gamma = 9$.
2. $2x - 5xy + 6\gamma = 9$.
3. $2x - 5y + 6e^{\gamma} = 9$.
4. $2x - 5y + 6\gamma - 4\delta = 9$.

Test Your Comprehension 17.1.4

If $\mathcal{A}$ is a non-null 1x4 matrix, then the linear equation

$$\mathcal{A}(Z) = 3\frac{\pi}{e^2}$$

has at least one solution for Z; i.e. at least one quadruple Z_o that makes the equality hold.

17.1.1 — : Lines And Planes In $\mathbb{E}^3$

17.2 Linear Systems

Terminology 17.2.1

More commonly one is faced with a task of solving several linear equations simultaneously. In such a case we deal with **a system of linear equations, or a linear system, for short**. The reader has surely encountered these in his/her previous study of mathematics.

For example,

$$\begin{cases} 3x + 4y + 5z + 6t = 7 \\ -2x + 7y + 5z - 5t = -e \\ \pi x + 10y - \pi z = 23 \\ -x - y - z - t = 0 \\ 4x + \frac{7}{9}y - \sqrt{2}z + t = -1 \end{cases} \tag{17.3}$$

is a linear system of 5 equations in 4 variables x, y, z, t.

A solution to a linear system in, say, 6 variables, is a six-tuple that is a simultaneous solution to all of the equations in the system.

For example, $(1, -2, 0)$ is a solution of the system

$$\begin{cases} 2x - 5y + 9z = 12 \\ -x + y + 3z = -3 \\ \pi x - \frac{2}{3}y + 4z = \pi + \frac{2}{3} \\ -3y + \sqrt{3}z = 6 \end{cases} .$$

Two linear systems are said to be **equivalent**, if they have exactly the same solutions.

Test Your Comprehension 17.2.2

Any eight equations in any number of variables each, can be viewed as constituting a linear system, even when different equations involve different variables.

Notation 17.2.3

Using notation 17.1.2, we can express the linear system (17.3) as

$$\begin{cases} \begin{bmatrix} 3 & 4 & 5 & 6 \end{bmatrix} \begin{pmatrix} x \\ y \\ z \\ t \end{pmatrix} = 7 \\ \\ \begin{bmatrix} -2 & 7 & 5 & -5 \end{bmatrix} \begin{pmatrix} x \\ y \\ z \\ t \end{pmatrix} = -e \\ \\ \begin{bmatrix} \pi & 10 & -\pi & 0 \end{bmatrix} \begin{pmatrix} x \\ y \\ z \\ t \end{pmatrix} = 23 \\ \\ \begin{bmatrix} -1 & -1 & -1 & -1 \end{bmatrix} \begin{pmatrix} x \\ y \\ z \\ t \end{pmatrix} = 0 \\ \\ \begin{bmatrix} 4 & \frac{7}{9} & \sqrt{2} & 1 \end{bmatrix} \begin{pmatrix} x \\ y \\ z \\ t \end{pmatrix} = -1 \end{cases} .$$

Recalling the row-centric way of evaluating matricial outputs, we can combine equtions (17.2.3) into a single matricial equation

$$\begin{bmatrix} 3 & 4 & 5 & 6 \\ -2 & 7 & 5 & -5 \\ \pi & 10 & -\pi & 0 \\ -1 & -1 & -1 & -1 \\ 4 & \frac{7}{9} & \sqrt{2} & 1 \end{bmatrix} \begin{pmatrix} x \\ y \\ z \\ t \end{pmatrix} = \begin{pmatrix} 7 \\ -e \\ 23 \\ 0 \\ -1 \end{pmatrix} , \tag{17.4}$$

with $\begin{bmatrix} 3 & 4 & 5 & 6 \\ -2 & 7 & 5 & -5 \\ \pi & 10 & -\pi & 0 \\ -1 & -1 & -1 & -1 \\ 4 & \frac{7}{9} & \sqrt{2} & 1 \end{bmatrix}$ being **the coefficient matrix of the system**, $\begin{pmatrix} x \\ y \\ z \\ t \end{pmatrix}$ – **the variable tuple**, and $\begin{pmatrix} 7 \\ -e \\ 23 \\ 0 \\ -1 \end{pmatrix}$ – **the right hand side tuple of the system, or the target tuple**.

If we are dealing with a linear system of 127 equations in 392 variables, then

- the coefficient matrix has size 127×392,
- the 12-th row of the matrix is comprised of the 392 coefficients appearing on the left hand side of the 12-th equation,
- the variable tuple is a 392-tuple,
- the target tuple is a 127-tuple.

In this way linear systems can be identified with matricial equations of the form

$$\mathcal{A}(X) = C ,$$

and solving a linear system amounts to identifying the inputs, if any, for $\mathcal{A}$ that produce the target tuple C as the output.

We shall refer to a matricial equation

$$\mathcal{A}(X) = C ,$$

as "a linear system", when convenient, with the understanding that we are referring to the system of liner equations represented by this matricial equation.

If the target tuple is null, the system is said to be **homogeneous**; in all other cases the system is said to be **non-homogeneous**.

Given a linear system Sys, the **corresponding homogeneous system** is the homogeneous system with the same coefficient matrix as that for Sys.

Test Your Comprehension 17.2.4

1. A linear system has a solution exactly when the right hand tuple of the system is in the range of the coefficient matrix of the system.

2. If the coefficient matrix of a linear system is injective, then the system has at most one solution.

3. The solutions of a homogeneous system with a coefficient matrix $\mathcal{A}$ constitute the nullspace of $\mathcal{A}$.

Observation 17.2.5

We can restate Theorem 12.1.7 in the language of linear systems (represented as matricial equations).

If X_o is a solution for a given linear system, then the complete set of solutions to that system is the set

$$\{\ X_o + Z \mid Z \text{ is a solution to the corresponding homogeneous system }\}\ .$$

In particular, solution sets for linear systems are either empty (when the system has no solutions at all) or are **translated subspaces**. A translated subspace $\boldsymbol{T}$ is a set of tuples obtained by adding the same fixed tuple X_o to every tuple in a given subspace $\boldsymbol{W}$:

$$\boldsymbol{T} = \{\ X_o + Z \mid Z \in \boldsymbol{W}\ \}\ .$$

Test Your Comprehension 17.2.6 : Translated subspaces of vectors

What do the translated subspaces look like in Υ^3? Find a nice geometric description.

Theorem 17.2.7

Given a matricial equation $\mathcal{A}(X) = C$, where X is a variable tuple, and an *injective* matrix $\mathcal{S}$ of an appropriate size, the equation

$$\big(\mathcal{S}\mathcal{A}\big)(X) = \mathcal{S}(C)$$

has exactly the same solutions as $\mathcal{A}(X) = C$.

This states that linear systems represented by matricial equations

$$\mathcal{A}(X) = C \quad \text{and} \quad \big(\mathcal{S}\mathcal{A}\big)(X) = \mathcal{S}(C)$$

are equivalent, when $\mathcal{S}$ is injective.

Test Your Comprehension 17.2.8

If the matrix $\mathcal{A}$ in Theorem 17.2.7 is of size $n \times m$, then to be "appropriately sized" $\mathcal{S}$ has to be a $k \times n$ matrix.

Proof of Theorem 17.2.7. Obviously $\big(\mathcal{S}\mathcal{A}\big)(X_o) = \mathcal{S}\Big(\mathcal{A}(X_o)\Big)$. Since $\mathcal{S}$ is injective,

$$\mathcal{S}\Big(\mathcal{A}(X_o)\Big) = \mathcal{S}(C)$$

holds true exactly when

$$\mathcal{A}(X_o) = C$$

holds true, as $\mathcal{S}$ does not map two distinct inputs to the same output. ■

Comment 17.2.9

What Theorem 17.2.7 tells us is that , when $\mathcal{S}$ is injective, for example – invertible, by simultaneously replacing the original $\mathcal{A}$ by $\mathcal{S}\mathcal{A}$, and the original C by $S(C)$, we neither gain nor lose any solutions.

This way we can trade in a given linear system for an equivalent one. If the new system is simpler than the original, then we are ahead. "Simpler" here means having a simpler coefficient matrix. Now it is clear why one may want to find ways of simplifying a given matrix via multiplying it on the left by an injective matrix, when one is interested in solving linear systems.

Of course, the reader remembers that multiplying a matrix by an invertible matrix from the left amounts to performing a sequence of elementary row operations on the original matrix.

17.3 Augmented Matrices

Terminology 17.3.1

Given a matricial equation $\mathcal{A}(X) = C$, where

$$\mathcal{A} = \begin{bmatrix} K_1 & K_2 & \cdots & K_m \end{bmatrix},$$

the matrix

$$\left[\, \mathcal{A} \;\middle\vert\; C \right] := \begin{bmatrix} K_1 & K_2 & \cdots & K_m & C \end{bmatrix},$$

is said to be **the augmented matrix** representing a matricial equation $\mathcal{A}(X) = C$, or equivalently – the corresponding linear system.

In other words, the augmented matrix representing $\mathcal{A}(X) = C$ is obtained by attaching C to $\mathcal{A}$ as an additional column on the right.

For example,

$$\left[\begin{array}{cccc|c} 3 & 4 & 5 & 6 & 7 \\ -2 & 7 & 5 & -5 & -e \\ \pi & 10 & -\pi & 0 & 23 \\ -1 & -1 & -1 & -1 & 0 \\ 4 & \frac{7}{9} & \sqrt{2} & 1 & -1 \end{array}\right]$$

is the augmented matrix representing the matricial equation

$$\begin{bmatrix} 3 & 4 & 5 & 6 \\ -2 & 7 & 5 & -5 \\ \pi & 10 & -\pi & 0 \\ -1 & -1 & -1 & -1 \\ 4 & \frac{7}{9} & \sqrt{2} & 1 \end{bmatrix} \begin{pmatrix} x \\ y \\ z \\ t \end{pmatrix} = \begin{pmatrix} 7 \\ -e \\ 23 \\ 0 \\ -1 \end{pmatrix}.$$

Comment 17.3.2

Of course it is clear that $\left[\ \mathcal{A}\ \middle|\ C\right]$ can be interpreted as a partitioned matrix

$$\left[\ \mathcal{A}\ \ [C]\right],$$

and this is a point of view we adopt. Yet we shall continue to use the notation $\left[\ \mathcal{A}\ \middle|\ C\right]$ because it is cleaner and is traditional.

Clearly, the augmented matrix for a linear system carries all of the information about that system, apart from the names of the variables.

Test Your Comprehension 17.3.3

Hint: Thm. 8.1.7.

If $\mathcal{B}$ is a matrix of an appropriate size, then

$$\mathcal{B}\left[\ \mathcal{A}\ \middle|\ C\right] = \left[\ \mathcal{B}\mathcal{A}\ \middle|\ \mathcal{B}(C)\right].$$

In view of TYC 17.3.3, Theorem 17.2.7 can now be interpreted as follows:

Multiplying an augmented matrix for a linear system on the left by an injective matrix of an appropriate size produces an augmented matrix for an equivalent linear system.

In particular, performing an elementary row operation on an augmented matrix for a linear system produces an augmented matrix for an equivalent linear system.

Using Gauss-Jordan elimination scheme, we can transform a given (augmented) matrix into an (augmented) matrix in an RREF. If one learns how to find solutions for linear systems whose augmented matrices are in an RREF, one has learned how to solve linear systems in general.

Comment 17.3.4

Multiplying an augmented matrix for a linear system on the RIGHT by a matrix (even an invertible one) will commonly produce an augmented matrix for a linear system that is NOT equivalent to the original one.

Test Your Comprehension 17.3.5

Suppose that a linear system has an augmented matrix $\mathcal{G}$ such that RREF($\mathcal{G}$) has a pivot in the last column. Argue that the system has no solutions.

Hint: Consider a linear system whose augmented matrix is RREF($\mathcal{G}$). Focus on the the equation which corresponds to the row of RREF($\mathcal{G}$) that contains the last-column pivot.

17.4 Solving Homogeneous Linear Systems

Since a homogeneous linear system can be expressed as a matrix equation

$$\mathcal{A}(X) = \mathbb{0} \ ,$$

solving such a system amounts to finding the nullspace of $\mathcal{A}$, or equivalently, the nullspace of RREF($\mathcal{A}$) (TYC 16.2.8). Assuming for non-triviality that $\mathcal{A}$ is not null, this task can be accomplished by deleting the zero rows from RREF($\mathcal{A}$), and then applying Algorithm 16.4.4 to express the nullspace of the resulting matrix as a range of an injective matrix.

This process gives a clear explicit description of the solution set as the set of all linear combinations of a list of tuples, and provides a away to generate the solutions at will.

Let us note that the task of testing whether a given tuple Z is a solution of a given homogeneous linear system is a fairly trivial one: just test to see if the coefficient matrix annihilates Z.

As usual, finding a solution is much harder than testing whether a given candidate is one.

The method for solving homogeneous linear systems relies on a reduction of the coefficient matrix to its RREF, which is best left to computers. While it is fairly easy to apply Algorithm 16.4.4 by hand when the matrix is not large, there is no need to do that. Modern computing systems will carry out the whole process of finding solutions for linear systems from start to finish at great speed.

The reader's task is to gain a comprehension of the process and the underlying ideas, and to learn the ways of asking for and understanding the answers given by computing systems.

The concepts involved in the basic algorithms we are presenting play an important role in further developments of the subject. A reader who continues with more advanced studies of matrix and linear algebra, and develops an interest in optimizing the efficiency of computational algorithms, will need a solid understanding of the underlying theory, and much further study.

17.5 Solving Non-Homogeneous Linear Systems

Theorem 17.5.1 ☞ **Solving non-homogeneous systems by solving homogeneous ones**

The following claims are equivalent for a matrix $\mathcal{A} \in \mathbb{M}_{n\times m}$, and $C \in \mathbb{R}^m$.

1. $\mathcal{A}(X) = C$ has a solution (for X).
2. *Nullspace* $\left[\ \mathcal{A} \ \vdots\, C\right]$ contains an $(m+1)$-tuple whose last entry is not zero.

If we express Z_o as $\begin{pmatrix} X_o \\ \alpha \end{pmatrix}$, where $X_o \in \mathbb{R}^m$ and $\alpha \neq 0$, then

$$\frac{-1}{\alpha} X_o \text{ is a solution for } \mathcal{A}(X) = C\ ,$$

and and the set of ALL solutions is given by

$$\left\{ \left. \frac{-1}{\alpha} X_o + Y \ \right|\ Y \in \mathit{Nullspace}\,(\mathcal{A}) \right\}\ .$$

Comment 17.5.2

Theorem 17.5.1 shows that solving a non-homogeneous system expressed as $\mathcal{A}(X) = C$ can be accomplished by finding the nullspaces of $\left[\ \mathcal{A} \ \vdots\, C\right]$ and $\mathcal{A}$, or equivalently, by solving the homogeneous systems with coefficient matrices $\left[\ \mathcal{A} \ \vdots\, C\right]$ and $\mathcal{A}$ respectively.

Since we already have an algorithm for solving homogeneous systems, we now have one for solving non-homogeneous systems as well.

Of course, present day computing systems are apt at carrying out the whole process quickly, and so the reader is expected to learn how to ask such a computing system for a solution, and how to interpret the answers given.

Test Your Comprehension 17.5.3

Using Algorithm 16.4.4 one can express the *Nullspace* $\left[\ \mathcal{A} \ \vdots\, C\right]$ in Theorem 17.5.1 as a range of an injective matrix $\mathcal{M}$.

Argue that condition 2. in Theorem 17.5.1 is equivalent to the claim that the last row of $\mathcal{M}$ is not null, and in such a case one of the columns of $\mathcal{M}$ is a desired Z_o.

Proof of Theorem 17.5.1. The implication 1. $\Longrightarrow$ 2. follows from the equivalence

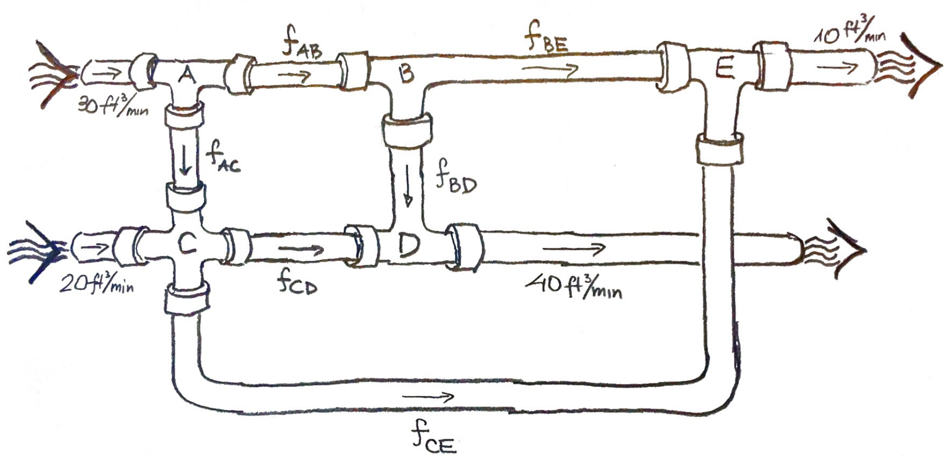
$$\begin{aligned} \mathcal{A}(W_o) = C &\iff \mathcal{A}(W_o) - C = \mathbb{0} \\ &\iff \left[\,\mathcal{A} \;\vdots\; C\right]\begin{pmatrix} W_o \\ -1 \end{pmatrix} = \mathbb{0} \qquad (17.5) \\ &\iff \begin{pmatrix} W_o \\ -1 \end{pmatrix} \in \textit{Nullspace}\left[\,\mathcal{A} \;\vdots\; C\right]. \end{aligned}$$

For the reverse implication 2. $\Longrightarrow$ 1., express Z_o as $\begin{pmatrix} X_o \\ \alpha \end{pmatrix}$, where $X_o \in \mathbb{R}^m$ and $\alpha \neq 0$. Then

$$\begin{pmatrix} \frac{-1}{\alpha} X_o \\ -1 \end{pmatrix} = \frac{-1}{\alpha}\begin{pmatrix} X_o \\ \alpha \end{pmatrix} = \frac{-1}{\alpha} Z_o \in \textit{Nullspace}\left[\,\mathcal{A} \;\vdots\; C\right].$$

The equivalence (17.5) indicates that $\frac{-1}{\alpha} X_o$ is a solution for $\mathcal{A}(X) = C$.

Theorem 12.1.7 establishes the remaining claim. See also Observation 17.2.5. ■



Exercise 17.5.4

Suppose that it is necessary to repair a pipe between connections C and D (see the diagram above), and that we would therefore would like to have the flow rate f_{CD} (measured in ft^3/min) be as small as possible.

At each of the connections A, B, C there is a built-in electronic valve (not shown) that can be used to regulate the flow rates $f_{AB}, f_{BE}, f_{AC}, f_{BD}, f_{CD}, f_{CE}$. The flow rates cannot be negative!

The total amount of water entering each junction within any given period of time must be the same as the total amount of water exiting the junction. The flow-in rates (30 and 20) and the flow-out rates (40 and 10) for the depicted portion of the plumbing system cannot be altered.

Construct a linear system such that you can characterize all possible tuples $\left(f_{AB}, f_{BE}, f_{AC}, f_{BD}, f_{CD}, f_{CE}\right)$ as its solutions with non-negative entries. Then among these find (with full justification!) those tuples that minimize f_{CD}.

17.6 Additional Problems

VI Coordinate Systems in $\mathbb{R}^n$

18. Linear Independence, Spans and Bases in $\mathbb{R}^n$

Last modified on December 8, 2018

18.1 Linear Independence

Terminology 18.1.1

Let us recall that a list $X_1, X_2, X_3, \ldots, X_m$ of n-tuples is **linearly independent** exactly when the matrix $\begin{bmatrix} X_1 & X_2 & X_3 & \ldots & X_m \end{bmatrix}$ is injective (Terminology 12.2.1 and Theorem 12.2.3).

When the nullspace of the matrix $\begin{bmatrix} X_1 & X_2 & X_3 & \ldots & X_m \end{bmatrix}$ is non-trivial (i.e. the matrix is not injective), we say that the list $X_1, X_2, X_3, \ldots, X_m$ is **linearly dependent**.

Since reordering the columns of a matrix $\mathcal{A}$ amounts to multiplying $\mathcal{A}$ by some elementary matrices from the right, this does not alter the jectivity of $\mathcal{A}$. Hence, linear (in)dependence is neither created nor destroyed by a change in the order in which the tuples are listed. We reflect this by saying that the concept of linear (in)dependence is **order-independent**.

In particular, we often say that n-tuples $X_1, X_2, X_3, \ldots, X_m$ are **(collectively) linearly (in)dependent**, when we want to indicate that they form a linearly (in)dependent list.

Test Your Comprehension 18.1.2

Argue that a linearly independent list cannot contain null tuples.

Test Your Comprehension 18.1.3

Argue that pivot columns of a non-null matrix in an RCEF are linearly independent.

Let us restate some of the conditions equivalent to the injectivity of a matrix (Synopsis 14.4.6) for the reader's convenience.

Synopsis 18.1.4

The following statements about a list of n-tuples $X_1, X_2, X_3, \ldots, X_m$ are equivalent (to the linear independence of $X_1, X_2, X_3, \ldots, X_m$).

Injectivity: $\begin{bmatrix} X_1 & X_2 & X_3 & \ldots & X_m \end{bmatrix}$ is injective.

Null linear combinations are trivial: The only linear combination of $X_1, X_2, X_3, \ldots, X_m$ that equals $\mathbb{0}_n$ is the trivial linear combination.

No linear combinations of others: None of $X_1, X_2, X_3, \ldots, X_m$ is null, and none are a linear combination of some of the others.

No linear combinations of preceding tuples: $X_1 \neq \mathbb{0}_n$, and no X_i is a linear combination of those preceding it on the list.

Comment 18.1.5

Obviously one obtains a list of conditions equivalent to linear dependence of the list $X_1, X_2, X_3, \ldots, X_m$ by negating the statements given in Synthesis 18.1.4.

Let us translate some of our results about the injectivity of matrices into the language of linear independence.

Test Your Comprehension 18.1.6

Each of the following conditions is equivalent to linear independence of $X_1, X_2, X_3, \ldots, X_m$.

1. For every $Y \in \mathbb{R}^n$, the equation $\begin{bmatrix} X_1 & X_2 & X_3 & \ldots & X_m \end{bmatrix}(Z) = Y$ has *at most one* solution for Z.

2. *Every element of $\mathbb{R}^n$ can be expressed in AT MOST ONE WAY as a linear combination of $X_1, X_2, X_3, \ldots, X_m$.*

Of course "at most one" allows the possibility of "none".

Test Your Comprehension 18.1.7

Please keep in mind that our "lists" are never empty. Exc. 14.1.8 can be helpful here.

1. The length of a linearly independent list in $\mathbb{R}^n$ is at most n.

2. A singleton list is linearly independent exactly when its (single) entry is not the null tuple.

3. A sublist of a linearly independent list is also linearly independent.

Exercise 18.1.8

Which of the following lists are linearly independent? In each case we have already consolidated the list into a matrix, so that the tuples in question are its columns.

$$\begin{bmatrix} 9 & 7 & 8 \\ 2 & 10 & 2 \\ 10 & 4 & 7 \\ 9 & 7 & 10 \end{bmatrix}, \qquad \begin{bmatrix} 1 & 2 & 3 & 4 \\ -2 & -3 & -4 & -1 \\ -3 & 2 & -5 & 5 \\ 0 & 2 & 0 & 1 \end{bmatrix}, \qquad \begin{bmatrix} 9 & 5 & 4 & 3 \\ 6 & 2 & 3 & 6 \\ 7 & 9 & 2 & 3 \end{bmatrix}, \qquad \begin{bmatrix} 25 & 8 & 7 & 4 \\ 12 & 5 & 4 & 2 \\ 36 & 4 & 8 & 4 \\ 32 & 10 & 9 & 5 \\ 15 & 2 & 3 & 2 \\ 39 & 5 & 3 & 8 \end{bmatrix},$$

$$\begin{bmatrix} 5.11905 & 8.96209 & 7.23809 & 3.49265 & 3.2032 \\ 4.07086 & 9.85003 & 9.18267 & 8.78583 & 1.06884 \\ 3.71832 & 2.01558 & 2.95635 & 2.90412 & 8.92439 \\ 6.55242 & 1.39381 & 7.56943 & 2.66038 & 8.51938 \\ 9.76072 & 1.16063 & 1.56601 & 4.25112 & 3.00871 \\ 7.71197 & 1.83115 & 8.89209 & 9.10654 & 8.58413 \end{bmatrix}.$$

Test Your Comprehension 18.1.9 **List operations that neither create nor destroy linear independence**

None of the following operations on a list of n-tuples creates or destroys linear independence*.

1. Inserting a tuple that is NOT a linear combination of the existing tuples on the list.

2. Scaling one of the tuples on the list by a non-zero scalar.

3. Rearranging the order in which the tuples appear on the list.

4. Adding to a tuple on the list a scalar multiple of another tuple on the list.

*... in the sense that the new list is linearly independent if and only if the original one is.

Exercise 18.1.10 **Injective matrices neither create nor destroy linear independence**

For an *injective* $\mathcal{S} \in \mathbb{M}_n$ the following claims about a list $X_1, X_2, X_3, \ldots, X_m$ of n-tuples are equivalent.

1. $X_1, X_2, X_3, \ldots, X_m$ are linearly independent.

2. $\mathcal{S}\left(X_1\right), \mathcal{S}\left(X_2\right), \mathcal{S}\left(X_3\right), \ldots, \mathcal{S}\left(X_m\right)$ are linearly independent.

Hint: Consider

$$\mathcal{S} \circ [X_1 \ \ X_2 \ \ X_3 \ \ \ldots \ \ X_m].$$

18.1.1 — : Linear Independence For Vectors

18.2 Spans

Terminology 18.2.1

The range of a matrix A is the set of all tuples that can be expressed as linear combinations of the columns of A. We state this more concisely by saying that the range of A is **the (linear) span** of its columns.

In general, **the (linear) span** $Span\left(X_1, X_2, \ldots, X_m\right)$ of a list $X_1, X_2, \ldots, X_m$ of n-tuples is the range of the matrix $\begin{bmatrix} X_1 & X_2 & \ldots & X_m \end{bmatrix}$.

In other words, $Span\left(X_1, X_2, \ldots, X_m\right)$ is the set of all linear combinations of the tuples $X_1, X_2, \ldots, X_m$.

We commonly drop off the word "linear" and just talk about **the span**.

The order in which the tuples are listed has no bearing on their span (TYC 10.2.10). This can be seen directly, since the operation of addition in $\mathbb{R}^n$ is commutative and associative, andhence it is irrelevant in which order the summands appear in a linear combination. In accordance with Terminology 18.1.1 we say that the concept of span is **order-independent**.

When the span of a list of tuples in a subspace$\boldsymbol{W}$ of $\mathbb{R}^n$ is all of $\boldsymbol{W}$, we say that **the list spans $\boldsymbol{W}$**. Alternatively, we say that the tuples **(collectively) span $\boldsymbol{W}$**.

Test Your Comprehension 18.2.2 **Spans are subspaces**

1. The span of a list of n-tuples is always a subspace of $\mathbb{R}^n$.

2. The span of a list of tuples in a *subspace* $\boldsymbol{W}$ of $\mathbb{R}^n$ is always a subspace of $\boldsymbol{W}$, and will be a proper subspace unless the list spans $\boldsymbol{W}$.

Test Your Comprehension 18.2.3

Argue that tuples $X_1, X_2, \ldots, X_m$ in a subspace $\boldsymbol{W}$ of $\mathbb{R}^n$ span $\boldsymbol{W}$ exactly when

$$Range\begin{bmatrix} X_1 & X_2 & \ldots & X_m \end{bmatrix} = \boldsymbol{W} \ . \tag{18.1}$$

This happens exactly when every element of $\boldsymbol{W}$ can be expressed as a linear combination of $X_1, X_2, \ldots, X_m$ in AT LEAST ONE WAY.

Comment 18.2.4

When $\boldsymbol{W}$ is a range of a given matrix, say $\boldsymbol{W} = Range(\mathcal{A})$, the equality (18.1) becomes the equality of the ranges:

$$Range\begin{bmatrix} X_1 & X_2 & \ldots & X_m \end{bmatrix} = Range(\mathcal{A}) \ .$$

Therefore the material of section 16.3 offers us a way for testing (based on an RCEF) whether a given list of tuples spans the range of a given matrix.

At this point let us proceed by restating some of the results we have presented previously now using the new terminology of "spans" .

Test Your Comprehension 18.2.5

Argue that if $X_1, X_2, \ldots, X_{47} \in \mathbb{R}^n$ then

$$Span\left(X_1, X_2, \ldots, X_{29}\right) \subseteq Span\left(X_1, X_2, \ldots, X_{47}\right) \ .$$

As we shall see in a moment, it CAN very well happen that $Span\left(X_1, X_2, \ldots, X_{29}\right) = Span\left(X_1, X_2, \ldots, X_{47}\right)$.

Test Your Comprehension 18.2.6

Argue that inserting n-tuples into a list that spans $\mathbb{R}^n$ produces another list that spans $\mathbb{R}^n$.

Test Your Comprehension 18.2.7 ☞ **List operations that do not alter the span**

Verify that none of the following operations on a list of n-tuples alters the span of the list.

1. Including or removing a null tuple.

2. Removing a tuple that is a linear combination of other tuples on the list.

3. Inserting a tuple that is a linear combination of the existing tuples on

the list.

Hint: Think of elementary column operations. TYC 10.2.10 can be useful here.

4. Scaling one of the tuples on the list by a non-zero scalar.

5. Adding to a tuple on the list a scalar multiple of another tuple on the list.

Exercise 18.2.8

Find a list of tuples $X_1, X_2, \dots, X_7$ which span the range of the matrix

$$\begin{bmatrix} 0 & 1 & 3 & 1 & 9 & 1 & 7 \\ 0 & 1 & 2 & 2 & 10 & 10 & 1 \\ 0 & 8 & 9 & 10 & 7 & 3 & 5 \\ 0 & 2 & 6 & 9 & 8 & 3 & 5 \end{bmatrix},$$

but such that none of them appear as the columns of this matrix.

Test Your Comprehension 18.2.9 ☞ **Reducing a list to a linearly independent list with the same span**

Hint: Thm. 14.1.4.

Argue that if not all n-tuples on a list are null, then by removing some of the tuples from the list we can arrive at a linearly independent list that has the same span as the original list.

Test Your Comprehension 18.2.10 ☞ **It takes at least n distinct n-tuples to span $\mathbb{R}^n$**

Hint: TYC 18.2.9.

Argue that if $X_1, X_2, \dots, X_m$ span $\mathbb{R}^{35}$, then there are at least 35 distinct tuples among $X_1, X_2, \dots, X_m$.

Exercise 18.2.11 ☞ **Matrices send lists that span their initial space to lists that span their range**

Hint: Consider $\mathcal{A} \circ [X_1 \ \ X_2 \ \ \dots \ \ X_m]$, and recall what you had learned about the range of a composition $f \circ g$, where g is a surjection.

Argue that if $X_1, X_2, \dots, X_k$ span $\mathbb{R}^m$, and $\mathcal{A} \in \mathbb{M}_{n\times m}$, then $\mathcal{A}(X_1), \mathcal{A}(X_2), \dots, \mathcal{A}(X_m)$ span the range of $\mathcal{A}$.

Test Your Comprehension 18.2.12 ☞ **Invertible matrices match the spanning lists with the spanning lists**

Argue that if $\mathcal{S} \in \mathbb{M}_n$ is *invertible*, the following claims about a list $X_1, X_2, \dots, X_m$ of n-tuples are equivalent.

Hint: Apply Exc. 18.2.11 to $\mathcal{S}$ and $\mathcal{S}^{-1}$.

1. $X_1, X_2, \dots, X_m$ span $\mathbb{R}^n$.

2. $S\left(X_1\right), S\left(X_2\right), \dots, S\left(X_m\right)$ span $\mathbb{R}^n$.

18.2.1 — 🚀 : Spans For Vectors

18.3 Coordinate Systems

In Section 4.2 we discussed the concept of Cartesian coordinates as a way of assigning unique addresses (tuples) to vectors. In TYC 4.2.2, we had observed that the entries of such an address for a vector $\vec{v}$ are the coefficients for the unique linear combination of vectors $\vec{\imath}, \vec{\jmath}$, and $\vec{k}$, that yields $\vec{v}$.

In this sense we can say that $\vec{\imath}, \vec{\jmath}$, and $\vec{k}$ generate a coordinate system for Υ^3. Every vector in Υ^3 is a unique linear combination of $\vec{\imath}, \vec{\jmath}$, and $\vec{k}$. The unique triple of the coefficients from such a linear combination serves as the address for the vector. Every vector receives a unique address, and all addresses are taken.

As we have seen in Section 4.2, such a coordinatization creates a bridge between the geometric universe Υ^3 and the algebraic universe $\mathbb{R}^3$.

Of course the vectors we call $\vec{\imath}, \vec{\jmath}$, and $\vec{k}$ depend on the choice of the coordinate axes for $\mathbb{E}^3$, and we know that there are infinitely many possible choices for these.

This suggests an interpretation of the coordinate systems for Υ^3 as being generated by some three vectors in Υ^3, rather than by the coordinate axes for $\mathbb{E}^3$.

If the generating vectors all have unit length and are mutually perpendicular, we can use them to build the axes of the corresponding Cartesian coordinate system for $\mathbb{E}^3$.

As long as every vector in Υ^3 can be resolved as a linear combination of these generating vectors in a unique fashion, it is not imperative that the generating vectors be of the same length or be perpendicular to each other. This way we can still use the triples of the coefficients (as addresses) to identify each vector in Υ^3.

If we were to use such a list of generating vectors to propagate the axes for a coordinate system, such axes will not be mutually perpendicular, and each may have its own unit of length (given by the length of the vector that propagated it). Such axes can still be used to assign to each point of $\mathbb{E}^3$ a unique triple of numbers as its address.

This way of thinking can be extended into the realm of $\mathbb{R}^n$ (and beyond!). The concept of coordinate systems yields a very powerful theory that lies at the center of many of the most effective tools of linear algebra.

Terminology 18.3.1

A list $X_1, X_2, \ldots, X_m$ of tuples in a subspace $\boldsymbol{W}$ of $\mathbb{R}^n$ is said to be **a coordinate system (a.k.a. a basis) of $\boldsymbol{W}$** if every tuple in $\boldsymbol{W}$ can be expressed IN EXACTLY ONE WAY* as a linear combination of $X_1, X_2, \ldots, X_m$.

In other words, for each element $V \in \boldsymbol{W}$ there is a unique m-tuple $(\alpha_1, \alpha_2, \ldots, \alpha_m)$ such that

$$V = \alpha_1 X_1 + \alpha_2 X_2 + \cdots + \alpha_m X_m \ .$$

*... apart from the order in which $X_1, X_2, \ldots, X_m$ appear in the linear combination expression.

Test Your Comprehension 18.3.2

Argue that a list of tuples in a subspace $\boldsymbol{W}$ of $\mathbb{R}^n$ is a coordinate system of $\boldsymbol{W}$ exactly when the list spans $\boldsymbol{W}$ and is linearly independent.

Test Your Comprehension 18.3.3

$X_1, X_2, \ldots, X_m$ is a coordinate system of a subspace $\boldsymbol{W}$ of $\mathbb{R}^n$ exactly when

1. $\begin{bmatrix} X_1 & X_2 & \ldots & X_m \end{bmatrix}$ is injective;
2. $\mathit{Range} \begin{bmatrix} X_1 & X_2 & \ldots & X_m \end{bmatrix} = \boldsymbol{W}$.

Hint: Exc. 14.1.1, TYC 16.2.22 and Thm. 18.1.3.

Exercise 18.3.4

Argue that the pivot columns of a non-null RCEF($\mathcal{A}$) form a coordinate system of the range of $\mathcal{A}$.

Exercise 18.3.5

Find a coordinate system of the range of the following matrix by using its RCEF as described in Exercise 18.3.4.

$$\mathcal{A} = \begin{bmatrix} -1 & 3 & 3 & 3 & 3 \\ -5 & 15 & 15 & 15 & 15 \\ 2 & -6 & -7 & -10 & -8 \\ -3 & 9 & 8 & 5 & 7 \\ -5 & 17 & 13 & -2 & 8 \\ 1 & -7 & -6 & 3 & -3 \\ 1 & 5 & 0 & -14 & -4 \end{bmatrix}.$$

Test Your Comprehension 18.3.6 ☞ **Operations on coordinate systems that produce coordinate systems**

Argue that the following operations performed on a coordinate system of a subspace $\boldsymbol{W}$ of $\mathbb{R}^n$ produces yet again a coordinate system.

1. Changing the order of the list.
2. Scaling one of the elements on the list by a non-zero scalar.
3. Adding to an element on the list a scalar multiple of another element on the list.

Hint: TYC's 18.1.9 and 18.2.7.

Test Your Comprehension 18.3.7

Argue that a trivial subspace $\{\mathbb{0}_n\}$ has no coordinate systems.

Test Your Comprehension 18.3.8 ☞ **Coordinate systems of $\mathbb{R}^n$ correspond to the invertible matrices in $\mathbb{M}_n$**

Argue that $X_1, X_2, \ldots, X_m$ is a coordinate system of $\mathbb{R}^n$ exactly when

$$\begin{bmatrix} X_1 & X_2 & \ldots & X_m \end{bmatrix} \text{ is an invertible matrix },$$

so that in particular we must have $m = n$.

Thus, every coordinate system of $\mathbb{R}^n$ has exactly n tuples in it.

Terminology 18.3.9

The list of the standard basis tuples $E_1, E_2, \ldots, E_n$ is a coordinate system of $\mathbb{R}^n$. This coordinate system is called **the standard coordinate system of $\mathbb{R}^n$**.

Hint: Start with the standard coordinate system and use TYC 18.3.6.

Exercise 18.3.10

Find a coordinate system of $\mathbb{R}^6$ made up of 6–tuples that only have entries 1 and -1.

Hint: Excs. 18.1.10 and 18.2.11 can be helpful here.

Exercise 18.3.11 ☞ **Injective matrices send bases of the initial space to bases of the range**

Argue that if $\mathcal{A} \in \mathbb{M}_{n\times m}$ is injective, and $X_1, X_2, \ldots, X_m$ is a coordinate system of $\mathbb{R}^m$, then

$$\mathcal{A}\left(X_1\right), \mathcal{A}\left(X_2\right), \ldots, \mathcal{A}\left(X_n\right) \text{ is a coordinate system of the range of } \mathcal{A};.$$

Hint: TYC 18.2.12, and Exc. 18.3.11 applied to $\mathcal{S}$ and $\mathcal{S}^{-1}$.

Test Your Comprehension 18.3.12 ☞ **Invertible matrices map bases to bases**

If $\mathcal{S} \in \mathbb{M}_n$ is *invertible*, the following claims about a list $X_1, X_2, \ldots, X_n$ of n–tuples are equivalent.

1. $X_1, X_2, \ldots, X_n$ is a coordinate system of $\mathbb{R}^n$.
2. $\mathcal{S}\left(X_1\right), \mathcal{S}\left(X_2\right), \ldots, \mathcal{S}\left(X_n\right)$ is a coordinate system of $\mathbb{R}^n$.

Test Your Comprehension 18.3.13 ☞ **Surjective matrices MAY NOT map bases to bases**

Give an example of a surjective 2×3 matrix that does not map the standard coordinate system to a coordinate system.

Theorem 18.3.14 ☞ **A matrix is completely determined by its action on a basis**

If $X_1, X_2, \ldots, X_m$ is a coordinate system of $\mathbb{R}^m$, and $Y_1, Y_2, \ldots, Y_m$ is any list of elements of $\mathbb{R}^n$, then there exists EXACTLY ONE $n \times m$ matrix $\mathcal{A}$ such that

$$\begin{aligned}\mathcal{A}\left(X_1\right) &= Y_1\\ \mathcal{A}\left(X_2\right) &= Y_2\\ &\vdots\\ \mathcal{A}\left(X_m\right) &= Y_m\ .\end{aligned} \tag{18.2}$$

Proof of Theorem 18.3.14. The equalities (18.2) can be simply expressed as a matricial equality

$$\mathcal{A} \circ \left[X_1 \quad X_2 \quad \cdots \quad X_m\right] = \left[Y_1 \quad Y_2 \quad \cdots \quad Y_m\right]. \tag{18.3}$$

Since $X_1, X_2, \ldots, X_m$ is a coordinate system of $\mathbb{R}^m$, $\begin{bmatrix} X_1 & X_2 & \cdots & X_m \end{bmatrix}$ is invertible, and therefore the equality (18.3) is, in turn, equivalent to the equality

$$\mathcal{A} = \begin{bmatrix} Y_1 & Y_2 & \cdots & Y_m \end{bmatrix} \circ \begin{bmatrix} X_1 & X_2 & \cdots & X_m \end{bmatrix}^{-1}.$$

This shows that $\begin{bmatrix} Y_1 & Y_2 & \cdots & Y_m \end{bmatrix} \circ \begin{bmatrix} X_1 & X_2 & \cdots & X_m \end{bmatrix}^{-1}$ is the unique matrix $\mathcal{A}$ that satisfies the equalities (18.2). ■

Test Your Comprehension 18.3.15 ☞ **Invertible matrices in $\mathbb{M}_n$ match pairs of bases of $\mathbb{R}^n$**

Suppose that $X_1, X_2, X_3, \ldots, X_n$ and $Y_1, Y_2, Y_3, \ldots, Y_n$ are two coordinate systems of $\mathbb{R}^n$. Argue that there is EXACTLY ONE invertible $\mathcal{S} \in \mathbb{M}_n$ such that

$$\mathcal{S}(X_i) = Y_i, \quad \text{for all} \quad i.$$

Hint: Thm. 18.3.14 and its proof.

Theorem 18.3.16 ☞ **Every linearly independent list in a subspace $\boldsymbol{W}$ is part of a basis of $\boldsymbol{W}$**

If $X_1, X_2, X_3, \ldots, X_k$ is a linearly independent list in a subspace $\boldsymbol{W}$ of $\mathbb{R}^n$, then by inserting some additional tuples it is possible to arrive at a coordinate system of $\boldsymbol{W}$.

Of course this applies to the case $\boldsymbol{W} = \mathbb{R}^n$ as well.

Proof of Theorem 18.3.16. The proof follows the same strategy as that used in the proof of Theorem 14.2.6, and is based on Theorem 14.2.4 and TYC 18.1.9. In the latter we had established that when an n-tuple Y is not in the span of a given linearly independent list of n-tuples, inserting Y into the list produces another linearly independent list.

If the linearly independent list $X_1, X_2, X_3, \ldots, X_k$ spans $\boldsymbol{W}$, it is already a coordinate system of $\boldsymbol{W}$ and we are done: no additional tuples need to be added to the list.

In the alternative case, the span of $X_1, X_2, X_3, \ldots, X_k$ is a proper subset of $\boldsymbol{W}$, and in that case at least one tuple Y of $\boldsymbol{W}$ is not in the span of $X_1, X_2, X_3, \ldots, X_k$. Hence, by TYC 18.1.9, $X_1, X_2, X_3, \ldots, X_k, Y$ is a (longer) linearly independent list in $\boldsymbol{W}$.

If this longer list spans $\boldsymbol{W}$, we are done. If it does not, we can repeat the procedure and add another tuple from $\boldsymbol{W}$ to the list without losing the linear independence.

This process will not go on forever, since linearly independent lists in $\mathbb{R}^n$ cannot have more than n tuples in it (TYC 18.1.7). Hence at some point the process terminates, and at that time we have arrived at the desired coordinate system of $\boldsymbol{W}$. ■

Comment 18.3.17

Let us note that our proof of Theorem 18.3.16 does NOT offer a practical algorithm for carrying out the described process of enlargement.

When $\boldsymbol{W} = \mathbb{R}^n$, we can use Algorithm 16.2.34) to enlarge a linearly independent list in $\mathbb{R}^n$ to a coordinate system of $\mathbb{R}^n$.

What about the case of $\{\mathbb{0}\} \subsetneq \boldsymbol{W} \subsetneq \mathbb{R}^n$?

In the section for exiled algorithms at the end of this chapter we present Algorithm 18.4.1 that applies in the case when one coordinate system of such a $\boldsymbol{W}$ is already known.

This case covers a lot of ground. Most of the time the subspaces of interest come already expressed as either a nullspace or a ranges of a matrix. In Section 16.4 we presented an algorithm for expressing a nullspace of a matrix as a range of a matrix. So, we can focus on just the ranges.

In Theorem 19.6.1 we shall present a simple algorithm for constructing a coordinate system of a range of a matrix (via the RREF).

Thus, Algorithm 18.4.1 applies (indirectly) to all subspaces $\{\mathbb{0}\} \subsetneq \boldsymbol{W} \subsetneq \mathbb{R}^n$ that are expressed as either a range or a nullspace of a matrix.

Corollary 18.3.18 ☞ **Sizes of bases of subspaces**

Every non-trivial subspace of $\mathbb{R}^n$ has a coordinate system with at most n tuples in it.

The whole $\mathbb{R}^n$ is the only subspace of $\mathbb{R}^n$ that has a coordinate system with exactly n tuples in it.

Proof of Corollary 18.3.18. A single non-null tuple from a non-trivial subspace $\boldsymbol{W}$ of $\mathbb{R}^n$ forms a linearly independent list. By Theorem 18.3.16, this list can be enlarged to a coordinate system of $\boldsymbol{W}$. This coordinate system of $\boldsymbol{W}$, being a linearly independent list in $\mathbb{R}^n$, has at most n tuples in it (TYC 18.1.7).

If a coordinate system $\boldsymbol{\Gamma}$ of $\boldsymbol{W}$ has exactly n tuples in it, then, being a linearly independent list in $\mathbb{R}^n$, $\boldsymbol{\Gamma}$ can be enlarged to a coordinate system of $\mathbb{R}^n$ (Theorem 18.3.16). Every coordinate system of $\mathbb{R}^n$ has exactly n tuples in it (TYC 18.3.8), and so no proper enlargement is possible.

In other words, $\boldsymbol{\Gamma}$ must be a coordinate system of $\mathbb{R}^n$. Hence

$$\mathbb{R}^n = Span(\boldsymbol{\Gamma}) = \boldsymbol{W}. \qquad \blacksquare$$

Test Your Comprehension 18.3.19 ☞ All subspaces are ranges

Argue that every non-trivial subspace of $\mathbb{R}^n$ is a range of an injective matrix.

Then argue that every subspace of $\mathbb{R}^n$ is a range of an $n \times n$ matrix.

Hint: To establish the second claim use Exercise 14.1.1 and the fact that injective matrices are portrait-shaped. Don't forget to deal with the trivial subspaces.

Comment 18.3.20

Since we already know that all matrix ranges are subspaces, this shows that *the subspaces of* $\mathbb{R}^n$ *are exactly the matrix ranges.*

Eventually (see TYC 24.2.6) we will show that every subspace in $\mathbb{R}^n$ is a nullspace of a matrix. This will establish the fact that *subspaces of* $\mathbb{R}^n$*, matrix ranges and matrix nullspaces are exactly the same objects*.

Test Your Comprehension 18.3.21 ☞ Images of subspaces are subspaces

If $\boldsymbol{W}$ is a subspace of $\mathbb{R}^m$, and $\mathcal{A} \in \mathbb{M}_{n\times m}$,

then $\mathcal{A}\langle \boldsymbol{W}]$ is a subspace of $\mathbb{R}^n$.

Hint: $\boldsymbol{W}$ must be a range of an $m \times m$ matrix $\mathcal{B}$. Show that $\mathcal{A}\langle \boldsymbol{W}]$ is the range of $\mathcal{AB}$. Exc. 2.3.10 can be very helpful here.

Test Your Comprehension 18.3.22 ☞ Every list that spans a non-trivial subspace contains a basis of that subspace as a sublist

Argue that if a list of n-tuples spans a non-trivial subspace $\boldsymbol{W}$ of $\mathbb{R}^n$, then by removing some tuples from the list it is possible to arrive at a coordinate system of $\boldsymbol{W}$.

"possible" $\neq$ "not impossible"!

Equivalently, argue that it is always possible to remove some columns from a matrix $\mathcal{A}$ in such a way that the remaining columns form a coordinate system of the range of $\mathcal{A}$.

Hint: TYC 18.2.9.

Theorem 18.3.23 ☞ The idea of a dimension

Every coordinate system of a given non-trivial subspace $\boldsymbol{W}$ of $\mathbb{R}^n$ contains exactly the same number of tuples.

Proof of Theorem 18.3.23. Suppose that $V_1, V_2, V_3, \ldots, V_k$ and $Z_1, Z_2, Z_3, \ldots, Z_p$ are two unspecified coordinate systems of $\boldsymbol{W}$. If we can deduce that $p \geq k$, then we will have shown that any coordinate system of $\boldsymbol{W}$ contains no more elements than any other coordinate system of $\boldsymbol{W}$, and the desired conclusion follows right away.

Consider matrices

$$\mathcal{A} := \begin{bmatrix} V_1 & V_2 & V_3 & \ldots & V_k \end{bmatrix}_{n\times k} \text{ and } \mathcal{B} := \begin{bmatrix} Z_1 & Z_2 & Z_3 & \ldots & Z_p \end{bmatrix}_{n\times p}.$$

$\mathcal{A}$ and $\mathcal{B}$ are injective matrices, both of which have $\boldsymbol{W}$ as the range (TYC 18.3.3).

By the range inclusion factorization (Thm. 13.1.2) we can write $\mathcal{A}_{n\times k} = \mathcal{B}_{n\times p}\mathcal{C}_{p\times k}$, for some $p \times k$ matrix $\mathcal{C}$. Since $\mathcal{A}$ is injective, so is $\mathcal{C}$ (TYC 12.1.13). Hence $\mathcal{C}$ is portrait-shaped; i.e. $p \geq k$, and we are done. ∎

Terminology 18.3.24

The common size of all of the coordinate systems of a non-trivial subspace $\boldsymbol{W}$ of $\mathbb{R}^n$ is said to be **the dimension of** $\boldsymbol{W}$, and is denoted by $\mathit{dim}(\boldsymbol{W})$. In a sense the dimension of a subspace is a measure of its size.

We adopt the convention that the dimension of the trivial subspace $\{\mathbb{O}_n\}$ is zero.

Test Your Comprehension 18.3.25 ☞ **Lengths of linearly independent and spanning lists in subspaces**

Suppose that $\boldsymbol{W}$ is a non-trivial k-dimensional subspace of $\mathbb{R}^n$. Then argue that the following hold.

1. Every linearly independent list in $\boldsymbol{W}$ has length at most k, and every list that spans $\boldsymbol{W}$ has length at least k.

2. If a list that spans $\boldsymbol{W}$ or a list that is linearly independent in $\boldsymbol{W}$ has exactly k entries, then that list is a coordinate system of $\boldsymbol{W}$.

Hint: Theorem 18.3.16 and TYC 18.3.22 can be helpful here.

Theorem 18.3.26 ☞ **(Strictly) Bigger subspaces have (strictly) bigger dimensions**

If $\boldsymbol{W}$ and $\boldsymbol{V}$ are subspaces of $\mathbb{R}^n$, and $\boldsymbol{W} \subseteq \boldsymbol{V}$, then $\mathit{dim}(\boldsymbol{W}) \leq \mathit{dim}(\boldsymbol{V})$, and the equality of dimensions holds exactly when $\boldsymbol{W} = \boldsymbol{V}$.

Proof of Theorem 18.3.26. The claim is obviously true if one of the subspaces involved is trivial. Let us deal with the case of $\boldsymbol{W}$ and $\boldsymbol{V}$ both being non-trivial.

Suppose that $\boldsymbol{F}$ is a coordinate system of $\boldsymbol{W}$. Then $\boldsymbol{F}$ has $\mathit{dim}(\boldsymbol{W})$ tuples in it, and is a linearly independent list in $\boldsymbol{W}$, and hence in $\boldsymbol{V}$. Thus $\boldsymbol{F}$ can be extended to a coordinate system $\boldsymbol{G}$ of $\boldsymbol{V}$ (Thm. 18.3.16), which has $\mathit{dim}(\boldsymbol{V})$ tuples in it. This shows that $\mathit{dim}(\boldsymbol{W}) \leq \mathit{dim}(\boldsymbol{V})$.

Obviously $\mathit{dim}(\boldsymbol{W}) = \mathit{dim}(\boldsymbol{V})$ whenever $\boldsymbol{W} = \boldsymbol{V}$. Let us demonstrate the reverse implication.

Suppose that $\mathit{dim}(\boldsymbol{W}) = \mathit{dim}(\boldsymbol{V})$. Then $\boldsymbol{F}$ and $\boldsymbol{G}$ contain the same number of tuples, and therefore $\boldsymbol{F} = \boldsymbol{G}$. Hence

$$\boldsymbol{V} = \mathit{Span}(\boldsymbol{G}) = \mathit{Span}(\boldsymbol{F}) = \boldsymbol{W} .$$ ∎

18.3.1 — 🚀 : Coordinate Systems For Vectors

18.4 Appendix: Exiled Algorithms

Algorithm 18.4.1 ☞ **Enlarging a linearly independent set to a basis of a subspace, that has a known basis**

Saying that a non-trivial subspace $\boldsymbol{W}$ of $\mathbb{R}^n$ has a known basis is equivalent to the statement that there is a known injective matrix $\mathcal{B}$ whose range is $\boldsymbol{W}$. (The columns of such a $\mathcal{B}$ form a basis of $\boldsymbol{W}$.)

A list of tuples is a linearly independent list in $\boldsymbol{W}$ exactly when the matrix $\mathcal{A}$ formed from the list is an injective matrix whose columns are in $\boldsymbol{W}$. So, let us start with an injective matrix

$$\mathcal{A} = \begin{bmatrix} A_1 & A_2 & \cdots & A_m \end{bmatrix} ,$$

where $A_i \in \boldsymbol{W}$, for all i.

> We aim to show how to adjoin columns to $\mathcal{A}$ to produce an injective matrix $\mathcal{C}$ whose range is $\boldsymbol{W}$. The columns of such a $\mathcal{C}$ are an enlargement of $A_1, A_2, \ldots, A_m$ to a coordinate system of $\boldsymbol{W}$.

Note that since $\boldsymbol{W}$ is a subspace of $\mathbb{R}^n$, and the columns of $\mathcal{A}$ are in $\boldsymbol{W}$, so are all of their linear combinations. Hence the range of $\mathcal{A}$ is a subset of $\boldsymbol{W}$ (TYC 6.1.3).

If the range of $\mathcal{A}$ equals $\boldsymbol{W}$, no enlargement is necessary, since $A_1, A_2, \ldots, A_m$ is already a coordinate system of $\boldsymbol{W}$. So, let us focus on the case that the range of $\mathcal{A}$ is a proper subset of $\boldsymbol{W}$.

> Here is the state of affairs: we have two injective matrices $\mathcal{A}$ and $\mathcal{B}$ such that
>
> $$\mathit{Range}\,(\mathcal{A}) \subsetneq \mathit{Range}\,(\mathcal{B}) \;,$$
>
> and we are trying to widen $\mathcal{A}$ to an injective matrix $\mathcal{C}$ whose range equals that of $\mathcal{B}$.

In the margin commentary for the proof of the range inclusion factorization (Thm. 13.1.2) we had indicated a procedure for finding a matrix $\mathcal{M}$ such that

$$\mathcal{A} = \mathcal{B}\mathcal{M}.$$

The procedure involves solving linear systems represented by matrical equations of the form

$$A_i = \mathcal{B}(X) \ .$$

Of course we have already seen how to solve such systems.

Let us write

$$\mathcal{M} = \begin{bmatrix} M_1 & M_2 & \cdots & M_m \end{bmatrix} ,$$

so that

$$A_i = \mathcal{B}\left(M_i\right) \ ,$$

for each i.

Since $\mathcal{A}$ is injective and $\mathcal{A} = \mathcal{B}\mathcal{M}$, $\mathcal{M}$ must be injective (Thm. 2.4.2). Thus we can apply Algorithm 16.2.34 to enlarge $\mathcal{M}$ to an invertible matrix $\mathcal{K}$:

$$\mathcal{K} = \begin{bmatrix} M_1 & M_2 & \cdots & M_m & K_{m+1} & \cdots & K_n \end{bmatrix} .$$

Now let

$$\mathcal{C} := \mathcal{B}\mathcal{K} \ .$$

We claim that this $\mathcal{C}$ has the required properties.

First of all, $\mathcal{C}$ is a composition of an injection and a bijection, and so is injective (Exc. 2.4.1). The range of $\mathcal{C}$ equals the range of $\mathcal{B}$, because $\mathcal{K}$ is surjective (Exc. 2.3.10). Finally

$$\begin{aligned} \mathcal{C} &= \mathcal{B} \circ \begin{bmatrix} M_1 & M_2 & \cdots & M_m & K_{m+1} & \cdots & K_n \end{bmatrix} \\ &\overset{\text{Thm. 8.1.7}}{=} \begin{bmatrix} \mathcal{B}\left(M_1\right) & \mathcal{B}\left(M_2\right) & \cdots & \mathcal{B}\left(M_m\right) & \mathcal{B}\left(K_{m+1}\right) & \cdots & \mathcal{B}\left(K_n\right) \end{bmatrix} \\ &= \begin{bmatrix} A_1 & A_2 & \cdots & A_m & \mathcal{B}\left(K_{m+1}\right) & \cdots & \mathcal{B}\left(K_n\right) \end{bmatrix} , \end{aligned}$$

which shows that $\mathcal{C}$ is a widening of $\mathcal{A}$.

19. Rank-Nullity Theorem

Last modified on December 8, 2018

19.1 Rank-Nullity Theorem

Every subspace of $\mathbb{R}^n$ is a range of an injective matrix (TYC 18.3.18). If a subspace $\boldsymbol{W}$ is expressed this way, then the columns of the matrix form a coordinate system of $\boldsymbol{W}$. Let us record this observation.

The dimension of the range of an *injective* $n \times m$ matrix is m.

Theorem 19.1.1

Rank of a matrix equals the dimension of its range.

Proof of Theorem 19.1.1. Since $\mathcal{A}$ and RCEF($\mathcal{A}$) have the same range and the same rank (Exc. 11.2.9 and TYC 16.2.22), it is sufficient to establish the claim for RCEF($\mathcal{A}$).

The claim is clearly true when $\mathcal{A}$ is null. If $\mathcal{A}$ is a non-null matrix, then the rank of RCEF($\mathcal{A}$) is the number of pivot columns it has (TYC 16.2.27).

The pivot columns of RCEF($\mathcal{A}$) form a coordinate system of the range of $\mathcal{A}$ (Exc. 18.3.4), and so their number is the dimension of the range of $\mathcal{A}$. ■

Synopsis 19.1.2 ☞ **Rank**

Let us collect some of the characterizations of matrix rank we have encountered so far.

The following numbers are equal for any non-null matrix $\mathcal{A}$.

1. $\mathit{Rank}(\mathcal{A}) \quad \big($namely the number of 1's in the SPI$(\mathcal{A})\big)$.
2. Rank of any matrix equivalent to $\mathcal{A}$.
3. The number of pivots in the RREF$(\mathcal{A})$.
4. The number of pivots in the RCEF$(\mathcal{A})$.
5. The dimension of the range of $\mathcal{A}$.
6. $\mathit{Rank}\left(\mathcal{A}^{T}\right)$.
7. The dimension of the range of $\mathcal{A}^{T}$.

Lemma 19.1.3

If $\begin{bmatrix}\mathcal{A} & \mathcal{B}\end{bmatrix}$ is injective then

$$\mathit{Range}(\mathcal{A}) \cap \mathit{Range}(\mathcal{B}) = \{\mathbb{0}\} .$$

Proof of Lemma 19.1.3. Suppose that $Z \in \mathit{Range}(\mathcal{A}) \cap \mathit{Range}(\mathcal{B})$. Then

$$\mathcal{A}(X) = Z = \mathcal{B}(Y) ,$$

for some X, Y. Hence

$$\begin{bmatrix}\mathcal{A} & \mathcal{B}\end{bmatrix}\left(\begin{smallmatrix} X \\ -Y \end{smallmatrix}\right) = \mathcal{A}(X) - \mathcal{B}(Y) = Z - Z = \mathbb{0} .$$

The injectivity of $\begin{bmatrix}\mathcal{A} & \mathcal{B}\end{bmatrix}$ entails

$$\left(\begin{smallmatrix} X \\ -Y \end{smallmatrix}\right) = \mathbb{0} ,$$

so that $X = \mathbb{0}$ (and $Y = \mathbb{0}$), from where

$$Z = \mathcal{A}(X) = \mathbb{0} .$$

This shows that $\mathbb{0}$ is the only common element of $\mathit{Range}(\mathcal{A})$ and $\mathit{Range}(\mathcal{B})$. ■

Theorem 19.1.4 ☞ **A basis of the range via extending a basis of the nullspace**

Let $\mathcal{A} \in \mathbb{M}_{n\times m}$ be a *non-injective non-null* matrix, and let $X_1, X_2, \ldots, X_k$ be a coordinate system of the nullspace of $\mathcal{A}$.

Then for ANY enlargement of $X_1, X_2, \ldots, X_k$ to a coordinate system

$$X_1, X_2, \ldots, X_k, Y_{k+1}, Y_{k+2}, \ldots, Y_m \quad \text{of} \quad \mathbb{R}^m,$$

$\mathcal{A}\left(Y_{k+1}\right), \mathcal{A}\left(Y_{k+2}\right), \ldots, \mathcal{A}\left(Y_m\right)$ is a coordinate system of the range of $\mathcal{A}$.

Comment 19.1.5

Note that Exercise 18.3.11 can be considered to be the analogue of Theorem 19.1.4 for the injective matrices.

Proof of Theorem 19.1.4. Let

$$\mathcal{X} := \left[X_1 \quad X_2 \quad \cdots X_k\right] \text{ and } \mathcal{Y} := \left[Y_{k+1} \quad Y_{k+2} \quad \cdots \quad Y_m\right].$$

Then $\mathcal{X}$ and $\mathcal{Y}$ are injective, and $\left[\mathcal{X}\ \mathcal{Y}\right]$ is an invertible matrix. By Lemma 19.1.3,

$$\{\mathbb{O}\} = Range\,(\mathcal{X}) \cap Range\,(\mathcal{Y}) = Nullspace\,(\mathcal{A}) \cap Range\,(\mathcal{Y}) \;. \tag{19.1}$$

We aim to show that

$$\left[\mathcal{A}\left(Y_{k+1}\right) \quad \mathcal{A}\left(Y_{k+2}\right) \quad \cdots \quad \mathcal{A}\left(Y_m\right)\right] \quad (= \mathcal{A}\mathcal{Y})$$

is an injective matrix whose range equals to that of $\mathcal{A}$.

Since $\left[\mathcal{X}\ \mathcal{Y}\right]$ is an invertible matrix, the range of $\mathcal{A} \circ \left[\mathcal{X}\ \mathcal{Y}\right]$ equals that of $\mathcal{A}$ (Thm. 2.4.2). Yet

$$\mathcal{A}[\mathcal{X}\ \mathcal{Y}] = [\mathcal{A}\mathcal{X} \quad \mathcal{A}\mathcal{Y}] = [\mathcal{O} \quad \mathcal{A}\mathcal{Y}] \;.$$

Removing null columns does not alter the range of a matrix (Exc. 14.1.1). Thus

$$Range\,(\mathcal{A}) = Range\,(\mathcal{A}\mathcal{S}) = Range\,(\mathcal{A}\mathcal{Y}) \;.$$

Our proof will be complete as soon as we demonstrate that $\mathcal{A}\mathcal{Y}$ is injective (TYC 18.3.3); i.e. has a trivial nullspace.

If $Z \in Nullspace\,(\mathcal{A}\mathcal{Y})$, then $\mathbb{O} = \mathcal{A}\mathcal{Y}(Z) = \mathcal{A}\Big(\mathcal{Y}(Z)\Big)$. So, $\mathcal{Y}(Z) \in Nullspace\,(\mathcal{A})$, and therefore

$$\mathcal{Y}(Z) \in Nullspace\,(\mathcal{A}) \cap Range\,(\mathcal{Y}) \overset{(19.1)}{=} \{\mathbb{O}\} \;.$$

Since $\mathcal{Y}$ is injective, this means that $Z = \mathbb{O}$. Thus, $\mathbb{O}$ is the only element of the nullspace of $\mathcal{A}\mathcal{Y}$, and the proof is complete. ■

Comment 19.1.6

In time we will discuss a famous cousin of Theorem 19.1.4. This supremely useful result is called a **Singular Value Decomposition**. Here is what it says.

$\Downarrow$

[A peek into the future: for any non-null matrix there is an orthonormal coordinate system of the initial space, the first part of which gets mapped to an orthogonal coordinate system of the range, and the rest (if any) forms an orthonormal coordinate system of the nullspace]

For any $\mathcal{A} \in \mathbb{M}_{n\times m}$ of rank r there exists *orthonormal* coordinate system $X_1, X_2, \ldots, X_m$ of $\mathbb{R}^m$ such that

$$\mathcal{A}\left(X_1\right), \mathcal{A}\left(X_2\right), \ldots, \mathcal{A}\left(X_r\right)$$

is an *orthogonal* coordinate system of the range of $\mathcal{A}$, and (if $m > r$)

$$X_{r+1}, X_{r+2}, \ldots, X_m$$

is an *orthonormal* coordinate system of the nullspace of $\mathcal{A}$.

Terminology 19.1.7

The dimension of the nullspace of a matrix $\mathcal{A}$ is said to be the **nullity of** $\mathcal{A}$.

Theorem 19.1.8 ☞ **Rank-Nullity Formula**

For any $\mathcal{A} \in \mathbb{M}_{n\times m}$,

$$Rank\left(\mathcal{A}_{n\times m}\right) + Nullity\left(\mathcal{A}_{n\times m}\right) = m\ .$$

In other words,

$$dim\left(Nullspace\left(\mathcal{A}\right)\right) \ + \ dim\left(Range\left(\mathcal{A}\right)\right) = dim\left(InitialSpace\left(\mathcal{A}\right)\right)\ .$$

Proof of Theorem 19.1.8. One proof of this theorem makes use of Theorems 18.3.16 and 19.1.4. We leave the details as an exercise for the reader (TYC 19.1.9).

We offer an alternate proof. By TYC 16.4.5, the nullspace of a non-injective $n \times m$ matrix $\mathcal{A}$ can be expressed as the range of an injective $m \times (m - r)$ matrix $\mathcal{M}$, where r is the rank of $\mathcal{A}$. Then the columns of $\mathcal{M}$ form a coordinate system of the nullspace of $\mathcal{A}$ (TYC 18.3.3), and so

$$Nullity(\mathcal{A}) = m - r = m - Rank(\mathcal{A}) \ ,$$

which yields the required formula. ■

Test Your Comprehension 19.1.9

Use Theorems 18.3.16 and 19.1.4 to derive the Rank-Nullity Formula. Don't forget to deal with injective matrices and null matrices.

Test Your Comprehension 19.1.10

Equivalent matrices have the same rank and the same nullity.

Hint: $Rank(\mathcal{A})$ and $Nullity(\mathcal{A})$ can be read off SPI($\mathcal{A}$).

19.2 Range and Nullspace of $\mathcal{A}^T\mathcal{A}$

One consequence of the Rank-Nullity formula is the following remarkable theorem. It highlights an extent to which the square matrix $\mathcal{A}^T\mathcal{A}$ combines the information about $\mathcal{A}$ and $\mathcal{A}^T$. Since $\mathcal{A}^T\mathcal{A}$ is a symmetric matrix (i.e. it equals its transpose) it enjoys especially nice properties.

Theorem 19.2.1

For any matrix $\mathcal{A}$,

$$Nullspace\left(\mathcal{A}^T\mathcal{A}\right) = Nullspace(\mathcal{A})$$

and

$$Range\left(\mathcal{A}^T\mathcal{A}\right) = Range\left(\mathcal{A}^T\right) \ .$$

Proof. The first part of this claim has been established previously (Thm. 12.1.18).

Let us focus on the second equality. If $\mathcal{A} \in \mathbb{M}_{n\times m}$ then $\mathcal{A}^T\mathcal{A} \in \mathbb{M}_{m\times m}$. By Rank-Nullity theorem and the first equality of the present theorem,

$$\begin{aligned} Rank\left(\mathcal{A}^T\mathcal{A}\right) &= m - Nullity\left(\mathcal{A}^T\mathcal{A}\right) \\ &= m - Nullity(\mathcal{A}) \\ &= Rank(\mathcal{A}) \ . \end{aligned}$$

This shows that the range of $\mathcal{A}^T\mathcal{A}$ and the range of $\mathcal{A}^T$ have the same di-

mension. Yet
$$Range\left(\mathcal{A}^T\mathcal{A}\right) \subseteq Range\left(\mathcal{A}^T\right) \ .$$
As we know, strictly bigger subspaces have strictly bigger dimensions (Theorem 18.3.26). Thus we can conclude that these two subspaces of $\mathbb{R}^m$ are in fact equal. ■

Test Your Comprehension 19.2.2

For any matrix $\mathcal{A}$,
$$Nullspace\left(\mathcal{A}\mathcal{A}^T\right) = Nullspace\left(\mathcal{A}^T\right)$$
and
$$Range\left(\mathcal{A}\mathcal{A}^T\right) = Range\left(\mathcal{A}\right) \ .$$

19.3 Ortho-Complements Revisited

Theorem 19.3.1 ☞ **Ortho-complements have complementary dimensions**

For any subspace $\boldsymbol{W}$ of $\mathbb{R}^n$:
$$dim\left(\boldsymbol{W}\right) + dim\left(\boldsymbol{W}^{\perp}\right) = n.$$

Proof of Theorem 19.3.1. There is a matrix $\mathcal{A} \in \mathbb{M}_n$ such that $\boldsymbol{W} = Range\left(\mathcal{A}\right)$ (TYC 18.3.19), and therefore
$$dim\left(\boldsymbol{W}^{\perp}\right) = dim\left(Range\left(\mathcal{A}\right)^{\perp}\right) \overset{\text{TYC 12.1.10}}{=} dim\left(Nullspace\left(\mathcal{A}^T\right)\right)$$
$$\overset{\text{Rank-Nullity}}{=} n - Rank\left(\mathcal{A}^T\right) = n - Rank\left(\mathcal{A}\right) = n - dim\left(\boldsymbol{W}\right) \ . \ ■$$

Theorem 19.3.2

For any *subspace* $\boldsymbol{W}$ of $\mathbb{R}^n$,
$$\left(\boldsymbol{W}^{\perp}\right)^{\perp} = \boldsymbol{W} \ .$$

Proof of Theorem 19.3.2. We shall demonstrate that
$$\boldsymbol{W} \subseteq \left(\boldsymbol{W}^{\perp}\right)^{\perp}, \text{ and that } \ dim\left(\boldsymbol{W}\right) = dim\left(\left(\boldsymbol{W}^{\perp}\right)^{\perp}\right) \ .$$

Together these claims imply the desired equality (Thm. 18.3.26).

The claimed inclusion is a consequence of a brain-teaser-type observation that every element of $\boldsymbol{W}$ is orthogonal to all vectors that are orthogonal to all elements of $\boldsymbol{W}$.

Now for the equality of dimensions:

$$dim\left(\left(\boldsymbol{W}^{\perp}\right)^{\perp}\right) \stackrel{\text{Thm. 19.3.1}}{=} n - dim\left(\boldsymbol{W}^{\perp}\right) \stackrel{\text{Thm. 19.3.1}}{=} n - (n - dim\,(\boldsymbol{W})) = dim\,(\boldsymbol{W})\ .$$

■

Terminology 19.3.3

Theorem 19.3.2 tells us that the subspaces of $\mathbb{R}^n$ come in pairs $\boldsymbol{W}$ and $\boldsymbol{V}$ where

$$\boldsymbol{V} = \boldsymbol{W}^{\perp} \quad \text{and} \quad \text{(consequently)}\ \boldsymbol{W} = \boldsymbol{V}^{\perp}\ .$$

We say that $\boldsymbol{W}$ and $\boldsymbol{V}$ are **ortho-complementary subspaces**, or **ortho-complements** (of each other) for short.

19.4 Transposition And Ranges/Nullspaces

Test Your Comprehension 19.4.1 ☞ **Range and nullspace of the transpose**

Use the fact that

$$Nullspace\left(\mathcal{A}^{T}\right) = \left(Range\,(\mathcal{A})\right)^{\perp}\ ,$$

for any matrix $\mathcal{A}$ (TYC 12.1.10), to deduce that

$$Range\left(\mathcal{A}^{T}\right) = \left(Nullspace\,(\mathcal{A})\right)^{\perp}.$$

Hint: Thm. 19.3.2.

Test Your Comprehension 19.4.2

Verify the following identities for a symmetric matrix $\mathcal{A}$.

$$\left(Range\,(\mathcal{A})\right)^{\perp} = Nullspace\,(\mathcal{A})$$

$$\left(Nullspace\,(\mathcal{A})\right)^{\perp} = Range\,(\mathcal{A})\ .$$

19.5 Nullspace Equality Theorems

As it seems to be often the case (and this will become less of a mystery as the reader progresses through the book), there are nullspace analogues of the theorems dealing with range equality presented in the last subsection.

Theorem 19.5.1 ☞ **Nullspace Equality For Matrices Of The Same Size**

When matrices $\mathcal{A}$ and $\mathcal{B}$ have the same size, the following are equivalent.

1. $\mathit{Nullspace}\,(\mathcal{A}) = \mathit{Nullspace}\,(\mathcal{B})$.
2. $\mathcal{A} \overset{\mathsf{L}}{\equiv} \mathcal{B}$ (i.e. $\mathcal{A}$ and $\mathcal{B}$ are left-equivalent).
3. $\mathcal{A}$ can be turned into $\mathcal{B}$ (and vice versa) through an application of a sequence of elementary row operations.
4. $\mathsf{RREF}(\mathcal{A}) = \mathsf{RREF}(\mathcal{B})$.

Proof of Theorem 19.5.1. The equivalence of the last three claims has been established in Theorems 11.4.3 and 16.2.9.

The implication 2. $\Longrightarrow$ 1. is the subject of TYC 12.1.16. We will complete the proof by establishing the implication 1. $\Longrightarrow$ 2. To this end, suppose that $\mathit{Nullspace}\,(\mathcal{A}) = \mathit{Nullspace}\,(\mathcal{B})$. Then (TYC 19.4.1)

$$\mathit{Range}\left(\mathcal{A}^{T}\right) = \mathit{Range}\left(\mathcal{B}^{T}\right) ,$$

and therefore

$$\mathcal{A}^{T} \overset{\mathsf{R}}{\equiv} \mathcal{B}^{T} ,$$

by Theorem 16.3.2. Since transposition switches one-sided equivalences (TYC 8.2.12),

$$\mathcal{A} \overset{\mathsf{L}}{\equiv} \mathcal{B} ,$$

and the proof is complete. ∎

Exercise 19.5.2 ☞ **Nullspace Equality For Matrices Of Different Size**

Hint: Emulate the proof of Cor. 16.3.5.

Given matrices $\mathcal{A} \in \mathbb{M}_{21\times m}$ and $\mathcal{B} \in \mathbb{M}_{328\times m}$, the following are equivalent.

1. $\mathit{Nullspace}\,(\mathcal{A}) = \mathit{Nullspace}\,(\mathcal{B})$.
2. $\mathcal{B} = \mathcal{G}\,\mathcal{A}$, for some *injective* $\mathcal{G} \in \mathbb{M}_{328\times 21}$.
3. $\mathsf{RREF}\left(\left[\begin{smallmatrix}\mathcal{A}\\ \mathcal{O}\end{smallmatrix}\right]_{(21|307)\times m}\right) = \mathsf{RREF}(\mathcal{B})$. *

*Note that $\left[\begin{smallmatrix}\mathcal{A}\\ \mathcal{O}\end{smallmatrix}\right]_{(21|307)\times m}$ is created by inserting enough null rows into $\mathcal{A}$ to produce a matrix of the same size as $\mathcal{B}$.

Exercise 19.5.3

Which of the following matrices have equal nullspaces?

$$\begin{bmatrix} 37 & -42 & -554 & -189 & -225 \\ 265 & -201 & -476 & -285 & -133 \\ 359 & -312 & -418 & -354 & -125 \\ -206 & 169 & 106 & 203 & -22 \\ -64 & -41 & 284 & 100 & -22 \\ -274 & 198 & 602 & 318 & 172 \end{bmatrix}, \quad \begin{bmatrix} 1 & 0 & 4 & 9 & -3 \\ 4 & -7 & -8 & -2 & -10 \\ 6 & 4 & -6 & 0 & 8 \\ 2 & -2 & 8 & -9 & 10 \\ 50 & -25 & -40 & -37 & 12 \\ 10 & -19 & 46 & -2 & 10 \\ -17 & 27 & 82 & 37 & 47 \end{bmatrix},$$

$$\begin{bmatrix} -8 & -22 & 23 & -10 & 14 & -4 \\ -23 & -1 & -5 & -14 & 21 & -15 \\ 2 & 24 & -8 & -10 & 2 & -6 \\ 10 & 3 & 21 & 13 & 13 & 11 \\ 11 & 1 & 13 & -16 & 18 & 11 \\ 18 & -7 & 0 & -10 & -13 & 8 \end{bmatrix}, \quad \begin{bmatrix} 33 & 17 & 6 & -70 & 109 \\ 26 & 31 & 26 & -57 & 126 \\ -149 & -139 & -143 & 271 & -622 \\ 1 & 24 & 70 & -1 & 79 \\ 26 & -3 & -58 & 39 & -42 \end{bmatrix}.$$

Test Your Comprehension 19.5.4

Given the set up of Exercise 19.5.2, explain why it can NEVER happen that there is an injective $\mathcal{G}$ such that $\mathcal{A} = \mathcal{G}\mathcal{B}$.

Hint: What would be the size of such a $\mathcal{G}$?

Comment 19.5.5

Just as in the case of the equality of ranges, we now have an algorithmic way to discern the equality of nullspaces via an algorithm for finding the RREF of a matrix.

19.6 Coordinate Systems of Ranges

Suppose that $\boldsymbol{W}$ is expressed as a range of a non-injective matrix $\mathcal{A}$. Then by deleting some columns of $\mathcal{A}$ we can arrive at an injective matrix $\mathcal{B}$ with the range equal to $\boldsymbol{W}$ (Thm. 14.1.4 and TYC 18.3.22). The columns of $\mathcal{B}$ form a coordinate system of $\boldsymbol{W}$.

How do we actually select the columns of $\mathcal{A}$ to be deleted? Let us present an algorithm for identifying the columns of $\mathcal{A}$ that should NOT be deleted. These columns form a coordinate system of the range of $\mathcal{A}$.

Theorem 19.6.1 ☞ **Pivots in RREF($\mathcal{A}$) point to a coordinate system of the range of $\mathcal{A}$**

Suppose that the pivots in RREF($\mathcal{A}$) occur in the $j_1, j_2, \ldots, j_k$-th columns.

Then the $j_1, j_2, \ldots, j_k$-th columns of $\mathcal{A}$ form a coordinate system of the range of $\mathcal{A}$.

Proof of Theorem 19.6.1. Let us write

$$\mathcal{A} = \begin{bmatrix} C_1 & C_2 & \dots & C_m \end{bmatrix} \text{ and } \operatorname{RREF}(\mathcal{A}) = \begin{bmatrix} Z_1 & Z_2 & \dots & Z_m \end{bmatrix}.$$

$\mathcal{A} = \mathcal{S} \circ \operatorname{RREF}(\mathcal{A})$, for some invertible matrix $\mathcal{S}$ (Cor. 16.2.4). For such an $\mathcal{S}$ we have

$$C_j = \mathcal{S}(Z_j), \text{ for all } j.$$

Since $Z_{j_1}, Z_{j_2}, \dots Z_{j_k}$ are the pivot columns of $\operatorname{RREF}(\mathcal{A})$, they are exactly the standard basis tuples

$$E_1, \dots, E_k,$$

and so form a linearly independent list. An application of an invertible matrix to a linearly independent list produces another such list (Exc. 18.1.10). Thus $C_{j_1}, C_{j_2}, \dots C_{j_k}$ is a linearly independent list of columns of $\mathcal{A}$, and so is a linearly independent list of tuples in the range of $\mathcal{A}$.

Therefore, the list $C_{j_1}, C_{j_2}, \dots C_{j_k}$ can be extended to a coordinate system of the range of $\mathcal{A}$ (Thm. 18.3.16).

Such a coordinate system has $Rank(\mathcal{A})$ tuples in it (Thm. 19.1.1). Yet $Rank(\mathcal{A})$ is the number of pivots in $\operatorname{RREF}(\mathcal{A})$ (Thm. 16.2.26), which is k.

This means that no proper extension were possible, and the list $C_{j_1}, C_{j_2}, \dots C_{j_k}$ is already a coordinate system of the range of $\mathcal{A}$. ■

Exercise 19.6.2

Let

$$\mathcal{A} = \begin{bmatrix} -1 & 3 & 3 & 3 & 3 \\ -5 & 15 & 15 & 15 & 15 \\ 2 & -6 & -7 & -10 & -8 \\ -3 & 9 & 8 & 5 & 7 \\ -5 & 17 & 13 & -2 & 8 \\ 1 & -7 & -6 & 3 & -3 \\ 1 & 5 & 0 & -14 & -4 \end{bmatrix}.$$

By removing some of the columns of $\mathcal{A}$ arrive at an injective matrix that has the same range as $\mathcal{A}$, and hence construct a coordinate system for the range of $\mathcal{A}$ made up of some columns of $\mathcal{A}$.

Since we know that all nullspaces are ranges (Section 16.4), we can adapt the methodology for finding coordinate systems of ranges to find coordinate systems of nullspaces as well.

Exercise 19.6.3

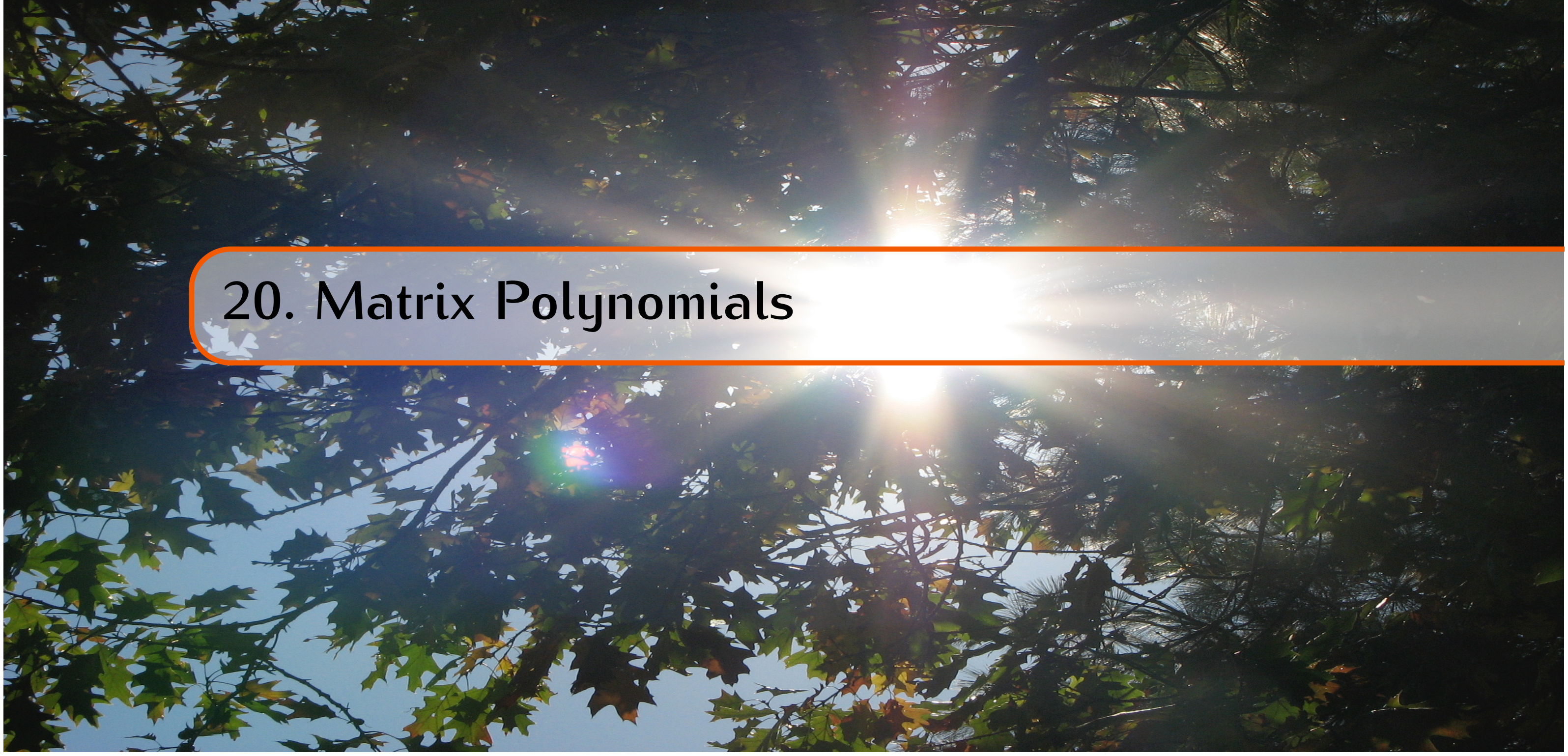
Hint: Start with Algorithm 16.4.4.

What is the dimension of the nullspace of the given matrix $\mathcal{A}$? Find a coordinate system of the nullspace of $\mathcal{A}$.

$$\mathcal{A} = \begin{bmatrix} -1 & 3 & 3 & 3 & 3 \\ -5 & 15 & 15 & 15 & 15 \\ 2 & -6 & -7 & -10 & -8 \\ -3 & 9 & 8 & 5 & 7 \\ -5 & 17 & 13 & -2 & 8 \\ 1 & -7 & -6 & 3 & -3 \\ 1 & 5 & 0 & -14 & -4 \end{bmatrix}.$$

VII

Matrices And Polynomials



20. Matrix Polynomials

Last modified on December 8, 2018

20.1 A Brief Review of Polynomial Algebra

Terminology 20.1.1

Polynomial functions on $\mathbb{R}$ are those expressible in the form

$$p(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_k x^k \ , \tag{20.1}$$

for some real numbers a_i and some non-negative integer k.

The polynomial function $p(x) := 0$ is said to be **the (constantly) zero polynomial**. The polynomial function $p(x) := 1$ is said to be **the (constantly) 1 polynomial**. The polynomial function $p(x) := x$ is said to be **the identity polynomial**.

We say that a polynomial is **non-zero** when it is not constantly zero.

The roots of a polynomial are the inputs that produce the zero output.

Notation 20.1.2

The reader is certainly familiar with the operations of addition, subtraction and multiplication for polynomials.

We shall denote the product of two unspecified polynomials p and q by $p \cdot q$, but may also write $p\,q$. For example, we shall usually write $3p$ for the product $3 \cdot p$, and refer to this polynomial as **a scalar multiple of the polynomial** p.

Fact 20.1.3 ☞ **Uniqueness of representation for polynomial functions**

A non-zero polynomial function can be expressed in exactly one way as $c_0 + c_1 x + c_2 x^2 + \cdots + c_n x^n$, with a non-zero c_n.*

* In this case, c_n is said to the **leading coefficient** of the polynomial, and n is the **degree** of the polynomial. We write $\deg p$ for the degree of p. A polynomial is **monic** if its leading coefficient is 1.

The zero polynomial has no degree and has no leading coefficient. It is certainly not monic.

Test Your Comprehension 20.1.4

Every non-zero polynomial can be expressed as a non-zero scalar multiple of a monic polynomial in exactly one way.

Test Your Comprehension 20.1.5 ☞ **Multiplication and degrees**

For any non-zero polynomials p, q, s,

1. $\deg(p \cdot q) = \deg p + \deg q$;
2. $\deg(p \cdot q \cdot s) = \deg p + \deg q + \deg s$;

Similar results hold for products of any number of non-zero polynomials.

What happens if we do not insist that all of the polynomials are non-zero?

Test Your Comprehension 20.1.6

A polynomial $a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n$ cannot be expressed as a product of more than n non-constant polynomials.

20.1.1 — Polynomial Division

Terminology 20.1.7 ☞ **Polynomial divisors/multiples**

We say that polynomial f **divides** polynomial g, if g can be expressed as a **polynomial multiple** of f; i.e. if there is a polynomial q such that

$$g = q \cdot f \ .$$

In this case we pronounce that f is a **polynomial divisor** of g. If additionally f is neither a constant polynomial nor a scalar multiple of g, we say that f is a **proper non-trivial polynomial divisor** of g.

Test Your Comprehension 20.1.8

1. A non-zero constant polynomial divides every polynomial.
2. A non-zero scalar multiple of a polynomial p is a polynomial divisor of p.
3. Every polynomial divides the zero polynomial.

Test Your Comprehension 20.1.9 ☞ **Divisibility and degrees**

If polynomial f divides polynomial g and the latter is not the zero polynomial, then

$$\deg f \leq \deg g \ .$$

Test Your Comprehension 20.1.10

Give an example of two polynomials f and g satisfying $\deg f \leq \deg g$, but such that f does NOT divide g.

Theorem 20.1.11 ☞ **Mutual divisibility for monics**

If monic polynomials p_1 and p_2 divide each other, then they are equal.

Proof of Theorem 20.1.11. Since p_1 and p_2 divide each other, neither can have a higher degree than the other. We can write

$$p_1 = q \cdot p_2 \ ,$$

for some monic polynomial q. Since

$$deg\left(q \cdot p_2\right) = deg\,(q) + deg\left(p_2\right) = deg\,(q) + deg\left(p_1\right) \ ,$$

it must be that the degree of q is zero, and so q, being monic, is a constantly 1 polynomial. Hence $p_1 = p_2$. ■

Test Your Comprehension 20.1.12 ☞ **Mutual divisibility**

Two polynomials f and g divide each other exactly when one of them is a non-zero scalar multiple of the other.

Hint: TYC20.1.4.

Fact 20.1.13 ☞ **Division with a remainder.**

Any monic polynomial can be divided by any other monic polynomial, with remainder.

In other words, given any two monic polynomials f and g, one can express f as a monic polynomial multiple of g plus a polynomial remainder.

More precisely, given any two monic polynomials f and g, there exist polynomials q and r such that

1. $f = q \cdot g + r$;
2. q is the zero polynomial or is a monic polynomial;
3. r is the zero polynomial or is a monic polynomial whose degree is strictly less than that of g.

Furthermore, such q and r are unique.

Mathematica command **PolynomialQuotientRemainder**[ ] can be used for finding polynomials q and r.

Theorem 20.1.14 ☞ **Roots and linear factors**

The following claims are equivalent for a non-zero polynomial p.

1. α is a root of p; i.e. $p(\alpha) = 0$.
2. Polynomial $x - \alpha$ divides p.

Proof of Theorem 20.1.14.

[2. $\Longrightarrow$ 1.] : If p is a polynomial multiple of $x - \alpha$, then we can write

$$p(x) = (x - \alpha) \cdot q(x) ,$$

for some polynomial q, and therefore

$$p(\alpha) = (\alpha - \alpha) \cdot q(\alpha) = 0 .$$

[1. $\Longrightarrow$ 2.] : We can write p as a non-zero scalar multiple of a monic polynomial p_o (TYC 20.1.4): say

$$p = c \cdot p_o .$$

Dividing p_o by $x - \alpha$ with a remainder (Fact 20.1.13) we can write

$$p_o(x) = q(x) \cdot (x - \alpha) + r(x) ,$$

where r is a constant polynomial. Hence

$$0 = p(\alpha) = c \cdot p_o(\alpha) = c \cdot q(\alpha) \cdot (\alpha - \alpha) + c \cdot r(\alpha) = c \cdot r(\alpha)\ .$$

Since $c \neq 0$, we have $r(\alpha) = 0$, and so r, being a constant polynomial, is the zero polynomial. Thus

$$p(x) = c \cdot p_o(x) = c \cdot q(x) \cdot (x - \alpha)\ ,$$

which shows that $(x - \alpha)$ divides p. ■

Fact 20.1.15 ☞ **Distinct roots**

Theorem 20.1.14 can be generalized. The following are equivalent for a non-zero polynomial p.

1. $\alpha_1, \alpha_2, \ldots, \alpha_k$ are some distinct roots of p.
2. $\left(x - \alpha_1\right) \cdot \left(x - \alpha_2\right) \cdots \left(x - \alpha_k\right)$ divides p.

Test Your Comprehension 20.1.16 ☞ **Maximum number of roots**

A non-zero polynomial of degree n cannot have more than n distinct roots.

Hint: TYC's 20.1.6 and 20.1.14 can be helpful here.

Observation 20.1.17 ☞ **Rootless quadratics**

Any monic quadratic polynomial $p(x) = x^2 + bx + c$ can be rewritten as $p(x) = (x + \frac{b}{2})^2 + \left(c - \frac{b^2}{4}\right)$, by "completing the square".

Thus such a p has no real roots exactly when $c - \frac{b^2}{4} > 0$. This can also be seen through the use of the quadratic formula.

It follows that

rootless monic quadratic polynomials p are exactly those that can be expressed as $p(x) = (x - \beta)^2 + \gamma^2$, with $\gamma \neq 0$.

20.1.2 — Prime Polynomials And The Fundamental Theorem Of Algebra

Terminology 20.1.18 ☞ **Prime polynomials**

A *non-constant monic* polynomial that has no non-trivial proper polynomial divisors is said to be **prime**.

Test Your Comprehension 20.1.19 ☞ **Non-primeness**

A polynomial is NOT prime if and only if it can be expressed as a product of two or more non-constant polynomials.

Exercise 20.1.20 ☞ **Prime polynomials of degrees 1 and 2**

1. Every monic polynomial of degree 1 is prime.

2. A monic quadratic polynomial is prime exactly when it has no real roots.*

*By Obs. 20.1.17 this happens exactly when the quadratic can be expressed as a non-zero scalar multiple of

$$(x-\beta)^2+\gamma^2\ ,$$

where $\gamma \neq 0$.

The Fundamental Theorem of Algebra, proved by Carl Friedrich Gauss (1777-1855) in his Ph.D. Thesis (1799), is one of the pillars of modern mathematics. Proved originally for the field of Complex numbers, it is presented here in its Real number form.

One consequence of the theorem is that in the Real setting the prime monic polynomials only come with small degrees and are of just two "flavors" (listed in Exc. 20.1.20):

$$x-\alpha \quad \text{and} \quad (x-\beta)^2+\gamma^2\ ,$$

where $\gamma \neq 0$.

Fact 20.1.21 ☞ **The (Real) Fundamental Theorem of Algebra**

1. The only prime polynomials are the monic polynomials of degree 1, and the monic polynomials of degree 2 with no Real roots.

2. Every non-constant monic polynomial can be expressed in exactly one way (apart from a reordering of the factors) as a product of prime polynomials*.

As usual "some" includes a possibility of "none". Also, we have NOT excluded a possibility that some factors may be repeated.

*i.e. as a product of some number of polynomials of the form $(x-r)$, (these r's are the roots of p), and some number of polynomials of the form $(x-\beta)^2+\gamma^2$, with $\gamma \neq 0$.

Terminology 20.1.22

The factorization described by the (Real) Fundamental Theorem of Algebra is said to be **the prime factorization of a (monic) polynomial**. In it, the degree 1 factors are said to be the **prime linear factors**, and the degree 2 factors are said to be the **prime quadratic factors**.

The prime linear factors correspond to the real roots of p, as per TYC 20.1.14.

A prime factor may be repeated a number of times within the prime factorization of a polynomial, in which case it is called **a repeated prime factor**, and the number of times it is repeated is its **multiplicity**.

For example, $z - \pi$ is a prime factor of multiplicity 3 for the polynomial

$$(z^2 + 25)(z - \pi)(z + 3)^4 \left((z - 2)^2 + 1\right)^2 (z - \pi)^2 (z + 3) .$$

Corollary 20.1.23

Every monic polynomial of an *odd* degree has a Real root.

Proof of Corollary 20.1.23. This is an immediate consequence of the (Real) Fundamental Theorem of Algebra, since a monic polynomial of an odd degree cannot be expressed as a product of monic polynomials of degree 2. ■

Theorem 20.1.24 ☞ **Divisibility criterion for monics**

A monic polynomial q divides a monic polynomial p exactly when both of the following conditions hold.

1. All of the prime factors of q are also prime factors of p.
2. The multiplicity of each prime factor in q does not exceed the multiplicity of it in p.

Proof of Theorem 20.1.24. We establish the forward implication and leave the verification of the converse implication as a TYC 20.1.25. The forward implication is trivially true whenever $q = 1$ or $q = p$. Let us assume henceforth that q is a proper non-trivial divisor of p. Then $p = q \cdot h$, for some non-constant monic polynomial h. Combining the prime factorizations of q and h, we obtain a representation of p as a product of prime polynomials. Since such a representation of p is unique by the (Real) Fundamental Theorem of Algebra, this must be the prime factorization of p, and the desired conclusion clearly follows. ■

Test Your Comprehension 20.1.25

Finish the proof of Theorem 20.1.24.

Test Your Comprehension 20.1.26

The only monic prime divisors of a monic polynomial p are its prime factors.

20.2 Introducing Matrix Polynomials

Terminology 20.2.1

As usual, we write $\mathcal{A}^n$ for the product $\mathcal{A}\,\mathcal{A}\cdots\mathcal{A}$ of a *square* matrix $\mathcal{A}$ with itself n times. Let us also agree that $\mathcal{A}^0 := \mathcal{I}$.

Given a polynomial $p(z) = \alpha_0 + \alpha_1 z + \alpha_2 z^2 + \alpha_3 z^3 + \cdots + \alpha_k z^k$, we define

$$p(\mathcal{A}) := \alpha_0 \mathcal{I} + \alpha_1 A + \alpha_2 A^2 + \alpha_3 A^3 + \cdots + \alpha_k A^k ,$$

and we say that $p(\mathcal{A})$ is **a polynomial in** $\mathcal{A}$.

Example 20.2.2

If $p(x) = 2 - 3x + 5x^2$, and $\mathcal{A} = \left[\begin{smallmatrix} -2 & 3 \\ 6 & 0 \end{smallmatrix}\right]$ then

$$p(\mathcal{A}) = 2\left[\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right] - 3\left[\begin{smallmatrix} -2 & 3 \\ 6 & 0 \end{smallmatrix}\right] + 5\left[\begin{smallmatrix} -2 & 3 \\ 6 & 0 \end{smallmatrix}\right]^2$$

$$= \left[\begin{smallmatrix} 2 & 0 \\ 0 & 2 \end{smallmatrix}\right] - \left[\begin{smallmatrix} -6 & 9 \\ 18 & 0 \end{smallmatrix}\right] + \left[\begin{smallmatrix} 110 & -30 \\ -60 & 90 \end{smallmatrix}\right] = \cdots$$

Test Your Comprehension 20.2.3

For any polynomial p,

$$p(\alpha \cdot \mathcal{I}) = p(\alpha) \cdot \mathcal{I}$$

Exercise 20.2.4

$$p\left(\mathcal{A}^T\right) = \left(p(\mathcal{A})\right)^T .$$

Test Your Comprehension 20.2.5 ☞ **Polynomials of block-diagonal matrices**

If $\mathcal{A}$, $\mathcal{B}$ and $\mathcal{C}$ are square matrices, then

$$p\left(\mathcal{A} \boxplus \mathcal{B} \boxplus \mathcal{C}\right) = p\left(\mathcal{A}\right) \boxplus p\left(\mathcal{B}\right) \boxplus p\left(\mathcal{C}\right) \ ,$$

for any polynomial p.

(This is true more generally, for direct sums of any number of square matrices, and for diagonal matrices as a consequence.)

Hint: TYC 9.2.5.

Exercise 20.2.6

Suppose that $\mathcal{B}$ is a *block-upper-triangular* matrix

$$\begin{bmatrix} \mathcal{A}_1 & \square & \dots & \square \\ \mathcal{O} & \mathcal{A}_2 & \dots & \square \\ \vdots & \vdots & \ddots & \vdots \\ \mathcal{O} & \mathcal{O} & \dots & \mathcal{A}_n \end{bmatrix} .$$

1. Argue that

$$\mathcal{B}^k = \begin{bmatrix} (\mathcal{A}_1)^k & \triangle & \dots & \triangle \\ \mathcal{O} & (\mathcal{A}_2)^k & \dots & \triangle \\ \vdots & \vdots & \ddots & \vdots \\ \mathcal{O} & \mathcal{O} & \dots & (\mathcal{A}_n)^k \end{bmatrix} .$$

2. Argue that for any polynomial p,

$$p(\mathcal{A}) = \begin{bmatrix} p(\mathcal{A}_1) & \star & \dots & \star \\ \mathcal{O} & p(\mathcal{A}_2) & \dots & \star \\ \vdots & \vdots & \ddots & \vdots \\ \mathcal{O} & \mathcal{O} & \dots & p(\mathcal{A}_n) \end{bmatrix} .$$

Test Your Comprehension 20.2.7

The analogue of the result Exercise 20.2.6 holds for block-lower-triangular matrices. In particular, it holds for the triangular matrices.

Hint: Exc 20.2.4.

Test Your Comprehension 20.2.8

If p and q are polynomials and $\mathcal{A}$ is a square matrix, then

1. $\big(p \cdot q\big)(\mathcal{A}) = p(\mathcal{A}) \circ q(\mathcal{A}) = q(\mathcal{A}) \circ p(\mathcal{A})$;
2. $\mathcal{A}$ commutes with $p(\mathcal{A})$;
3. $\big(5 \cdot p + 3 \cdot q\big)(\mathcal{A}) = 5p(\mathcal{A}) + 3q(\mathcal{A})$.

Hint: See Exc. 8.2.19, and note that $\mathcal{S}^{-1}\mathcal{P}\mathcal{S} + \mathcal{S}^{-1}\mathcal{Q}\mathcal{S} = \mathcal{S}^{-1}(\mathcal{P}\mathcal{S} + \mathcal{Q}\mathcal{S}) = \mathcal{S}^{-1}(\mathcal{P} + \mathcal{Q})\,\mathcal{S}$.

Exercise 20.2.9

Suppose that $\mathcal{S}$ is an invertible matrix, and $\mathcal{B} = \mathcal{S}^{-1}\mathcal{A}\mathcal{S}$. Argue that for any polynomial p,

$$p(\mathcal{B}) = \mathcal{S}^{-1} p(\mathcal{A})\, \mathcal{S}\ .$$

20.3 Annihilating Polynomials

This does NOT mean that a matrix is a root of p. Roots of p are numbers.

Terminology 20.3.1

We say that a **polynomial** p **annihilates a matrix** $\mathcal{A}$ if $p(\mathcal{A}) = \mathcal{O}$. In such a case we call p **an annihilating polynomial** for $\mathcal{A}$.

Example 20.3.2

1. The constantly zero annihilates every square matrix.
2. The constantly 3 polynomial does not annihilate any matrix.
3. Polynomial p defined by $p(x) = x$ annihilates only null matrices.
4. Polynomial p defined by $p(x) = x^2$ annihilates $\begin{bmatrix} 1 & 1 \\ -1 & -1 \end{bmatrix}$, $\begin{bmatrix} 0&0&0&0 \\ 1&0&0&0 \\ 0&0&0&1 \\ 0&0&0&0 \end{bmatrix}$, and many other matrices, including any matrix that has a partitioning of the form $\begin{bmatrix} \mathcal{O} & \mathcal{B} \\ \mathcal{O} & \mathcal{O} \end{bmatrix}_{(k|m)\times(k|m)}$.

Test Your Comprehension 20.3.3

Polynomial $p(x) = x - 5$ annihilates exactly the matrices $5\mathcal{I}_n$.

Thus, the only scalar multiples of an identity can be annihilated by degree 1 monic polynomial.

Exercise 20.3.4

Monic polynomial $p(x) = (x - a)(x - d) - bc$ annihilates $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$.

Test Your Comprehension 20.3.5

1. If p is a polynomial that annihilates $\mathcal{A}$, then so does every polynomial multiple of p.

2. If p and q are polynomials that annihilate $\mathcal{A}$, then so does every linear combination of p and q.

Terminology 20.3.6

Recall that when a square matrix $\mathcal{A}$ raised to some power produces a null matrix, we say that $\mathcal{A}$ is **nilpotent**. Nilpotent matrices are exactly the matrices annihilated by a polynomial of the form $p(x) = x^n$.

A square matrix is **idempotent** if it squares to itself. Idempotent matrices are exactly the matrices annihilated by the polynomial $p(x) = x^2 - x$.

A square matrix that squares to identity is said to be an **involution** matrix. Involution matrices are exactly the matrices annihilated by the polynomial $p(x) = x^2 - 1$.

Test Your Comprehension 20.3.7

Polynomial p annihilates a null matrix exactly when $p(0) = 0$.

Theorem 20.3.8 ☞ **Existence of annihilating polynomials**

For any $\mathcal{A} \in \mathbb{M}_n$ there exists a monic polynomial of degree at most n^2 that annihilates $\mathcal{A}$.

In other words, for some $k \in \{1, 2, \ldots, n^2\}$, $\mathcal{A}^k$ is a linear combination of the smaller non-negative powers of $\mathcal{A}$.

Comment 20.3.9

Before too long we shall demonstrate that we can replace n^2 with n in Theorem 20.3.8.

Proof of Theorem 20.3.8.

Synopsis of the proof: We will use the operation of matrix tupling developed in section 8.3.1 to convert the powers of $\mathcal{A}$ into n^2-tuples, and then appeal to the fact that $n^2 + 1$ tuples in R^{n^2} cannot be linearly independent.

A list of more than m tuples in $\mathbb{R}^m$ cannot be linearly independent (TYC 18.1.7). Hence either the first tuple on the list is null, or one of the tuples is a linear combination of the preceding tuples (Synopsis 14.4.6).

If $\mathcal{A} \in \mathbb{M}_n$ then

$$\mathfrak{C}(\mathcal{I}), \mathfrak{C}(\mathcal{A}), \mathfrak{C}\left(\mathcal{A}^2\right), \mathfrak{C}\left(\mathcal{A}^3\right), \ldots, \mathfrak{C}\left(\mathcal{A}^{n^2}\right)$$

is a list of n^2+1 tuples in R^{n^2}; (don't forget to count starting at zero, thinking of $\mathcal{I}$ as $\mathcal{A}^0$). Therefore this list is linearly dependent. Since $\mathfrak{C}(\mathcal{I})$ is not null, one of the tuples on the list (let us say the k-th one) is a linear combination of the previous tuples on the list:

$$\mathfrak{C}\left(\mathcal{A}^k\right) = \alpha_0\mathfrak{C}(\mathcal{I}) + \alpha_1\mathfrak{C}(\mathcal{A}) + \alpha_2\mathfrak{C}\left(\mathcal{A}^2\right) + \cdots + \alpha_{k-1}\mathfrak{C}\left(\mathcal{A}^{k-1}\right)$$

$$= \mathfrak{C}\left(\alpha_0\mathcal{I} + \alpha_1\mathcal{A} + \alpha_2\mathcal{A}^2 + \cdots + \alpha_{k-1}\mathcal{A}^{k-1}\right) .$$

Returning to matrix form, we have

$$\mathcal{A}^k = \alpha_0\mathcal{I} + \alpha_1\mathcal{A} + \alpha_2\mathcal{A}^2 + \cdots + \alpha_{k-1}\mathcal{A}^{k-1} , \quad \text{(TYC 8.3.10)},$$

or equivalently

$$-\alpha_0\mathcal{I} - \alpha_1\mathcal{A} - \alpha_2\mathcal{A}^2 - \cdots - \alpha_{k-1}\mathcal{A}^{k-1} + 1\mathcal{A}^k = \mathcal{O} .$$

■

The **free term** of a polynomial p is $p(0)$.

Theorem 20.3.10 ☞ **Free terms of annihilating polynomials**

If a square matrix $\mathcal{A}$ is annihilated by a non-constant polynomial with a non-zero free term, then $\mathcal{A}$ is invertible.

Proof of Theorem 20.3.10. A non-constant polynomial p with a non-zero free term can be expressed as $p(x) = x \cdot q(x) + a$, where $a \neq 0$, and q is a polynomial. If $\mathcal{A}$ is annihilated by such a p, we can use TYC 20.2.8 to conclude that

$$\mathcal{O} = \mathcal{A} \circ q(\mathcal{A}) + a \cdot \mathcal{I} .$$

Hence

$$\mathcal{A} \circ q(\mathcal{A}) = -a \cdot \mathcal{I} = \text{a bijection} .$$

Therefore $\mathcal{A}$ must be surjective, and being square, is invertible. ■

In other words, either

$$\mathcal{A} - \lambda\mathcal{I}$$

is non-jective for some λ, or

$$(\mathcal{A} - \beta\mathcal{I})^2 + \gamma^2\mathcal{I}$$

is non-jective for some β and some $\gamma \neq 0$. Please keep in mind that "either-or" is inclusive, i.e. it includes the possibility of both clauses holding true.

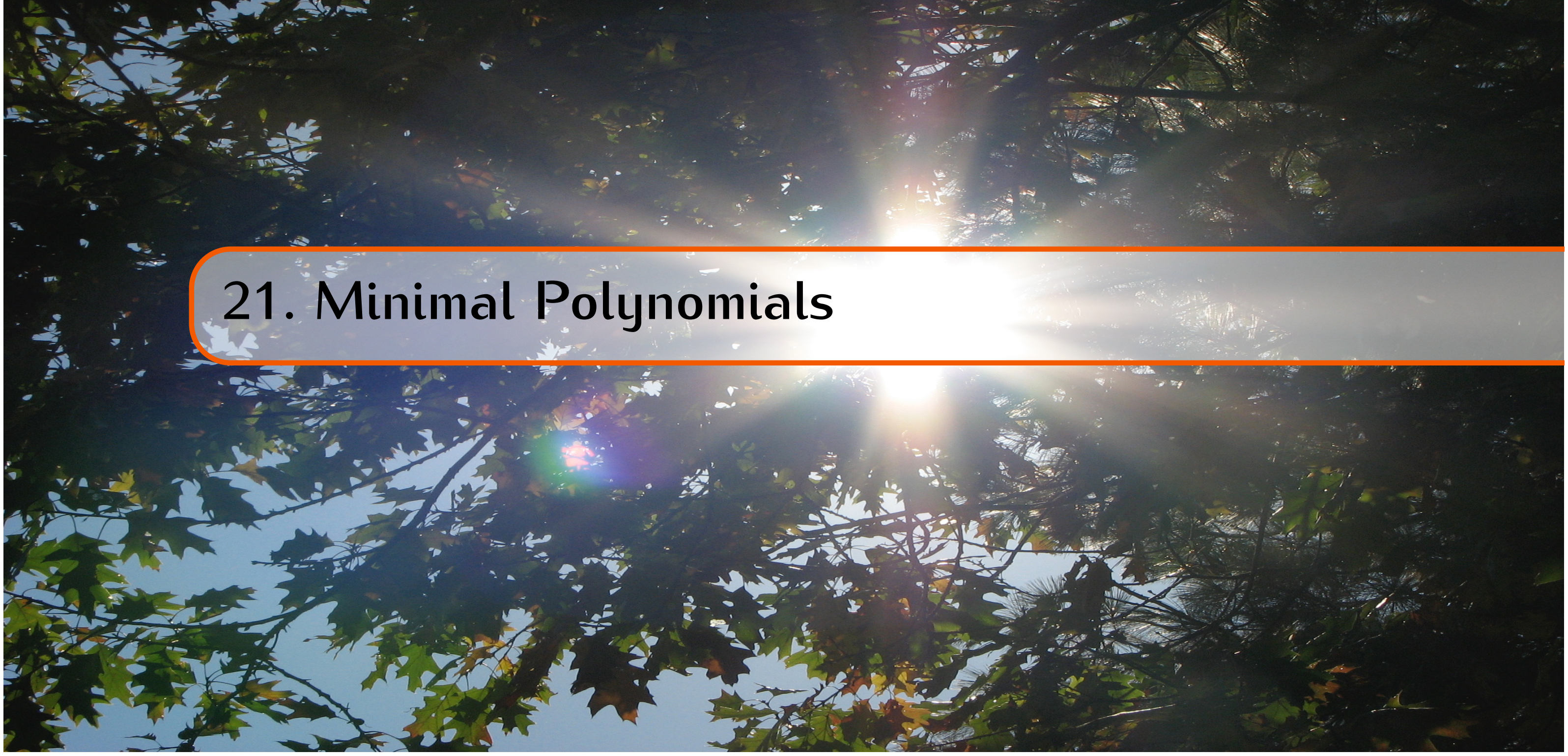
Theorem 20.3.11

For every square matrix $\mathcal{A}$ there is a prime polynomial p such that $p(\mathcal{A})$ is non-jective (i.e. is not invertible).

Proof of Theorem 20.3.11. By Theorem 20.3.8, there is a non-constant monic polynomial q that annihilates $\mathcal{A}$. By the (Real) Fundamental Theorem of

Algebra, q is a product of prime polynomials p_i.

Since $\mathcal{O} = q(\mathcal{A})$, $\mathcal{O}$ is composition of matrices $p_i(\mathcal{A})$ (TYC 20.2.8). Yet $\mathcal{O}$ is not a bijection, and so at least one $p_i(\mathcal{A})$ is not bijective. For square matrices non-jectivity is equivalent to the lack of bijectivity. ■



21. Minimal Polynomials

Last modified on December 8, 2018

21.1 Minimal (Annihilating) Polynomials

Terminology 21.1.1

Given a square matrix $\mathcal{A}$ let us consider the collection $\mathbb{P}_{\mathcal{A}}$ of all polynomials that annihilate $\mathcal{A}$.

This collection contains the constantly zero polynomial, as well as a monic polynomial (Thm. 20.3.8). Furthermore, a linear combination of any polynomials in $\mathbb{P}_{\mathcal{A}}$ is again in $\mathbb{P}_{\mathcal{A}}$, as is a polynomial multiple of a polynomial in $\mathbb{P}_{\mathcal{A}}$ (TYC 20.3.5). To refer to these properties of $\mathbb{P}_{\mathcal{A}}$ whole-sale, we shall say that $\mathbb{P}_{\mathcal{A}}$ is **a non-trivial ideal in the ring of polynomials**. We will often abbreviate this terminology and just refer to $\mathbb{P}_{\mathcal{A}}$ as **an ideal**.

Obviously, among the degrees of all of the polynomials in $\mathbb{P}_{\mathcal{A}}$ there is the smallest positive one. This degree is said to be **the minimal degree of** $\mathbb{P}_{\mathcal{A}}$.

Test Your Comprehension 21.1.2

If polynomials p and h annihilate matrix $\mathcal{A}$ (i.e. $p, h \in \mathbb{P}_{\mathcal{A}}$), and we divide p by h with a remainder (Fact 20.1.13):

$$p(x) = q(x)h(x) + r(x) ,$$

then r also annihilates $\mathcal{A}$ (i.e. $r \in \mathbb{P}_{\mathcal{A}}$).

In other words, $\mathbb{P}_{\mathcal{A}}$ contains the remainder from a division of any one of its members by any other.

Theorem 21.1.3

For any square matrix $\mathcal{A}$, $\mathbb{P}_{\mathcal{A}}$ contains *exactly one* monic polynomial $\mu_{\mathcal{A}}$ whose degree is the minimal degree of $\mathbb{P}_{\mathcal{A}}$.

In fact, $\mathbb{P}_{\mathcal{A}}$ is exactly the set of all possible polynomial multiples of $\mu_{\mathcal{A}}$, i.e.

$$\mathbb{P}_{\mathcal{A}} = \left\{ \; p \cdot \mu_{\mathcal{A}} \; \middle| \; p \text{ is a polynomial} \; \right\}$$

Terminology 21.1.4

Due to the first claim of Theorem 21.1.3, $\mu_{\mathcal{A}}$ is said to be **the minimal (annihilating) polynomial of** $\mathcal{A}$. With the inclusion of the second claim, it is also said to be **the (monic) generator of** $\mathbb{P}_{\mathcal{A}}$.

Proof of Theorem 21.1.3.

Synopsis of the proof: Since $\mathbb{P}_{\mathcal{A}}$ is an ideal, subtracting two different monic polynomials of the smallest degree in $\mathbb{P}_{\mathcal{A}}$ would produce a non-zero polynomial of even smaller degree in $\mathbb{P}_{\mathcal{A}}$, which cannot be.

To validate the second claim of the theorem we divide polynomials in $\mathbb{P}_{\mathcal{A}}$ by $\mu_{\mathcal{A}}$ with remainder. Since $\mathbb{P}_{\mathcal{A}}$ is an ideal, the remainder must also lie in $\mathbb{P}_{\mathcal{A}}$. Yet the degree of the remainder is less than that of $\mu_{\mathcal{A}}$, which means that the remainder has to be zero.

Let k be the minimal degree of $\mathbb{P}_{\mathcal{A}}$. Then $\mathbb{P}_{\mathcal{A}}$ contains a (non-zero) polynomial g of degree k, and no non-zero polynomials of smaller degree. Some scalar multiple of g is monic. Since $\mathbb{P}_{\mathcal{A}}$ is an ideal, it contains this monic polynomial μ of minimal degree.

Let us argue that μ is the only monic polynomial of this minimal degree k in $\mathbb{P}_{\mathcal{A}}$. If someone claims to have found another such polynomial ν in $\mathbb{P}_{\mathcal{A}}$, then the difference $\mu - \nu$ is a polynomial of degree strictly less than k: the leading term x^k appearing in both $\mu(x)$ and $\nu(x)$ disappears in the difference $\mu - \nu$.

Since $\mathbb{P}_{\mathcal{A}}$ is an ideal, $\mu - \nu$ is in $\mathbb{P}_{\mathcal{A}}$, and has the degree that is strictly smaller than the minimal degree of $\mathbb{P}_{\mathcal{A}}$. Hence $\mu - \nu$ is the zero polynomial, and $\nu = \mu$. This shows that there can not exists two distinct monic polynomials of minimal degree in $\mathbb{P}_{\mathcal{A}}$.

Now that the uniqueness has been established, let us write $\mu_{\mathcal{A}}$ for μ, and let us show that every polynomial in $\mathbb{P}_{\mathcal{A}}$ is a polynomial multiple of $\mu_{\mathcal{A}}$.

Let q be a polynomial in $\mathbb{P}_{\mathcal{A}}$. Divide q by $\mu_{\mathcal{A}}$ with a remainder:

$$p(x) = p(x)\mu_{\mathcal{A}}(x) + r(x) \; .$$

Either r is the zero polynomial, or the degree of r is strictly smaller than the degree of $\mu_{\mathcal{A}}$, which is k. Since r is in $\mathbb{P}_{\mathcal{A}}$ (TYC 21.1.2), and $\mathbb{P}_{\mathcal{A}}$ does not contain non-zero polynomials of degree smaller than k, r must be the zero polynomial.

Therefore $q = p \cdot \mu_{\mathcal{A}}$. This shows that every polynomial in $\mathbb{P}_{\mathcal{A}}$ is a polynomial multiple of $\mu_{\mathcal{A}}$. That every polynomial multiple of $\mu_{\mathcal{A}}$ is in $\mathbb{P}_{\mathcal{A}}$, is a consequence of the latter being an ideal in the ring of polynomials. ■

Test Your Comprehension 21.1.5

If a monic polynomial annihilates $\mathcal{A}$ and has the same degree as $\mu_{\mathcal{A}}$, then it equals $\mu_{\mathcal{A}}$.

Test Your Comprehension 21.1.6 ☞ **Minimal polynomials of 2×2 matrices**

If $\mathcal{A} = \left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right]$ is not a scalar multiple of the identity, then

$$\mu_{\mathcal{A}}(x) = (x-a)(x-d) - bc.$$

Hint: Exercise 20.3.4, Theorem 21.1.3 and TYC 21.1.5 can be helpful here.

Theorem 21.1.7 ☞ **Transposition does not alter annihilating polynomials**

A matrix $\mathcal{A} \in \mathbb{M}_n$ has exactly the same annihilating polynomials as $\mathcal{A}^T$, and therefore

$$\mu_{\mathcal{A}^T} = \mu_{\mathcal{A}} .$$

Proof of Theorem 21.1.7. For any polynomial p,

$$\left(p(\mathcal{A})\right)^T = p\left(\mathcal{A}^T\right) \quad \text{(Exc. 20.2.4)} .$$

This shows that $p(\mathcal{A}) = \mathcal{O}$ exactly when $p\left(\mathcal{A}^T\right) = \mathcal{O}$. ■

The following innocuous theorem deserves a second look. It tells us that when we study annihilating and minimal polynomials, we may trade a matrix in for a similar (and hopefully simpler) matrix, without loss of the relevant information. This is one of the central themes of linear algebra.

Theorem 21.1.8 ☞ **Similarity does not alter the annihilating polynomials**

Similar square matrices have exactly the same annihilating polynomials, and thus the same minimal polynomial.

Proof of Theorem 21.1.8. If $\mathcal{B} = \mathcal{S}^{-1}\mathcal{A}\mathcal{S}$, then

$$p(\mathcal{B}) = \mathcal{S}^{-1} p(\mathcal{A})\, \mathcal{S} \; ,$$

for any polynomial p (Exercise 20.2.9). So, if $p(\mathcal{A}) = \mathcal{O}$, then $p(\mathcal{B}) = \mathcal{O}$. Reversing the roles of $\mathcal{A}$ and $\mathcal{B}$ (i.e. by using the symmetry of the equivalence relation of similarity), we see that the converse implication also holds. ■

Exercise 21.1.9

1. Argue that matrices $\begin{bmatrix} 0&1&0&0\\0&0&0&0\\0&0&0&0\\0&0&0&0 \end{bmatrix}$ and $\begin{bmatrix} 0&1&0&0\\0&0&0&0\\0&0&0&1\\0&0&0&0 \end{bmatrix}$ have the same minimal polynomial: x^2.

2. Argue that the matrices in part 1 have different rank, and therefore are not equivalent. In particular they are not similar.

This shows that non-similar matrices may have identical minimal polynomials.

21.2 Finding Minimal Polynomials Of General Matrices

Let us lay the groundwork towards an algorithm for finding minimal polynomials of square matrices.

Test Your Comprehension 21.2.1

Hint: Synopsis 14.4.6.

Suppose that the first column of a matrix $\mathcal{A}$ is not null, and the seventh column is the first one that is a linear combination of the previous columns of $\mathcal{A}$. Then the first six columns of $\mathcal{A}$ are linearly independent.

Theorem 21.2.2 ☞ Constructing minimal polynomials

Given a square matrix $\mathcal{A}$, let k be the first natural number such that $\mathfrak{C}\left(\mathcal{A}^{k}\right)$ is a linear combination of

$$\mathfrak{C}(\mathcal{I})\,, \mathfrak{C}(\mathcal{A})\,, \mathfrak{C}\left(\mathcal{A}^{2}\right), \mathfrak{C}\left(\mathcal{A}^{3}\right), \ldots, \mathfrak{C}\left(\mathcal{A}^{k-1}\right) \;.^{*}$$

Say,

$$\mathfrak{C}\left(\mathcal{A}^{k}\right) = \alpha_0 \mathfrak{C}(\mathcal{I}) + \alpha_1 \mathfrak{C}(\mathcal{A}) + \cdots + \alpha_{k-1}\mathfrak{C}\left(\mathcal{A}^{k-1}\right) \; .$$

Then

$$\mu_{\mathcal{A}}(x) = -\alpha_0 - \alpha_1 x - \cdots - \alpha_{k-1}x^{k-1} + x^{k} \; .$$

Note that a tuple can be expressed in at most one way as a linear combination of a linearly independent list of tuples (TYC 18.1.6).

*In particular, $\mathfrak{C}(\mathcal{I}), \mathfrak{C}(\mathcal{A}), \mathfrak{C}\left(\mathcal{A}^2\right), \mathfrak{C}\left(\mathcal{A}^3\right), \ldots, \mathfrak{C}\left(\mathcal{A}^{k-1}\right)$ are linearly independent by TYC 21.2.1.

A proof of Theorem 21.2.2 is presented in the appendix to the chapter.

Test Your Comprehension 21.2.3

Given a square matrix $\mathcal{A}$, let k be the first natural number such that $\mathcal{A}^k$ is a linear combination of the smaller non-negative powers of $\mathcal{A}$, say

$$\mathcal{A}^k = \alpha_0\mathcal{I} + \alpha_1\mathcal{A} + \cdots + \alpha_{k-1}\mathcal{A}^{k-1} .$$

Then

$$\mu_{\mathcal{A}}(x) = -\alpha_0 - \alpha_1 x - \cdots - \alpha_{k-1}x^{k-1} + x^k ,$$

Theorem 21.2.2 is the foundation of an algorithm for finding a minimal polynomial of a matrix.

Algorithm 21.2.4

Step 1: Test to see whether $\mathcal{A}$ is a multiple of $\mathcal{I}$ (i.e. whether $\mathfrak{C}(\mathcal{A})$ is a scalar multiple of $\mathfrak{C}(\mathcal{I})$).

- If it is, say $\mathcal{A} = \pi\mathcal{I}$, then $\mu_{\mathcal{A}}(x) = -\pi + x$. Exit the procedure.
- If not, go to the next step.

Step 2: Solve the system

$$\left[\mathfrak{C}(\mathcal{I})\ \ \mathfrak{C}(\mathcal{A})\right](X) = \mathfrak{C}\left(\mathcal{A}^2\right) .$$

- If the system has a solution, say $X = \binom{-4}{3}$, then

$$\mathfrak{C}\left(\mathcal{A}^2\right) = (-4)\mathfrak{C}(\mathcal{I}) + 3\mathfrak{C}(\mathcal{A}) ,$$

  and $\mu_{\mathcal{A}}(x) = -(-4) - 3x + x^2$. Exit the procedure.

- If the system has no solutions, go to the next step.

Step 3: Solve the system

$$\left[\mathfrak{C}(\mathcal{I})\ \ \mathfrak{C}(\mathcal{A})\ \ \mathfrak{C}\left(\mathcal{A}^2\right)\right](X) = \mathfrak{C}\left(\mathcal{A}^3\right) .$$

- If the system has a solution, say $X = \begin{pmatrix} 2 \\ 6 \\ -1 \end{pmatrix}$, then

$$\mathfrak{C}\left(\mathcal{A}^{3}\right) = 2\mathfrak{C}(\mathcal{I}) + 6\mathfrak{C}(\mathcal{A}) + (-1)\mathfrak{C}\left(\mathcal{A}^{2}\right),$$

  and $\mu_{\mathcal{A}}(x) = -2 - 6x - (-1)x^2 + x^3$. Exit the procedure.

- If the system has no solutions, go to the next step.

Step 4: Etc.

Comment 21.2.5

Theorems 20.3.8 and 21.2.2 guarantee that the procedure in Algorithm 21.2.4 will terminate after at most n^2 steps; (and in fact after no more than n steps, as we shall establish later).

The systems that one solves at each step either have a unique solution or no solutions. This is because the coefficient matrices in these systems are injective, as their columns are a sublist of a linearly independent list (Theorem 21.2.2, TYC 18.1.7).

Computer software packages such as *Mathematica*, *Maple* and MATLAB, have computationally efficient ways of finding minimal polynomials of matrices.

Test Your Comprehension 21.2.6

Find the minimal polynomials of the following matrices:

$$[-\pi]_{1\times 1}, \quad \mathcal{O}_{n\times n}, \quad \mathcal{I}_{m}, \quad 3\mathcal{I}_{m}, \quad \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad \begin{bmatrix} 0 & 2 \\ 2 & 0 \end{bmatrix}, \quad \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix}, \quad \begin{bmatrix} 1 & 2 \\ 0 & 3 \end{bmatrix}.$$

21.2.1 — Minimal Polynomials Via An RREF

With a bit more effort we can streamline Algorithm 21.2.4. The main idea is to show that we can perform elementary row operations on the matrix

$$\mathcal{B} := \left[\mathfrak{C}(\mathcal{I}) \quad \mathfrak{C}(\mathcal{A}) \quad \mathfrak{C}\left(\mathcal{A}^{2}\right) \quad \mathfrak{C}\left(\mathcal{A}^{3}\right) \quad \ldots \quad \mathfrak{C}\left(\mathcal{A}^{n^2}\right)\right]$$

to transform it into RREF($\mathcal{B}$), and then "read off" the minimal polynomial of $\mathcal{A}$ from RREF($\mathcal{B}$). Later we shall show that one may even substitute n for n^2. We develop the procedure in the following sequence of exercises.

Exercise 21.2.7

The following statements are equivalent for a list $C_1, C_2, C_3, \ldots, C_{35}$ in $\mathbb{R}^n$.

1. 12 is the first natural number k such that C_k is a linear combination of the preceding tuples on the list.

2. Nullspace of $\begin{bmatrix} C_1 & C_2 & C_3 & \cdots & C_{35} \end{bmatrix}$ contains a tuple that ends in 23 zeros, but contains no non-null tuples that end in 24 zeros.

3. Nullspace of $\begin{bmatrix} C_1 & C_2 & C_3 & \cdots & C_{35} \end{bmatrix}$ contains a tuple that ends in 1 followed by 23 zeros, but contains no non-null tuples that end in 24 zeros.

Hint: Examine the proof of Theorem 12.2.5 for inspiration.

If $(\alpha_1, \alpha_2, \ldots, \alpha_{11}, 1, 0, \ldots, 0)$ is a tuple described in part 3., then
$C_{12} = -\alpha_1 C_1 - \cdots - \alpha_{11} C_{11}$.

Exercise 21.2.8

Given a matrix $\mathcal{M}$ in an RREF with a non-null first column, how does one discern whether one of the columns is a linear combination of the previous columns?

If there is such a column, how does one find the first (i.e. left-most) such column? In such a case what are the coefficients of the corresponding linear combination?

Please give an answer in a form of a *short* algorithm that your classmates can follow and carry out without performing calculations.

Comment 21.2.9

A nullspace of a matrix describes the linear interdependencies of the columns. Not surprisingly, according to Exercise 21.2.7, the nullspace describes which of the columns is first at being a linear combination of the preceding columns, and with which coefficients.

In particular, any two matrices with the same nullspace will have exactly the same property of this type. If the seventh column of one is the first column that is a linear combination of the previous columns, with coefficients $\alpha_1, \alpha_2, \alpha_3, \ldots, \alpha_6$, then exactly the same statement holds true for the other matrix, including the very same coefficients $\alpha_1, \alpha_2, \alpha_3, \ldots, \alpha_6$.

If the first column in each of these matrices is not null, then the first six columns of each form linearly independent lists (TYC 21.2.1), and so the scalars $\alpha_1, \alpha_2, \alpha_3, \ldots, \alpha_6$ described above must be unique (TYC 18.1.6).

Test Your Comprehension 21.2.10 ☞ **Row operations do not alter column interdependence relations**

Suppose that the first column of a matrix

$$\mathcal{A} = \begin{bmatrix} C_1 & C_2 & C_3 & \cdots & C_m \end{bmatrix}$$

is not null, and that the 7-th is the *first* column of $\mathcal{A}$ that is a linear combination of the previous columns, with

$$C_7 = \alpha_1 C_1 + \cdots + \alpha_6 C_6.$$

Suppose that $\mathcal{B}$ is a matrix obtained from $\mathcal{A}$ through a sequence of elementary ROW operations, and

$$\mathcal{B} = \begin{bmatrix} K_1 & K_2 & K_3 & \cdots & K_m \end{bmatrix}.$$

Hint: TYC 12.1.16 and Comment 21.2.9 can be helpful here.

Then the first column of $\mathcal{B}$ is not null, the 7-th is the *first* column of $\mathcal{B}$ that is a linear combination of the previous columns, and

$$K_7 = \alpha_1 K_1 + \cdots + \alpha_6 K_6.$$

Exercise 21.2.11

Combine Theorem 21.2.2 and TYC 21.2.10 and Exercise 21.2.8 to produce a step-by-step algorithm for finding the minimal polynomial of a matrix $\mathcal{A}$ via computing

$$\mathrm{RREF}\left[\mathfrak{C}(\mathcal{I}) \quad \mathfrak{C}(\mathcal{A}) \quad \mathfrak{C}\left(\mathcal{A}^2\right) \quad \mathfrak{C}\left(\mathcal{A}^3\right) \quad \ldots \quad \mathfrak{C}\left(\mathcal{A}^{n^2}\right)\right].$$

Apply your procedure to the matrix $\begin{bmatrix} 0 & 1 & 5 \\ -5 & 2 & -1 \\ 0 & -3 & -5 \end{bmatrix}$. You are allowed to borrow from the future and replace n^2 by n in this case.

21.3 Minimal Polynomials Of Block-$\triangle^r$ Matrices

Test Your Comprehension 21.3.1 ☞ **Annihilating polynomials of block-diagonal matrices**

Hint: TYC 20.2.5.

A polynomial p annihilates a block-diagonal matrix $\mathcal{A}_1 \boxplus \mathcal{A}_2 \boxplus \cdots \boxplus \mathcal{A}_k$ with square $\mathcal{A}_i$'s, exactly when it annihilates each $\mathcal{A}_i$, or equivalently, when it is a multiple of (equivalently, divisible by) each of the $\mu_{\mathcal{A}_i}$'s.

Fact 21.3.2 ☞ **Least common polynomial multiples**

If $p_1, p_2, \ldots, p_k$ are non-zero polynomials, then among the monic polynomials that are divisible by *all* of the p_i's there is a unique one of minimal degree. This unique monic polynomial is said to be **the least common multiple** of the polynomials $p_1, p_2, \ldots, p_k$, and is denoted by

$$\mathrm{LCM}\big(p_1, p_2, \ldots, p_k\big).$$

The prime factors of $\mathrm{LCM}\big(p_1, p_2, \ldots, p_k\big)$ are exactly the polynomials that appear as a prime factor in at least one p_i, and the multiplicity of such a prime factor in $\mathrm{LCM}\big(p_1, p_2, \ldots, p_k\big)$ is the largest of its multiplicities as a prime factor of the p_i's.

Mathematica command **PolynomialLCM**[ ] can be used to calculate the least common multiple of a given list of polynomials.

Test Your Comprehension 21.3.3 ☞ **Minimal Polynomials of Block-Diagonal Matrices**

When all of the $\mathcal{A}_i$'s are square,

$$\mu_{\mathcal{A}_1 \boxplus \mathcal{A}_2 \boxplus \cdots \boxplus \mathcal{A}_k} = \mathrm{LCM}(\mu_{\mathcal{A}_1}, \mu_{\mathcal{A}_2}, \ldots, \mu_{\mathcal{A}_k}) \,.$$

Exercise 21.3.4

1. Find the minimal polynomial of the diagonal matrix

$$\begin{bmatrix} 3 & 0 & 0 & 0 & 0 & 0 \\ 0 & -2 & 0 & 0 & 0 & 0 \\ 0 & 0 & \pi & 0 & 0 & 0 \\ 0 & 0 & 0 & \pi & 0 & 0 \\ 0 & 0 & 0 & 0 & -2 & 0 \\ 0 & 0 & 0 & 0 & 0 & 2 \end{bmatrix},$$

2. State and prove a general claim about minimal polynomials of diagonal matrices. You result should imply that

   > the minimal polynomial of a diagonal matrix factors as a product of distinct linear factors (corresponding to the distinct diagonal entries of the matrix).

Lemma 21.3.5 **The minimal polynomial of $\left[\begin{smallmatrix}\mathcal{A} & \mathcal{B}\\ \mathcal{O} & \mathcal{D}\end{smallmatrix}\right]$**

If $\mathcal{T} = \left[\begin{smallmatrix}\mathcal{A} & \mathcal{B}\\ \mathcal{O} & \mathcal{D}\end{smallmatrix}\right]$, where $\mathcal{A}$ and $\mathcal{D}$ are square, then $\mu_{\mathcal{A}}$ and $\mu_{\mathcal{D}}$ divide $\mu_{\mathcal{T}}$, which, in turn, divides $\mu_{\mathcal{A}}\mu_{\mathcal{D}}$.*

In particular, the prime factors of $\mu_{\mathcal{T}}$ are exactly the prime factors of $\mu_{\mathcal{A}}$ and of $\mu_{\mathcal{D}}$.

*In other words, the multiplicity of a prime factor of $\mu_{\mathcal{T}}$ is no less than either of its multiplicities as a prime factor of $\mu_{\mathcal{A}}$ and of $\mu_{\mathcal{D}}$. It is no greater than the sum of these multiplicities. We maintain the convention of saying that the multiplicity of f in a polynomial p is zero whenever f is NOT a factor of p.

Proof of Lemma 21.3.5. By TYC 20.2.7,

$$\mathcal{O} = \mu_{\mathcal{T}}(\mathcal{T}) = \begin{bmatrix} \mu_{\mathcal{T}}(\mathcal{A}) & \star \\ \mathcal{O} & \mu_{\mathcal{T}}(\mathcal{D}) \end{bmatrix}.$$

This shows that $\mu_{\mathcal{T}}$ annihilates $\mathcal{A}$ and $\mathcal{D}$, and consequently is divisible by $\mu_{\mathcal{A}}$ and $\mu_{\mathcal{D}}$ (Thm. 21.1.3).

To demonstrate that $\mu_{\mathcal{T}}$ divides $\mu_{\mathcal{A}}\mu_{\mathcal{D}}$ it is sufficient (Thm. 21.1.3) to show that $\mu_{\mathcal{A}}\mu_{\mathcal{D}}$ annihilates $\mathcal{T}$. The following calculation shows that this is indeed so.

$$(\mu_{\mathcal{A}}\mu_{\mathcal{D}})(\mathcal{T}) \overset{\text{TYC 20.2.8}}{=} \Big(\mu_{\mathcal{A}}(\mathcal{T})\Big)\Big(\mu_{\mathcal{D}}(\mathcal{T})\Big) \overset{\text{TYC 20.2.7}}{=} \begin{bmatrix} \mu_{\mathcal{A}}(\mathcal{A}) & \square \\ \mathcal{O} & \mu_{\mathcal{A}}(\mathcal{D}) \end{bmatrix} \begin{bmatrix} \mu_{\mathcal{D}}(\mathcal{A}) & \diamondsuit \\ \mathcal{O} & \mu_{\mathcal{D}}(\mathcal{D}) \end{bmatrix}$$

$$= \begin{bmatrix} \mathcal{O} & \square \\ \mathcal{O} & \mu_{\mathcal{A}}(\mathcal{D}) \end{bmatrix} \begin{bmatrix} \mu_{\mathcal{D}}(\mathcal{A}) & \diamondsuit \\ \mathcal{O} & \mathcal{O} \end{bmatrix} = \mathcal{O}. \qquad \blacksquare$$

Hint: Theorem 21.1.7 can be helpful here.

Exercise 21.3.6

Prove the analogue of Lemma 21.3.5 for partitioned matrices of the form $\left[\begin{smallmatrix}\mathcal{B} & \mathcal{O}\\ \mathcal{C} & \mathcal{D}\end{smallmatrix}\right]$.

Test Your Comprehension 21.3.7

If $\mu_{\mathcal{A}}$ and $\mu_{\mathcal{D}}$ share NO prime factors then the minimal polynomial of $\left[\begin{smallmatrix}\mathcal{A} & \mathcal{B}\\ \mathcal{O} & \mathcal{D}\end{smallmatrix}\right]$ is $\mu_{\mathcal{A}}\mu_{\mathcal{D}}$.

Exercise 21.3.8 **The minimal polynomial of $\left[\begin{smallmatrix}\mathcal{A} & \mathcal{B}\\ \mathcal{O} & \mathcal{D}\end{smallmatrix}\right]$ may be neither LCM$\left(\mu_{\mathcal{A}}, \mu_{\mathcal{D}}\right)$ nor $\mu_{\mathcal{A}}\mu_{\mathcal{D}}$.**

Let $\mathcal{A} = \mathcal{D} = \left[\begin{smallmatrix}0 & 1\\ 0 & 0\end{smallmatrix}\right]$, and let

$$\mathcal{T} := \left[\begin{smallmatrix}\mathcal{A} & \mathcal{I}\\ \mathcal{O} & \mathcal{D}\end{smallmatrix}\right].$$

Argue that the minimal polynomial of $\mathcal{T}$ is x^3, and then argue that this is neither LCM $\left(\mu_{\mathcal{A}}, \mu_{\mathcal{D}}\right)$ nor $\mu_{\mathcal{A}}\mu_{\mathcal{D}}$.

Theorem 21.3.9 ☞ Minimal polynomials of block-△ʳ matrices

For a block-triangular matrix $\mathcal{A}$ with square diagonal blocks, each of the minimal polynomials of the diagonal blocks divides $\mu_{\mathcal{A}}$, which, in turn, divides the product of these minimal polynomials.

In particular, the prime factors of $\mu_{\mathcal{A}}$ are exactly the prime factors of the minimal polynomials of the diagonal blocks.

Proof of Theorem 21.3.9. The result is trivial if $\mathcal{A}$ has only one block. By Lemma 21.3.5 the result holds true when $\mathcal{A}$ has 2 diagonal blocks.

If the claim of the theorem were not true in general, there would be counterexamples to it, and among these there would be one (say $\mathcal{A}_{\circ}$) with the *smallest* number of diagonal blocks, say $n_{\circ}$. We know that $n_{\circ}$ has to be at least 3, and that the claim holds true for all block-triangular matrices with fewer than $n_{\circ}$ diagonal blocks.

Since transposition does not alter minimal polynomials (Thm. 21.1.7), by transposing if necessary, we can take $\mathcal{A}_{\circ}$ to be a block-upper-triangular matrix.

$\mathcal{A}_{\circ}$ can be sup-partitoned as $\left[\begin{smallmatrix} \mathcal{B} & \mathcal{C} \\ \mathcal{O} & \mathcal{D} \end{smallmatrix}\right]$, where $\mathcal{B}$ and $\mathcal{D}$ are square block-upper-triangular matrices, with fewer than $n_{\circ}$ diagonal blocks each. Let us denote such diagonal blocks by $\mathcal{B}_{ii}$ and $\mathcal{D}_{jj}$ respectively.

Therefore the claim of the theorem holds true for $\mathcal{B}$ and $\mathcal{D}$. Thus each $\mu_{\mathcal{B}_{ii}}$ divides $\mu_{\mathcal{B}}$, and the latter divides the product of all $\mu_{\mathcal{B}_{ii}}$'s. Similarly for D and D_{jj}'s.

Applying Lemma 21.3.5 to $\left[\begin{smallmatrix} \mathcal{B} & \mathcal{C} \\ \mathcal{O} & \mathcal{D} \end{smallmatrix}\right]$ we see that $\mu_{\mathcal{B}}$ and $\mu_{\mathcal{D}}$ divide $\mu_{\mathcal{A}_{\circ}}$, which in turn divides $\mu_{\mathcal{B}}\mu_{\mathcal{D}}$.

Hence, all $\mu_{\mathcal{B}_{ii}}$'s and $\mu_{\mathcal{D}_{jj}}$'s divide $\mu_{\mathcal{A}_{\circ}}$, and the latter divides $\mu_{\mathcal{B}}\mu_{\mathcal{D}}$, which in turn divides the product of all $\mu_{\mathcal{B}_{ii}}$'s and $\mu_{\mathcal{D}_{jj}}$'s.

This shows that $\mathcal{A}_{\circ}$ satisfies the claim of the theorem, contrary to our choice of $\mathcal{A}_{\circ}$. Therefore the only feasible conclusion must be that there are no counterexamples to the theorem, and consequently the proof is complete. ∎

Exercise 21.3.10 ☞ Minimal polynomials of △ʳ matrices

1. The minimal polynomial of a triangular matrix $\mathcal{A}$ has only linear prime factors, and these are exactly the factors $x - \alpha$, where α ranges over the diagonal entries of $\mathcal{A}$.

2. The multiplicity of each such factor in $\mu_{\mathcal{A}}$ is NO LARGER than the number of times α appears on the diagonal of $\mathcal{A}$.

Test Your Comprehension 21.3.11

If a matrix $\mathcal{A}$ is similar to a triangular matrix, then the minimal polynomial of $\mathcal{A}$ does not have any quadratic prime factors; in other words, it has a factorization of the form

$$\left(x - r_1\right)^{m_1} \left(x - r_2\right)^{m_2} \cdots \left(x - r_k\right)^{m_k} .$$

It turns out that the converse of the claim in TYC 21.3.11 is also true, and this will gives us a complete characterization of the matrices that are similar to triangular matrices, in terms of their minimal polynomials. This result is based on the classical Schur's Block-Tiangularization Theorem (Thm. 27.1.1).

Exercise 21.3.12

Argue that the minimal polynomial of the $n \times n$ matrix

$$\begin{bmatrix} 0 & 1 & 0 & 0 & \dots & 0 \\ 0 & 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & 0 & \dots & 1 \\ 0 & 0 & 0 & 0 & \dots & 0 \end{bmatrix}$$

is x^n.

21.4 Companion Matrices

Is every non-constant monic polynomial a minimal polynomial of some matrix? The following remarkable theorem gives an affirmative answer.

Theorem 21.4.1

Matrix

$$\mathcal{A} := \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & -\alpha_0 \\ 1 & 0 & 0 & 0 & 0 & -\alpha_1 \\ 0 & 1 & 0 & 0 & 0 & -\alpha_2 \\ 0 & 0 & 1 & 0 & 0 & -\alpha_3 \\ 0 & 0 & 0 & 1 & 0 & -\alpha_4 \\ 0 & 0 & 0 & 0 & 1 & -\alpha_5 \end{bmatrix}_{6\times 6}$$

has the minimal polynomial

$$\mu_{\mathcal{A}}(x) = x^6 + \alpha_5 x^5 + \alpha_4 x^4 + \cdots + \alpha_1 x + \alpha_0 ,$$

as do all matrices of the form $\mathcal{A} \boxplus \mathcal{O}_k$ (TYC 20.2.5).

This holds true in a general, and shows that every monic polynomial of positive degree n is a minimal polynomial of some $n \times n$ matrix, and of some matrices of all larger sizes.

A proof of Theorem 21.4.1 is presented in the appendix to the chapter.

Terminology 21.4.2

Matrix $\mathcal{A}$ shown in Theorem 21.4.1 is said to be **the companion matrix** of the polynomial $x^6 + \alpha_5 x^5 + \alpha_4 x^4 + \cdots + \alpha_1 x + \alpha_0$.

21.5 Appendix: Exiled Proofs

Proof of Theorem 21.2.2.

Let us argue that the following are equivalent. This will establish the equivalence of claims 1. and 2. in the theorem.

- A monic polynomial of degree k annihilates $\mathcal{A}$.
- $\mathfrak{C}\left(\mathcal{A}^k\right)$ is a linear combination of

$$\mathfrak{C}(\mathcal{I}), \mathfrak{C}(\mathcal{A}), \mathfrak{C}\left(\mathcal{A}^2\right), \mathfrak{C}\left(\mathcal{A}^3\right), \ldots, \mathfrak{C}\left(\mathcal{A}^{k-1}\right).$$

$p(x) := \gamma_0 + \gamma_1 x + \cdots + \gamma_{k-1} x^{k-1} + x^k$ annihilates $\mathcal{A}$ exactly when

$$\mathcal{O} = \gamma_0 \mathcal{I} + \gamma_1 \mathcal{A} + \gamma_2 \mathcal{A}^2 + \cdots + \gamma_{k-1} \mathcal{A}^{k-1} + 1\mathcal{A}^k. \tag{21.1}$$

Equality (21.1) is equivalent to

$$\mathcal{A}^k = -\gamma_0 \mathcal{I} - \gamma_1 \mathcal{A} - \gamma_2 \mathcal{A}^2 - \cdots - \gamma_{k-1} \mathcal{A}^{k-1},$$

which, in turn, is equivalent to

$$\mathfrak{C}\left(\mathcal{A}^k\right) = -\gamma_0 \mathfrak{C}(\mathcal{I}) - \gamma_1 \mathfrak{C}(\mathcal{A}) - \cdots - \gamma_{k-1} \mathfrak{C}\left(\mathcal{A}^{k-1}\right).$$

The last claim of the theorem has also been established in the process.

Let us verify the second-to-last claim, and thus complete the proof.

We will argue that no tuple on the list

$$\mathfrak{C}(\mathcal{I}), \mathfrak{C}(\mathcal{A}), \mathfrak{C}\left(\mathcal{A}^2\right), \mathfrak{C}\left(\mathcal{A}^3\right), \ldots, \mathfrak{C}\left(\mathcal{A}^{k-1}\right)$$

is a linear combination of the preceding tuples on the list. Since $\mathfrak{C}(\mathcal{I})$ is not null, this will automatically show that the list is linearly independent (Synopsis 14.4.6).

If we had

$$\mathfrak{C}\left(\mathcal{A}^{m}\right) = \beta_0 \mathfrak{C}(\mathcal{I}) + \beta_1 \mathfrak{C}(\mathcal{A}) + \cdots + \beta_{m-1} \mathfrak{C}\left(\mathcal{A}^{m-1}\right) ,$$

for some natural $m < k$, then

$$\mathcal{A}^{m} = \beta_0 \mathcal{I} + \beta_1 \mathcal{A} + \beta_2 \mathcal{A}^{2} + \cdots + \beta_{m-1} \mathcal{A}^{m-1} ,$$

or equivalently

$$-\beta_0 \mathcal{I} - \beta_1 \mathcal{A} - \beta_2 \mathcal{A}^{2} - \cdots - \beta_{m-1} \mathcal{A}^{m-1} + 1\mathcal{A}^{k} = \mathcal{O} .$$

In that case $-\beta_0 - \beta_1 x - \cdots - \beta_{m-1} x^{m-1} + x^{m}$ would be a monic polynomial of degree less than k that annihilates $\mathcal{A}$. This cannot happen (Theorem 21.1.3). ■

Proof of Theorem 21.4.1. Let us write

$$p(x) := x^6 + \alpha_5 x^5 + \alpha_4 x^4 + \cdots + \alpha_1 x + \alpha_0 .$$

The reader should verify that the following equations describe (the columns of) $\mathcal{A}$:

$$\begin{cases} E_2 = \mathcal{A}\left(E_1\right) \\ E_3 = \mathcal{A}\left(E_2\right) = \mathcal{A}^{2}\left(E_1\right) \\ E_4 = \mathcal{A}\left(E_3\right) = \mathcal{A}^{3}\left(E_1\right) \\ E_5 = \mathcal{A}\left(E_4\right) = \mathcal{A}^{4}\left(E_1\right) \\ E_6 = \mathcal{A}\left(E_5\right) = \mathcal{A}^{5}\left(E_1\right) \\ \mathcal{A}\left(E_6\right) = -\alpha_5 E_6 - \alpha_4 E_5 - \cdots - \alpha_1 E_2 - \alpha_0 E_1 \end{cases} \tag{21.2}$$

Using the first six equations, the last of the equations can be expressed as

$$\mathcal{A}^{6}\left(E_1\right) = -\alpha_5 \mathcal{A}^{5}\left(E_1\right) - \alpha_4 \mathcal{A}^{4}\left(E_1\right) - \cdots - \alpha_1 \mathcal{A}\left(E_1\right) - \alpha_0 \mathcal{I}\left(E_1\right);$$

or equivalently as

$$\Big(p(\mathcal{A})\Big)\left(E_1\right) = \mathbb{0} .$$

Claim 1: p annihilates $\mathcal{A}$.

To show that $p(\mathcal{A}) = \mathcal{O}$ we shall show that all columns of $p(\mathcal{A})$ are null; namely that $\Big(p(\mathcal{A})\Big)(E_i) = \mathbb{O}$ for $i = 1, 2, 3, \ldots, 6$.

To this end note that

$$\begin{aligned}
\Big(p(\mathcal{A})\Big)(E_i) &= \Big(p(\mathcal{A})\Big)\Big(\mathcal{A}^i(E_1)\Big) \\
&= \Big(p(\mathcal{A})\ \mathcal{A}^i\Big)(E_1) \\
&\overset{\text{TYC 20.2.8}}{=} \Big(\mathcal{A}^i\ p(\mathcal{A})\Big)(E_1) \\
&= \mathcal{A}^i\Big(\big(p(\mathcal{A})\big)(E_1)\Big) \\
&= \mathcal{A}^i(\mathbb{O}) = \mathbb{O}\ ,
\end{aligned}$$

for any appropriate i.

Claim 2: No monic polynomial of degree less than 6 can annihilate $\mathcal{A}$.

It is sufficient to show that for $k < 6$, $\mathcal{A}^k$ is not a linear combination of the lower powers of $\mathcal{A}$ (TYC 21.2.3). If this were not the case then for some such k we would have

$$\mathcal{A}^k = a_0\mathcal{I} + a_1\mathcal{A} + \cdots + a_{k-1}\mathcal{A}^{k-1}\ .$$

Then it would follow that

$$\mathcal{A}^k(E_1) = a_0\mathcal{I}(E_1) + a_1\mathcal{A}(E_1) + \cdots + a_{k-1}\mathcal{A}^{k-1}(E_1)\ .$$

By (21.2), this would state that

$$E_{k-1} = a_0 E_1 + a_1 E_2 + \cdots + a_{k-1}E_{k-2};$$

which is obviously false, since the standard basis tuples form a linearly independent list.

Putting the two claims together we see that p must be the minimal polynomial of $\mathcal{A}$. ■

VIII

Orthogonality

22. Linear Isometries

Last modified on December 8, 2018

22.1 Orthogonality-Preserving Matrices

Which matrices **preserve orthogonality**? In other words, for which matrices the orthogonality of a pair of inputs entails the orthogonality of the corresponding outputs? More formally, which matrices $\mathcal{A}$ have the property that

$$\mathcal{A}(X) \bullet \mathcal{A}(Y) = 0 \quad \text{whenever} \quad X \bullet Y = 0?$$

Of course, any scalar multiple of an identity matrix has this property, but orthogonality-preserving matrices do not have to be square. Even among the square matrices (of size bigger than 1×1) there are orthogonality preserving matrices that are not scalar multiples of an identity.

Terminology 22.1.1

A list of tuples is said to be **an orthogonal list** if the tuples on the list are mutually orthogonal. Such a list can contain null tuples.

Obviously, matrices that preserve orthogonality map orthogonal lists of inputs to orthogonal lists of outputs.

Test Your Comprehension 22.1.2

Argue that the columns of an orthogonality-preserving matrix form an orthogonal list.

Hint: Columns of a matrix $\mathcal{A}$ have the form $\mathcal{A}\left(E_i\right)$.

Theorem 22.1.3

If a matrix $\mathcal{A}$ preserves orthogonality, then all columns of $\mathcal{A}$ have the same length.

Proof of Theorem 22.1.3. Supposing that $\mathcal{A}$ preserves orthogonality, and assuming for non-triviality that $\mathcal{A}$ has more than one column, we aim to show that

$$\left\|\mathcal{A}(E_i)\right\| = \left\|\mathcal{A}\left(E_j\right)\right\|, \quad \text{for any} \quad i \neq j\,.$$

Since E_i and E_j are mutually orthogonal when $i \neq j$, so are $\mathcal{A}(E_i)$ and $\mathcal{A}\left(E_j\right)$.

It is easy to check that

$$\left(E_i + E_j\right) \bullet \left(E_i - E_j\right) = 0.$$

Hence we must have

$$\mathcal{A}\left(E_i + E_j\right) \bullet \mathcal{A}\left(E_i - E_j\right) = \left(\mathcal{A}(E_i) + \mathcal{A}\left(E_j\right)\right) \bullet \left(\mathcal{A}(E_i) - \mathcal{A}\left(E_j\right)\right) = 0\,. \quad (22.1)$$

Distributing $\bullet$ in (22.1), and keeping in mind that $\mathcal{A}(E_i) \bullet \mathcal{A}\left(E_j\right) = 0$, we arrive at

$$\mathcal{A}(E_i) \bullet \mathcal{A}(E_i) - \mathcal{A}\left(E_j\right) \bullet \mathcal{A}\left(E_j\right) = 0\,,$$

which can be rewritten as

$$\left\|\mathcal{A}(E_i)\right\|^2 - \left\|\mathcal{A}\left(E_j\right)\right\|^2 = 0\,.$$

The desired conclusion follows. ■

Terminology 22.1.4

Recall that a tuple of Euclidean length 1 is said to be **a unit tuple**, and a list of tuples is said to be **an orthonormal list** if it is an orthogonal list of unit tuples.

A matrix whose columns form an orthonormal list is said to be a **linear isometry**. Since the only isometries we shall deal with are the linear ones, we usually drop off the word "linear". Common alternative terms are **"an orthogonal matrix"** and **"an orthonormal matrix"**.

Terms such as **an orthogonal coordinate system** and **an orthonormal coordinate system** are now self-explanatory.

Corollary 22.1.5

Every orthogonality-preserving matrix is a scalar multiple of an isometry.

Proof of Corollary 22.1.5. Suppose that $\mathcal{A}$ preserves orthogonality. If $\mathcal{A} = \mathcal{O}$ then $\mathcal{A} = 0 \cdot \mathcal{I}$, and the desired conclusion holds. If $\mathcal{A} \neq \mathcal{O}$, then the columns of $\mathcal{A}$ are mutually orthogonal tuples of equal length $\alpha > 0$. In that case $\frac{1}{\alpha} \cdot \mathcal{A}$ is an isometry, and of course $\mathcal{A} = \alpha\left(\frac{1}{\alpha}\mathcal{A}\right)$. ■

As we shall demonstrate shortly, orthogonality-preserving matrices are exactly the scalar multiples of the isometries.

Comment 22.1.6 : Orthogonality-Preserving Linear Functions on Vectors

22.2 Isometries

Example 22.2.1

$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$ and $\begin{bmatrix} \frac{1}{2} & \frac{1}{2} \\ -\frac{1}{2} & -\frac{1}{2} \\ -\frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \end{bmatrix}$ are isometries.

Test Your Comprehension 22.2.2

Argue that scaling a column of an isometry by -1 produces another isometry.

Exercise 22.2.3

Recalling the formula

$$\left(\mathcal{A}^T\mathcal{A}\right)[\![i,j]\!] = C_i \bullet C_j,$$

argue that the following statements are equivalent for an $m \times n$ matrix $\mathcal{A}$.

1. $\mathcal{A}$ is an isometry.
2. $\mathcal{A}^T\mathcal{A} = \mathcal{I}_n$.

Argue that every isometry is an injection and is therefore portrait-shaped.

Test Your Comprehension 22.2.4

Argue that a direct sum $A \boxplus B$ of two isometries is also an isometry.

Hint: TYC 9.2.5.

Theorem 22.2.5 ☞ **Orthogonality and linear independence**

An orthogonal list of *non-null* tuples is always linearly independent.

In particular, every orthonormal list is linearly independent.

Proof of Theorem 22.2.5. Let us suppose that $X_1, X_2, \dots, X_k$ is an orthogonal list of tuples none of which are null. Scale the tuples by appropriate non-zero scalars $\alpha_1, \alpha_2, \dots, \alpha_k$ to produce an orthonormal list $\alpha_1 X_1, \alpha_2 X_2, \dots, \alpha_k X_k$.

Then $[\alpha_1 X_1, \alpha_2 X_2, \dots, \alpha_k X_k]$ is an isometry and so is injective. Since one arrives at $[\alpha_1 X_1, \alpha_2 X_2, \dots, \alpha_k X_k]$ by performing a sequence of elementary column operations (scalings) on $[X_1 \;\; X_2 \;\; \dots \;\; X_k]$, the two matrices have the same jectivity.

Therefore $[X_1 \;\; X_2 \;\; \dots \;\; X_k]$ is injective, and we are done. ∎

The following theorem demonstrates that the isometries are exactly the matrices that do not alter (the Euclidean) length.

Let us say that a matrix **preserves the dot product** if the dot product of two inputs equals the dot product of the corresponding outputs.

It turns out that the property of preserving the length is equivalent to that of preserving the dot product.

This connection between a "structural" and a "behavioral" descriptions makes the theorem remarkable.

Theorem 22.2.6

The following are equivalent for a matrix $\mathcal{A} \in \mathbb{M}_{n \times m}$.

1. $\mathcal{A}$ is an isometry.
2. $\mathcal{A}(X) \bullet \mathcal{A}(Y) = X \bullet Y$, for all $X, Y \in \mathbb{R}^m$.
   i.e. $\mathcal{A}$ **preserves the dot product**.
3. $\|\mathcal{A}(Z)\| = \|Z\|$, for all $Z \in \mathbb{R}^m$.
   i.e. $\mathcal{A}$ **preserves the Euclidean length**.

A proof of Theorem 22.2.6 is presented in the appendix to the chapter.

Hint: Cor. 22.1.5 and Thm. 22.2.6.

Test Your Comprehension 22.2.7

Argue that the orthogonality-preserving matrices are exactly the scalar multiples of the isometries.

Test Your Comprehension 22.2.8

Argue that a product of two isometries is also an isometry.

Hint: A composition of two matrices each of which preserves length ... Alternatively, consider $(\mathcal{AB})^T(\mathcal{AB})$.

Test Your Comprehension 22.2.9 ☞ **Isometries are exactly the orthonormality-preserving matrices**

Argue that a matrix is an isometry if and only if it maps an orthonormal list of inputs to an orthonormal list of outputs.

Hint: A single unit tuple constitutes an orthonormal list. Thm. 22.2.6 can be helpful here.

Next we explore the matrices $\mathcal{A} \in \mathbb{M}_{n\times m}$ which satisfy the condition

$$\mathcal{A}^T\mathcal{A} = \mathcal{I}_k \oplus \mathcal{O}_{m-k} = \begin{bmatrix} \mathcal{I}_k & \mathcal{O} \\ \mathcal{O} & \mathcal{O} \end{bmatrix}_{m\times m},$$

which is obviously related to the condition that describes the isometries (Exc. 22.2.3). It turns out that such matrices are indeed very much related to the isometries, and are examples of the **partial isometries**. Of course SPI's are such matrices, but there are others.

Theorem 22.2.10

A matrix $\mathcal{A} \in \mathbb{M}_{n\times m}$ satisfies the condition

$$\mathcal{A}^T\mathcal{A} = \begin{bmatrix} \mathcal{I}_k & \mathcal{O} \\ \mathcal{O} & \mathcal{O} \end{bmatrix}_{m\times m}$$

exactly when $\mathcal{A} = \begin{bmatrix} \mathcal{B} & \mathcal{O} \end{bmatrix}_{n\times m}$ and $\mathcal{B}$ is an $n \times k$ isometry.

Proof of Theorem 22.2.10. If $\mathcal{A} = \begin{bmatrix} \mathcal{B} & \mathcal{O} \end{bmatrix}_{n\times m}$, where $\mathcal{B}$ is an $n \times k$ isometry, then

$$\mathcal{A}^T\mathcal{A} = \begin{bmatrix} \mathcal{B}^T \\ \mathcal{O} \end{bmatrix}_{m\times n} \begin{bmatrix} \mathcal{B} & \mathcal{O} \end{bmatrix}_{n\times m} = \begin{bmatrix} \mathcal{B}^T\mathcal{B} & \mathcal{O} \\ \mathcal{O} & \mathcal{O} \end{bmatrix}_{m\times m} = \begin{bmatrix} \mathcal{I}_k & \mathcal{O} \\ \mathcal{O} & \mathcal{O} \end{bmatrix}_{m\times m}.$$

To verify the reverse implication, we suppose that $\mathcal{A}^T\mathcal{A} = \begin{bmatrix} \mathcal{I}_k & \mathcal{O} \\ \mathcal{O} & \mathcal{O} \end{bmatrix}_{m\times m}$, and recall the formula

$$\left(\mathcal{A}^T\mathcal{A}\right)[\![i,j]\!] = C_i \bullet C_j,$$

which involves the columns of $\mathcal{A}$. The equality

$$\begin{bmatrix} \mathcal{I}_k & \mathcal{O} \\ \mathcal{O} & \mathcal{O} \end{bmatrix}_{m\times m} [\![i,j]\!] = C_i \bullet C_j$$

tells us that the columns of $\mathcal{A}$ are mutually orthogonal (i.e. that $C_i \bullet C_j = 0$, when $i \neq j$). It also tells us that

$$\|C_i\|^2 = C_i \bullet C_i = \begin{cases} 1, & \text{if } 1 \leq i \leq k \\ 0, & \text{otherwise} \end{cases} .$$

Therefore the first k columns of $\mathcal{A}$ are unit tuples, and the rest of the columns are null. This shows that $\mathcal{A}$ is obtained by attaching null columns to an $n \times k$ isometry from the right, and we are done. ■

Comment 22.2.11 : **Isometries on Vectors** (A Visit To A Parallel Universe)

22.3 Appendix: Exiled Proofs

Proof of Theorem 22.2.6.

[**1.** $\Longrightarrow$ **2.**]: Suppose that $\mathcal{A}$ is an isometry. Then $\mathcal{A}^T\mathcal{A} = \mathcal{I}_m$. (Exc. 22.2.3). Consequently, using the fundamental property of transposition, we have

$$\mathcal{A}(X) \bullet \mathcal{A}(Y) = \mathcal{A}^T\mathcal{A}(X) \bullet Y = \mathcal{I}_m(X) \bullet Y = X \bullet Y .$$

[**2.** $\Longrightarrow$ **3.**]: Suppose that $\mathcal{A}$ preserves the dot product. Then

$$\|\mathcal{A}(Z)\|^2 = \mathcal{A}(Z) \bullet \mathcal{A}(Z) = Z \bullet Z = \|Z\|^2 .$$

Since Euclidean length is non-negative, this yields

$$\|\mathcal{A}(Z)\| = \|Z\| .$$

[**3.** $\Longrightarrow$ **1.**]: Suppose that $\mathcal{A}$ preserves the Euclidean length. We aim to show that the columns $\mathcal{A}(E_i)$ of $\mathcal{A}$ are mutually orthogonal unit tuples.

Since every standard basis tuple E_i has length 1, and $\mathcal{A}$ preserves length, each $\mathcal{A}(E_i)$ has length 1.

What remains to be shown is that

$$\mathcal{A}(E_i) \bullet \mathcal{A}(E_j) = 0\ ,$$

whenever $i \neq j$. We shall verify the claim in the case $i = 1$ and $j = 2$ to keep the notation simple. A general proof follows exactly the same path.

$$\begin{aligned}
2 &\overset{\text{calculate}}{=} \left\| E_1 + E_2 \right\|^2 \overset{\mathcal{A}\text{ preserves length}}{=} \left\| \mathcal{A}\left(E_1 + E_2\right) \right\|^2 \\
&\overset{\text{linearity}}{=} \left\| \mathcal{A}\left(E_1\right) + \mathcal{A}\left(E_2\right) \right\|^2 = \Big(\mathcal{A}\left(E_1\right) + \mathcal{A}\left(E_2\right) \Big) \bullet \Big(\mathcal{A}\left(E_1\right) + \mathcal{A}\left(E_2\right) \Big) \\
&\overset{\bullet\text{ distributes}/+}{=} \mathcal{A}\left(E_1\right) \bullet \mathcal{A}\left(E_1\right) + \mathcal{A}\left(E_1\right) \bullet \mathcal{A}\left(E_2\right) + \mathcal{A}\left(E_2\right) \bullet \mathcal{A}\left(E_1\right) \\
&\qquad + \mathcal{A}\left(E_2\right) \bullet \mathcal{A}\left(E_2\right) \\
&\overset{\bullet\text{ is commutative}}{=} \left\| \mathcal{A}\left(E_1\right) \right\|^2 + 2 \cdot \mathcal{A}\left(E_1\right) \bullet \mathcal{A}\left(E_2\right) + \left\| \mathcal{A}\left(E_2\right) \right\|^2 \\
&\overset{\mathcal{A}\text{ preserves length}}{=} \left\| E_1 \right\|^2 + 2 \cdot \mathcal{A}\left(E_1\right) \bullet \mathcal{A}\left(E_2\right) + \left\| E_2 \right\|^2 \\
&= 2 + 2 \cdot \mathcal{A}\left(E_1\right) \bullet \mathcal{A}\left(E_2\right)\ .
\end{aligned}$$

It follows that $\mathcal{A}\left(E_1\right) \bullet \mathcal{A}\left(E_2\right) = 0$, and we are done. ■

23. Unitary Matrices

Last modified on December 8, 2018

23.1 General Unitary Matrices

Terminology 23.1.1

A **unitary matrix** is a *square* isometry. Unitary matrices play a central role in matrix theory.

Example 23.1.2

For example, $\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$, $\mathcal{I}_5$, $\begin{bmatrix} 1 & 0 & 0 \\ 0 & \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \\ 0 & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \end{bmatrix}$ and $\begin{bmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{bmatrix}$ (for any θ) are unitary matrices.

Test Your Comprehension 23.1.3

Argue that every unitary matrix is invertible, and that the inverse of a unitary matrix is its transpose.

Exercise 23.1.4

Verify that the following statements are equivalent for an $n \times n$ matrix $\mathcal{U}$.

1. $\mathcal{U}$ is a unitary matrix.
2. $\mathcal{U}^T\mathcal{U} = \mathcal{I} = \mathcal{U}\mathcal{U}^T$.
3. $\mathcal{U}^T$ is a unitary matrix.
4. $\mathcal{U}$ is invertible and $\mathcal{U}^{-1} = \mathcal{U}^T$.

5. $\mathcal{U}$ is invertible and $\mathcal{U}^{-1}$ is a unitary matrix.

6. The columns of $\mathcal{U}$ form an orthonormal coordinate system of $\mathbb{R}^n$.

7. The rows of $\mathcal{U}$ form an orthonormal coordinate system of $\mathbb{R}^n$.

Observation 23.1.5

Note that while the columns of a non-square isometry form an orthonormal list, the rows of an isometry may not be mutually orthogonal. For example, consider the isometry

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

Hint: Consider $(A \boxplus B)^T (A \boxplus B)$.

Test Your Comprehension 23.1.6

Argue that a direct sum $A \boxplus B$ of two unitary matrices is also a unitary matrix.

Hint: Consider $(AB)^T (AB)$.

Test Your Comprehension 23.1.7

Argue that a product of two $n \times n$ unitary matrices is also a unitary matrix.

Terminology 23.1.8

Matrix $\mathcal{B}$ is said to be **unitarily similar** to a matrix $\mathcal{A}$, exactly when there is a unitary matrix $\mathcal{U}$ such that

$$\mathcal{B} = \mathcal{U}^{-1} \mathcal{A} \mathcal{U} \quad (= \mathcal{U}^T \mathcal{A} \mathcal{U}) .$$

In such a case we write $\mathcal{A} \simeq \mathcal{B}$.

Test Your Comprehension 23.1.9

1. Argue that $\simeq$ is a particular kind of a similarity and a particular kind of a congruence at the same time.

2. Show that the relation $\simeq$ is reflexive, symmetric and transitive.

Hint: TYC 22.2.9. To establish the last claim, apply the matrix to the standard coordinate system of the departure space.

Test Your Comprehension 23.1.10 **Unitary matrices are exactly the orthonormal-coordinate-system-preserving matrices**

Argue that a matrix is unitary if and only if it maps any orthonormal coordinate system of its “departure space” to an orthonormal coordinate system of its “destination space”.

Theorem 23.1.11

If $X_1, X_2, \ldots, X_n$ and $Y_1, Y_2, Y_3, \ldots, Y_n$ are two orthonormal coordinate systems of $\mathbb{R}^n$, then there *exists exactly one* unitary matrix $\mathcal{U} \in \mathbb{M}_n$ such that

$$\mathcal{U}(X_i) = Y_i, \quad \text{for all} \quad i. \tag{23.1}$$

Proof of Theorem 23.1.11. Let

$$\mathcal{A} := \begin{bmatrix} X_1 & X_2 & X_3 & \ldots & X_n \end{bmatrix} \quad \text{and} \quad \mathcal{B} := \begin{bmatrix} Y_1 & Y_2 & Y_3 & \ldots & Y_n \end{bmatrix}.$$

Then $\mathcal{A}$ and $\mathcal{B}$ are unitary matrices (Exercise 23.1.4), and the condition (23.1) can be rewritten as

$$\mathcal{U}\mathcal{A} = \mathcal{B},$$

or as

$$\mathcal{U} = \mathcal{A}^{-1}\mathcal{B}.$$

It is obvious that $\mathcal{U} := \mathcal{A}^{-1}\mathcal{B}$ is the only matrix satisfying such a condition, and this matrix is unitary by Exercise 23.1.4 and TYC 23.1.7. ■

Exercise 23.1.12 ☞ 2×2 **Unitary Matrices**

Verify the following claims.

1. The unitary matrices in $\mathbb{M}_2$ are exactly the matrices that can be expressed in one of the following four forms:

$$\begin{bmatrix} a & \sqrt{1-a^2} \\ -\sqrt{1-a^2} & a \end{bmatrix}, \quad \begin{bmatrix} a & -\sqrt{1-a^2} \\ \sqrt{1-a^2} & a \end{bmatrix}, \quad \begin{bmatrix} a & -\sqrt{1-a^2} \\ -\sqrt{1-a^2} & -a \end{bmatrix}, \quad \begin{bmatrix} a & \sqrt{1-a^2} \\ \sqrt{1-a^2} & -a \end{bmatrix},$$

   with $a \in [-1, 1]$.

2. The unitary matrices in $\mathbb{M}_2$ are exactly the matrices that can be expressed in one of the following two forms:

$$\begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix}, \qquad \begin{bmatrix} \cos\theta & \sin\theta \\ \sin\theta & -\cos\theta \end{bmatrix},$$

   with $\theta \in \mathbb{R}$.

Comment 23.1.13 : A visit to the parallel universe

23.1.1 — Householder Unitaries

We have observed previously that every elementary $n \times n$ matrix has the form $\mathcal{I}_n + X \boxtimes Y$ for some $X, Y \in \mathbb{R}^n$. Now we shall explore the unitary matrices that can be expressed in such a form. Obviously, when either X or Y is null, the matrix $\mathcal{I}_n + X \boxtimes Y$ is the identity matrix, and so is unitary. This is not the only possible scenario.

Terminology 23.1.14

A unitary $n \times n$ matrix of the form $\mathcal{I}_n + X \boxtimes Y$ and *distinct from* $\mathcal{I}_n$ is said to be a **Householder matrix**.

Lemma 23.1.15

For every unit n-tuple X the matrix $\mathcal{I}_n - 2(X \boxtimes X)$ is a Householder unitary.

A proof of Lemma 23.1.15 is presented in the appendix to the chapter.

Theorem 23.1.16

Every Householder unitary in $\mathbb{M}_n$ has the form $\mathcal{I}_n - 2(X \boxtimes X)$ for some *unit* n-tuple X.

Therefore, matrices of this form are exactly the Householder unitaries in $\mathbb{M}_n$.

A proof of Theorem 23.1.16 is presented in the appendix to the chapter.

Notation 23.1.17

When X is a unit tuple, the Householder unitary $\mathcal{I} - 2(X \boxtimes X)$ is denoted by $\mathcal{H}_X$.

The main goal of this section is to demonstrate that the collection of Householder unitaries is plentiful enough to guarantee that for any two distinct tuples X and Y of equal length there is a (unique!) Householder unitary that maps X to Y. This is the content of Theorem 23.1.22 and TYC 23.1.23.

Test Your Comprehension 23.1.18

Verify the following identities.

1. $\mathcal{H}_{-X} = \mathcal{H}_X$.
2. $\mathcal{H}_X^{-1} = \mathcal{H}_X^T = \mathcal{H}_X$.

In particular, all Householder unitaries are symmetric.

Exercise 23.1.19 ☞ **Fixed tuples for Householder unitaries**

Argue that the following statements are equivalent.

1. $\mathcal{H}_X(Y) = Y$.
2. Y is orthogonal to X.

Lemma 23.1.20 ☞ **If two Householder unitaries agree at a tuple that they do not send to itself, then they are equal**

If $\mathcal{H}_X(Y_{\circ}) = \mathcal{H}_Z(Y_{\circ}) \neq Y_{\circ}$, for *some* $Y_{\circ}$, then

$$\mathcal{H}_X = \mathcal{H}_Z \, .$$

A proof of Lemma 23.1.20 is presented in the appendix to the chapter.

Exercise 23.1.21

Give a concrete example to show that Lemma 23.1.20 becomes false if the condition $\mathcal{H}_Z(Y_{\circ}) \neq Y_{\circ}$ is omitted.

Theorem 23.1.22

If Y and Z are *distinct* unit tuples, then

$$\mathcal{H} := \mathcal{H}_{\frac{1}{\|Y-Z\|}\cdot(Y-Z)}$$

is the unique Householder unitary such that

$$\mathcal{H}(Y) = Z \, .$$

A proof of Theorem 23.1.22 is presented in the appendix to the chapter.

Test Your Comprehension 23.1.23

Argue that for any two distinct n-tuples X and Y that have the same length, there is exactly one Householder unitary that maps X to Y.

23.2 Permutation Matrices

Definition 23.2.1

A matrix function $P : \mathbb{R}^5 \longrightarrow \mathbb{R}^5$ is a **permutation matrix** when its columns are exactly (all of) the standard basis vectors of $\mathbb{R}^5$ appearing in some order (not necessarily the usual one).

Test Your Comprehension 23.2.2

Argue that the permutation matrices are unitary.

Example 23.2.3

For example, $\begin{bmatrix} 0&1&0&0&0\\ 0&0&0&0&1\\ 0&0&0&1&0\\ 1&0&0&0&0\\ 0&0&1&0&0 \end{bmatrix}$ is a permutation matrix, while $\begin{bmatrix} 0&1&0&0&0\\ 0&0&0&0&0\\ 0&0&0&1&0\\ 1&0&0&0&0\\ 0&0&1&0&1 \end{bmatrix}$ is not.

Test Your Comprehension 23.2.4

Argue that every swap * is a permutation matrix.

*Recall that a swap is an elementary matrix.

Test Your Comprehension 23.2.5

Verify that the following statements are equivalent for an $n \times n$ matrix $\mathcal{A}$.

1. $\mathcal{A}$ is a permutation matrix.
2. $\mathcal{A}$ is invertible, and it sends every standard basis n-tuple to a standard basis n-tuple.

Hint: The injectivity of $\mathcal{A}$ dictates that no two columns of $\mathcal{A}$ are identical, so that no two standard basis tuples are sent to the same standard basis tuple.

Test Your Comprehension 23.2.6

Argue that a permutation matrix produces its outputs by reordering the entries of the inputs according to a fixed pattern.

Test Your Comprehension 23.2.7

Argue that a product of $n \times n$ permutation matrices is a permutation matrix.

Hint: A product of matrices is their composition. Use TYC 23.2.5.

Exercise 23.2.8

Verify that a direct sum $\boxplus$ of two permutation matrices is a permutation matrix.

Test Your Comprehension 23.2.9

Argue that by performing some number of column swaps on a permutation matrix one can always arrive at the identity matrix.

Don't forget to deal with the case that the original matrix is the identity matrix.

Test Your Comprehension 23.2.10

Argue that the following statements are equivalent for an $n \times n$ matrix $\mathcal{A}$.

1. $\mathcal{A}$ is a permutation matrix.
2. Every column and every row of $\mathcal{A}$ has exactly one non-zero entry, and that entry is 1.
3. A has exactly n non-zero entries, all of which are 1, and $\mathcal{A}$ has no null rows and no null columns.

Test Your Comprehension 23.2.11

Argue that the following statements are equivalent for a matrix $\mathcal{A}$.

1. $\mathcal{A}$ is a permutation matrix.
2. $\mathcal{A}^T$ is a permutation matrix.

Hint: TYC 23.2.10.

Test Your Comprehension 23.2.12

Argue that every permutation matrix is a unitary matrix, and so are its inverse and its transpose, which are also permutation matrices.

Hint: TYC 23.2.2 and TYC 23.2.11.

Theorem 23.2.13

Every permutation matrix can be expressed as a product of swaps.*

*Swaps are elementary matrices.

Please keep in mind that a swap is a product of a list of swaps, with a single swap on the list!

Test Your Comprehension 23.2.14

Argue that the permutation matrices are exactly the matrices that can be expressed as products of swaps.

Hint: TYC's 23.2.4 and 23.2.7.

Proof of Theorem 23.2.13. Performing column swaps on a matrix is equivalent to multiplying the matrix on the right by an appropriate swap matrix.

Given an $n \times n$ permutation matrix $\mathcal{P}$, we know that $\mathcal{P}^{-1}$ a permutation matrix

(TYC 23.2.12). So there exist swap matrices $\mathcal{S}_1, \mathcal{S}_2, \mathcal{S}_3, \ldots, \mathcal{S}_k$ such that

$$\mathcal{P}^{-1}\mathcal{S}_1\mathcal{S}_2\mathcal{S}_3\cdots\mathcal{S}_k = \mathcal{I} \quad \text{(TYC 23.2.9)} .$$

It follows that

$$\mathcal{S}_1\mathcal{S}_2\mathcal{S}_3\cdots\mathcal{S}_k = \left(\mathcal{P}^{-1}\right)^{-1} = \mathcal{P} . \qquad \blacksquare$$

Exercise 23.2.15

Argue that the following claims are equivalent when $\mathcal{D} \in \mathbb{M}_n$ is a diagonal matrix.

1. $\mathcal{C}$ is a diagonal matrix obtained by a "shuffling" of the diagonal entries of $\mathcal{D}$ in some fashion.

2. $\mathcal{C} = \mathcal{P}^T\mathcal{D}\mathcal{P}$, for some permutation matrix $\mathcal{P}$.

Hint: Exercise 10.2.12 and Theorem 23.2.13.

Terminology 23.2.16

Matrices $\mathcal{A}$ and $\mathcal{B}$ in $\mathbb{M}_n$ are said to be **permutationally similar** if there exists a permutation matrix $\mathcal{P}$ such that

$$\mathcal{B} = \mathcal{P}^T\mathcal{A}\mathcal{P} \quad (= \mathcal{P}^{-1}\mathcal{A}\mathcal{P}) .$$

Test Your Comprehension 23.2.17

Argue that the relation of being permutationally similar is reflexive, symmetric and transitive, in the sense of Exercise 8.2.2.

Theorem 23.2.18

Diagonal matrices $\mathcal{D}$ and $\mathcal{C}$ are unitarily similar exactly when they are permutationally similar; i.e. exactly when one can be obtained from the other by a reordering of the diagonal entries.

Proof of Theorem 23.2.18. Since permutation matrices are unitary, we need to verify only the forward implication. Suppose that $\mathcal{C} = \mathcal{U}^{-1}\mathcal{D}\mathcal{U}$ for some unitary matrix $\mathcal{U}$.

Let us begin by recalling that the rank of a diagonal matrix $\mathcal{A}$ is the number of indices i such that $\mathcal{A}[\![i,i]\!] \neq 0$.Thus by the Rank-Nullity theorem, the nullity of $\mathcal{A}$ is the number of zero entries on its diagonal. Since equivalent matrices have the same rank and the same nullity, it must be that equivalent diagonal matrices have the same number of zero entries on their diagonals.

What we would like to show, in order to complete the proof, is that any scalar

α appears as many times on the diagonal of $\mathcal{C}$ as it does on the diagonal of $\mathcal{D}$.

For any scalar α,

$$\mathcal{U}^{-1}(\mathcal{D}-\alpha\mathcal{I})\mathcal{U}=\mathcal{U}^{-1}\mathcal{D}\mathcal{U}-\alpha\mathcal{U}^{-1}\mathcal{U}=\mathcal{C}-\alpha\mathcal{I}\ .$$

This shows that the diagonal matrices $\mathcal{D}-\alpha\mathcal{I}$ and $\mathcal{C}-\alpha\mathcal{I}$ are unitarily similar, and so have the same number of zeros on their diagonals. The number of zeros on the diagonals of $\mathcal{D}-\alpha\mathcal{I}$ and $\mathcal{C}-\alpha\mathcal{I}$ is the number of times α appears on the diagonals of $\mathcal{D}$ and $\mathcal{C}$ respectively. ■

Notation 23.2.19

Consider the function $f_{[4]}:\mathbb{R}^4\longrightarrow\mathbb{R}^4$ defined by the formula:

$$f_{[4]}(x_1,x_2,x_3,x_4):=(x_1-x_2)(x_1-x_3)(x_1-x_4)(x_2-x_3)(x_2-x_4)(x_3-x_4).$$

$f_{[4]}(x_1,x_2,x_3,x_4)$ is the product of all possible factors of the form (x_i-x_j), with $i<j$.

Functions $f_{[n]}$ can be defined similarly for all natural $n>1$.

Observation 23.2.20

Since $f_{[4]}$ is not constantly zero, $f_{[4]}$ and $-f_{[4]}$ are NOT equal as functions; ($f_{[4]}=-f_{[4]}$ would entail $2f_{[4]}=\mathcal{O}$, i.e. $f_{[4]}=\mathcal{O}$.)

Exercise 23.2.21

Verify that for any swap $\mathcal{S}\in\mathbb{M}_n$,

$$f_n\circ\mathcal{S}=-f_n\ .$$

Hint: ILLUSTRATION

Theorem 23.2.22

Every permutation matrix falls into exactly one of the following two categories:

(I) those expressible as a composition of an odd number of swaps*;

(II) those expressible as a composition of an even number of swaps.

*Swaps are elementary matrices.

Proof of Theorem 23.2.22. Suppose that $\mathcal{P}$ is an $n \times n$ permutation matrix. Then $\mathcal{P}$ is a product of swaps (Theorem 23.2.13), say

$$\mathcal{P} = \mathcal{S}_1 \mathcal{S}_2 \mathcal{S}_3 \cdots \mathcal{S}_k .$$

BY TYC 23.2.21 we have

$$\begin{aligned}
f_{[n]} \circ \mathcal{P} &= f_{[n]} \circ \mathcal{S}_1 \circ \mathcal{S}_2 \circ \mathcal{S}_3 \circ \cdots \circ \mathcal{S}_k \\
&= (-1)\, f_{[n]} \circ \mathcal{S}_2 \circ \mathcal{S}_3 \circ \cdots \circ \mathcal{S}_k \\
&= (-1)^2\, f_{[n]} \circ \mathcal{S}_3 \circ \cdots \circ \mathcal{S}_k \\
&\;\;\vdots \\
&= (-1)^{k-1}\, f_{[n]} \circ \mathcal{S}_k \\
&= (-1)^{k}\, f_{[n]} .
\end{aligned}$$

Equality $f_{[n]} \circ \mathcal{P} = f_{[n]}$ happens exactly when $\mathcal{P}$ can be written as a product of an even number of swaps.

Equality $f_{[n]} \circ \mathcal{P} = -f_{[n]}$ happens exactly when $\mathcal{P}$ can be written as a product of an odd number of swaps.

Since $f_{[n]} \neq -f_{[n]}$, exactly one of the equalities $f_{[n]} \circ \mathcal{P} = f_{[n]}$ and $f_{[n]} \circ \mathcal{P} = -f_{[n]}$ takes place for each permutation $\mathcal{P}$. ■

Terminology 23.2.23

Based on Theorem 23.2.22 we can classify all permutation matrices as being either **even** or **odd** (but never both!).

Let us define a **sign of a permutation** so as to indicate the distinction:

$$\operatorname{Sign}(\mathcal{P}) := \begin{cases} 1 & \text{if } \mathcal{P} \text{ is an even permutation} \\ -1 & \text{if } \mathcal{P} \text{ is an odd permutation} \end{cases}$$

Then for $\mathcal{P} \in \mathbb{M}_n$,

$$f_{[n]} \circ \mathcal{P} = \operatorname{Sign}(\mathcal{P}) \cdot f_{[n]} .$$

Permutations and their signs will play a central role in the theory of determinants that we will be exploring later.

23.3 (PD) LU Factorization

23.4 Appendix: Exiled Proofs

Proof of Lemma 23.1.15. To demonstrate that $\mathcal{I}_n - 2(X \boxtimes X)$ is a unitary matrix it is sufficient to verify the following identity (TYC 3.4.2):

$$\Big(\mathcal{I}_n - 2(X \boxtimes X)\Big)^T \Big(\mathcal{I}_n - 2(X \boxtimes X)\Big) = \mathcal{I}_n .$$

Note that

$$\Big(\mathcal{I}_n - 2(X \boxtimes X)\Big)^T = \mathcal{I}_n^T - 2(X \boxtimes X)^T = \mathcal{I}_n - 2(X \boxtimes X) \ ,$$

and that

$$(X \boxtimes X)(X \boxtimes X) = (X \bullet X)(X \boxtimes X) = \left\|X\right\|^2 (X \boxtimes X) = X \boxtimes X \ .$$

Therefore

$$\Big(\mathcal{I}_n - 2(X \boxtimes X)\Big)^T \Big(\mathcal{I}_n - 2(X \boxtimes X)\Big) = \Big(\mathcal{I}_n - 2(X \boxtimes X)\Big) \Big(\mathcal{I}_n - 2(X \boxtimes X)\Big)$$

$$\overset{\text{distribute}}{=} \mathcal{I}_n - 2(X \boxtimes X) - 2(X \boxtimes X) + 4(X \boxtimes X)(X \boxtimes X)$$

$$= \mathcal{I}_n - 4(X \boxtimes X) + 4(X \boxtimes X) = \mathcal{I}_n ,$$

as required. ■

Proof of Theorem 23.1.16. Suppose $\mathcal{A} = \mathcal{I}_n + U \boxtimes W$ defines a Householder matrix. Then $U, W \neq \mathbb{0}$, and so (TYC 15.2.5) we can write

$$\mathcal{A} = \mathcal{I}_n + \left(\frac{1}{\left\|U\right\|} \cdot U\right) \boxtimes \Big(\left\|U\right\| \cdot W \Big) \ .$$

In other words, we can express $\mathcal{A}$ as $\mathcal{I}_n + X \boxtimes Y$, where X is a unit tuple (and Y is non-null, of course). Note that

$$X \bullet X = \left\|X\right\|^2 = 1 \ .$$

Using the properties of rank one matrices developed in section 15, we can make the following calculations.

$$\mathcal{I}_n = (\mathcal{I}_n + X \boxtimes Y)^T (\mathcal{I}_n + X \boxtimes Y) = (\mathcal{I}_n + Y \boxtimes X)(\mathcal{I}_n + X \boxtimes Y)$$

$$\overset{\text{distribute}}{=} \mathcal{I}_n + X \boxtimes Y + Y \boxtimes X + (Y \boxtimes X)(X \boxtimes Y)$$

$$= \mathcal{I}_n + X \boxtimes Y + Y \boxtimes X + (X \bullet X) \cdot Y \boxtimes Y$$

$$= \mathcal{I}_n + X \boxtimes Y + Y \boxtimes X + Y \boxtimes Y$$

$$= \mathcal{I}_n + X \boxtimes Y + \left(\frac{1}{2} \cdot Y\right) \boxtimes Y + Y \boxtimes X + Y \boxtimes \left(\frac{1}{2} \cdot Y\right)$$

$$= \mathcal{I}_n + \left(X + \frac{1}{2} \cdot Y\right) \boxtimes Y + Y \boxtimes \left(X + \frac{1}{2} \cdot Y\right) .$$

It follows that

$$\left(X + \frac{1}{2} \cdot Y\right) \boxtimes Y + Y \boxtimes \left(X + \frac{1}{2} \cdot Y\right) = \mathcal{O},$$

or equivalently that

$$\left(X + \frac{1}{2} \cdot Y\right) \boxtimes Y = -Y \boxtimes \left(X + \frac{1}{2} \cdot Y\right) .$$

This is an equality of two rank one matrices, and we know that $Y \neq \mathbb{0}$.

If it were the case that $X + \frac{1}{2} \cdot Y \neq \mathbb{0}$, then by Theorem 15.2.12 there would exist a non-zero scalar β such that

$$\left(X + \frac{1}{2} \cdot Y\right) = -\beta \cdot Y \quad \text{and} \quad Y = \frac{1}{\beta} \cdot \left(X + \frac{1}{2} \cdot Y\right) .$$

These two equalities would be rewritten as

$$X = \left(-\beta - \frac{1}{2}\right) \cdot Y \quad \text{and} \quad X = \left(\beta - \frac{1}{2}\right) \cdot Y .$$

Since $X, Y \neq \mathbb{0}$, the equalities lead to the conclusion

$$-\beta - \frac{1}{2} = \beta - \frac{1}{2} ,$$

which indicates that $\beta = 0$, forcing a contradiction.

Hence it must be that $X + \frac{1}{2} \cdot Y = \mathbb{O}$; i.e. $Y = -2X$, which tells us that

$$\mathcal{A} = \mathcal{I}_n - 2 \cdot X \boxtimes X ,$$

as required. ∎

Proof of Lemma 23.1.20. If $X, Y_{\circ}, Z$ are as described, then

$$\begin{array}{rlll} Y_{\circ} \neq & \mathcal{H}_X(Y_{\circ}) & = (\mathcal{I} - 2\, X \boxtimes X)\,(Y_{\circ}) = Y_{\circ} - 2(Y_{\circ} \bullet X)\, X \\ & \Vert & \\ Y_{\circ} \neq & \mathcal{H}_Z(Y_{\circ}) & = (\mathcal{I} - 2\, Z \boxtimes Z)\,(Y_{\circ}) = Y_{\circ} - 2(Y_{\circ} \bullet Z)\, Z\ . \end{array}$$

Therefore

$$(Y_{\circ} \bullet X)\, X = (Y_{\circ} \bullet Z)\, Z \neq \mathbb{O}\ . \tag{23.2}$$

Thus, keeping in mind that X and Z have length 1, we have

$$|Y_{\circ} \bullet X| = \big\|(Y_{\circ} \bullet X)\, X\big\| = \big\|(Y_{\circ} \bullet Z)\, Z\big\| = |Y_{\circ} \bullet Z| \neq 0\ .$$

Therefore

$$Y_{\circ} \bullet X = \pm Y_{\circ} \bullet Z \neq 0\ .$$

Inserting this into (23.2) we arrive at

$$X = \pm Z\ ,$$

and in that case,

$$\mathcal{H}_X = \mathcal{H}_Z \quad \text{(TYC 23.1.18)}\ .$$

∎

Proof of Theorem 23.1.22. Let us write $X = \frac{1}{\|Y-Z\|} \cdot (Y - Z)$ and compute:

$$\begin{aligned} \mathcal{H}(Y) &= \Big(\mathcal{I} - 2(X \boxtimes X)\Big)(Y) = Y - 2(Y \bullet X)X \\ &= Y - 2\left(Y \bullet \frac{1}{\big\|Y - Z\big\|} \cdot (Y - Z)\right) \frac{1}{\big\|Y - Z\big\|} \cdot (Y - Z) \\ &= Y - \frac{2}{\big\|Y - Z\big\|^2}\Big(Y \bullet (Y - Z)\Big) \cdot (Y - Z). \end{aligned}$$

To establish the claim that $\mathcal{H}(Y) = Z$ it is sufficient to show that

$$\frac{2}{\big\|Y - Z\big\|^2}\Big(Y \bullet (Y - Z)\Big) = 1\ ,$$

i.e. that

$$2Y \bullet (Y - Z) = \left\| Y - Z \right\|^2 \ . \tag{23.3}$$

Let us manipulate the expressions appearing in this desired equality (23.3).

$$2Y \bullet (Y - Z) = 2Y \bullet Y - 2Y \bullet Z = 2\left\| Y \right\|^2 - 2Y \bullet Z = 2 - 2Y \bullet Z \ .$$

$$\begin{aligned}\left\| Y - Z \right\|^2 &= (Y - Z) \bullet (Y - Z) = Y \bullet Y - Y \bullet Z - Z \bullet Y + Z \bullet Z \\ &= \left\| Y \right\|^2 - 2Y \bullet Z + \left\| Z \right\|^2 = 1 - 2Y \bullet Z + 1 = 2 - 2Y \bullet Z \ .\end{aligned}$$

It is now obvious that (23.3) holds, and therefore $\mathcal{H}(Y) = Z$.

The fact that $\mathcal{H}$ is *the only* Householder unitary with this property follows immediately from Lemma 23.1.20. If $\mathcal{K}$ is another such, then

$$\mathcal{K}(Y) = \mathcal{H}(Y) = Z \neq Y \ ,$$

and hence $\mathcal{K} = \mathcal{H}$. ■

24. Orthonormality

Last modified on December 8, 2018

24.1 Gram-Schmidt Process

Theorem 24.1.1 ☞ **Widening matrices with equal ranges**

If

$$\mathit{Range}\left(\mathcal{A}_{n\times m}\right) = \mathit{Range}\left(\mathcal{B}_{n\times k}\right) \ ,$$

Then

$$\mathit{Range}\left(\left[\mathcal{A} \ \ \mathcal{M}\right]\right) = \mathit{Range}\left(\left[\mathcal{B} \ \ \mathcal{M}\right]\right) \ ,$$

for any matrix $\mathcal{M} \in \mathbb{M}_{n\times p}$.

Proof of Theorem 24.1.1. Since the roles of $\mathcal{A}$ and $\mathcal{B}$ can be reversed, it is sufficient to demonstrate that

$$\mathit{Range}\left[\mathcal{A} \ \ \mathcal{M}\right] \subseteq \mathit{Range}\left[\mathcal{B} \ \ \mathcal{M}\right] .$$

Since $\mathit{Range}(\mathcal{A}) = \mathit{Range}(\mathcal{B})$, there exists a matrix $\mathcal{C} \in \mathbb{M}_{k\times m}$ such that

$$\mathcal{A} = \mathcal{B}\mathcal{C} \quad \text{(Thm. 13.1.2)} .$$

Then by the fundamental formula for partitioned matrix multiplication

$$\left[\mathcal{A} \ \ \mathcal{M}\right]_{n\times(m|p)} = \left[\mathcal{B} \ \ \mathcal{M}\right]_{n\times(k|p)} \left[\begin{smallmatrix} \mathcal{C} & \mathcal{O} \\ \mathcal{O} & \mathcal{I}_p \end{smallmatrix}\right]_{(k|p)\times(m|p)} .$$

By the range inclusion factorization (Thm. 13.1.2), we can conclude that

$$\mathit{Range}\left[\mathcal{A} \ \ \mathcal{M}\right] \subseteq \mathit{Range}\left[\mathcal{B} \ \ \mathcal{M}\right] . \qquad \blacksquare$$

Test Your Comprehension 24.1.2

If
$$Span\left(X_1, X_2, X_3, \ldots, X_m\right) = Span\left(Y_1, Y_2, Y_3, \ldots, Y_k\right) ,$$
then
$$Span\left(X_1, X_2, X_3, \ldots, X_m, Z\right) = Span\left(Y_1, Y_2, Y_3, \ldots, Y_k, Z\right) .$$

Observation 24.1.3

Suppose that we would like to upgrade a given list $X_1, \ldots, X_k, Z$ of tuples to *an orthonormal list having the same span*, and we are willing to trade in Z for another tuple.

Obviously we cannot always succeed. For example, if $X_1, \ldots, X_k$ is not an orthonormal list already, changing Z alone will not orthonormalize the X_i's.

What if $X_1, \ldots, X_k$ is an orthonormal list? Is that enough? The answer is still "No". Let us write $\boldsymbol{W}$ for the span of $X_1, \ldots, X_k, Z$.

If our Z is a linear combination of the X_i's, then we can completely remove it from the list without changing the span (Thm. 14.1.3). This means that the X_i's form a coordinate system of $\boldsymbol{W}$, and the dimension of $\boldsymbol{W}$ is k.

If we could replace Z with Y to produce an orthonormal list $X_1, \ldots, X_k, Y$ with the same span, then
$$Span\left(X_1, \ldots, X_k, Y\right) = Span\left(X_1, \ldots, X_k, Z\right) = \boldsymbol{W} .$$

Since orthonormal lists are linearly independent (Thm. 22.2.5), this would state that the $k+1$ tuples $X_1, \ldots, X_k, Y$ form a coordinate system of the k-dimensional $\boldsymbol{W}$, which is not possible (Thm. 18.3.23).

So, to have any hope of success we must start with a list $X_1, \ldots, X_k, Z$ where $X_1, \ldots, X_k$ are orthonormal and Z is NOT a linear combination of the X_i's. Is that enough to guarantee success? This time the answer is "Yes!".

Lemma 24.1.4 ☞ **Gram-Schmidt Replacement Step**

The following conditions are equivalent for n-tuples.

1. $X_1, \ldots, X_k$ is an orthonormal list and Y is not in its span.

2. There is an n-tuple Y such that $X_1, \ldots, X_k, Y$ is an orthonormal list and
$$Span\left(X_1, \ldots, X_k, Y\right) = Span\left(X_1, \ldots, X_k, Z\right) .$$

A proof of Lemma 24.1.4 is presented in the appendix to the chapter. This proof includes a practical algorithm for the construction of a required Y.

Theorem 24.1.5 ☞ **Gram-Schmidt Orthonormal Replacement Process**

If $X_1, X_2, X_3, \ldots, X_k$ is a *linearly independent* list in $\mathbb{R}^n$, then there is an *orthonormal* list $Y_1, Y_2, Y_3, \ldots, Y_k$ such that

$$\begin{aligned} Span\left(X_1\right) &= Span\left(Y_1\right) \\ Span\left(X_1, X_2\right) &= Span\left(Y_1, Y_2\right) \\ Span\left(X_1, X_2, X_3\right) &= Span\left(Y_1, Y_2, Y_3\right) \\ &\vdots \\ Span\left(X_1, X_2, X_3, \ldots, X_k\right) &= Span\left(Y_1, Y_2, Y_3, \ldots, Y_k\right). \end{aligned}$$

A proof of Theorem 24.1.5 is presented in the appendix to the chapter. This proof includes a practical algorithm for the construction of $Y_1, Y_2, Y_3, \ldots, Y_k$.

Test Your Comprehension 24.1.6

For every *injective* matrix $\mathcal{A} \in \mathbb{M}_{n\times m}$ there is an isometry $\mathcal{B} \in \mathbb{M}_{n\times m}$ such that, not only

$$Range\,(\mathcal{A}) = Range\,(\mathcal{B}) \ ,$$

but also

$$Range\,(\mathcal{A}_i) = Range\,(\mathcal{B}_i)\,, \quad \text{for all} \quad i\,,$$

where $\mathcal{A}_i$ is a matrix comprised of the first i columns of $\mathcal{A}$, and $\mathcal{B}_i$ is a matrix comprised of the first i columns of $\mathcal{B}$.

Exercise 24.1.7

Check that the columns of the matrix $\begin{bmatrix} -1 & 2 & 0 & -3 \\ -3 & 3 & -2 & -2 \\ 3 & 1 & -3 & 1 \\ 2 & 1 & -3 & 2 \\ -1 & -3 & -2 & 1 \end{bmatrix}$ are linearly independent (i.e. that the matrix is injective).

Consequently apply Gram-Schmidt process to find a corresponding orthonormal list.

Use of computer software is recommended.

24.1.1 — Orthonormal Coordinate Systems

Theorem 24.1.8 ☞ **Existence of the orthonormal bases**

Every non-trivial subspace of $\mathbb{R}^n$ has an orthonormal coordinate system.

In other words, every non-trivial subspace of $\mathbb{R}^n$ is a range of an isometry.

Proof of Theorem 24.1.8. Every non-trivial subspace $\boldsymbol{W}$ of $\mathbb{R}^n$ has a coordinate system. Being a linearly independent list that spans $\boldsymbol{W}$, this coordinate system can be replaced, via Gram-Schmidt orthonormal replacement process, with an orthonormal list that has the same span, i.e. spans $\boldsymbol{W}$. ∎

Exercise 24.1.9

Find orthonormal coordinate systems of the range and of the nullspace of the matrix

$$\begin{bmatrix} 148 & -\frac{623}{2} & 320 & 316 & \frac{753}{2} & 381 \\ -28 & 10 & 116 & 40 & -53 & 68 \\ 125 & -70 & -102 & 75 & 158 & -50 \\ -142 & \frac{639}{2} & -426 & -426 & -\frac{781}{2} & -497 \\ 10 & 108 & 60 & 6 & -118 & -4 \\ 58 & -\frac{295}{2} & 419 & 262 & \frac{321}{2} & 417 \end{bmatrix}.$$

Use of computer software is recommended.

Theorem 24.1.10 ☞ Orthonormal extension

Every orthonormal list in a subspace $\boldsymbol{W}$ of $\mathbb{R}^n$ is part of an orthonormal coordinate system of $\boldsymbol{W}$.

Proof of Theorem 24.1.10. Orthonormal lists are always linearly independent (Thm. 22.2.5). Given such a list, if it already spans $\boldsymbol{W}$, then it is itself an orthonormal coordinate system of $\boldsymbol{W}$.

If the list does not span $\boldsymbol{W}$, then Theorem 18.3.16 states that the list can be enlarged to a coordinate system of $\boldsymbol{W}$ (and Comment 18.3.17 indicates how this may be done in practice). Applying Gram-Schmidt orthonormal replacement process (Thm. 24.1.5) to this coordinate system produces an orthonormal coordinate system for $\boldsymbol{W}$. ∎

Test Your Comprehension 24.1.11 ☞ Enlarging isometries to unitaries

The following are equivalent for a matrix $\mathcal{A}$.

1. $\mathcal{A}$ is an isometry.

2. By inserting some columns into $\mathcal{A}$ it is possible to arrive at a unitary matrix.

Formula (25.3) and its derivation in the proof of Lemma 24.1.4 deserve attention. The formula leads to a practical way of constructing a non-null tuple that is orthogonal to all of the tuples in a given orthonormal list.

Furthermore, in deriving the formula we concurrently developed a practical way of discerning whether a given tuple is in the range of a given *isometry* $\mathcal{A}$, and if so, which (unique) input produces that tuple (see Comment 24.2.1).

⇩

Exercise 24.1.12 ☞ **Orthogonal extensions of orthonormal sets**

Suppose that $Z_1, Z_2, \ldots, Z_k$ is an orthonormal list of n-tuples.

Then for any $W \in \mathbb{R}^n$,

$$W - \left(W \bullet Z_1\right) Z_1 - \left(W \bullet Z_2\right) Z_2 - \cdots - \left(W \bullet Z_k\right) Z_k \,,$$

is a tuple that is orthogonal to every Z_i.

This tuple is non-null exactly when W is NOT in the span of $Z_1, Z_2, \ldots, Z_k$.

Hint: Emulate the derivation of (25.3).

Exercise 24.1.13 ☞ **Resolution in orthonormal sets**

Suppose W is in the span of an orthonormal list $Z_1, Z_2, \ldots, Z_k$. Then

$$W = \left(W \bullet Z_1\right) Z_1 + \left(W \bullet Z_2\right) Z_2 + \cdots + \left(W \bullet Z_k\right) Z_k \,.$$

Hint: Emulate the derivation of (25.3).

24.2 Isometries Revisited

Comment 24.2.1

Since orthonormal lists of tuples can be interpreted as lists of columns of isometries, we can re-interpret the results of Exercises 24.1.12 and 24.1.13 as statements about isometries.

These exercises provide us with a wonderful way of testing whether a given tuple is in the range of a given isometry, and if so, which (unique) input produces that tuple as an output.

With the columns of an isometry forming an orthonormal list $Z_1, Z_2, \ldots, Z_k$ of n-tuples, for any n-tuple W we simply calculate

$$\left(W \bullet Z_1\right) Z_1 + \left(W \bullet Z_2\right) Z_2 + \cdots + \left(W \bullet Z_k\right) Z_k \,. \tag{24.1}$$

If this linear combination is not equal to W, then, by Exercise 24.1.13, W is NOT in the span of $Z_1, Z_2, \ldots, Z_k$, i.e is NOT in the range of $\mathcal{A}$.

The expression (24.1) can be rewritten as

$$\mathcal{A}\begin{pmatrix} W\bullet Z_1 \\ W\bullet Z_2 \\ \vdots \\ W\bullet Z_k \end{pmatrix}, \text{ which equals } \mathcal{A}\mathcal{A}^T(W)\,, \tag{24.2}$$

because

$$\begin{pmatrix} W\bullet Z_1 \\ W\bullet Z_2 \\ \vdots \\ W\bullet Z_k \end{pmatrix} = \begin{bmatrix} \longleftarrow & Z_1 & \longrightarrow \\ & \vdots & \\ \longleftarrow & Z_k & \longrightarrow \end{bmatrix}(W)\,.$$

Let us record this fact.

If $\mathcal{A}$ is an *isometry* with (orthonormal) columns $C_1, C_2, \ldots, C_m$ then

$$\mathcal{A}\mathcal{A}^T(X) = \left(X \bullet C_1\right) C_1 + \left(X \bullet C_2\right) C_2 + \cdots + \left(X \bullet C_m\right) C_m\,. \tag{24.3}$$

Hence Exercise 24.1.13 states that

W is in the range of an *isometry* $\mathcal{A}$ exactly when $W = \mathcal{A}\mathcal{A}^T(W)$.

Test Your Comprehension 24.2.2 ☞ **Range formula for the isometries**

Argue that the following statements are equivalent for any *isometry* $\mathcal{A}$.

- $W \in \mathit{Range}\,(\mathcal{A})$.
- $W = \mathcal{A}\mathcal{A}^T(W)$.
- $W \in \mathit{Nullspace}\left(I - \mathcal{A}\mathcal{A}^T\right)$.

Conclude that for any *isometry* $\mathcal{A}$,

$$\mathit{Range}\,(\mathcal{A}) = \left\{\ W \mid W = \mathcal{A}\mathcal{A}^T(W)\ \right\} = \mathit{Nullspace}\left(\mathcal{I} - \mathcal{A}\mathcal{A}^T\right)\,.$$

Comment 24.2.3

Given an orthonormal coordinate system $\mathfrak{O}$ for a given subspace $\boldsymbol{W}$, we can form a corresponding isometry $\mathcal{A}$ whose columns are the tuples in $\mathfrak{O}$. Then

$$\boldsymbol{W} = \mathit{Range}\,(\mathcal{A}) = \left\{\ W \mid W = \mathcal{A}\mathcal{A}^T(W)\ \right\} = \mathit{Nullspace}\left(\mathcal{I} - \mathcal{A}\mathcal{A}^T\right)\,,$$

which offers a straight-forward way of verifying whether a given tuple belongs to $\boldsymbol{W}$: check whether it is annihilated by $\mathcal{I} - \mathcal{A}\mathcal{A}^T$.

Furthermore, resolving a member W of $\boldsymbol{W}$ with respect to $\mathfrak{O}$ (i.e. expressing W as a linear combination of the tuples in $\mathfrak{O}$) is equally easy: the required coefficients are the entries of $\mathcal{A}^T(W)$, since this is the input into $\mathcal{A}$ that produces the output W.

Let us contrast this with having a regular (non-orthonormal) coordinate system $\mathfrak{R}$ for $\boldsymbol{W}$. In order to test whether a given tuple W is in $\boldsymbol{W}$, we would have to solve the linear system

$$\mathcal{B}(X) = W ,$$

where the columns of $\mathcal{B}$ are the tuples in $\mathfrak{R}$. When the solution exists, W is in $\boldsymbol{W}$, and the entries of the solution are the coefficients needed to express W as a linear combination of the tuples in $\mathfrak{R}$.

Test Your Comprehension 24.2.4

If Y is in the range of an isometry $\mathcal{A}$, then $\mathcal{A}^T(Y)$ is the unique input that leads to the output Y.

Exercise 24.2.5

Test to see if the following matrices are isometries, and then test to see if the given tuples are in their range. For each tuple that is in the range, find the input that leads to that tuple as an output.

$$\begin{bmatrix} -\frac{1}{2} & \frac{1}{4} & \frac{1}{4\sqrt{3}} & -\frac{5}{\sqrt{78}} \\ \frac{1}{2} & -\frac{1}{4} & -\frac{1}{4\sqrt{3}} & -\frac{7}{\sqrt{78}} \\ -\frac{1}{2} & \frac{1}{4} & \frac{1}{4\sqrt{3}} & -\sqrt{\frac{2}{39}} \\ 0 & -\frac{1}{2} & \frac{\sqrt{3}}{2} & 0 \\ -\frac{1}{2} & -\frac{3}{4} & -\frac{\sqrt{3}}{4} & 0 \end{bmatrix}, \quad \begin{bmatrix} 0 & -\frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{3}} & -\frac{1}{\sqrt{31}} \\ \frac{2}{3} & -\frac{1}{3\sqrt{2}} & \frac{1}{\sqrt{3}} & -\frac{1}{\sqrt{31}} \\ \frac{2}{3} & \frac{\sqrt{2}}{3} & -\frac{1}{\sqrt{3}} & \frac{1}{\sqrt{31}} \\ \frac{1}{3} & -\frac{\sqrt{2}}{3} & 0 & \frac{2}{\sqrt{31}} \\ 0 & 0 & 0 & \frac{5}{\sqrt{31}} \end{bmatrix}, \quad \begin{bmatrix} 0 & -\sqrt{\frac{6}{17}} & -\frac{2}{\sqrt{85}} & \frac{1}{\sqrt{10}} \\ 0 & -\sqrt{\frac{6}{17}} & -\frac{2}{\sqrt{85}} & \frac{1}{\sqrt{10}} \\ -\frac{1}{\sqrt{6}} & -\frac{5}{\sqrt{102}} & \sqrt{\frac{5}{17}} & -\sqrt{\frac{2}{5}} \\ -\sqrt{\frac{2}{3}} & \sqrt{\frac{2}{51}} & \frac{9}{5\sqrt{85}} & \frac{4\sqrt{\frac{2}{5}}}{5} \\ -\frac{1}{\sqrt{6}} & \frac{1}{\sqrt{102}} & -\frac{38}{5\sqrt{85}} & -\frac{3\sqrt{\frac{2}{5}}}{5} \end{bmatrix};$$

$$\begin{pmatrix} \frac{31}{3}\left(-12-3\sqrt{62}+\sqrt{93}\right) \\ -\frac{31}{3}\left(12-3\sqrt{31}+\sqrt{62}+\sqrt{93}\right) \\ \frac{31}{3}\left(12+6\sqrt{31}+2\sqrt{62}+\sqrt{93}\right) \\ 248+31\sqrt{31}-\frac{62\sqrt{62}}{3} \\ 620 \end{pmatrix}, \quad \begin{pmatrix} -2 \\ -8 \\ -6 \\ 0 \\ 0 \end{pmatrix}, \quad \begin{pmatrix} -78-39\sqrt{3}+15\sqrt{78} \\ 78+39\sqrt{3}+21\sqrt{78} \\ -78-39\sqrt{3}+6\sqrt{78} \\ 78\left(4-3\sqrt{3}\right) \\ 39\left(14+3\sqrt{3}\right) \end{pmatrix}.$$

Test Your Comprehension 24.2.6 ☞ Subspaces are nullspaces

Every subspace of $\mathbb{R}^n$ is the nullspace of an $n \times n$ matrix.

Hint: Argue that every matrix range is a matrix nullspace. TYC 24.2.2 can be useful here. Don't forget about the trivial subspace.

25. Ortho-Projections

Last modified on December 8, 2018

25.1 Symmetric Idempotents

As we shall soon show, symmetric idempotent matrices form a vitally important class of matrices and are fundamental to matrix theory and linear algebra.

Test Your Comprehension 25.1.1

A direct sum $A \boxplus B$ of two symmetric idempotents is a symmetric idempotent.

Test Your Comprehension 25.1.2

Matrices

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}, \begin{bmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{bmatrix}, \begin{bmatrix} \frac{1}{3} & \frac{1}{3} & \frac{1}{3} \\ \frac{1}{3} & \frac{1}{3} & \frac{1}{3} \\ \frac{1}{3} & \frac{1}{3} & \frac{1}{3} \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \begin{bmatrix} \frac{1}{2} & 0 & \frac{1}{2} \\ 0 & 1 & 0 \\ \frac{1}{2} & 0 & \frac{1}{2} \end{bmatrix}, \begin{bmatrix} \frac{41}{169} & \frac{72}{169} & \frac{8}{169} \\ \frac{72}{169} & \frac{257}{338} & -\frac{9}{338} \\ \frac{8}{169} & -\frac{9}{338} & \frac{337}{338} \end{bmatrix}$$

are symmetric idempotents.

Test Your Comprehension 25.1.3

For any <u>*isometry*</u> $\mathcal{A}$, $\mathcal{A}\mathcal{A}^T$ is a symmetric idempotent matrix.

Later in this section we will show that all symmetric idempotent matrices have this form. For now we shall have to settle for demonstrating some of their wonderful properties without the benefit of knowing that all such matrices have this form.

[**A peek into the future**]

Non-null symmetric idempotent matrices are exactly the matrices of the form $\mathcal{A}\mathcal{A}^T$, where $\mathcal{A}$ is an isometry.

Theorem 25.1.4 ☞ **Ranges of idempotents**

A matrix $\mathcal{C}$ is *idempotent* exactly when it acts as an identity on its own range, in the sense that

$$\mathcal{C}(X) = X \ , \quad \text{for any} \quad X \in \mathit{Range}\,(\mathcal{C}) \ .$$

Consequently, for any *idempotent* matrix $\mathcal{C}$,

$$\mathit{Range}\,(\mathcal{C}) = \{ \ W \mid \mathcal{C}(W) = W \ \} = \mathit{Nullspace}\,(\mathcal{I} - \mathcal{C}) \ .$$

Proof of Theorem 25.1.4. If C is idempotent and $X \in \mathit{Range}\,(\mathcal{C})$, then $X = \mathcal{C}(Z)$, for some Z, and therefore

$$\mathcal{C}(X) = \mathcal{C}\big(\mathcal{C}(Z)\big) = \mathcal{C}^2(Z) = \mathcal{C}(Z) = X \ .$$

Conversely, if $\mathcal{C}$ is a matrix such that $\mathcal{C}(X) = X$ for every $X \in \mathit{Range}\,(\mathcal{C})$, then

$$\mathcal{C}\big(\mathcal{C}(Y)\big) = \mathcal{C}(Y) \ ,$$

for every Y, since $\mathcal{C}(Y) \in \mathit{Range}\,(\mathcal{C})$. This shows that $\mathcal{C} \circ \mathcal{C} = \mathcal{C}$, i.e. that $\mathcal{C}$ is idempotent.

The equality $\{ \ W \mid \mathcal{C}(W) = W \ \} = \mathit{Nullspace}\,(\mathcal{I} - \mathcal{C})$ follows from TYC 12.3.2. Let us verify that for any *idempotent* matrix $\mathcal{C}$,

$$\mathit{Range}\,(\mathcal{C}) = \{ \ W \mid \mathcal{C}(W) = W \ \} \ .$$

We have already demonstrated that every $X \in \mathit{Range}\,(\mathcal{C})$ is sent to itself by $\mathcal{C}$, and thus we have

$$\mathit{Range}\,(\mathcal{C}) \subseteq \{ \ W \mid \mathcal{C}(W) = W \ \} \ .$$

On the other hand, if $\mathcal{C}(W) = W$ then W is an output from $\mathcal{C}$ and hence is in the range of $\mathcal{C}$. This shows that

$$\mathit{Range}\,(\mathcal{C}) \supseteq \{ \ W \mid \mathcal{C}(W) = W \ \} \ .$$

Thus $\mathit{Range}\,(\mathcal{C}) = \{ \ W \mid \mathcal{C}(W) = W \ \}$. ■

Corollary 25.1.5 **Ranges and nullspaces of symmetric idempotents**

For any *symmetric idempotent* matrix $\mathcal{P}$,

$$Range(\mathcal{P}) = Nullspace(\mathcal{I} - \mathcal{P}) \ ,$$

and

$$Nullspace(\mathcal{P}) = \Big(Range(\mathcal{P})\Big)^{\perp} = Range(\mathcal{I} - \mathcal{P}) \ .$$

Proof of Corollary 25.1.5. The first equality comes from Theorem 25.1.4. The second is verified as follows.

$$\begin{aligned} Nullspace(\mathcal{P}) &\overset{\text{TYC 19.4.2}}{=} \Big(Range(\mathcal{P})\Big)^{\perp} \\ &= \Big(Nullspace(\mathcal{I} - \mathcal{P})\Big)^{\perp} \\ &\overset{\text{TYC's 8.4.4 \& 19.4.2}}{=} Range(\mathcal{I} - \mathcal{P}) \ . \end{aligned}$$

■

Test Your Comprehension 25.1.6

Argue that if $\mathcal{P}$ is a symmetric idempotent then so is $\mathcal{I} - \mathcal{P}$.

It turns out that symmetric idempotents are completely determined by their ranges. This is a fundamental property of symmetric idempotents.

Theorem 25.1.7 **Range equality gives equality for symmetric idempotents**

The following statements are equivalent for *symmetric idempotent* matrices $\mathcal{P}$ and $\mathcal{Q}$.

1. $Range(\mathcal{P}) = Range(\mathcal{Q})$.
2. $\mathcal{P} = \mathcal{Q}$.

A proof of Theorem 25.1.7 is presented in the appendix to the chapter.

We already know how to decide whether two given matrices have the same range. The process involves a calculation of RCEF. See section 16.3 for the details. In the case of isometries, the task can be greatly simplified by Theorem 25.1.7.

Hint: TYC's 19.2.2 and 25.1.3.

Test Your Comprehension 25.1.8 ☞ **Range equality for isometries**

The following statements are equivalent for *isometries* $\mathcal{A}$ and $\mathcal{B}$.

1. $\mathit{Range}\,(\mathcal{A}) = \mathit{Range}\,(\mathcal{B})$.

2. $\mathcal{A}\mathcal{A}^T = \mathcal{B}\mathcal{B}^T$.

Comment 25.1.9

TYC 25.1.8 is a remarkable result. Here is what it tells us. Given an orthonormal coordinate system $\mathfrak{C}$ for a subspace $\boldsymbol{W}$ of $\mathbb{R}^n$, we can form an isometry matrix $\mathcal{A}$, whose columns are the tuples of $\mathfrak{C}$, arranged in some order. Then the symmetric idempotent matrix $\mathcal{P} := \mathcal{A}\mathcal{A}^T$ depends only on $\boldsymbol{W}$, and not at all on $\mathfrak{C}$!

In other words, if we start with *any other* orthonormal coordinate system $\mathfrak{G}$ for $\boldsymbol{W}$, and form an isometry matrix $\mathcal{B}$ whose columns are the tuples in $\mathfrak{G}$, then $\mathcal{B}\mathcal{B}^T$ is again the very same symmetric idempotent $\mathcal{P}$.

Definition 25.1.10 ☞ $\mathcal{P}_{\boldsymbol{W}}$

In view of Theorem 24.1.8, TYC 25.1.8 and Comment 25.1.9, for every non-trivial subspace $\boldsymbol{W}$ we define $\mathcal{P}_{\boldsymbol{W}}$ to stand for the matrix $\mathcal{A}\mathcal{A}^T$, where $\mathcal{A}$ is any isometry whose range is $\boldsymbol{W}$. The choice of such an $\mathcal{A}$ is immaterial.

By Theorem 25.1.7, $\mathcal{P}_{\boldsymbol{W}}$ is the one and only symmetric idempotent whose range is $\boldsymbol{W}$.

It is a common convention to let $\mathcal{P}_{\{\mathbb{O}\}} := \mathcal{O}$.

Test Your Comprehension 25.1.11

Argue that $\mathcal{P}_{R^n} = \mathcal{I}$.

Now one can establish the theorem alluded to at the start of this subsection.

Test Your Comprehension 25.1.12

Every non-nil symmetric idempotent can be expressed as $\mathcal{A}\mathcal{A}^T$, for some isometry $\mathcal{A}$.

Let us summarize the properties of $\mathcal{P}_{\boldsymbol{W}}$.

Test Your Comprehension 25.1.13 **Properties of $\mathcal{P}_{\boldsymbol{W}}$**

Verify the following properties of the matrix $\mathcal{P}_{\boldsymbol{W}}$.

1. $\mathcal{P}^2_{\boldsymbol{W}} = \mathcal{P}_{\boldsymbol{W}} = \mathcal{P}^T_{\boldsymbol{W}}$.
2. $\mathit{Range}\,(\mathcal{P}_{\boldsymbol{W}}) = \boldsymbol{W} = \mathit{Nullspace}\,(\mathcal{I} - \mathcal{P}_{\boldsymbol{W}})$.
3. $\mathit{Nullspace}\,(\mathcal{P}_{\boldsymbol{W}}) = \boldsymbol{W}^{\perp} = \mathit{Range}\,(\mathcal{I} - \mathcal{P}_{\boldsymbol{W}})$.
4. $\boldsymbol{W} = \{\ W \mid \mathcal{P}_{\boldsymbol{W}}(W) = W\ \}$.
5. $\mathcal{I} - \mathcal{P}_{\boldsymbol{W}} = \mathcal{P}_{\boldsymbol{W}^{\perp}}$.
6. For ANY orthonormal coordinate system $C_1, C_2, \ldots, C_m$ of $\boldsymbol{W}$,
$$\mathcal{P}_{\boldsymbol{W}}(X) = \big(X \bullet C_1\big)\, C_1 + \big(X \bullet C_2\big)\, C_2 + \cdots + (X \bullet C_m)\, C_m\ .$$

25.2 The Closest Point Property

A linear system $\mathcal{A}(X) = C$ has a solution exactly when C is in the range of $\mathcal{A}$. In that case the solutions of the system give us "the departure points from which the airline $\mathcal{A}$ will deliver us to the location C".

When C is not in the range of $\mathcal{A}$, there is no way for us to arrive at C "flying with the airline $\mathcal{A}$". In such a case it is natural to ask how close to C we can actually get (still "flying with $\mathcal{A}$").

Since all subspaces are ranges, we can reformulate the questions thus:

> *Given an n-tuple Z and a subspace $\boldsymbol{W}$ of $\mathbb{R}^n$, is there always an element W of $\boldsymbol{W}$ that is closest to Z, in the sense that no other element of $\boldsymbol{W}$ is strictly closer?*
>
> *When the answer is affirmative, can there be more than one such W, or is such a W unique?*

It should not come as a complete surprise that these questions are highly relevant in applications, such as, for example, finding a straight line that is a best fit for a given set of planar data points. It is not uncommon to see the process referred to as "the least squares approximation".

It turns out that the answers to the posed questions are affirmative, and that symmetric idempotents play a central role in the matter.

Theorem 25.2.1 ☞ **The closest point property**

If $\boldsymbol{W}$ is a subspace of $\mathbb{R}^n$ then for any $Z \in \mathbb{R}^n$,

$\mathcal{P}_{\boldsymbol{W}}(Z)$ is the element of $\boldsymbol{W}$ that is uniquely closest to Z . *

If $W_1, W_2, \ldots, W_k$ form an orthonormal coordinate system of $\boldsymbol{W}$, then for any $Z \in \mathbb{R}^n$,

$$\big(Z \bullet W_1\big)\, W_1 + \big(Z \bullet W_2\big)\, W_2 + \cdots + \big(Z \bullet W_k\big)\, W_k \tag{25.1}$$

is the element of $\boldsymbol{W}$ that is uniquely closest to Z.

*In the sense that every other element of $\boldsymbol{W}$ is strictly further away from Z, in the sense of the usual Euclidean distance.

Test Your Comprehension 25.2.2

Verify Theorem 25.2.1 in the case $\boldsymbol{W} = \{\mathbb{0}\}$.

Proof of Theorem 25.2.1. If $W \in \boldsymbol{W}$, then the distance from W to Z is given by $\|Z - W\|$. By TYC 25.1.13,

$$\mathcal{I} = \mathcal{P}_{\boldsymbol{W}} + \mathcal{P}_{\boldsymbol{W}^\perp} ,$$

and therefore

$$Z = \mathcal{P}_{\boldsymbol{W}}(Z) + \mathcal{P}_{\boldsymbol{W}^\perp}(Z) .$$

Hence

$$\begin{aligned}
\|Z - W\|^2 &= \left\|\mathcal{P}_{\boldsymbol{W}}(Z) + \mathcal{P}_{\boldsymbol{W}^\perp}(Z) - W\right\|^2 \\
&= \left\|\Big(\mathcal{P}_{\boldsymbol{W}}(Z) - W\Big) + \mathcal{P}_{\boldsymbol{W}^\perp}(Z)\right\|^2 \\
&\overset{\text{Thm. 3.4.5}}{=} \left\|\mathcal{P}_{\boldsymbol{W}}(Z) - W\right\|^2 + \left\|\mathcal{P}_{\boldsymbol{W}^\perp}(Z)\right\|^2 \\
&\geq \left\|\mathcal{P}_{\boldsymbol{W}^\perp}(Z)\right\|^2 \\
&= \left\|Z - \mathcal{P}_{\boldsymbol{W}}(Z)\right\|^2 ,
\end{aligned}$$

where the equality holds exactly when $W = \mathcal{P}_{\boldsymbol{W}}(Z)$. Note that $\mathcal{P}_{\boldsymbol{W}}(Z) - W \in \boldsymbol{W}$, while $\mathcal{P}_{\boldsymbol{W}^{\perp}}(Z) \in \boldsymbol{W}^{\perp}$. Hence Pythagorean Theorem 3.4.5 was applicable.

It follows that $\|Z - W\| \geq \|Z - \mathcal{P}_{\boldsymbol{W}}(Z)\|$, and the equality holds exactly when $W = \mathcal{P}_{\boldsymbol{W}}(Z)$. This gives the required result.

The second claim of the theorem is a direct consequence of TYC 25.1.13. ■

25.3 Orthogonal Decomposition Of $\mathbb{R}^n$

Theorem 25.3.1 ☞ **Orthogonal decomposition of $\mathbb{R}^n$**

Given a subspace $\boldsymbol{W}$ in $\mathbb{R}^n$, every element Z of $\mathbb{R}^n$ can be expressed in a *unique* way as $X + Y$, where $X \in \boldsymbol{W}$ and $Y \in \boldsymbol{W}^{\perp}$.

The unique summands are

$$X = P_{\boldsymbol{W}}(Z) \quad \text{and} \quad Y = P_{\boldsymbol{W}^{\perp}}(Z)\,.$$

A proof of Theorem 25.3.1 is presented in the appendix to the chapter.

Notation 25.3.2

It is common to express the result of Theorem 25.3.1 by writing

$$\mathbb{R}^n = \boldsymbol{W} \oplus \boldsymbol{W}^{\perp},$$

or

$$\mathbb{R}^n = \boldsymbol{W} \ominus \boldsymbol{W}^{\perp}\,.$$

We shall prefer the latter notation.

Furthermore, it is helpful to write $Z_{\boldsymbol{W}}$ for $P_{\boldsymbol{W}}(Z)$. This way, for example, Theorem 25.3.1 tells us that every tuple Z can be decomposed uniquely as a sum of a tuple in $\boldsymbol{W}$ and a tuple in $\boldsymbol{W}^{\perp}$, and this unique decomposition is given by

$$Z = Z_{\boldsymbol{W}} + Z_{\boldsymbol{W}^{\perp}}\,.$$

Terminology 25.3.3

Theorem 25.3.1 and geometric considerations prompt us to introduce a more standard terminology and to refer to symmetric idempotents as **ortho-projections**.

25.4 : Ortho-projections On Vectors

25.5 A More General Formula For $\mathcal{P}_W$

Whenever we have an orthonormal coordinate system of a subspace $\boldsymbol{W}$ of $\mathbb{R}^n$ at our disposal, TYC 25.1.13 gives us formulas for $\mathcal{P}_{\boldsymbol{W}}$.

It is natural to seek other formulas for $\mathcal{P}_{\boldsymbol{W}}$, which do not require the availability of an orthonormal coordinate system for $\boldsymbol{W}$.

It turns out that any coordinate system for $\boldsymbol{W}$, even a non-orthonormal one, generates a nice formula for $\mathcal{P}_{\boldsymbol{W}}$.

Theorem 25.5.1 **A more general formula for $\mathcal{P}_{\boldsymbol{W}}$**

If $\mathcal{B}$ is an *injection* with a range $\boldsymbol{W}$, then

$$\mathcal{P}_{\boldsymbol{W}} = \mathcal{B}\left(\mathcal{B}^{T}\mathcal{B}\right)^{-1}\mathcal{B}^{T} \;. \tag{25.2}$$

A proof of Theorem 25.5.1 is presented in the appendix to the chapter.

Test Your Comprehension 25.5.2

Argue that when $\mathcal{B}$ is an isometry with a range $\boldsymbol{W}$, formula (25.2) reduces to a formula we already have.

In this sense Theorem 25.5.1 generalizes our previous results.

25.6 Least Squares Approximation

Terminology 25.6.1

Suppose that we are given a linear system $\mathcal{A}(X) = C$, which may not have solutions, and we are to find the inputs X that will get as as close as possible to the output C (in the sense of the usual Euclidean distance). Such X are said to be the **least squares solutions** for $\mathcal{A}(X) = C$.

An examination of the proof of Theorem 25.5.1 leads to a method of finding the least squares solutions for any linear system $A(X) = C$.

Theorem 25.6.2 Least Squares Solutions

The least squares solutions for the system $\mathcal{A}(X) = C$ are exactly the (actual) solutions of the associated system

$$\mathcal{A}^{T}\mathcal{A}(X) = \mathcal{A}^{T}(C)\ .$$

If $\mathcal{A}$ happens to be injective, then $X = \left(\mathcal{A}^{T}\mathcal{A}\right)^{-1}\mathcal{A}^{T}(C)$ is the unique least squares solution.

A proof of Theorem 25.6.2 is presented in the appendix to the chapter.

Exercise 25.6.3

Let $A = \begin{bmatrix} 2 & -6 & 9 & 6 & 5 \\ -1 & 3 & -3 & 0 & 5 \\ 3 & -9 & 11 & 4 & 2 \\ 0 & 0 & 1 & 2 & 5 \\ 1 & -3 & 4 & 2 & 1 \end{bmatrix}$ and let $Y_{o} = \begin{pmatrix} -2 \\ 19 \\ -6 \\ 16 \\ -2 \end{pmatrix}$.

Find ALL least squares solutions for the system $A(X) = Y_{o}$.

MORE EXAMPLES: line fitting, curve fitting, plane fitting etc.

Theorem 25.6.4 ☞ $\mathcal{QR}$ **Factorization**

Every *portrait-shaped* matrix $\mathcal{A}_{n\times m}$ can be expressed as a product

$$\mathcal{Q}_{n\times m}\mathcal{R}_{m\times m} \ ,$$

where $\mathcal{Q}$ is an isometry, and $\mathcal{R}$ is an upper-triangular matrix.

In particular, if $\mathcal{A}$ is a square matrix then $\mathcal{Q}$ is a unitary matrix.

Furthermore, $\mathcal{A}$ is injective exactly when $\mathcal{R}$ is invertible.

A proof of Theorem 25.6.4 is presented in the appendix to the chapter.

25.7 Appendix: Exiled Proofs

Proof of Lemma 24.1.4. We have provided the justification of the validity of the implication 2. $\Longrightarrow$ 1. in Observation 24.1.3. Let us focus on the implication 1. $\Longrightarrow$ 2. Here is what we are trying to prove:

> If $X_1, \ldots, X_k$ is an orthonormal list, and Z is not a linear combination of the X_i's, then there is a unit tuple Y orthogonal to every X_i such that
> $$Span\left(X_1, \ldots, X_k, Y\right) = Span\left(X_1, \ldots, X_k, Z\right) \ ;$$
> i.e.
> $$Range\begin{bmatrix} X_1 & \cdots & X_k & Y \end{bmatrix} = Range\begin{bmatrix} X_1 & \cdots & X_k & Z \end{bmatrix} .$$

As you know, elementary column operations cannot alter a range of a matrix (TYC 10.2.10). Our strategy shall be to perform column adjustments and a scaling that alter the last column only, in such a way as to transform $\begin{bmatrix} X_1 & \ldots & X_k & Z \end{bmatrix}$ into a $\begin{bmatrix} X_1 & \cdots & X_k & Y \end{bmatrix}$, with Y satisfying the required conditions.

Performing a sequence of column adjustments of the last column only, we can arrive at a matrix

$$\begin{bmatrix} X_1 & \cdots & X_k & \left(Z - \alpha_1 X_1 - \cdots - \alpha_k X_k\right) \end{bmatrix} ,$$

for any choice of α_j's.

Let us write $V = Z - \alpha_1 X_1 - \cdots - \alpha_k X_k$. Since Z is not a linear combination of the X_i's, we know that $V \neq \mathbb{O}$ for any α_j's.

We will look for a choice of α_j's that makes V orthogonal to all X_i's. If we find such, we will scale the last column of $\begin{bmatrix} X_1 & \ldots & X_k & V \end{bmatrix}$ by $\frac{1}{\|V\|}$ and arrive at an $\begin{bmatrix} X_1 & \dots & X_k & Y \end{bmatrix}$, where $Y = \frac{1}{\|V\|}V$ is a unit tuple orthogonal to all of the X_i's. This will complete the proof.

Is there a choice of α_j's that makes V orthogonal to all X_{i_0}'s? Let us make some calculations.

$$\begin{aligned} V \bullet X_{i_0} &= \left(Z - \alpha_1 X_1 - \cdots - \alpha_k X_k\right) \bullet X_{i_0} \\ &\overset{\text{distribute}}{=} Z \bullet X_{i_0} - \alpha_1 X_1 \bullet X_{i_0} - \cdots - \alpha_k X_k \bullet X_{i_0} \\ &\overset{\text{orthonormality}}{=} Z \bullet X_{i_0} - \alpha_{i_0} \ . \end{aligned}$$

Hence, by setting

$$\begin{array}{rcl} \alpha_1 & := & Z \bullet X_1 \\ & \vdots & \\ \alpha_k & := & Z \bullet X_k \end{array} ,$$

we arrive at the formula

$$V = Z - \left(Z \bullet X_1\right) \cdot X_1 - \cdots - \left(Z \bullet X_k\right) \cdot X_k \tag{25.3}$$

for a non-null tuple V that is orthogonal to every X_i. ■

Proof of Theorem 24.1.5. Being (collectively) linearly independent, none of the X_i's are null (TYC 18.1.2), and no X_{i_0} is a linear combination of the preceding X_i's on the list.

Step 1: Let $Y_1 := \frac{1}{\|X_1\|}X_1$. Then

$$Span\left(Y_1\right) = Span\left(X_1\right) \ . \tag{25.4}$$

(A quick way to see this is to note that $[Y_1]$ is produced from $[X_1]$ by scaling a column.)

Step 2: Since Y_1 constitutes a singleton orthonormal list, and

$$X_2 \notin Span\left(X_1\right) \overset{(25.4)}{=} Span\left(Y_1\right) \ ,$$

by Gram-Schmidt replacement step we can replace X_2 on the list Y_1, X_2 (with some Y_2) to arrive an an orthonormal list with the same span. Then

$$Span\left(Y_1, Y_2\right) = Span\left(Y_1, X_2\right) \overset{(25.4)\ \&\ \text{Thm. } 24.1.1}{=} Span\left(X_1, X_2\right) \ . \tag{25.5}$$

Step 3: Since

$$X_3 \notin Span\left(X_1, X_2\right) \overset{(25.5)}{=} Span\left(Y_1, Y_2\right) ,$$

by Gram-Schmidt replacement step we can replace X_3 on the list Y_1, Y_2, X_3 (with some Y_3) to arrive an an orthonormal list with the same span. Then

$$\begin{aligned} Span\left(Y_1, Y_2, Y_3\right) &= Span\left(Y_1, Y_2, X_3\right) \\ &\overset{(25.5)\ \&\ \text{Thm. } 24.1.1}{=} Span\left(X_1, X_2, X_3\right) . \end{aligned} \tag{25.6}$$

Step 4: Since

$$X_4 \notin Span\left(X_1, X_2, X_3\right) \overset{(25.6)}{=} Span\left(Y_1, Y_2, Y_3\right) ,$$

by Gram-Schmidt replacement step we can replace X_4 on the list Y_1, Y_2, Y_3, X_4 (with some Y_4) to arrive an an orthonormal list with the same span. Then

$$Span\left(Y_1, Y_2, Y_3, Y_4\right) = Span\left(Y_1, Y_2, Y_3, X_4\right) \overset{(25.6)\ \&\ \text{Thm. } 24.1.1}{=} Span\left(X_1, X_2, X_3, X_4\right) .$$

This process can be continued for the required k steps. The reader is encouraged to show how one performs 235-th step, after the first 234 steps have been completed (and assuming $k \geq 235$). This should be enough to convince the reader of the validity of the procedure in general. ■

Those who seek more rigidity in the proof will have to apply the method of mathematical induction or the well-ordering principle. We chose to leave this as an exercise for the appropriately educated and motivated readers.

Proof of Theorem 25.1.7. Only the implication [1. $\Longrightarrow$ 2.] deserves attention. By Theorem 25.1.4,

$$Nullspace\,(\mathcal{I} - \mathcal{Q}) = Range\,(\mathcal{Q}) = Range\,(\mathcal{P}) = Nullspace\,(\mathcal{I} - \mathcal{P}) .$$

Passing to ortho-complements we get

$$\begin{aligned} Range\left((\mathcal{I} - \mathcal{Q})^{T}\right) &= \left(Nullspace\,(\mathcal{I} - \mathcal{Q})\right)^{\perp} \\ &= \left(Nullspace\,(\mathcal{I} - \mathcal{P})\right)^{\perp} = Range\left((\mathcal{I} - \mathcal{P})^{T}\right) . \end{aligned}$$

Since $\mathcal{P}$, $\mathcal{Q}$ and $\mathcal{I}$ are symmetric, so are $\mathcal{I} - \mathcal{P}$ and $\mathcal{I} - \mathcal{Q}$. Therefore we have

$$\begin{aligned}
\mathit{Range}(\mathcal{I}-\mathcal{Q}) &= \mathit{Range}(\mathcal{I}-\mathcal{P}) \\
&= \Big(\mathit{Nullspace}(\mathcal{I}-\mathcal{P})\Big)^{\perp} \\
&= \Big(\mathit{Range}(\mathcal{P})\Big)^{\perp} \\
&= \mathit{Nullspace}\Big(\mathcal{P}^{T}\Big) \\
&= \mathit{Nullspace}(\mathcal{P}) \quad .
\end{aligned}$$

It follows that

$$\mathcal{P}\Big(\big(\mathcal{I}-\mathcal{Q}\big)(Z)\Big) = \mathbb{0} \ , \quad \text{for any} \quad Z \ ,$$

since $\big(\mathcal{I}-\mathcal{Q}\big)(Z) \in \mathit{Range}(\mathcal{I}-\mathcal{Q}) = \mathit{Nullspace}(\mathcal{P})$. This shows that

$$\mathcal{P}\big(\mathcal{I}-\mathcal{Q}\big) = \mathcal{O} \ ,$$

or equivalently that

$$\mathcal{P} = \mathcal{P}\mathcal{Q}.$$

Thus

$$\mathcal{P}(Y) = \mathcal{P}\Big(\mathcal{Q}(Y)\Big) \ , \quad \text{for any} \quad Y \ .$$

Yet $\mathcal{Q}(Y) \in \mathit{Range}(\mathcal{Q}) = \mathit{Range}(\mathcal{P})$, and $\mathcal{P}$, being an idempotent, acts as an identity on its range, which tells us that

$$\mathcal{P}\Big(\mathcal{Q}(Y)\Big) = \mathcal{Q}(Y) \ .$$

This shows that

$$\mathcal{P}(Y) = \mathcal{Q}(Y) \ , \quad \text{for any} \quad Y \ ,$$

and therefore $\mathcal{P} = \mathcal{Q}$. ■

Proof of Theorem 25.3.1. Since

$$Z = P_{\boldsymbol{W}}(Z) + Z - P_{\boldsymbol{W}}(Z) = P_{\boldsymbol{W}}(Z) + \Big(\mathcal{I} - P_{\boldsymbol{W}}\Big)(Z) \overset{\text{TYC ??}}{=} P_{\boldsymbol{W}}(Z) + P_{\boldsymbol{W}^{\perp}}(Z) \ ,$$

we see that every Z can be expressed as a sum of a tuple in $\boldsymbol{W}$ and a tuple in $\boldsymbol{W}^{\perp}$.

Let us show that such a decomposition is unique. We shall argue that there is no *other* way to express Z as a sum of a tuple in $\boldsymbol{W}$ and a tuple in $\boldsymbol{W}^{\perp}$.

Were Z expressed as such a sum, say $W + V$, we would have

$$W + V = Z = P_{\boldsymbol{W}}(Z) + P_{\boldsymbol{W}^\perp}(Z) ,$$

and consequently

$$U := W - P_{\boldsymbol{W}}(Z) = P_{\boldsymbol{W}^\perp}(Z) - V .$$

$W - P_{\boldsymbol{W}}(Z)$ is a linear combination of tuples in $\boldsymbol{W}$, and is therefore a tuple in $\boldsymbol{W}$. $P_{\boldsymbol{W}^\perp}(Z) - V$ is a linear combination of tuples in $\boldsymbol{W}^\perp$, and is therefore a tuple in $\boldsymbol{W}^\perp$.

This shows that U is in both $\boldsymbol{W}$ and $\boldsymbol{W}^\perp$. Thus $U = \mathbb{0}$ (TYC 3.5.12). Therefore

$$W = P_{\boldsymbol{W}}(Z) \text{ and } V = P_{\boldsymbol{W}^\perp}(Z) ,$$

which establishes the uniqueness claim. ■

Proof of Theorem 25.5.1. Such an injection $\mathcal{B} \in \mathbb{M}_{n\times m}$ has the following properties.

1. $\mathit{Nullspace}\left(\mathcal{B}^T\right) \overset{\text{TYC 12.1.10}}{=} \boldsymbol{W}^\perp$.

2. $\mathcal{B}^T\mathcal{B}$ is invertible (TYC 12.1.19).

Let $Z \in \mathbb{R}^n$ be given. Then $Z \overset{\text{Thm. 25.3.1}}{=} Z_{\boldsymbol{W}} + Z_{\boldsymbol{W}^\perp}$. Note that

$$Z_{\boldsymbol{W}^\perp} \in \boldsymbol{W}^\perp = \mathit{Nullspace}\left(\mathcal{B}^T\right) .$$

Since $Z_{\boldsymbol{W}} \in \boldsymbol{W} = \mathit{Range}(\mathcal{B})$, we can write

$$Z_{\boldsymbol{W}} = \mathcal{B}(X), \text{ for some } X \in \mathbb{R}^m.$$

Now

$$\begin{aligned}\mathcal{B}^T(Z) &= \mathcal{B}^T\left(Z_{\boldsymbol{W}} + Z_{\boldsymbol{W}^\perp}\right)\\ &= \mathcal{B}^T\left(Z_{\boldsymbol{W}}\right) + \mathcal{B}^T\left(Z_{\boldsymbol{W}^\perp}\right)\\ &= \mathcal{B}^T\mathcal{B}(X) + \mathbb{0}\\ &= \mathcal{B}^T\mathcal{B}(X) .\end{aligned}$$

Hence $X = \left(\mathcal{B}^T\mathcal{B}\right)^{-1}\mathcal{B}^T(Z)$, and therefore

$$\mathcal{P}_{\boldsymbol{W}}(Z) = Z_{\boldsymbol{W}} = \mathcal{B}(X) = \mathcal{B}\left(\mathcal{B}^T\mathcal{B}\right)^{-1}\mathcal{B}^T(Z) \ ,$$

which gives the required formula. ■

Proof of Theorem 25.6.2. From the Closest Point Property (Thm. 25.2.1), we know that $C_{Range(\mathcal{A})} := \mathcal{P}_{Range(\mathcal{A})}(C)$ is the point of $Range\,(\mathcal{A})$ that is uniquely closest to C.

Therefore the least squares solutions we seek for $\mathcal{A}(X) = C$ are exactly the solutions to the associated linear system

$$\mathcal{A}(X) = C_{Range(\mathcal{A})} \ .$$

We know this system has solutions because the target tuple $C_{Range(\mathcal{A})}$ is in the range of $\mathcal{A}$.

Let us recall that

$$Nullspace\left(\mathcal{A}^T\right) = \left(Range\,(\mathcal{A})\right)^{\perp} \quad \text{(TYC 12.1.10)},$$

and therefore

$$\begin{aligned}\mathcal{A}^T(C) = \mathcal{A}^T &\left(C_{Range(\mathcal{A})} + C_{Range(\mathcal{A})^{\perp}}\right) \\ &= \mathcal{A}^T\left(C_{Range(\mathcal{A})}\right) + \mathbb{0} = \mathcal{A}^T\left(C_{Range(\mathcal{A})}\right) \ . \end{aligned} \qquad (25.7)$$

We aim to show that linear systems $\mathcal{A}(X) = C_{Range(\mathcal{A})}$ and $\mathcal{A}^T\mathcal{A}(X) = \mathcal{A}^T(C)$ are equivalent (i.e. have the same solutions). By (25.7), the latter system can be expressed as

$$\mathcal{A}^T\mathcal{A}(X) = \mathcal{A}^T\left(C_{Range(\mathcal{A})}\right) \ .$$

It is obvious that any solution of $\mathcal{A}(X) = C_{Range(\mathcal{A})}$ is also a solution of $\mathcal{A}^T\mathcal{A}(X) = \mathcal{A}^T\left(C_{Range(\mathcal{A})}\right)$.

For the converse implication, suppose that X_o is a solution of $\mathcal{A}^T\mathcal{A}(X) = \mathcal{A}^T\left(C_{Range(\mathcal{A})}\right)$. Then

$$\mathcal{A}^T\left(\mathcal{A}(X_o) - C_{Range(\mathcal{A})}\right) = \mathbb{0} \ ,$$

so that

$$\mathcal{A}(X_o) - C_{Range(\mathcal{A})} \in Nullspace\left(\mathcal{A}^T\right) = \left(Range\,(\mathcal{A})\right)^{\perp} \quad \text{(TYC 12.1.10)} \ .$$

Yet $\mathcal{A}(X_o) - C_{Range(\mathcal{A})}$ is a linear combination of two elements of $Range\,(\mathcal{A})$, and so is an element of $Range\,(\mathcal{A})$. This shows that

$$\mathcal{A}(X_o) - C_{Range(\mathcal{A})} \in Range\,(\mathcal{A}) \cap \left(Range\,(\mathcal{A})\right)^{\perp} \overset{\text{TYC 3.5.12}}{=} \{\mathbb{O}\}\ .$$

Thus

$$\mathcal{A}(X_o) - C_{Range(\mathcal{A})} = \mathbb{O}$$

and X_o is a solution of the system $\mathcal{A}(X) = C_{Range(\mathcal{A})}$.

The last claim of the theorem follows from the first, by TYC 12.1.19. ■

Proof of Theorem 25.6.4. The proof is accomplished through a number of steps.

Step 1: Let us verify the claim in the case when $\mathcal{A}$ is an injection.

In this case the columns $X_1, \ldots, X_m$ of $\mathcal{A}$ form a linearly independent list. We can use Gram-Schmidt process to create an orthonormal list $Y_1, \ldots, Y_m$. Since

$$Y_i \in Span\left(Y_1, \ldots, Y_i\right) = Span\left(X_1, \ldots, X_i\right), \qquad \text{for } i = 1, \ldots m\ ,$$

every Y_i is a linear combination of $X_1, \ldots, X_i$. Let us write

$$\begin{aligned}
Y_1 &= \alpha_{1,1}X_1\ ;\\
Y_2 &= \alpha_{2,1}X_1 + \alpha_{2,2}X_2\ ;\\
Y_3 &= \alpha_{3,1}X_1 + \alpha_{3,2}X_2 + \alpha_{3,3}X_3\ ;\\
Y_4 &= \alpha_{4,1}X_1 + \alpha_{4,2}X_2 + \alpha_{4,3}X_3 + \alpha_{4,4}X_4\ ;\\
&\vdots\\
Y_m &= \alpha_{m,1}X_1 + \alpha_{m,2}X_2 + \alpha_{m,3}X_3 + \alpha_{m,4}X_4 + \cdots + \alpha_{m,m}X_m\ .
\end{aligned}$$

Then (via the column-centric evaluation of matrix products (Theorem 8.1.7)) we have

$$\mathcal{A} = \begin{bmatrix} Y_1 & Y_2 & Y_3 & \ldots & Y_m \end{bmatrix} = \begin{bmatrix} X_1 & X_2 & X_3 & \ldots & X_m \end{bmatrix} \begin{bmatrix} \alpha_{1,1} & \alpha_{2,1} & \alpha_{3,1} & \cdots & \alpha_{m,1}\\ 0 & \alpha_{2,2} & \alpha_{3,2} & \cdots & \alpha_{m,2}\\ 0 & 0 & \alpha_{3,3} & \cdots & \alpha_{m,3}\\ \vdots & \vdots & \vdots & \ddots & \vdots\\ 0 & 0 & 0 & \cdots & \alpha_{m,m} \end{bmatrix}.$$

Since $\begin{bmatrix} X_1 & X_2 & X_3 & \ldots & X_m \end{bmatrix}$ is an isometry, our proof of the present case is complete.

Step 2: Let us verify the claim in the case when $\mathcal{A}$ is a square matrix.

By Gauss-Jordan elimination scheme

$$\mathcal{A} = \mathcal{S} \circ \mathrm{RREF}(\mathcal{A}) \qquad \text{(Cor. 16.2.4)}\ ,$$

where $\mathcal{S}$ is an invertible matrix.

By the result of Step 1, $\mathcal{S}$ can be expressed as $\mathcal{QR}$, where $\mathcal{Q}$ is a unitary matrix, and $\mathcal{R}$ is an upper-triangular matrix. Thus

$$\mathcal{A} = \mathcal{Q} \circ \Big(\mathcal{R} \circ \mathrm{RREF}(\mathcal{A})\Big)\ .$$

Since $\mathcal{R} \circ \mathrm{RREF}(\mathcal{A})$ is a product of two upper-triangular matrices, it is upper-triangular and the proof of this case is complete.

Step 3: Let us verify the claim in the case when $\mathcal{A} \in \mathbb{M}_{n\times m}$ is a strictly portrait-shaped matrix (i.e. when $n > m$).

Let us write

$$\mathcal{A} = \begin{bmatrix} X_1 & \cdots & X_m \end{bmatrix}_{n\times m}$$

and

$$\mathcal{B} = \begin{bmatrix} X_1 & \cdots & X_m & \mathbb{0} & \cdots & \mathbb{0} \end{bmatrix}_{n\times n} = \begin{bmatrix} \mathcal{A} & \mathcal{O} \end{bmatrix}_{n\times(m|n-m)}\ .$$

By the result of Step 2, we can express $\mathcal{B}$ as $\mathcal{Q}_{n\times n}\mathcal{R}_{n\times n}$, where $\mathcal{Q}$ is an isometry and $\mathcal{R}$ is an upper-triangular matrix.

Let us express $\mathcal{Q}$ as a partitioned matrix $\begin{bmatrix} \mathcal{C} & \mathcal{D} \end{bmatrix}_{n\times(m|n-m)}$, with both $\mathcal{C}$ and $\mathcal{D}$ being isometries (their column lists are orthonormal).

Let us also express $\mathcal{R}$ as a partitioned matrix

$$\left[\begin{smallmatrix} \mathcal{M} & \mathcal{K} \\ \mathcal{Q} & \mathcal{L} \end{smallmatrix}\right]_{(m|n-m)\times(m|n-m)}\ .$$

Since $\mathcal{R}$ is upper-triangular, $\mathcal{Q} = \mathcal{O}$, while $\mathcal{M}$ and $\mathcal{L}$ are upper-triangular matrices.

Since $\mathcal{B} = \mathcal{QR}$, we have

$$\begin{bmatrix} \mathcal{A} & \mathcal{O} \end{bmatrix}_{n\times(m|n-m)} = \begin{bmatrix} \mathcal{C} & \mathcal{D} \end{bmatrix}_{n\times(m|n-m)} \left[\begin{smallmatrix} \mathcal{M} & \mathcal{K} \\ \mathcal{O} & \mathcal{L} \end{smallmatrix}\right]_{(m|n-m)\times(m|n-m)}\ ,$$

and by the fundamental formula for partitioned matrix multiplication we can conclude that $\mathcal{A} = \mathcal{CM} + \mathcal{DO} = \mathcal{CM}$, which completes the proof of this step.

The only claims that still remain to be validated are the last two claims of the theorem.

Let us deal with the first of these. Obviously, if $\mathcal{R}$ is invertible, then $\mathcal{QR}$ is a product of two injections (isometries are injective), and so is injective.

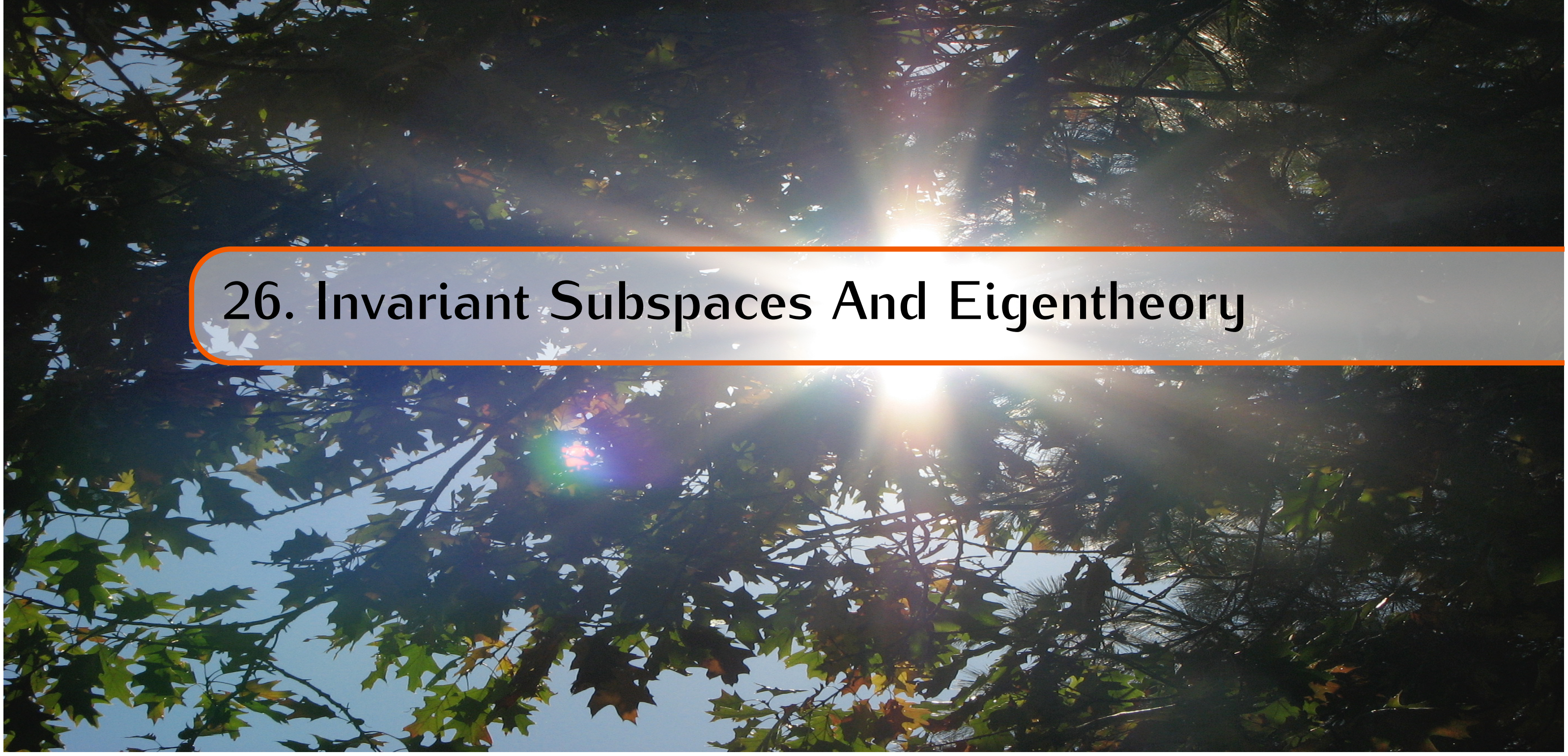
Conversely, suppose that $\mathcal{A}$ is injective. Then $\mathcal{A}$ injective has a left inverse that is a matrix (Theorem 13.2.1), say $\mathcal{G}$. In that case

$$\mathcal{I} = \mathcal{G}\mathcal{A} = (\mathcal{G}\mathcal{Q})\mathcal{R} \ ,$$

which shows that $\mathcal{R}$ has a left inverse, and so is injective (Theorem 13.2.1). Since $\mathcal{R}$ is a square matrix, it is invertible (TYC 11.2.4).

Now it is the last claim's turn. Since unitary matrices are square, as are upper-triangular matrices, if $\mathcal{Q}$ is a unitary matrix, then $\mathcal{Q}\mathcal{R}$ is a square matrix. Conversely, if $\mathcal{A}$ is a square matrix, then so is $\mathcal{Q}$ (since $\mathcal{R}$ is a square matrix), and square isometries are unitary matrices. ■

IX Invariant Subspaces And Eigentheory



26. Invariant Subspaces And Eigentheory

Last modified on December 8, 2018

26.1 Relatively Prime Polynomials

Terminology 26.1.1

If polynomials p and q have NO common non-trivial polynomial divisors, we say that p and q are **relatively prime**.

Test Your Comprehension 26.1.2 ☞ **"Relatively prime" means no common prime factors**

The following statements are equivalent for monic polynomials f and g.

1. f and g have a common non-trivial polynomial divisor.

2. f and g have a common prime factor.

Conclude that the following claims are (mutually) equivalent.

1. f and g are relatively prime.

2. f and g have no common prime factors.

It is remarkable, that for any non-zero f and g, division with a remainder leads to a practical algorithm (the "Euclidean algorithm") which can be used to test whether f and g are relatively prime.

Fact 26.1.3 ☞ **Characterization of the relative primeness**

The following claims are equivalent for polynomials f and g.

1. f and g are relatively prime.

2. There exist polynomials p_1 and p_2 such that

$$p_1 \cdot f + p_2 \cdot g = 1 \; .$$

Such p_1 and p_2 can be found via the Euclidean Algorithm, and need not be unique.

Exercise 26.1.4

Argue that the second claim in Fact 26.1.3 implies the first.

Hint: TYC's 20.1.8 and 20.1.9 can be helpful here.

Test Your Comprehension 26.1.5

Verify the claim of Fact 26.1.3 in the case when one of f and g is the zero polynomial.

Comment 26.1.6

At this point the reader should explore the ways of using a computing software to test whether two given polynomials are relatively prime, and if they are, to find the polynomials p_1 and p_2 mentioned in Fact 26.1.3.

In *Mathematica* , the command **PolynomialExtendedGCD**[ ] can be used for this purpose.

Theorem 26.1.7

If $\mathcal{A}$ and $\mathcal{B}$ are square matrices (not necessarily of the same size), *such that $\mu_{\mathcal{A}}$ and $\mu_{\mathcal{B}}$ are relatively prime*, then for any matrix $\mathcal{C}$ of appropriate size,

$$\begin{bmatrix} \mathcal{A} & \mathcal{C} \\ \mathcal{O} & \mathcal{B} \end{bmatrix} \text{ is similar to } \begin{bmatrix} \mathcal{A} & \mathcal{O} \\ \mathcal{O} & \mathcal{B} \end{bmatrix} .$$

Proof of Theorem 26.1.7. By Fact 26.1.3, there exist polynomials f and g such that

$$\mu_{\mathcal{A}}(x) \cdot f(x) + \mu_{\mathcal{B}}(x) \cdot g(x) = 1 \; .$$

In particular,

$$\mathcal{I} = \mu_{\mathcal{A}}(\mathcal{A}) \circ f(\mathcal{A}) + \mu_{\mathcal{B}}(\mathcal{A}) \circ g(\mathcal{A}) = \mu_{\mathcal{B}}(\mathcal{A}) \circ g(\mathcal{A}) \; ,$$

which shows that $\mu_{\mathcal{B}}(\mathcal{A})$ is invertible and has the inverse $g(\mathcal{A})$.

By Exercise 20.2.6,

$$\mu_{\mathcal{B}}\left(\begin{bmatrix} \mathcal{A} & \mathcal{C} \\ \mathcal{O} & \mathcal{B} \end{bmatrix}\right) = \begin{bmatrix} \mu_{\mathcal{B}}(\mathcal{A}) & \mathcal{D} \\ \mathcal{O} & \mu_{\mathcal{B}}(\mathcal{A}) \end{bmatrix} = \begin{bmatrix} \mu_{\mathcal{B}}(\mathcal{A}) & \mathcal{D} \\ \mathcal{O} & \mathcal{O} \end{bmatrix} ,$$

for some $\mathcal{D}$.

By TYC 20.2.8, $\mu_{\mathcal{B}}\left(\begin{bmatrix}\mathcal{A} & \mathcal{C}\\ \mathcal{O} & \mathcal{B}\end{bmatrix}\right)$ commutes with $\begin{bmatrix}\mathcal{A} & \mathcal{C}\\ \mathcal{O} & \mathcal{B}\end{bmatrix}$, in other words,

$$\begin{bmatrix}\mathcal{A} & \mathcal{C}\\ \mathcal{O} & \mathcal{B}\end{bmatrix}\begin{bmatrix}\mu_{\mathcal{B}}(\mathcal{A}) & \mathcal{D}\\ \mathcal{O} & \mathcal{O}\end{bmatrix} = \begin{bmatrix}\mu_{\mathcal{B}}(\mathcal{A}) & \mathcal{D}\\ \mathcal{O} & \mathcal{O}\end{bmatrix}\begin{bmatrix}\mathcal{A} & \mathcal{C}\\ \mathcal{O} & \mathcal{B}\end{bmatrix}.$$

One of the consequences of thisy is the equality

$$\mathcal{A}\mathcal{D} = \mu_{\mathcal{B}}(\mathcal{A})\mathcal{C} + \mathcal{D}\mathcal{B}\,. \tag{26.1}$$

Using (26.1), one can verify the following identity.*

$$\begin{bmatrix}\mu_{\mathcal{B}}(\mathcal{A}) & \mathcal{D}\\ \mathcal{O} & \mathcal{I}\end{bmatrix}\begin{bmatrix}\mathcal{A} & \mathcal{C}\\ \mathcal{O} & \mathcal{B}\end{bmatrix} = \begin{bmatrix}\mathcal{A} & \mathcal{O}\\ \mathcal{O} & \mathcal{B}\end{bmatrix}\begin{bmatrix}\mu_{\mathcal{B}}(\mathcal{A}) & \mathcal{D}\\ \mathcal{O} & \mathcal{I}\end{bmatrix}.$$

Since $\begin{bmatrix}\mu_{\mathcal{B}}(\mathcal{A}) & \mathcal{D}\\ \mathcal{O} & \mathcal{I}\end{bmatrix}$ is invertible by Theorem 13.2.12, we have

$$\begin{bmatrix}\mathcal{A} & \mathcal{C}\\ \mathcal{O} & \mathcal{B}\end{bmatrix} = \begin{bmatrix}\mu_{\mathcal{B}}(\mathcal{A}) & \mathcal{D}\\ \mathcal{O} & \mathcal{I}\end{bmatrix}^{-1}\begin{bmatrix}\mathcal{A} & \mathcal{O}\\ \mathcal{O} & \mathcal{B}\end{bmatrix}\begin{bmatrix}\mu_{\mathcal{B}}(\mathcal{A}) & \mathcal{D}\\ \mathcal{O} & \mathcal{I}\end{bmatrix},$$

and the proof is complete. ■

*Keep in mind that $\mathcal{A}$ commutes with $\mu_{\mathcal{B}}(\mathcal{A})$.

Theorem 26.1.8 ☞ **Block-diagonalizing block-$\triangle^{r}$ matrices**

If $\mathcal{A}_i$ are square matrices, not necessarily of the same size, such that *such that $\mu_{\mathcal{A}_i}$ and $\mu_{\mathcal{A}_j}$ are relatively prime* for $i \neq j$, then

any matrix of the form $\begin{bmatrix}\mathcal{A}_1 & \square & \dots & \square\\ \mathcal{O} & \mathcal{A}_2 & \dots & \square\\ \vdots & \vdots & \ddots & \vdots\\ \mathcal{O} & \mathcal{O} & \dots & \mathcal{A}_k\end{bmatrix}$ is similar to $\begin{bmatrix}\mathcal{A}_1 & \mathcal{O} & \dots & \mathcal{O}\\ \mathcal{O} & \mathcal{A}_2 & \dots & \mathcal{O}\\ \vdots & \vdots & \ddots & \vdots\\ \mathcal{O} & \mathcal{O} & \dots & \mathcal{A}_k\end{bmatrix}$.

Proof of Theorem 26.1.8. By Theorem 26.1.7, the claim holds true when $k = 2$. If the claim fails for some k, then there is the minimal such k, say k_o, and $k_o > 2$. In this case there is a matrix $\mathcal{A}$ of the form $\begin{bmatrix}\mathcal{A}_1 & \square & \dots & \square\\ \mathcal{O} & \mathcal{A}_2 & \dots & \square\\ \vdots & \vdots & \ddots & \vdots\\ \mathcal{O} & \mathcal{O} & \dots & \mathcal{A}_{k_o}\end{bmatrix}$ that is NOT similar to $\begin{bmatrix}\mathcal{A}_1 & \mathcal{O} & \dots & \mathcal{O}\\ \mathcal{O} & \mathcal{A}_2 & \dots & \mathcal{O}\\ \vdots & \vdots & \ddots & \vdots\\ \mathcal{O} & \mathcal{O} & \dots & \mathcal{A}_{k_o}\end{bmatrix}$, even though $\mu_{\mathcal{A}_i}$ and $\mu_{\mathcal{A}_j}$ are relatively prime for $i \neq j$.

Let

$$B = \begin{bmatrix} \mathcal{A}_2 & \square & \dots & \square \\ \mathcal{O} & \mathcal{A}_3 & \dots & \square \\ \vdots & \vdots & \ddots & \vdots \\ \mathcal{O} & \mathcal{O} & \dots & \mathcal{A}_{k_o} \end{bmatrix}.$$

Then

$$\mathcal{A} = \begin{bmatrix} \mathcal{A}_1 & \mathcal{C} \\ \mathcal{O} & \mathcal{B} \end{bmatrix},$$

for the appropriate $\mathcal{C}$. By the minimality of k_o, $\mathcal{B}$ is similar to $\begin{bmatrix} \mathcal{A}_2 & \mathcal{O} & \dots & \mathcal{O} \\ \mathcal{O} & \mathcal{A}_3 & \dots & \mathcal{O} \\ \vdots & \vdots & \ddots & \vdots \\ \mathcal{O} & \mathcal{O} & \dots & \mathcal{A}_{k_o} \end{bmatrix}$, which we denote by $\mathcal{D}$. Therefore $\mathcal{A}$ is similar to $\begin{bmatrix} \mathcal{A}_1 & \mathcal{C} \\ \mathcal{O} & \mathcal{D} \end{bmatrix}$, (Exc. 9.2.10).

The prime factors of the minimal polynomial of $\mathcal{D}$ are exactly the prime factors of the polynomials $\mu_{\mathcal{A}_i}$, $i = 2, 3, \dots, k_o$; (TYC 21.3.3). Thus $\mu_{\mathcal{D}}$ shares no prime factors with $\mu_{\mathcal{A}_1}$. We apply Theorem 26.1.7 to conclude that $\begin{bmatrix} \mathcal{A}_1 & \mathcal{C} \\ \mathcal{O} & \mathcal{D} \end{bmatrix}$ is similar to $\begin{bmatrix} \mathcal{A}_1 & \mathcal{O} \\ \mathcal{O} & \mathcal{D} \end{bmatrix}$, which equals $\mathcal{A}_1 \boxplus \mathcal{A}_1 \boxplus \cdots \boxplus \mathcal{A}_{k_o}$.

By the transitivity of the matrix relation of similarity, $\mathcal{A}$ is similar to $\mathcal{A}_1 \boxplus \mathcal{A}_1 \boxplus \cdots \boxplus \mathcal{A}_{k_o}$, which contradict the hypothesis that $\mathcal{A}$ was a counterexample to the claim of the theorem. Hence no counterexample exists, and the proof is complete. ∎

26.2 The Invertibility Of $p(\mathcal{A})$

In this section we demonstrate that the prime factors of the minimal polynomial of $\mathcal{A}$ completely determine whether $p(\mathcal{A})$ is invertible for any given polynomial p.

The main result of the section states that $p(\mathcal{A})$ is NOT invertible exactly when p shares a prime factor with $\mu_{\mathcal{A}}$.

Lemma 26.2.1

The following are equivalent for a non-constant monic polynomial p and a square matrix $\mathcal{A}$.

1. $p(\mathcal{A})$ is NOT invertible.

2. $g(\mathcal{A})$ is NOT invertible for at least one prime factor g of p.

Proof of Lemma 26.2.1. By the (Real) Fundamental Theorem of Algebra we can express p as a product of its prime factors g_i. Then $p(\mathcal{A})$ is a composition of matrices $g_i(\mathcal{A})$, all square. An appeal to Theorem 13.2.11 completes the proof. ■

We can say more in a case of a minimal polynomial.

Lemma 26.2.2

For any square matrix $\mathcal{A}$, $g(\mathcal{A})$ is NOT invertible for EVERY prime factor g of $\mu_{\mathcal{A}}$.

Proof of Lemma 26.2.2. Given a prime factor g of $\mu_{\mathcal{A}}$, we can write

$$\mu_{\mathcal{A}} = q\, g\ ,$$

for some monic polynomial q of degree strictly less than that of $\mu_{\mathcal{A}}$. Consequently q does not annihilate $\mathcal{A}$, and yet

$$\mathcal{O} = \mu_{\mathcal{A}}(\mathcal{A}) = q(\mathcal{A})\, g(\mathcal{A})\ .$$

If $p(\mathcal{A})$ were invertible, we would have

$$\mathcal{O} = \mu_{\mathcal{A}}(\mathcal{A})\Big(g(\mathcal{A})\Big)^{-1} = q(\mathcal{A})\, g(\mathcal{A})\Big(g(\mathcal{A})\Big)^{-1} = q(\mathcal{A})\ ,$$

contradicting the fact that q does not annihilate $\mathcal{A}$. Hence $g(\mathcal{A})$ is NOT invertible. ■

Theorem 26.2.3 ☞ **The invertibility of $p(\mathcal{A})$**

The following are equivalent for a *non-constant* monic polynomial p, and any square matrix $\mathcal{A}$.

1. $p(\mathcal{A})$ is invertible.
2. p and $\mu_{\mathcal{A}}$ share no prime factors.

Proof of Theorem 26.2.3.

2. $\implies$ 1. : If p and $\mu_{\mathcal{A}}$ are relatively prime, so that their greatest common divisor is the constantly 1 polynomial, then the Euclidean Algorithm guarantees (Fact 26.1.3) the existence of polynomials s_1 and s_2 such that

$$s_1 \cdot p + s_2 \cdot \mu_{\mathcal{A}} = 1\ .$$

In that case

$$s_1(\mathcal{A})p(\mathcal{A}) + s_2(\mathcal{A})\mu_{\mathcal{A}}(\mathcal{A}) = \mathcal{I}\ .$$

Since $\mu_{\mathcal{A}}(\mathcal{A}) = \mathcal{O}$,

$$s_1(\mathcal{A})p(\mathcal{A}) = \mathcal{I}\ ,$$

which shows that $p(\mathcal{A})$ is (left-)invertible, and hence is invertible, being a square matrix.

1. $\Longrightarrow$ **2. :** Suppose that $p(\mathcal{A})$ is invertible. Let us show that p and $\mu_{\mathcal{A}}$ are relatively prime. If this were not the case, then p and $\mu_{\mathcal{A}}$ would share a prime factor g (TYC 26.1.2). Then $g(\mathcal{A})$ would not be invertible (Lem. 26.2.2), and so $p(\mathcal{A})$ would not be invertible by Lemma 26.2.1, contradicting our hypothesis. ■

Comment 26.2.4

At this point the reader should explore the ways of using computing software to test whether two given polynomials share prime factors. Two polynomials share no prime factors exactly when their "greatest common divisor" (which we shall not define here) equals the constantly 1 polynomial.

In *Mathematica* , the command **PolynomialGCD**[ ] yields the "greatest common divisor", and so can be used to determine whether two given polynomials share prime factors.

26.3 Eigenvalues And Eigenvectors

Terminology 26.3.1

When $\mathcal{A}$ is a square matrix, $\mathcal{A} - \lambda\mathcal{I}$ is non-jective exactly when it is not injective; i.e. when it has a non-trivial nullspace. This is equivalent to $\mathcal{A} - \lambda\mathcal{I}$ annihilating a non-null tuple Z, which amounts to the equality

$$\mathcal{A}(Z) = \lambda Z \ .$$

When $\mathcal{A}$ sends a *non-null* tuple X to a scalar multiple of itself, i.e. $\mathcal{A}(X) \in$ *Span* (X), we say that X is an **eigenvector** for $\mathcal{A}$. *

Despite its name, an eigenvector of a matrix $\mathcal{A}$ is NOT a (geometric) vector: it is a tuple.

The scalar by which an eigenvector is altered through an application of $\mathcal{A}$ is said to be the corresponding **eigenvalue** for $\mathcal{A}$. Together, an eigenvector and the corresponding eigenvalue form an **eigenpair** for $\mathcal{A}$. We will list the eigenvalue first, and the eigenvector second.

So, (λ, X) is an eigenpair for $\mathcal{A}$ exactly when X is not null and $\mathcal{A}(X) = \lambda X$.

As we shall see later, not every matrix has eigenpairs.

While eigenvectors are never null, zero can be an eigenvalue of a matrix.

*One translation of "eigen" from German is "peculiar (to)". In this sense an eigenvector is a "vector peculiar to" a matrix, except that it is not a vector but a tuple!

Geometric intuition: A function sends a vector to a multiple of itself when it simply stretches or shrinks it, and perhaps reverses its direction, without rotating it off its original line, so to speak.

A rotation of vectors in Υ^2_P by 45 degrees within P does not send any non-null vector to a multiple of itself, while a rotation of vectors in Υ^3 by 45 degrees about a given axis does.

Test Your Comprehension 26.3.2

A matrix $\mathcal{A}$ sends a tuple X to itself exactly when either X is null, or $(1, X)$ is an eigenpair for $\mathcal{A}$.

Test Your Comprehension 26.3.3 ☞ **Eigenvalues and the non-jectivity of $\mathcal{A} - \lambda\mathcal{I}$**

The following statements are equivalent for $\mathcal{A} \in \mathbb{M}_n$.

1. λ is an eigenvalue of $\mathcal{A}$.
2. $\mathcal{A} - \lambda\mathcal{I}$ is not injective.
3. $\mathcal{A} - \lambda\mathcal{I}$ is not surjective.
4. $\mathcal{A} - \lambda\mathcal{I}$ is not invertible.

In such a case the non-null tuples in $\mathit{Nullspace}(\mathcal{A} - \lambda\mathcal{I})$ are exactly the eigenvectors of $\mathcal{A}$ corresponding to the eigenvalue λ.

In particular, any non-null linear combination of eigenvectors for $\mathcal{A}$ corresponding to the same eigenvalue λ, is again an eigenvector corresponding to λ. Of course this includes the non-zero multiples of the eigenvectors.

Consequently, each eigenvalue corresponds to infinitely many eigenvectors.

Notation 26.3.4

When λ is an eigenvalue for $\mathcal{A}$, we shall write $\boldsymbol{E}_{\mathcal{A}}(\lambda)$ for $\mathit{Nullspace}(\mathcal{A} - \lambda\mathcal{I})$, and say that this space is the **eigenspace** for $\mathcal{A}$ corresponding to the eigenvalue λ.

Exercise 26.3.5

Suppose that $\mathcal{D}$ is a diagonal matrix in $\mathbb{M}_{64}$, and α appears on the diagonal of $\mathcal{D}$ exactly 39 times. Argue that the dimension of the eigenspace $\boldsymbol{E}_{\mathcal{D}}(\alpha)$ is 39.

Hint: Rank-Nullity theorem can be useful here.

Test Your Comprehension 26.3.6 ☞ **A matrix with no eigenvectors**

Show that matrix $\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$ has no eigenvectors.

The following fundamental result shows that in order to find the eigenvalues of a matrix we need to find the roots of its minimal polynomial. In one sense this is welcome news, but in another – it is a testament to the inaccessibility of the spectrum. One of the fundamental theories of abstract algebra indicates that there can be no general formulas[1] for finding roots of polynomials of degree 5 or higher.

The reader is certainly familiar with the quadratic formula, and may be aware that analogous, but far more complex formulas exist for finding the exact roots of cubic and quartic polynomials. Yet in working with matrices whose minimal polynomials have higher degrees, we often have to settle for approximating the eigenvalues. It is one of the aims of the subject of Numerical Linear Algebra to extract as much information as possible from such an approximation.

Despite this setback, the role of eigenvalues and eigenvectors remains central in matrix theory.

Corollary 26.3.7 ☞ **Where to look for the eigenvalues of $\mathcal{A}$**

The eigenvalues of $\mathcal{A}$ are exactly the real roots of $\mu_{\mathcal{A}}$.

Proof of Corollary 26.3.7. By TYC 26.3.3, λ is an eigenvalue of $\mathcal{A}$ exactly when $p(\mathcal{A})$ is not invertible, where $p(x) = x - \lambda$. By Theorem 26.2.3 this happens exactly when p shares a prime factor with $\mu_{\mathcal{A}}$. Yet our p has a single prime factor: itself. Thus, λ is an eigenvalue of $\mathcal{A}$ exactly when $x - \lambda$ is a prime factor of $\mu_{\mathcal{A}}$, and so exactly when λ is a root of $\mu_{\mathcal{A}}$. ∎

26.3.1 — The Real Spectrum

Even though a geometric intuition suggests that eigenvectors are the primary objects, and the eigenvalues are auxiliary, this is not a correct assessment. The importance of eigenvalues in linear algebra is paramount.

Terminology 26.3.8

λ is an eigenvalue of a matrix $\mathcal{A}$ when it corresponds to an eigenvector of $\mathcal{A}$. The set of all eigenvalues of $\mathcal{A}$ is denoted by $\sigma_{\mathbb{R}}(\mathcal{A})$, and is said to be the **real spectrum** of $\mathcal{A}$. Sometimes this set is empty (TYC 26.3.6).

[1]... involving the basic algebraic operations of addition/subtraction, multiplication/division, and extraction of roots.

Exercise 26.3.9 ☞ **Spectrum of a $\triangle^r$ matrix**

Argue that the real spectrum of a triangular matrix is the set of numbers that appear on its diagonal.

Hint: Cor. 13.2.18.

Exercise 26.3.10

Find the real spectrum of each of the following 37×37 matrices.

1. The identity matrix.
2. A swap.
3. A partial scaling.
4. A shear.

Hint: Look for the vectors that are sent to multiples of themselves.

Test Your Comprehension 26.3.11 ☞ **When 0 is an eigenvalue**

Argue that the following claims are equivalent for an $\mathcal{A} \in \mathbb{M}_n$.

1. $0 \in \sigma_{\mathbb{R}}(\mathcal{A})$.
2. $\mathcal{A}$ is NOT invertible.
3. *Nullspace* $(\mathcal{A})$ is non-trivial .

In such a case,

$$\mathit{Nullspace}\,(\mathcal{A}) = \boldsymbol{E}_{\mathcal{A}}(0) \ .$$

Theorem 26.3.12 ☞ **Spectrum is invariant under transposition**

For any $\mathcal{A} \in \mathbb{M}_n$,

$$\sigma_{\mathbb{R}}(\mathcal{A}) = \sigma_{\mathbb{R}}\left(\mathcal{A}^{T}\right) \ .$$

Proof of Theorem 26.3.12. λ is an eigenvalue of $\mathcal{A}$ exactly when $\mathcal{A} - \lambda\mathcal{I}$ is not invertible. The latter condition is equivalent to the non-invertibility of $(\mathcal{A} - \lambda\mathcal{I})^{T}$ (TYC 26.3.3); i.e. to the non-invertibility of $\mathcal{A}^{T} - \lambda\mathcal{I}$. Yet $\mathcal{A}^{T} - \lambda\mathcal{I}$ is non-invertible exactly when λ is an eigenvalue of $\mathcal{A}^{T}$. This argument shows that

$$\lambda \in \sigma_{\mathbb{R}}(\mathcal{A}) \iff \lambda \in \sigma_{\mathbb{R}}\left(\mathcal{A}^{T}\right) \ ,$$

which establishes the required equality of sets $\sigma_{\mathbb{R}}(\mathcal{A})$ and $\sigma_{\mathbb{R}}\left(\mathcal{A}^{T}\right)$. ■

Exercise 26.3.13

Find an example of a 2×2 matrix $\mathcal{A}$ and an eigenpair (λ, X) for $\mathcal{A}$ such that (λ, X) is NOT an eigenpair for $\mathcal{A}^{T}$.

How does this relate to Theorem 26.3.12?

Theorem 26.3.14 ☞ **Spectrum is invariant under similarity**

For any $\mathcal{A} \in \mathbb{M}_n$ and any invertible $\mathcal{S} \in \mathbb{M}_n$,

$$\sigma_{\mathbb{R}}(\mathcal{A}) = \sigma_{\mathbb{R}}\left(\mathcal{S}^{-1}\mathcal{A}\mathcal{S}\right) .$$

Proof of Theorem 26.3.14. The key to the argument is the following observation.

$$\begin{aligned} \mathcal{S}^{-1}\mathcal{A}\mathcal{S} - \lambda\mathcal{I} &= \mathcal{S}^{-1}\mathcal{A}\mathcal{S} - \lambda\mathcal{S}^{-1}\mathcal{S} \\ &= \mathcal{S}^{-1}\mathcal{A}\mathcal{S} - \lambda\mathcal{S}^{-1}\mathcal{I}\mathcal{S} \\ &= \mathcal{S}^{-1}\left(\mathcal{A} - \lambda\mathcal{I}\right)\mathcal{S} , \end{aligned}$$

which shows that matrices $\mathcal{S}^{-1}\mathcal{A}\mathcal{S} - \lambda\mathcal{I}$ and $\mathcal{A} - \lambda\mathcal{I}$ are similar, hence have the same jectivity, and therefore

$$\mathcal{S}^{-1}\mathcal{A}\mathcal{S} - \lambda\mathcal{I} \text{ is not invertible} \iff \mathcal{A} - \lambda\mathcal{I} \text{ is not invertible;}$$

i.e. (TYC 26.3.3)

$$\lambda \in \sigma_{\mathbb{R}}\left(\mathcal{S}^{-1}\mathcal{A}\mathcal{S}\right) \iff \lambda \in \sigma_{\mathbb{R}}(\mathcal{A}) .$$ ■

Comment 26.3.15

Spectrum is NOT invariant under matrix equivalence. Recall that two $n \times n$ matrices are equivalent exactly when they have the same rank. In particular any two invertible $n \times n$ matrices are equivalent. It is easy to give an example of two diagonal invertible matrices that have very different entries on the diagonal, and hence very different spectra (Exc. 26.3.9).

Exercise 26.3.16

Argue that the following statements are equivalent for a matrix $\mathcal{A} \in \mathbb{M}_n$.

1. $\lambda \in \sigma_{\mathbb{R}}(\mathcal{A})$.

2. $0 \in \sigma_{\mathbb{R}}(\mathcal{A} - \lambda\mathcal{I})$.

3. $73\lambda \in \sigma_{\mathbb{R}}(73\,\mathcal{A})$.

Theorem 26.3.17 ☞ **Spectrum and inversion**

For any *invertible* $\mathcal{A}$,

$$\sigma_{\mathbb{R}}\left(\mathcal{A}^{-1}\right) = \left\{ \lambda^{-1} \;\middle|\; \lambda \in \sigma_{\mathbb{R}}(\mathcal{A}) \right\} = \left\{ \frac{1}{\lambda} \;\middle|\; \lambda \in \sigma_{\mathbb{R}}(\mathcal{A}) \right\} .$$

Proof of Theorem 26.3.17. The following formula is the key to the argument. Here $\alpha \neq 0$.

$$\begin{aligned} \mathcal{A}^{-1} - \alpha\mathcal{I} &= \mathcal{A}^{-1}\left(\mathcal{I} - \alpha\mathcal{A}\right) \\ &= \alpha\mathcal{A}^{-1}\left(\frac{1}{\alpha}\mathcal{I} - \mathcal{A}\right) \\ &= -\alpha\mathcal{A}^{-1}\left(\mathcal{A} - \frac{1}{\alpha}\mathcal{I}\right) . \end{aligned}$$

Since $-\alpha\mathcal{A}^{-1}$ is invertible, matrices $\mathcal{A}^{-1} - \alpha\mathcal{I}$ and $\mathcal{A} - \frac{1}{\alpha}\mathcal{I}$ are equivalent square matrices, and hence have the same jectivity. Therefore

$$\mathcal{A}^{-1} - \alpha\mathcal{I} \text{ is not invertible} \iff \mathcal{A} - \tfrac{1}{\alpha}\mathcal{I} \text{ is not invertible.}$$

This shows (TYC 26.3.3) that for $\alpha \neq 0$,

$$\alpha \in \sigma_{\mathbb{R}}\left(\mathcal{A}^{-1}\right) \iff \frac{1}{\alpha} \in \sigma_{\mathbb{R}}(\mathcal{A}) .$$

In other words, the non-zero numbers in $\sigma_{\mathbb{R}}\left(\mathcal{A}^{-1}\right)$ are exactly the reciprocals of the non-zero numbers in $\sigma_{\mathbb{R}}(\mathcal{A})$. Yet, $\mathcal{A}^{-1}$ and $\mathcal{A}$ are invertible matrices, and so 0 is NOT in the spectrum of either (TYC 26.3.11). Thus the required formula has been established. ∎

Theorem 26.3.18 ☞ **The spectral mapping theorem**

If $\mathcal{A}(X) = \alpha X$, then

$$\Big(p(\mathcal{A})\Big)(X) = p(\alpha)\, X ,$$

for any polynomial p.

In particular, if (α, X) is an eigenpair for $\mathcal{A}$, then $\big(p(\alpha), X\big)$ is an eigenpair for $p(\mathcal{A})$.

Proof of Theorem 26.3.18. The following formulas are the key to the proof.

$$\mathcal{I}(X) = 1\,X\,;$$

$$\mathcal{A}(X) = \alpha\,X\,;$$

$$\mathcal{A}^2(X) = \mathcal{A}\Big(\mathcal{A}(X)\Big) = \mathcal{A}\Big(\alpha\,X\Big) = \alpha\,\mathcal{A}(X) = \alpha^2\,X\,;$$

$$\mathcal{A}^3(X) = \mathcal{A}\Big(\mathcal{A}^2(X)\Big) = \mathcal{A}\Big(\alpha^2\,X\Big) = \alpha^2\,\mathcal{A}(X) = \alpha^3\,X\,;$$

$$\mathcal{A}^4(X) = \mathcal{A}\Big(\mathcal{A}^3(X)\Big) = \mathcal{A}\Big(\alpha^3\,X\Big) = \alpha^3\,\mathcal{A}(X) = \alpha^4\,X\,;$$

etc.

Given a polynomial $p(z) := \sum_{i=0}^{k} c_i\,z^i$, we have

$$p(\mathcal{A}) = \sum_{i=0}^{k} c_i\,\mathcal{A}^i \quad\text{and}\quad p(\alpha) = \sum_{i=0}^{k} c_i\,\alpha^i\,.$$

Using the formulas above, we can make the following calculation, which completes the argument.

$$\left(\sum_{i=0}^{k} c_i\,\mathcal{A}^i\right)(X) = \sum_{i=0}^{k} c_i\,\Big(\mathcal{A}^i(X)\Big) = \sum_{i=0}^{k} c_i\,\Big(\alpha^i\,X\Big) = \left(\sum_{i=0}^{k} c_i\,\alpha^i\right)\,X\,. \quad \blacksquare$$

Comment 26.3.19

From Theorem 26.3.18 we know that if $\lambda \in \sigma_{\mathbb{R}}(\mathcal{A})$, then $p(\lambda) \in \sigma_{\mathbb{R}}\Big(p(\mathcal{A})\Big)$. This demonstrates the inclusion

$$\{\ p(\lambda)\ |\ \lambda \in \sigma_{\mathbb{R}}(\mathcal{A})\ \} \subseteq \sigma_{\mathbb{R}}\Big(p(\mathcal{A})\Big)\,,$$

and states that

a polynomial p maps the spectrum of $\mathcal{A}$ into the spectrum of $p(\mathcal{A})$.

This explains the name of Theorem 26.3.18.

It is natural to wonder whether the inclusion is actually an equality. Alas it is not. There examples of matrices $\mathcal{A}$ and polynomials p for which the set on the right is strictly larger than the set on the left. Here is one such.

Let $\mathcal{A} = \left[\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right]$ and let $p(x) = x^2$. As we know from TYC 26.3.6, this $\mathcal{A}$ has no eigenvalues. Yet

$$p(\mathcal{A}) = \mathcal{A}^2 = -\mathcal{I}_2 ,$$

and therefore (Exc. 26.3.9)

$$\sigma_{\mathbb{R}}\left(\mathcal{A}^2\right) = \{-1\} .$$

In this case

$$\left\{ \lambda^2 \;\middle|\; \lambda \in \sigma_{\mathbb{R}}(\mathcal{A}) \right\} = \left\{ \lambda^2 \;\middle|\; \lambda \in \emptyset \right\} = \emptyset \subsetneq \{-1\} = \sigma_{\mathbb{R}}\left(\mathcal{A}^2\right) .$$

An observant reader will discern an obvious obstacle to the equality: no real number can square to -1.

26.4 Invariant Subspaces

Terminology 26.4.1

A subspace $\boldsymbol{W}$ of $\mathbb{R}^n$ is said to be **invariant*** for a given matrix $\mathcal{A} \in \mathbb{M}_n$, if

$$\mathcal{A}(W) \in \boldsymbol{W}, \text{ whenever } W \in \boldsymbol{W} .$$

In other words, $\mathcal{A}$ does not map any inputs from $\boldsymbol{W}$ to outputs that are outside of $\boldsymbol{W}$; i.e.

$$\mathcal{A}\langle \boldsymbol{W}] \subseteq \boldsymbol{W}.$$

Obviously, $\{\mathcal{O}\}$ and $\mathbb{R}^n$ are invariant subspaces for any $\mathcal{A} \in \mathbb{M}_n$. Invariant subspaces other than these are the **non-trivial proper invariant subspaces**.

*A better term would be "**closed under the action of**".

Geometric intuition: Consider a line L within $\mathbb{E}^3$, and let $\mathcal{F}$ be a linear function that rotates each vector in Υ^3 by 45° about the line L in a prescribed "clockwise" direction. The null vector is sent to itself.

Since every vector in the subspace Υ^1_L is sent to itself by $\mathcal{F}$, we can think of Υ^1_L as being closed under the action of $\mathcal{F}$, or "invariant" under $\mathcal{F}$.

If we consider a plane P that is perpendicular to L, then every vector in Υ^2_P is mapped by $\mathcal{F}$ to a vector in Υ^2_P. So, Υ^2_P is also invariant under $\mathcal{F}$.

Test Your Comprehension 26.4.2

Every subspace of $\mathbb{R}^n$ is invariant under $\alpha\mathcal{I}_n$.

Hint: TYC 26.3.3.

Exercise 26.4.3

If $\lambda \in \sigma_{\mathbb{R}}(\mathcal{A})$ then the corresponding eigenspace $\boldsymbol{E}_{\mathcal{A}}(\lambda)$ is an invariant subspace for $\mathcal{A}$.

26.4.1 — Invariant Subspaces Of Dimensions 1 or 2

Theorem 26.4.4 ☞ **Existence of the invariant subspaces of small dimension**

Every matrix $\mathcal{A}$ in $\mathbb{M}_n$ has either a 1-dimensional invariant subspace, or a 2-dimensional invariant subspace.

Proof of Theorem 26.4.4. For non-triviality we may assume that $n \geq 3$. Otherwise the whole $\mathbb{R}^n$ being invariant under $\mathcal{A}$ settles the matter.

If $\mathcal{A}$ has has an eigenpair (λ, X), then $\mathcal{A}$ maps every multiple aX of X to a multiple of X (namely: λaX). Hence the 1-dimensional subspace $Span(X)$ is invariant under $\mathcal{A}$.

If $\mathcal{A}$ has no eigenvalues/eigenvectors, then by Theorem 20.3.11, $(\mathcal{A}-\beta\mathcal{I})^2 + \gamma^2\mathcal{I}$ is not injective for some β, γ, and so annihilates a non-null tuple Y.

In that case

$$\begin{aligned}\mathbb{O} &= \Big((\mathcal{A}-\beta\mathcal{I})^2 + \gamma^2\mathcal{I}\Big)(Y)\\ &= (\mathcal{A}-\beta\mathcal{I})^2(Y) + \gamma^2 Y\\ &= \mathcal{A}^2(Y) - 2\beta\mathcal{A}(Y) + \beta^2 Y + \gamma^2 Y\,,\end{aligned}$$

which shows that

$$\mathcal{A}^2(Y) = 2\beta\mathcal{A}(Y) - \Big(\beta^2 + \gamma^2\Big)\,Y\,.$$

Thus

$$\mathcal{A}^2(Y) \in Span\Big(Y, \mathcal{A}(Y)\Big)\,.$$

Consequently, for any a, b,

$$\mathcal{A}\Big(aY + b\mathcal{A}(Y)\Big) = a\mathcal{A}(Y) + b\mathcal{A}^2(Y) \in Span\Big(Y, \mathcal{A}(Y)\Big)\,,$$

which shows that $Span\Big(Y, \mathcal{A}(Y)\Big)$ is an invariant subspace for $\mathcal{A}$.

Since we are dealing with the case of $\mathcal{A}$ having no eigenvalues/eigenvectors, $\mathcal{A}(Y)$ is not a scalar multiple of Y, and therefore the list $Y, \mathcal{A}(Y)$ is a linearly independent list that spans $Span\Big(Y, \mathcal{A}(Y)\Big)$. In other words, $Y, \mathcal{A}(Y)$ is a coordinate system of $Span\Big(Y, \mathcal{A}(Y)\Big)$. This shows that $Span\Big(Y, \mathcal{A}(Y)\Big)$ is a 2-dimensional invariant subspace for $\mathcal{A}$. ■

Test Your Comprehension 26.4.5

The 1-dimensional invariant subspaces of a matrix $\mathcal{A}$ are exactly the subspaces $Span\,(X)$, where X is an eigenvector of $\mathcal{A}$.

26.5 Invariance of Ranges and Nullspaces

The following theorem is supremely useful, since we know that every subspace of $\mathbb{R}^n$ is a range of an $n \times n$ matrix.

Theorem 26.5.1 ☞ **Range invariance equation**

For matrices $\mathcal{A} \in \mathbb{M}_n$ and $\mathcal{B} \in \mathbb{M}_{n\times m}$ the following are equivalent.

1. $Range\,(\mathcal{B})$ is an invariant subspace for $\mathcal{A}$.

2. $\mathcal{AB} = \mathcal{BC}$, for some matrix $C \in \mathbb{M}_m$.

Proof of Theorem 26.5.1.

2. $\Longrightarrow$ 1.: We want to show that $\mathcal{A}(Z) \in Range\,(\mathcal{B})$, whenever $Z \in Range\,(\mathcal{B})$. If $Z \in Range\,(\mathcal{B})$, then $Z = \mathcal{B}(Y)$ for some $Y \in \mathbb{R}^m$. Then

$$\mathcal{A}(Z) = \mathcal{A}\Big(\mathcal{B}(Y)\Big) = (\mathcal{AB})(Y) = (\mathcal{BC})(Y) = \mathcal{B}\Big(\mathcal{C}(Y)\Big) \in Range\,(\mathcal{B}) \ .$$

1. $\Longrightarrow$ 2.: Suppose that $\mathcal{A}\left\langle Range\,(\mathcal{B})\right] \subseteq Range\ \mathcal{B}$. By Excercise 2.3.10,

$$\mathcal{A}\left\langle Range\,(\mathcal{B})\right] = Range\,(\mathcal{AB})\,.$$

Hence

$$Range\,(\mathcal{AB}) \subseteq Range\,(\mathcal{B}) \ ,$$

and we can apply Range Inclusion Factorization (Theorem 13.1.2) to conclude that $\mathcal{AB} = \mathcal{BC}$, for some matrix $C \in \mathbb{M}_m$. ■

Theorem 26.5.2 ☞ **Invariant subspaces and transposition**

The following statements are equivalent for a matrix $\mathcal{A}$.

1. $\boldsymbol{W}$ is an invariant subspace for $\mathcal{A}$.

2. $\boldsymbol{W}^{\perp}$ is an invariant subspace for $\mathcal{A}^{T}$.

A proof of Theorem 26.5.2 is presented in the appendix to the chapter.

Test Your Comprehension 26.5.3

The following statements are equivalent for a matrix $\mathcal{A}$.

1. $\boldsymbol{W}$ is an invariant subspace for $\mathcal{A}^{T}$.

2. $\boldsymbol{W}^{\perp}$ is an invariant subspace for $\mathcal{A}$.

Exercise 26.5.4 ☞ **Nullspace invariance equation**

For matrices $\mathcal{A} \in \mathbb{M}_n$ and $\mathcal{B} \in \mathbb{M}_{m\times n}$ the following are equivalent.

1. $\mathit{Nullspace}\,(\mathcal{B})$ is an invariant subspace for $\mathcal{A}$.

2. $\mathcal{B}\mathcal{A} = \mathcal{C}\mathcal{B}$, for some matrix $C \in \mathbb{M}_m$.

Hint: By TYC 19.4.1, $\mathit{Nullspace}\,(\mathcal{B}) = \left(\mathit{Range}\left(\mathcal{B}^{T}\right)\right)^{\perp}$. TYC 26.5.3 and Thm. 26.5.1 can be helpful here.

Test Your Comprehension 26.5.5

If matrices $\mathcal{A}$ and $\mathcal{B}$ commute, then the range and the nullspace of $\mathcal{B}$ are invariant subspaces for $\mathcal{A}$.

26.6 Invariant Subspaces and Partitioning

Theorem 26.6.1 ☞ **Invariant Subspaces and Partitioning**

The following statements about a matrix $\mathcal{A} \in \mathbb{M}_{13}$ are equivalent.

1. $\mathcal{A}$ can be expressed as a partitioned matrix $\begin{bmatrix} \mathcal{B} & \mathcal{G} \\ \mathcal{O} & \mathcal{D} \end{bmatrix}_{(5|8)\times(5|8)}$.

2. $\mathit{Span}\left(E_1, E_2, \ldots, E_5\right)$ is an invariant subspace of $\mathcal{A}$.

This result holds in general as well.

Proof of Theorem 26.6.1. Let $\mathcal{A}$ be partitioned as $\left[\begin{smallmatrix}\mathcal{B} & \mathcal{G}\\ \mathcal{L} & \mathcal{D}\end{smallmatrix}\right]_{(5|8)\times(5|8)}$.

Each of the following statements is clearly equivalent to the adjacent claims.

- $Span\left(E_1, E_2, \dots, E_5\right)$ is invariant under $\mathcal{A}$.
- $Range\left(\begin{bmatrix}E_1 & E_2 & \cdots & E_5\end{bmatrix}_{13\times 5}\right)$ is invariant under $\mathcal{A}$.
- There is a matrix $\mathcal{C} \in \mathbb{M}_5$ such that

$$\mathcal{A}\begin{bmatrix}E_1 & E_2 & \cdots & E_5\end{bmatrix} = \begin{bmatrix}E_1 & E_2 & \cdots & E_5\end{bmatrix}\mathcal{C} \quad \text{(Thm. 26.5.1)}\ ,$$

  i.e.

$$\left[\begin{smallmatrix}\mathcal{B} & \mathcal{G}\\ \mathcal{L} & \mathcal{D}\end{smallmatrix}\right]_{(5|8)\times(5|8)}\begin{bmatrix}\mathcal{I}_5\\ \mathcal{O}\end{bmatrix} = \begin{bmatrix}\mathcal{I}_5\\ \mathcal{O}\end{bmatrix}\mathcal{C}\ ,$$

  i.e.

$$\left[\begin{smallmatrix}\mathcal{B}\\ \mathcal{L}\end{smallmatrix}\right]_{(5|8)\times 5} = \left[\begin{smallmatrix}\mathcal{C}\\ \mathcal{O}\end{smallmatrix}\right]_{(5|8)\times 5}\ .$$

- $\mathcal{L} = \mathcal{O}$. ■

Theorem 26.6.2 ☞ **Invariant Subspaces And Similarity**

Suppose that $\boldsymbol{W}$ is subspace of $\mathbb{R}^n$, $\mathcal{A} \in \mathbb{M}_n$, and $\mathcal{S} \in \mathbb{M}_n$ is an invertible matrix. Then the following are equivalent.

1. $\boldsymbol{W}$ is invariant under $\mathcal{S}^{-1}\mathcal{A}\mathcal{S}$.
2. $\mathcal{S}\left\langle\boldsymbol{W}\right]$ is invariant under $\mathcal{A}$.

Proof of Theorem 26.6.2. Since every subspace of $\mathbb{R}^n$ can be expressed as a range of an $n \times n$ matrix, let us say that $\boldsymbol{W} = Range(\mathcal{B})$, where $\mathcal{B} \in \mathbb{M}_n$. Then

$$\mathcal{S}\left\langle\boldsymbol{W}\right] = \mathcal{S}\left\langle Range(\mathcal{B})\right] \overset{\text{Exc. 2.5.18}}{=} Range(\mathcal{S}\mathcal{B})\ ,$$

and by the range invariance equation (Thm. 26.5.1), condition 2. is equivalent to the following statement:

$$\mathcal{A}\mathcal{S}\mathcal{B} = \mathcal{S}\mathcal{B}\mathcal{C}, \quad \text{for some } \mathcal{C} \in \mathbb{M}_n\ . \tag{26.2}$$

Similarly, condition 1. is equivalent to the following statement:

$$\mathcal{S}^{-1}\mathcal{A}\mathcal{S}\mathcal{B} = \mathcal{B}\mathcal{D}. \quad \text{for some } \mathcal{D} \in \mathbb{M}_n\ . \tag{26.3}$$

The latter is equivalent to the claim:

$$\mathcal{A}\mathcal{S}\mathcal{B} = \mathcal{S}\mathcal{B}\mathcal{D}, \quad \text{for some } \mathcal{D} \in \mathbb{M}_n\ , \tag{26.4}$$

obtained via multiplying (26.6) through by $\mathcal{S}$ on the left.

Since (26.2) and (26.4) are obviously equivalent, the proof is complete. ■

Theorem 26.6.3 ☞ **Invariant Subspaces, Similarity and Partitioning**

The following statements about a matrix $\mathcal{A} \in \mathbb{M}_{13}$ are equivalent.

1. $\mathcal{A}$ has a 5-dimensional invariant subspace.

2. $\mathcal{A}$ is similar to a matrix that can be partitioned as $\begin{bmatrix} \mathcal{B} & \mathcal{C} \\ \mathcal{O} & \mathcal{D} \end{bmatrix}_{(5|8)\times(5|8)}$.

3. $\mathcal{A}$ is unitarily similar to a matrix that can be partitioned as $\begin{bmatrix} \mathcal{B} & \mathcal{C} \\ \mathcal{O} & \mathcal{D} \end{bmatrix}_{(5|8)\times(5|8)}$.

This result holds in general as well.

Proof of Theorem 26.6.3. The implication 3. $\Longrightarrow$ 2. is trivial. Let us verify the validity of 2. $\Longrightarrow$ 1. and 1. $\Longrightarrow$ 3.

In view of Theorem 26.6.1, statement 2. is equivalent to the claim that there is an invertible matrix $\mathcal{S} \in \mathbb{M}_{13}$ such that

$$\textit{Range}\begin{bmatrix} E_1 & E_2 & \cdots & E_5 \end{bmatrix} \text{ is invariant under } \mathcal{S}^{-1}\mathcal{A}\,\mathcal{S};$$

i.e. such that

$$\mathcal{S}\left\langle \textit{Range}\begin{bmatrix} E_1 & E_2 & \cdots & E_5 \end{bmatrix}\right] \text{ is invariant under } \mathcal{A} \text{ (Thm. 26.6.2);}$$

i.e. such that

$$\textit{Range}\begin{bmatrix} \mathcal{S}\left(E_1\right) & \mathcal{S}\left(E_2\right) & \cdots & \mathcal{S}\left(E_5\right) \end{bmatrix} \text{ is invariant under } \mathcal{A} \text{ (Thm. 2.3.10).}$$

Statement 3. is equivalent to a similar claim, with the additional condition that $\mathcal{S}$ is a unitary matrix.

2. $\Longrightarrow$ 1.: If condition 2. holds then *Range* $\begin{bmatrix} \mathcal{S}\left(E_1\right) & \mathcal{S}\left(E_2\right) & \cdots & \mathcal{S}\left(E_5\right) \end{bmatrix}$ is invariant under $\mathcal{A}$. It remains for us to establish that this subspace is 5-dimensional.

Since $\mathcal{S}$ is an invertible matrix, its columns (given by $\mathcal{S}\left(E_i\right)$) are linearly independent. Therefore $\begin{bmatrix} \mathcal{S}\left(E_1\right) & \mathcal{S}\left(E_2\right) & \cdots & \mathcal{S}\left(E_5\right) \end{bmatrix}_{13\times 5}$ is an injection, and so has nullity zero. By Rank-Nullity theorem, *Range* $\begin{bmatrix} \mathcal{S}\left(E_1\right) & \mathcal{S}\left(E_2\right) & \cdots & \mathcal{S}\left(E_5\right) \end{bmatrix}$ is a 5-dimensional subspace of $\mathbb{R}^{13}$.

1. $\Longrightarrow$ 3.: Suppose that $\boldsymbol{W}$ is a 5-dimensional invariant subspace of $\mathcal{A}$. Then $\boldsymbol{W}$ has an orthonormal coordinate system $W_1, W_2, W_3, \ldots, W_5$ (Thm. 24.1.8). This coordinate system, being an orthonormal list in $\mathbb{R}^{13}$, can be extended to an orthonormal coordinate system of $\mathbb{R}^{13}$ through an insertion of some eight tuples $Z_1, Z_2, Z_3, \ldots, Z_8$ into the list (Thm. 24.1.10). Then

$$\mathcal{U} := \begin{bmatrix} W_1 & W_2 & \cdots & W_5 & Z_1 & Z_2 & \cdots & Z_8 \end{bmatrix}_{13\times 13}$$

defines a unitary matrix and

$$\begin{aligned} &Range\left[\mathcal{U}\left(E_1\right)\ \ \mathcal{U}\left(E_2\right)\ \cdots\ \mathcal{U}\left(E_5\right)\right] \\ &= Range\left[W_1\ \ W_2\ \cdots\ W_5\right] = \boldsymbol{W}\ . \end{aligned}$$

Hence $Range\left[\mathcal{U}\left(E_1\right)\ \ \mathcal{U}\left(E_2\right)\ \cdots\ \mathcal{U}\left(E_5\right)\right]$ is invariant under $\mathcal{A}$, and our argument at the beginning of the proof shows that $\mathcal{U}^{-1}\mathcal{A}\mathcal{U}$ has the required partitioned form. ■

Test Your Comprehension 26.6.4

For $n \geq 3$, every $\mathcal{A} \in \mathbb{M}_n$ is unitarily similar to a matrix that can be partitioned as $\left[\begin{smallmatrix} \mathcal{B} & \mathcal{C} \\ \mathcal{O} & \mathcal{D} \end{smallmatrix}\right]$, with $\mathcal{B}$ in $\mathbb{M}_1$ or $\mathbb{M}_2$.

Hint: Thms. 26.4.4 and 26.6.3 can be very helpful here.

Theorem 26.6.5 ☞ **Eigenvalues and partitioning**

The following are equivalent for a matrix $\mathcal{M} \in \mathbb{M}_n$.

1. $\lambda \in \sigma_{\mathbb{R}}(\mathcal{M})$; i.e. λ is an eigenvalue of $\mathcal{M}$.

2. $\mathcal{M}$ is similar to a partitioned matrix of the form $\left[\begin{smallmatrix} [\lambda] & \mathcal{B} \\ \mathcal{O} & \mathcal{D} \end{smallmatrix}\right]$;

   i.e. $\mathcal{M}$ is similar to a matrix whose first column is λE_1.

3. $\mathcal{M}$ is *unitarily* similar to a partitioned matrix of the form $\left[\begin{smallmatrix} [\lambda] & \mathcal{B} \\ \mathcal{O} & \mathcal{D} \end{smallmatrix}\right]$;

   i.e. $\mathcal{M}$ is unitarily similar to a matrix whose first column is λE_1. *

*In the proof we show that if $\mathcal{M}$ cannot itself be partitioned in the described fashion, then the mentioned unitary can be chosen to be a Householder matrix.

Proof of Theorem 26.6.5. A proof of this theorem follows the same steps as the proof of Theorem 26.6.3. An alternative proof which uses Householder unitaries is presented in the appendix to this chapter. ■

26.6.1 — A Degree Bound for Minimal Polynomials

Theorem 26.6.6 ☞ **A degree bound for minimal polynomials**

The degree of the minimal polynomial $\mu_{\mathcal{A}}$ of an $n \times n$ matrix $\mathcal{A}$ is never greater than n.

Proof of Theorem 26.6.6. In view of Theorem 21.1.3, it shall be sufficient to show that every $\mathcal{A} \in \mathbb{M}_n$ is annihilated by some monic polynomial of degree n.

We already know that this holds true when $n = 1$ and $n = 2$ (TYC 20.3.3 and Exercise 20.3.4). To establish the claim for all square matrices, let us show that there are no exceptions to the rule, i.e. no counterexamples.

If there were counterexamples to the claim, among them there would be one (say $\mathcal{A}_{\circ}$) of *smallest* size $n_{\circ}$. We know that $n_{\circ}$ has to be at least 3, and that the claim holds true for all square matrices of size smaller than $n_{\circ} \times n_{\circ}$.

By TYC 26.6.4, there exists a unitary $\mathcal{U} \in \mathbb{M}_{n_{\circ}}$ such that $\mathcal{M} := \mathcal{U}^{-1}\mathcal{A}_{\circ}\mathcal{U}$ can be partitioned as $\left[\begin{smallmatrix} \mathcal{B} & \mathcal{C} \\ \mathcal{O} & \mathcal{D} \end{smallmatrix}\right]$, with $\mathcal{B}$ in $\mathbb{M}_k$, where k is 1 or 2. Note that $\mathcal{M}$ has exactly the same minimal polynomial as $\mathcal{A}_{\circ}$ (Thm. 21.1.8).

This explains why it is worth developing the theory of invariant subspaces: the existence of invariant subspaces often allows us to replace a given matrix with a block-upper-triangular one (more on this in the next section).

Now, $\mathcal{B}$ and $\mathcal{D}$ are square matrices that are strictly smaller than our minimal presumed counterexample $\mathcal{A}_{\circ}$. Hence there are monic polynomials p and q of degrees k and $n_{\circ} - k$ respectively, that annihilate $\mathcal{B}$ and $\mathcal{D}$ respectively.

We shall show that the monic polynomial pq of degree $n_{\circ}$ annihilates $\mathcal{M}$, and so annihilates $\mathcal{A}_{\circ}$ as well (Thm. 21.1.8). Yet this will imply that $\mathcal{A}_{\circ}$ is NOT a counterexample to the claim of the theorem, which contradicts our choice of $\mathcal{A}_{\circ}$. Therefore, at that point, the only feasible conclusion shall be that there are no counterexamples to the theorem.

The following calculation shows that pq annihilates $\mathcal{M}$.

$$(pq)(\mathcal{M}) \overset{\text{TYC 20.2.8}}{=} \Big(p(\mathcal{M})\Big)\Big(q(\mathcal{M})\Big) \overset{\text{Exc. 20.2.6}}{=} \begin{bmatrix} p(\mathcal{B}) & \square \\ \mathcal{O} & p(\mathcal{D}) \end{bmatrix} \begin{bmatrix} q(\mathcal{B}) & \diamondsuit \\ \mathcal{O} & q(\mathcal{D}) \end{bmatrix}$$

$$= \begin{bmatrix} \mathcal{O} & \square \\ \mathcal{O} & p(\mathcal{D}) \end{bmatrix} \begin{bmatrix} q(\mathcal{B}) & \diamondsuit \\ \mathcal{O} & \mathcal{O} \end{bmatrix} = \mathcal{O} \,. \qquad \blacksquare$$

Hint: Cor. 26.3.7.

Test Your Comprehension 26.6.7

An $n \times n$ matrix cannot have more than n eigenvalues.

Corollary 26.6.8

If $\mathcal{A} \in \mathbb{M}_n$ is a nilpotent matrix then $\mathcal{A}^n = \mathcal{O}$.

Comment 26.6.9

Recall that a matrix is nilpotent when some power of it is null. In particular, Corollary 26.6.8 tells us that the 7-th power of a 7×7 matrix is null if any power of it (say, 148362-th) is null.

Proof of Corollary 26.6.8. If $\mathcal{A} \in \mathbb{M}_n$ is nilpotent, then it is annihilated by some polynomial $p(x) = x^k$, and therefore this p is a polynomial multiple of $\mu_{\mathcal{A}}$.

Note that

$$p(x) = (x-0)(x-0)\cdots(x-0)$$

is the prime factorization of p. Hence $\mu_{\mathcal{A}}(x) = x^m$ for some $m \leq n$ (Thms. 20.1.24 and 26.6.6). Thus $q(x) = x^n = x^{n-m}\mu_{\mathcal{A}}$ annihilates $\mathcal{A}$ (Thm. 21.1.3). ■

26.7 Appendix: Exiled Proofs

Proof of Theorem 26.5.2. Let us verify the implication **1.** $\Longrightarrow$ **2.** Once this is done, the implication **2.** $\Longrightarrow$ **1.** follows: simply treat $\mathcal{A}^T$ as a new matrix $\mathcal{A}_o$ and $\boldsymbol{W}^\perp$ as a new subspace $\boldsymbol{W}_o$. Then recall that

$$\left(\boldsymbol{W}^\perp\right)^\perp \overset{\text{Thm. 19.3.2}}{=} \boldsymbol{W} \,.$$

1. $\Longrightarrow$ **2. :** Suppose that $\boldsymbol{W}$ is invariant subsapce for $\mathcal{A}$. Since every subspace of $\mathbb{R}^n$ is a range of a matrix (TYC 18.3.19), we can express $\boldsymbol{W}$ as the range of a matrix $\mathcal{B}$. Then

$$\mathcal{A}\mathcal{B} = \mathcal{B}\mathcal{C} \,, \tag{26.5}$$

for some matrix C, by the range invariance equation (Thm. 26.5.1).

At the same time,

$$\boldsymbol{W}^\perp = \left(\mathit{Range}\,(\mathcal{B})\right)^\perp \overset{\text{TYC 12.1.10}}{=} \mathit{Nullspace}\left(\mathcal{B}^T\right) \,.$$

So, out goal is to show that $\mathit{Nullspace}\left(\mathcal{B}^T\right)$ is an invariant subspace for $\mathcal{A}^T$.

To this end, we will show that for any tuple X in $\mathit{Nullspace}\left(\mathcal{B}^T\right)$:

$$\mathcal{A}^T(X) \in \mathit{Nullspace}\left(\mathcal{B}^T\right) \,.$$

In other words, we will show that for any X annihilated by $\mathcal{B}^T$: $\mathcal{A}^T(X)$ is also annihilated by $\mathcal{B}^T$.

Equivalently, we aim to show that

$$\mathcal{B}^T\left(\mathcal{A}^T(X)\right) = \mathbb{O} ,$$

whenever

$$\mathcal{B}^T(X) = \mathbb{O} .$$

By transposing both sides of the equality in (26.5), we arrive at the equality

$$\mathcal{B}^T\mathcal{A}^T = \mathcal{C}^T\mathcal{B}^T ,$$

which shows that

$$\mathcal{B}^T\mathcal{A}^T(X) = \mathcal{C}^T\mathcal{B}^T(X) ,$$

and therefore validates the implication

$$\mathcal{B}^T(X) = \mathbb{O} \implies \mathcal{B}^T\left(\mathcal{A}^T(X)\right) = \mathbb{O} . \qquad \blacksquare$$

Proof of Theorem 26.6.5. Let us entertain the reader with a slick alternate proof which uses Householder unitaries.

We shall verify the implications 1. $\implies$ 3. and 2. $\implies$ 1., since the implication 3. $\implies$ 2. is trivial.

1. $\implies$ 3.: If λ is an eigenvalue of $\mathcal{M}$, let X be a corresponding eigenvector for $\mathcal{M}$. We may choose X to be a unit tuple, since a scalar multiple of an eigenvector is again an eigenvector. Obviously

$$\mathcal{M}(X) = \lambda X .$$

If $X = E_1$, then

$$\mathcal{M}(E_1) = \lambda E_1 ,$$

so that the first column of $\mathcal{M}$ is already λE_1, and we are done (since $\mathcal{M}$ is unitarily similar to itself, of course).

If $X \neq E_1$, then there exists a Householder unitary $\mathcal{H}$ that maps E_1 to X (Thm. 23.1.22), and consequently $\mathcal{H}^{-1}(X) = E_1$.

In this case,

$$\left(\mathcal{H}^{-1}\mathcal{M}\mathcal{H}\right)(E_1) = \left(\mathcal{H}^{-1}\mathcal{M}\right)(X) = \mathcal{H}^{-1}(\lambda X) = \lambda E_1 ,$$

which shows that the first column of $\mathcal{H}^{-1}\mathcal{M}\mathcal{H}$ is λE_1.

2. $\Longrightarrow$ **1.:** If $\mathcal{S}$ is an invertible matrix such that the first column of $\mathcal{S}^{-1}\mathcal{M}\mathcal{S}$ is λE_1, then

$$\mathcal{S}^{-1}\mathcal{M}\mathcal{S}(E_1) = \lambda E_1 \ ,$$

and consequently

$$\mathcal{M}\Big(\mathcal{S}(E_1)\Big) = \lambda \mathcal{S}(E_1) \ .$$

This shows that the non-null tuple $\mathcal{S}(E_1)$ belongs to the nullspace of $\mathcal{M} - \lambda\mathcal{I}$, which shows that the latter is not invertible. Hence λ is an eigenvalue of $\mathcal{M}$ (TYC 26.3.3). ∎

27. Triangularization and Diagonalization

Last modified on December 8, 2018

27.1 Schur's Block-Triangularization Theorem

Theorem 27.1.1 ☞ **Schur's block-triangularization**

Every $\mathcal{A} \in \mathbb{M}_n$ is unitarily similar to a block-upper-triangular matrix and to a block-lower-triangular matrix, with all diagonal blocks being either 1×1 or 2×2, and all 2×2 diagonal blocks having prime quadratic minimal polynomials.

A proof of Theorem 27.1.1 is presented in the appendix to the chapter.

Exercise 27.1.2

In Schur's block-triangularization theorem, the 1×1 diagonal blocks give all of the eigenvalues of $\mathcal{A}$ (and so all of the linear prime factors of $\mu_{\mathcal{A}}$), and the 2×2 diagonal blocks give all of the quadratic prime factors of $\mu_{\mathcal{A}}$ (as their minimal polynomials).

Hint: Thm. 21.3.9 can be useful here. Recall that (unitarily) similar matrices have identical minimal polynomials (Thm. 21.1.8).

Corollary 27.1.3 ☞ **Triangularization Criterion**

The following are equivalent for a matrix $\mathcal{A} \in \mathbb{M}_n$.

1. $\mathcal{A}$ is unitarily similar to an upper-triangular matrix.
2. $\mathcal{A}$ is similar to an upper-triangular matrix.
3. The minimal polynomial $\mu_{\mathcal{A}}$ can be expressed as a product of linear factors.

4. $\mathcal{A}$ is similar to a lower-triangular matrix.

5. $\mathcal{A}$ is unitarily similar to a lower-triangular matrix.

In this case, the distinct diagonal entries of these triangular matrices are exactly the eigenvalues of $\mathcal{A}$.*

*Some may be repeated on the diagonal more than once.

Proof of Theorem 27.1.3. TYC 21.3.11 established the validity of the implications 2. $\implies$ 3. and 4. $\implies$ 3. The implications 1. $\implies$ 2. and 5. $\implies$ 4. are trivial.

[**3.** $\implies$ **1.**]: By Schur's block-triangularization theorem, $\mathcal{A}$ is unitarily similar to a matrix $\mathcal{B}$ that can be partitioned as a block-*upper*-triangular matrix with the diagonal blocks being either 1×1 or 2×2, and the minimal polynomials of these blocks being all of the prime factors of $\mu_{\mathcal{A}}$ (Exc. 27.1.2).

Since 1x1 blocks have linear minimal polynomials (Thm. 26.6.6), and we are assuming that $\mu_{\mathcal{A}}$ has no quadratic prime factors, neither does $\mu_{\mathcal{B}}$ (Thm. 21.1.8). This tells us that none of the diagonal blocks of $\mathcal{B}$ are 2×2, and therefore $\mathcal{B}$ is an upper-triangular matrix.

[**3.** $\implies$ **5.**]: Use the second part of Schur's block-triangularization theorem. The rest of the argument is the same as that for 3. $\implies$ 1. ■

Terminology 27.1.4

When the conditions of Theorem 27.1.3 hold for a matrix $\mathcal{A}$, we say that $\mathcal{A}$ is **triangularizable**.

Test Your Comprehension 27.1.5

Every upper-triangular matrix is unitarily similar to a lower-triangular matrix.

Hint: The result of the Exercise 23.1.9 can be helpful here.

Comment 27.1.6

It turns out that every square matrix is similar to its own transpose, but this is not an easy claim to prove.

It is easy to see that every 2×2 matrix is unitarily similar to its transpose:

$$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}^{-1} \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = \cdots = \begin{bmatrix} a & c \\ b & d \end{bmatrix}.$$

Alas, there are matrices of every size larger than 2×2 that are not unitarily

similar to their transposes. ******

Exercise 27.1.7

The following are equivalent for a partitioned matrix

$$\mathcal{M} = \begin{bmatrix} \mathcal{A} & \mathcal{B} \\ \mathcal{O} & \mathcal{D} \end{bmatrix}$$

with square diagonal blocks.

1. $\mathcal{M}$ is triangularizable.

2. $\mathcal{A}$ and $\mathcal{D}$ are triangularizable.

Hint: Recall that $\mu_{\mathcal{A}}$ and $\mu_{\mathcal{D}}$ divide $\mu_{\mathcal{M}}$, which in turn divides $\mu_{\mathcal{A}}\mu_{\mathcal{D}}$ (Lem. 21.3.5). Of course Thm. 27.1.3 can be useful here as well.

Exercise 27.1.8

Develop a generalization of Exercise 27.1.7 for block-triangular matrices.

When $\mathcal{M}$ is triangularizable, the algorithm below can be used to construct a unitary matrix $\mathcal{U}$ such that $\mathcal{U}^{-1}\mathcal{M}\mathcal{U}$ is an upper-triangular matrix. An easy modification can produce a unitary that yields a lower-triangular matrix.

We present a recursive algorithm, which can be interpreted as a sequence of algorithms ALG_k, one for each matrix size. Each of these algorithms "passes the buck to" (i.e. employs) the lower size algorithms to perform its procedure. Recursive algorithms can be implemented very efficiently in electronic computing. (Carrying out such algorithms by hand would be a masochistic activity.)

For example, given a 7×7 matrix $\mathcal{A}$, ALG_7 will do a bit of work with $\mathcal{A}$ and create some 6×6 matrix $\mathcal{B}$ that it will pass to ALG_6. When ALG_6 brings back a unitary and an upper-triangular matrices associated with $\mathcal{B}$, ALG_7 will use these to construct a unitary and an upper-triangular matrices for $\mathcal{A}$.

Of course, ALG_6 performs its task is by doing a bit of work with $\mathcal{B}$ and creating a 5×5 matrix $\mathcal{C}$ that it will pass to ALG_5. When ALG_5 brings back a unitary and an upper-triangular matrices associated with $\mathcal{C}$, ALG_6 will use these to construct a unitary and an upper-triangular matrices for $\mathcal{B}$.

Etc.

The algorithm we present can be carried out for any square matrix $\mathcal{A}$ *with a known spectrum*, and it will determine whether the matrix is triangularizable.

When $\mathcal{A}$ is triangularizable, the algorithm will produce a unitary matrix $\mathcal{U}$ and an upper-triangular matrix $\mathcal{Z}$ such that

$$\mathcal{U}^{-1}\mathcal{A}\mathcal{U} = \mathcal{Z}.$$

We shall assume that the spectrum of the original matrix is part of a common domain accessible by all algorithms involved.

Algorithm 27.1.9

Let us describe ALG_{137} as applied to a matrix $\mathcal{M} \in \mathbb{M}_{137}$ and a list $\mathfrak{L}$ of numbers that is known to contain all eigenvalues of $\mathcal{M}$, if $\mathcal{M}$ has any. $\mathfrak{L}$ may contain other numbers as well.

If no number on the list $\mathfrak{L}$ is an eigenvalue of $\mathcal{M}$, then clearly $\mathcal{M}$ has no eigenvalues, $\sigma_{\mathbb{R}}(\mathcal{M})$ is empty, and so $\mathcal{M}$ not triangularizable. We stop and signal that the process is over and the traingularization is not possible.

If $\mathfrak{L}$ contains an eigenvalue λ of $\mathcal{M}$, we apply the technique of the alternate proof of Theorem 26.6.5 to find a unitary matrix $\mathcal{U}_1 \in \mathbb{M}_{137}$ (which will be either a Householder matrix or the identity matrix) such that

$$\mathcal{U}_1^{-1}\mathcal{M}\mathcal{U}_1 = \begin{bmatrix} [\lambda] & \mathcal{B} \\ \mathcal{O} & \mathcal{D} \end{bmatrix}.$$

Then we pass $\mathcal{D}$ to ALG_{136}, which will test $\mathcal{D}$ for triangularizability, etc. Recall that if $\mathcal{D}$ is not triangularizable, then neither is $\mathcal{M}$ (Exc. 27.1.7).

If/when ALG_{136} brings us back a unitary matrix $\mathcal{W}$ and an upper triangular matrix $\mathcal{T}$ in $\mathbb{M}_{136}$ such that

$$\mathcal{W}^{-1}\mathcal{D}\mathcal{W} = \mathcal{T}\ ,$$

we let

$$\mathcal{U}_2 := \begin{bmatrix} [1] & \mathcal{O} \\ \mathcal{O} & \mathcal{W} \end{bmatrix} = \mathcal{I}_1 \boxplus \mathcal{W}\ .$$

Then $\mathcal{U}_2$ is a direct sum of two unitary matrices and hence is itself unitary (TYC 23.1.6). Furthermore,

$$\mathcal{U}_2^{-1} = \begin{bmatrix} [1] & \mathcal{O} \\ \mathcal{O} & \mathcal{W}^{-1} \end{bmatrix} = \mathcal{I}_1 \boxplus \mathcal{W}\ .$$

In such a case,

$$
\begin{aligned}
(\mathcal{U}_1\mathcal{U}_2)^{-1}\,\mathcal{M}\,(\mathcal{U}_1\mathcal{U}_2) &= \mathcal{U}_2^{-1}\mathcal{U}_1^{-1}\mathcal{M}\,\mathcal{U}_1\mathcal{U}_2 \\
&= \mathcal{U}_2^{-1}\begin{bmatrix} [\boldsymbol{\lambda}] & \mathcal{B} \\ \mathcal{O} & \mathcal{D} \end{bmatrix}\mathcal{U}_2 \\
&= \begin{bmatrix} [\boldsymbol{\lambda}] & \mathcal{B}\mathcal{W} \\ \mathcal{O} & \mathcal{W}^{-1}\mathcal{D}\mathcal{W} \end{bmatrix} \\
&= \begin{bmatrix} [\boldsymbol{\lambda}] & \mathcal{B}\mathcal{W} \\ \mathcal{O} & \mathcal{T} \end{bmatrix} \overset{\text{TYC 9.1.7}}{=} \text{upper-triangular matrix.}
\end{aligned}
$$

This shows that the unitary matrix $\mathcal{U}_1\mathcal{U}_2$ (TYC 23.1.7) and the triangular matrix $\begin{bmatrix} [\boldsymbol{\lambda}] & \mathcal{B}\mathcal{W} \\ \mathcal{O} & \mathcal{T} \end{bmatrix}$ are matrices we seek for $\mathcal{M}$.*

The description of the whole process would not be complete without some words about ALG_1, which is the only algorithm in the sequence that does not "pass the buck". This algorithm tests whether a given 1×1 matrix $[a]$ is triangularizable, and the answer is always "YES", since every such matrix is in fact already diagonal.

So ALG_1 simply returns the unitary matrix $\mathcal{I}_1$ and the original matrix $[a]$ as the requested unitary and upper-triangular matrices. Even though it does not "pass the buck", ALG_1 may be the laziest algorithm in the sequence.

* Such matrices are not unique!

Test Your Comprehension 27.1.10

Modify Algorithm 27.1.9 so that the diagonal entries of the upper-triangular matrix it produces for any triangularizable matrix $\mathcal{M}$ always appear in increasing order.

27.2 A Diagonalization Criterion for Similarity

It is natural to ask for a condition that characterizes matrices which are (unitarily) similar to diagonal ones. Such conditions exist, but are distinct for the case of similarity and that of unitary similarity, in contrast to the triangularization criterion (Cor. 27.1.3).

The criterion for a diagonalization via a unitary similarity will be developed in a later section as a corollary to the Spectral Theorem For Normal Matrices.

Lemma 27.2.1

If $\mathcal{M} = \begin{bmatrix} \mathcal{A} & \mathcal{B} \\ \mathcal{O} & \mathcal{D} \end{bmatrix}$ and $\mathcal{D}$ is similar to $\mathcal{D}_0$, then $\mathcal{M}$ is similar to a matrix of the form

$$\begin{bmatrix} \mathcal{A} & \triangle \\ \mathcal{O} & \mathcal{D}_0 \end{bmatrix}.$$

Proof of Lemma 27.2.1. Let $\mathcal{S}$ be an invertible matrix such that $\mathcal{S}^{-1}\mathcal{D}\mathcal{S} = \mathcal{D}_0$. Then

$$\begin{bmatrix} \mathcal{I} & \mathcal{O} \\ \mathcal{O} & \mathcal{S} \end{bmatrix}^{-1} \begin{bmatrix} \mathcal{A} & \mathcal{B} \\ \mathcal{O} & \mathcal{D} \end{bmatrix} \begin{bmatrix} \mathcal{I} & \mathcal{O} \\ \mathcal{O} & \mathcal{S} \end{bmatrix} \overset{\text{Exc. 9.2.6}}{=} \begin{bmatrix} \mathcal{I} & \mathcal{O} \\ \mathcal{O} & \mathcal{S}^{-1} \end{bmatrix} \begin{bmatrix} \mathcal{A} & \mathcal{B} \\ \mathcal{O} & \mathcal{D} \end{bmatrix} \begin{bmatrix} \mathcal{I} & \mathcal{O} \\ \mathcal{O} & \mathcal{S} \end{bmatrix} = \begin{bmatrix} \mathcal{A} & \mathcal{B}\mathcal{S} \\ \mathcal{O} & \mathcal{S}^{-1}\mathcal{D}\mathcal{S} \end{bmatrix} = \begin{bmatrix} \mathcal{A} & \mathcal{B}\mathcal{S} \\ \mathcal{O} & \mathcal{D}_0 \end{bmatrix}. \blacksquare$$

Theorem 27.2.2 ☞ **A criterion for a diagonalization via similarity**

The following are equivalent for any matrix $\mathcal{M} \in \mathbb{M}_n$.

1. $\mathcal{M}$ is similar to a diagonal matrix.
2. The minimal polynomial of $\mathcal{M}$ factors out as a product of *distinct linear factors*;

   i.e. $\mu_{\mathcal{M}}$ has NO quadratic prime factors, and all linear prime factors have multiplicity 1.

A proof of Theorem 27.2.2 is presented in the appendix to the chapter.

Comment 27.2.3

Similarity does not alter the spectrum, and the spectrum of a diagonal matrix is exactly the set of its diagonal entries. Therefore if a matrix $\mathcal{A}$ is similar to a diagonal matrix, the diagonal entries of the latter are exactly the distinct eigenvalues of $\mathcal{A}$, but some may appear more than once.

Exercise 27.2.4 ☞ **Shuffling the diagonal entries of a diagonal matrix**

Hint: Exc. 10.2.12.

Suppose that a diagonal matrix $\mathcal{D}$ is obtained from a diagonal matrix $\mathcal{G}$ by rearranging the order of appearance of its diagonal entries. Argue that $\mathcal{D}$ and $\mathcal{G}$ are similar matrices.

Test Your Comprehension 27.2.5

Hint: Exc. 27.2.4

Argue that when $\mathcal{A}$ is similar to a diagonal matrix $\mathcal{D}$, it is also similar to every diagonal matrix obtained from $\mathcal{D}$ by rearranging the order of appearance of its diagonal entries.

Comment 27.2.6

By mimicking Algorithm 27.1.9, it is possible to convert our proof of Theorem 27.2.2 into a recursive algorithm that could be carried out for any square matrix $\mathcal{A}$ *with a known spectrum*. This algorithm will determine whether the matrix is similar to a diagonal matrix, and if it is, will produce an invertible matrix $\mathcal{S}$ and a diagonal matrix $\mathcal{D}$ such that

$$\mathcal{S}^{-1}\mathcal{A}\,\mathcal{S} = \mathcal{D}.$$

One can even arrange for the diagonal entries of $\mathcal{D}$ to appear in a desired order (compare this to TYC 27.2.5).

To exhibit a variety of possible approaches, we shall present another algorithm in the following section (27.3).

27.3 Eigenbases

Terminology 27.3.1

A coordinate system of $\mathbb{R}^n$ comprised entirely of eigenvectors of a matrix $\mathcal{A}$ is said to be an **$\mathcal{A}$-eigenbasis** for $\mathbb{R}^n$.

Theorem 27.3.2 ☞ **Diagonalizability and eigenbases**

The following are equivalent for a matrix $\mathcal{A} \in \mathbb{M}_n$.

1. $\mathcal{A}$ is similar to a diagonal matrix.
2. There is an $\mathcal{A}$-eigenbasis of $\mathbb{R}^n$.

Proof of Theorem 27.3.2. The following statements are mutually equivalent.

1. $X_1, X_2, \ldots, X_n$ is a coordinate system of $\mathbb{R}^n$ such that $\mathcal{A}(X_i) = \lambda_i X_i$, for every i.
2. $\begin{bmatrix} X_1 & X_2 & \cdots & X_n \end{bmatrix}_{n\times n}$ is an invertible matrix such that

$$\mathcal{A}\begin{bmatrix} X_1 & X_2 & \cdots & X_n \end{bmatrix} = \begin{bmatrix} \lambda_1 X_1 & \lambda_2 X_2 & \cdots & \lambda_n X_n \end{bmatrix}.$$

3. $\begin{bmatrix} X_1 & X_2 & \cdots & X_n \end{bmatrix}_{n\times n}$ is an invertible matrix such that

$$\mathcal{A}\begin{bmatrix} X_1 & X_2 & \cdots & X_n \end{bmatrix} = \begin{bmatrix} X_1 & X_2 & \cdots & X_n \end{bmatrix}\begin{bmatrix} \lambda_1 & & & \\ & \lambda_2 & & \\ & & \ddots & \\ & & & \lambda_n \end{bmatrix}.$$

4. $\mathcal{S} := \begin{bmatrix} X_1 & X_2 & \cdots & X_n \end{bmatrix}_{n\times n}$ is an invertible matrix such that

$$\mathcal{A}\mathcal{S} = \mathcal{S}\begin{bmatrix} \lambda_1 & & & \\ & \lambda_2 & & \\ & & \ddots & \\ & & & \lambda_n \end{bmatrix}.$$

5. $\mathcal{S} := \begin{bmatrix} X_1 & X_2 & \cdots & X_n \end{bmatrix}_{n\times n}$ is an invertible matrix such that

$$\mathcal{S}^{-1}\mathcal{A}\mathcal{S} = \begin{bmatrix} \lambda_1 & & & \\ & \lambda_2 & & \\ & & \ddots & \\ & & & \lambda_n \end{bmatrix}.$$

■

Test Your Comprehension 27.3.3

Argue that the following claims are equivalent for a square $n \times n$ matrices $\mathcal{A}$ and $\mathcal{S}$, with the latter being invertible.

1. $\mathcal{S}^{-1}\mathcal{A}\,\mathcal{S}$ is a diagonal matrix.

2. The columns of $\mathcal{S}$ form an $\mathcal{A}$-eigenbasis of $\mathbb{R}^n$.

Test Your Comprehension 27.3.4

If all columns of a matrix $\mathcal{B}$ come from an eigenspace $\boldsymbol{E}_{\mathcal{A}}(\lambda)$, then

$$\mathcal{A}\mathcal{B} = \lambda\mathcal{B}\,.$$

Theorem 27.3.5 ☞ **Concatenating lists of eigenvectors**

Suppose that $\lambda_1, \lambda_2, \ldots, \lambda_k$ are (some) *distinct* eigenvalues of a square matrix $\mathcal{A}$, and for each i, $\mathfrak{S}_i$ is a linearly independent list of eigenvectors in $\boldsymbol{E}_{\mathcal{A}}(\lambda_i)$.

Then the concatenation of the lists $\mathfrak{S}_1, \mathfrak{S}_2, \ldots, \mathfrak{S}_k$ is a linearly independent list.

A proof of Theorem 27.3.5 is presented in the appendix to the chapter.

Corollary 27.3.6

The sum of the dimensions of the eigenspaces of $\mathcal{A} \in \mathbb{M}_n$ corresponding to the distinct real eigenvalues is never greater than n.

Proof of Corollary 27.3.6. Taking the sets $\mathfrak{C}_i$ in Theorem 27.3.5 to be the bases of the distinct eigenspaces of $\mathcal{A}$, we see that the total number of the elements in their concatenation is at most n, since linearly independent sets in $\mathbb{R}^n$ cannot have more than n elements. Yet this total number of elements is exactly the sum of the dimensions of the eigenspaces. ■

Exercise 27.3.7 ☞ **Diagonalizability and the eigenspaces**

Argue that the following claims are equivalent for a square $n \times n$ matrix $\mathcal{A}$.

1. $\mathcal{A}$ is similar to a diagonal matrix.
2. The sum of the dimensions of the eigenspaces of $\mathcal{A} \in \mathbb{M}_n$ corresponding to the distinct real eigenvalues is n.

Hint: Thms. 27.3.2 and 27.3.5.

Comment 27.3.8

When a matrix $\mathcal{A}$ is similar to a diagonal matrix, TYC 27.3.3, Theorem 27.3.5 and Exercise 27.3.7 can be used to develop an algorithm for constructing an invertible matrix $\mathcal{S}$ such that $\mathcal{S}^{-1}\mathcal{A}\mathcal{S}$ is a diagonal matrix.

Each eigenspace $\boldsymbol{E}_{\mathcal{A}}(\lambda)$ is a nullspace of $\mathcal{A} - \lambda\mathcal{I}$, and we have already seen several algorithms for constructing coordinate systems of nullspaces. *Mathematica* command **NullSpace**[] can be used for this purpose.

When $\mathcal{A}$ is diagonalizable, concatenating the coordinate systems of its distinct eigenspaces produces an $\mathcal{A}$-eigenbasis , and such can be used to construct an $\mathcal{S}$ (Exc. 27.3.7).

Terminology 27.3.9

When λ is an eigenalue of $\mathcal{A}$, the dimension of $\boldsymbol{E}_{\mathcal{A}}(\lambda)$ is said to be the **geometric multiplicity** of λ as an eigenvalue of $\mathcal{A}$.

Comment 27.3.10

We know that similar matrices have the same spectrum and the same minimal polynomial. Since the multiplicities of the eigenvalues as roots of the minimal polynomial are completely determined by the minimal polynomial, similar matrices enjoy the same such multiplicities for their mutual eigenvalues.

Can the same be said about the geometric multiplicities? If $\mathcal{S}^{-1}\mathcal{A}\mathcal{S} = \mathcal{B}$, and

$\lambda \in \sigma_{\mathbb{R}}(\mathcal{A}) = \sigma_{\mathbb{R}}(\mathcal{B})$, can we conclude that

$$dim\left(\boldsymbol{E}_{\mathcal{A}}(\lambda)\right) = dim\left(\boldsymbol{E}_{\mathcal{B}}(\lambda)\right)?$$

Recall that $\boldsymbol{E}_{\mathcal{A}}(\lambda)$ is the nullspace of $\mathcal{A}-\lambda\mathcal{I}$, with a similar statement holding true for $\mathcal{B}$. Hence our question asks whether the nullity of $\mathcal{A}-\lambda\mathcal{I}$ equals that of $\mathcal{B}-\lambda\mathcal{I}$.

Note that

$$\mathcal{B}-\lambda\mathcal{I} = \mathcal{S}^{-1}\mathcal{A}\mathcal{S} - \mathcal{S}^{-1}\lambda\mathcal{I}\mathcal{S} = \mathcal{S}^{-1}\Big(\mathcal{A}-\lambda\mathcal{I}\Big)\mathcal{S}\ .$$

This shows that matrices $\mathcal{B}-\lambda\mathcal{I}$ are similar, and hence they have the same nullity (Exc. 19.1.10).

Let us summarize.

Similar matrices not only have the same spectrum, but enjoy the same geometric multiplicities of their (common) eigenvalues, and these also have the same multiplicities as roots of the common minimal polynomial.

Recall that the nullity of a diagonal matrix is the number of times zero appears on its diagonal (Exc. 26.3.5).

Thus, if a matrix $\mathcal{A}$ is diagonalizable, i.e. is similar to a diagonal matrix $\mathcal{D}$, then the diagonal entries of $\mathcal{D}$ are exactly the distinct eigenvalues of $\mathcal{A}$, each appearing on the diagonal its geometric multiplicity times.

Obviously this specifies the matrix $\mathcal{D}$ completely, apart from the order in which its diagonal entries appear (TYC 27.2.5).

Exercise 27.3.11

For each of the following matrices $\mathcal{A}$ decide if it is diagonalizable, and if it is, find an invertible $\mathcal{S}$ and a diagonal matrix $\mathcal{D}$ such that

$$\mathcal{S}^{-1}\mathcal{A}\mathcal{S} = \mathcal{D}\ .$$

27.4 Appendix: Exiled Proofs

Proof of Theorem 27.1.1. We will establish the first claim of the theorem and then use transposition to infer the second from it.

This claim is trivially true in the case $n = 1$, since every 1×1 matrix is already (block-)diagonal.

Let us verify the case $n = 2$. In this case if $\mu_{\mathcal{A}}$ is an prime quadratic polynomial, the claim is true, as $\mathcal{A}$ itself has the required block-diagonal form. If $\mu_{\mathcal{A}}$ is not an prime quadratic polynomial, then it is either linear or is a product of two linear factors (Thm. 26.6.6). In either scenario $\mathcal{A}$ has eigenvalues/eigenvectors, and so, by Theorem 26.6.5, $\mathcal{A}$ is unitarily similar to a matrix of the form $\left[\begin{smallmatrix} b & c \\ 0 & d \end{smallmatrix}\right]$. Hence $\mathcal{A}$ satisfies the required condition in this case.

Let us now deal with a larger n. If the (first) claim of the theorem were not true in general, there would be counterexamples to it, and among these there would be one (say $\mathcal{A}_{\text{o}}$) of the *smallest* size, say $n_{\text{o}} \times n_{\text{o}}$. We know that n_{o} has to be at least 3, and that the claim holds true for all matrices of size smaller than n_{o}.

By TYC 26.6.4, $\mathcal{A}_{\text{o}}$ is unitarily similar to a matrix $\mathcal{M}$ that can be partitioned as $\left[\begin{smallmatrix} \mathcal{B} & \mathcal{C} \\ \mathcal{O} & \mathcal{D} \end{smallmatrix}\right]_{(k|n_{\text{o}}-k)\times(k|n_{\text{o}}-k)}$, with k being either 1 or 2.

Square matrices $\mathcal{B}$ and $\mathcal{D}$ are strictly smaller than $\mathcal{A}_{\text{o}}$, and so each is unitarily equivalent to a matrix of the form described in the theorem; say

$$\mathcal{K} = \mathcal{U}^{-1}\mathcal{B}\mathcal{U} \quad \text{and} \quad \mathcal{L} = \mathcal{W}^{-1}\mathcal{D}\mathcal{W}\,.$$

Then

$$\begin{bmatrix} \mathcal{U} & \mathcal{O} \\ \mathcal{O} & \mathcal{W} \end{bmatrix}^{-1} \begin{bmatrix} \mathcal{B} & \mathcal{C} \\ \mathcal{O} & \mathcal{D} \end{bmatrix} \begin{bmatrix} \mathcal{U} & \mathcal{O} \\ \mathcal{O} & \mathcal{W} \end{bmatrix} = \begin{bmatrix} \mathcal{U}^{-1} & \mathcal{O} \\ \mathcal{O} & \mathcal{W}^{-1} \end{bmatrix} \begin{bmatrix} \mathcal{B} & \mathcal{C} \\ \mathcal{O} & \mathcal{D} \end{bmatrix} \begin{bmatrix} \mathcal{U} & \mathcal{O} \\ \mathcal{O} & \mathcal{W} \end{bmatrix} = \begin{bmatrix} \mathcal{K} & \spadesuit \\ \mathcal{O} & \mathcal{L} \end{bmatrix}$$

It is easy to see that $\begin{bmatrix} \mathcal{K} & \spadesuit \\ \mathcal{O} & \mathcal{L} \end{bmatrix}$ can be partitioned as a block-*upper*-triangular matrix with the diagonal blocks being either 1×1 or 2×2, with all 2×2 diagonal blocks having prime quadratic minimal polynomials, because this is true for both $\mathcal{K}$ and $\mathcal{L}$.

Furthermore, $\begin{bmatrix} \mathcal{U} & \mathcal{O} \\ \mathcal{O} & \mathcal{W} \end{bmatrix}$, being a direct sum of two unitary matrices, is a unitary matrix (TYC 23.1.6).

This shows that $\mathcal{M}$ is unitarily equivalent to a matrix that can be partitioned as a block-*upper*-triangular matrix with the diagonal blocks being either 1×1 or 2×2, with all 2×2 diagonal blocks having prime quadratic minimal polynomials. Since unitary similarity is a transitive relation (Exc. 23.1.9), $\mathcal{A}_{\text{o}}$ is also a unitarily equivalent to this matrix, in contradiction to the way $\mathcal{A}_{\text{o}}$ was chosen.

Therefore the only feasible conclusion must be that there are no counterexamples to the theorem, and consequently the proof of the "block-upper-triangular" claim of the theorem is complete.

To establish the "secondblock-lower-traingular" claim, apply the first already established "block-upper-triangular" portion of the theorem to $\mathcal{A}^T$, and conclude that

$$\mathcal{A}^T = \mathcal{U}^{-1}\mathcal{G}\mathcal{U} = \mathcal{U}^T\mathcal{G}\mathcal{U} ,$$

for some unitary matrix $\mathcal{U}$ and some block-upper-triangular matrix $\mathcal{G}$ described in the first part of the theorem.

Then

$$\mathcal{A} = \left(\mathcal{U}^T\mathcal{G}\mathcal{U}\right)^T = \mathcal{U}^T\mathcal{G}^T\mathcal{U} = \mathcal{U}^{-1}\mathcal{G}^T\mathcal{U} .$$

It is now easy to see that $\mathcal{G}^T$ has the required lower-block-triangular form (TYC 9.1.4). Keep in mind that transposition does not alter minimal polynomials (Thm. 21.1.7), and so the diagonal blocks of $\mathcal{G}^T$ have the same minimal polynomials as the diagonal blocks of $\mathcal{G}$. ∎

Proof of Theorem 27.2.2. The implication 1. $\Longrightarrow$ 2. is quite trivial, since similarity does not alter minimal polynomials (Thm. 21.1.8), and a minimal polynomial of a diagonal matrix factors as a product of distinct linear factors (Exc. 21.3.4).

Let us confirm the validity of the implication 2. $\Longrightarrow$ 1.

The implication is trivially true when $n = 1$, since every 1×1 matrix $[a]$ is a diagonal matrix, and has the minimal polynomial $x - a$.

If the implication 2. $\Longrightarrow$ 1. were not true in general, there would be a counterexample $\mathcal{M}_o$ of the smallest size, which would have to be at least 2×2. So, we can write $\mathcal{M}_o \in \mathbb{M}_{m+1}$; $m \in \mathbb{N}$. $\mu_{\mathcal{M}_o}$ would be a product of distinct linear factors, but $\mathcal{M}_o$ would not be similar to a diagonal matrix.

Furthermore, by the minimality of $\mathcal{M}_o$, any square matrix strictly smaller than $\mathcal{M}_o$ with a minimal polynomial that factors out as a product of distinct linear factors, would be similar to a diagonal matrix.

Synopsis of the proof: Here is the outline of what is about to happen. We shall pass from $\mathcal{M}_o$ to a simpler matrix $\mathcal{L}$ via similarity. Then we will pass from $\mathcal{L}$ to an even simpler matrix $\mathcal{K}$, again via similarity. After that we will pass from $\mathcal{K}$ to a more convenient matrix $\mathcal{J}$, still via similarity.

Then we will demonstrate that this $\mathcal{J}$ is similar to a diagonal matrix, which means that so is $\mathcal{M}_o$. Yet this contradicts the choice of $\mathcal{M}_o$, and therefore no such choice is possible. Hence there is no counterexample to the implication 2. $\Longrightarrow$ 1.

$\mathcal{M}_\circ \rightsquigarrow \mathcal{L}$: We have

$$\mu_{\mathcal{M}_\circ}(x) = (x-\lambda_1)(x-\lambda_2)\cdots(x-\lambda_{m+1}) ,$$

for some distinct scalars λ_i. By Theorem 26.6.5, $\mathcal{M}_\circ$ is similar to a matrix $\mathcal{L}$ of the form $\begin{bmatrix} [\lambda_1] & \mathcal{B} \\ \mathcal{O} & \mathcal{D} \end{bmatrix}$. $\mathcal{L}$ has the same size and the same minimal polynomial as $\mathcal{M}_\circ$ (Thm. 21.1.8).

$\mathcal{L} \rightsquigarrow \mathcal{K}$: Since $\mu_{\mathcal{D}}$ divides $\mu_{\mathcal{L}}$ (Lem. 21.3.5), $\mu_{\mathcal{D}}$ factors out as a product of distinct linear factors, which are also factors of $\mu_{\mathcal{L}}$. Yet $\mathcal{D}$ is strictly smaller than $\mathcal{L}$ and $\mathcal{M}_\circ$. Hence it must be similar to a diagonal matrix $\mathcal{G}$.

By Lemma 27.2.1, $\mathcal{L}$ is similar to a matrix of the form $\begin{bmatrix} [\lambda_1] & \triangle \\ \mathcal{O} & \mathcal{G} \end{bmatrix}$, which we denote by $\mathcal{K}$. This matrix $\mathcal{K}$ is also similar to $\mathcal{M}_\circ$ (similarity is a transitive relation) and thus has the same minimal polynomial as $\mathcal{M}$.

$\mathcal{K} \rightsquigarrow \mathcal{J}$: Since $\mu_{\mathcal{G}}$ divides $\mu_{\mathcal{K}}$ (which equals $\mu_{\mathcal{M}_\circ}$), and $\mu_{\mathcal{G}}$ factors out as a product of distinct linear factors corresponding to the distinct diagonal entries of $\mathcal{G}$ (Exc. 21.3.4), every diagonal entry of $\mathcal{G}$ must be equal to one of the λ_i's (Thm. 20.1.24).

Next we use a permutation similarity to shuffle the entries of $\mathcal{G}$ in such a way that all of λ_1's (if any are present) float up to the top (****). There is a permutation matrix $\mathcal{P}$, such that $\mathcal{P}^{-1}\mathcal{G}\mathcal{P}$ is a diagonal matrix

$$\mathcal{H} := \begin{bmatrix} \lambda_1 & & & & & \\ & \ddots & & & & \\ & & \lambda_1 & & & \\ & & & \lambda_{i_1} & & \\ & & & & \ddots & \\ & & & & & \lambda_{i_t} \end{bmatrix} ,$$

where $i_1, \ldots, i_t > 1$, and λ_1's may not be present at all.

By Lemma 27.2.1, $\mathcal{K}$ is similar to a matrix of the form $\begin{bmatrix} [\lambda_1] & \diamond \\ \mathcal{O} & \mathcal{H} \end{bmatrix}$, which we denote by $\mathcal{J}$. $\mathcal{J}$ is similar to our original matrix $\mathcal{M}_\circ$ by the transitivity of similarity. Thus $\mathcal{J}$ and $\mathcal{M}_\circ$ have the same minimal polynomial.

$\mathcal{J}$ is similar to a diagonal matrix: Sub-partition $\mathcal{J}$ into the form $\begin{bmatrix} \mathcal{A} & \mathcal{T} \\ \mathcal{O} & \mathcal{F} \end{bmatrix}$, where

$$\mathcal{F} = \begin{bmatrix} \lambda_{i_1} & & & \\ & \lambda_{i_2} & & \\ & & \ddots & \\ & & & \lambda_{i_t} \end{bmatrix} \quad \text{and} \quad \mathcal{A} = \begin{bmatrix} \lambda_1 & \square & \ldots & \square \\ 0 & \lambda_1 & \ldots & \square \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & \lambda_1 \end{bmatrix} .$$

Let us argue that $\mathcal{A} = \lambda_1 \mathcal{I}$. Note that $\mu_{\mathcal{A}}$ divides $\mu_{\mathcal{J}}$ (i.e. $\mu_{\mathcal{M}_0}$). Yet $\mathcal{A}$ is upper-triangular, and so its minimal polynomial has to be of the form $\left(x-\lambda_1\right)^m$ (Exc. 21.3.10).

Since the multiplicity of $\left(x-\lambda_1\right)$ in $\mu_{\mathcal{J}}$ is 1, it must be that $m=1$, and the minimal polynomial of $\mathcal{A}$ is $x-\lambda_1$. Hence $A-\lambda_1\mathcal{I}=0$ and so $\mathcal{A}=\lambda_1\mathcal{I}$.

Now,

$$\mathcal{J} = \begin{bmatrix} \lambda_1\mathcal{I} & \mathcal{T} \\ \mathcal{O} & \mathcal{F} \end{bmatrix}, \quad \text{and} \quad \mathcal{F}-\lambda_1\mathcal{I}_t = \begin{bmatrix} \lambda_{i_1}-\lambda_1 & & & \\ & \lambda_{i_2}-\lambda_1 & & \\ & & \ddots & \\ & & & \lambda_{i_t}-\lambda_1 \end{bmatrix} = \text{invertible},$$

because $\lambda_{i_1}, \lambda_{i_2}, \ldots, \lambda_{i_t}$ are distinct from λ_1. This allows us to find a matrix $\mathcal{N}$ such that

$$\begin{bmatrix} \mathcal{I} & -\mathcal{N} \\ \mathcal{O} & \mathcal{I} \end{bmatrix} \mathcal{J} \begin{bmatrix} \mathcal{I} & \mathcal{N} \\ \mathcal{O} & \mathcal{I} \end{bmatrix}$$

is a diagonal matrix. As the reader will recall, By Theorem 9.1.10, $\begin{bmatrix} \mathcal{I} & \mathcal{N} \\ \mathcal{O} & \mathcal{I} \end{bmatrix}$ is always invertible, and its inverse is $\begin{bmatrix} \mathcal{I} & -\mathcal{N} \\ \mathcal{O} & \mathcal{I} \end{bmatrix}$.

Here are the details.

Let $\mathcal{N} = \mathcal{T}\left(\mathcal{F}-\lambda_1\mathcal{I}_t\right)^{-1}$. Then

$$\begin{aligned}
\begin{bmatrix} \mathcal{I} & -\mathcal{N} \\ \mathcal{O} & \mathcal{I} \end{bmatrix} \mathcal{J} \begin{bmatrix} \mathcal{I} & \mathcal{N} \\ \mathcal{O} & \mathcal{I} \end{bmatrix} &= \begin{bmatrix} \mathcal{I} & -\mathcal{N} \\ \mathcal{O} & \mathcal{I} \end{bmatrix} \begin{bmatrix} \lambda_1\mathcal{I} & \mathcal{T} \\ \mathcal{O} & \mathcal{F} \end{bmatrix} \begin{bmatrix} \mathcal{I} & \mathcal{N} \\ \mathcal{O} & \mathcal{I} \end{bmatrix} \\
&= \begin{bmatrix} \lambda_1\mathcal{I} & \mathcal{T}-\mathcal{N}\mathcal{F} \\ \mathcal{O} & \mathcal{F} \end{bmatrix} \begin{bmatrix} \mathcal{I} & \mathcal{N} \\ \mathcal{O} & \mathcal{I} \end{bmatrix} \\
&= \begin{bmatrix} \lambda_1\mathcal{I} & \lambda_1\mathcal{N}+\mathcal{T}-\mathcal{N}\mathcal{F} \\ \mathcal{O} & \mathcal{F} \end{bmatrix}.
\end{aligned}$$

We defined $\mathcal{N}$ in a way that makes $\lambda_1\mathcal{N}+\mathcal{T}-\mathcal{N}\mathcal{F}$ null:

$$\begin{aligned}
\lambda_1\mathcal{N}+\mathcal{T}-\mathcal{N}\mathcal{F} &= \mathcal{T}-\mathcal{N}\left(\mathcal{F}-\lambda_1\mathcal{I}\right) \\
&= \mathcal{T}-\mathcal{T}\left(\mathcal{F}-\lambda_1\mathcal{I}\right)^{-1}\left(\mathcal{F}-\lambda_1\mathcal{I}\right) = \mathcal{T}-\mathcal{T} = \mathcal{O}.
\end{aligned}$$

So,

$$\begin{bmatrix} \mathcal{I} & -\mathcal{N} \\ \mathcal{O} & \mathcal{I} \end{bmatrix} \mathcal{J} \begin{bmatrix} \mathcal{I} & \mathcal{N} \\ \mathcal{O} & \mathcal{I} \end{bmatrix} = \begin{bmatrix} \lambda_1\mathcal{I} & \mathcal{O} \\ \mathcal{O} & \mathcal{F} \end{bmatrix} = \text{a diagonal matrix.}$$

This shows that $\mathcal{J}$ is similar to a diagonal matrix. The same holds true for $\mathcal{M}_0$, by the transitivity of similarity. This contradicts the way $\mathcal{M}_0$ was chosen. Hence there is no such counterexample $\mathcal{M}_0$ to the implication 2. $\Longrightarrow$ 1. Thus the implication holds true in general. ■

Proof of Theorem 27.3.5. The claim is clearly true if $k = 1$. If the claim were not true in general, there would be the smallest k, call it k_o, for which the claim fails. Then $k_o \geq 2$, and the claim is true when $k = k_o - 1$.

For the simplicity of notation we will take $k_o = 4$. A general proof follows exactly the same path, but using the general notation.

Since the claim fails for $k = 4$, there must be an example of the lists $\mathfrak{S}_1, \mathfrak{S}_2, \ldots, \mathfrak{S}_4$ described in the statement of the theorem, such that their concatenation is not a linearly independent list.

Let $\mathcal{B}_i$ be the injective matrix having the columns listed in $\mathfrak{S}_i$, and let

$$\mathcal{M} := \begin{bmatrix} \mathcal{B}_1 & \cdots & \mathcal{B}_4 \end{bmatrix} .$$

Then $\mathcal{M}$ is not an injective matrix, whereas

$$\mathcal{C} = \begin{bmatrix} \mathcal{B}_1 & \cdots & \mathcal{B}_3 \end{bmatrix}$$

is an injection since the claim of the theorem holds true when $k = 3$.

We perform a lengthy calculation:

$$\begin{aligned}
\big(\mathcal{A}-\lambda_4\mathcal{I}\big)\mathcal{M} &= \mathcal{A}\big[\mathcal{B}_1 \quad \cdots \quad \mathcal{B}_4\big] - \lambda_4\mathcal{M} \\
&= \big[\mathcal{A}\mathcal{B}_1 \quad \cdots \quad \mathcal{A}\mathcal{B}_4\big] - \lambda_4\mathcal{M} \\
&\overset{\text{TYC 27.3.4}}{=} \big[\lambda_1\mathcal{B}_1 \quad \cdots \quad \lambda_{k_o}\mathcal{B}_4\big] - \lambda_4\mathcal{M} \\
&= \big[\mathcal{B}_1 \quad \cdots \quad \mathcal{B}_4\big]\begin{bmatrix} \lambda_1\mathcal{I} & & \\ & \ddots & \\ & & \lambda_4\mathcal{I} \end{bmatrix} - \lambda_4\mathcal{M} \\
&= \mathcal{M}\begin{bmatrix} \lambda_1\mathcal{I} & & \\ & \ddots & \\ & & \lambda_4\mathcal{I} \end{bmatrix} - \lambda_4\mathcal{M} \\
&= \mathcal{M}\begin{bmatrix} (\lambda_1-\lambda_4)\mathcal{I} & & & \\ & (\lambda_2-\lambda_4)\mathcal{I} & & \\ & & (\lambda_3-\lambda_4)\mathcal{I} & \\ & & & \mathcal{O} \end{bmatrix} \\
&= [\mathcal{C} \quad \mathcal{B}_4]\begin{bmatrix} (\lambda_1-\lambda_4)\mathcal{I} & & & \\ & (\lambda_2-\lambda_4)\mathcal{I} & & \\ & & (\lambda_3-\lambda_4)\mathcal{I} & \\ & & & \mathcal{O} \end{bmatrix} \\
&= \big[\mathcal{C}\mathcal{D} \quad \mathcal{O}\big] ,
\end{aligned}$$

where

$$\mathcal{D} = \begin{bmatrix} (\lambda_1-\lambda_4)\mathcal{I} & & \\ & (\lambda_2-\lambda_4)\mathcal{I} & \\ & & (\lambda_3-\lambda_4)\mathcal{I} \end{bmatrix} .$$

It is clear that $\mathcal{D}$ is invertible, since it is a diagonal matrix with non-zero diagonal entries.

Since $\mathcal{M} = [\mathcal{C} \quad \mathcal{B}_4]$ is not injective, it annihilates a non-null $\left(\begin{smallmatrix} X \\ Y \end{smallmatrix}\right)$, and so

$$\mathbb{O} = \big(\mathcal{A}-\lambda_4\mathcal{I}\big)\mathcal{M}\left(\begin{smallmatrix} X \\ Y \end{smallmatrix}\right) = \mathcal{C}\mathcal{D}(X) + \mathcal{O}(Y) = \mathcal{C}\mathcal{D}(X) .$$

Being a composition of two injections, $\mathcal{C}\mathcal{D}$ is injective, i.e. has a trivial nullspace, and therefore it must be that $X = \mathbb{0}$. Yet in this case

$$\begin{aligned}\mathbb{0} &= \mathcal{M}\binom{X}{Y} \\ &= [\mathcal{C} \quad \mathcal{B}_4]\binom{X}{Y} \\ &= \mathcal{C}(X) + \mathcal{B}_4(Y) \\ &= \mathcal{C}(\mathbb{0}) + \mathcal{B}_4(Y) = \mathcal{B}_4(Y)\ .\end{aligned}$$

As $\mathcal{B}_4$ is injective, we can conclude that Y is null. This shows that $\binom{X}{Y}$ is null contrary to its selection.

The consequent conclusion is that there cannot exist a k for which the claim of the theorem fails. ■

X General Linearity

28. Linear Spaces

Last modified on December 8, 2018

28.1 Linear Spaces

Terminology 28.1.1

By a **linear space** we mean a non-empty collection $\boldsymbol{V}$ of objects which can be “added” ($+$) and “scaled by real numbers” ($\cdot$), with the results still in $\boldsymbol{V}$, in a way that sports the same operational properties as addition and scaling on $\mathbb{R}^n$.

These properties of include:

- commutativity and associativity of the addition $+$:

$$V+W = W+V \quad \text{and} \quad (V+W)+Z = V+(W+Z)\ .$$

- the existence of an additively neutral element $\mathbb{0}_{+}$:

$$V+\mathbb{0}_{\boldsymbol{V}} = V\ .$$

- the fact that every element V has an **additively antipodal element** $\neg V$ with respect to a neutral element $\mathbb{0}_{\boldsymbol{V}}$:

$$V+\neg V = \mathbb{0}_{\boldsymbol{V}}\ .$$

- the fact that scalar multiplication distributes over addition:

$$\alpha\cdot(W+Z) = (\alpha\cdot W)+(\alpha\cdot Z)\ .$$

- the fact that scaling an element by 1 does not alter it:

$$1\cdot V = V\ .$$

- the property that we can scale once by a product of scalars, or by each scalar in turn, and will get the same answer either way:

$$(\pi\alpha)\cdot V = \pi\cdot(\alpha\cdot V)\ .$$

- the property that we can scale once by a sum of scalars, or by each scalar individually then adding the results together, and will get the same answer either way:

$$(\pi+\alpha)\cdot V = (\pi\cdot V) + (\alpha\cdot V)\ .$$

It is important to note that we are only considering the high-level operational properties, and not the way the operations $+$ and $\cdot$ are actually carried out. The goal is to identify other environments that our theory can be ported to in a natural way.

Notation 28.1.2

$\mathcal{Y}^{\mathcal{X}}$ denotes the set of ALL functions $f : \mathcal{X} \longrightarrow \mathcal{Y}$.

Examples 28.1.3

Here are some examples of linear spaces. What is the additively neutral element in each case?

- $\mathbb{R}^n$ with our usual operations of tuple addition and scaling.
- Any subspace of $\mathbb{R}^n$ under the inherited (from $\mathbb{R}^n$) operations of addition and scaling.
- The set $\mathbb{M}_{5\times 7}$ of 5×7 matrices under our usual operations of addition and scaling of matrices.
- The sets Υ^1_L, Υ^2_P and Υ^3 of linear (with line L), planar (with plane P), and all geometric vectors in $\mathbb{E}^3$ respectively, under the geometrically described operations of addition and scaling.
- The set Υ^0 containing just the null vector.
- The set $R^{(0,1)}$ of all functions $f : (0,1) \longrightarrow \mathbb{R}$, under the usual Calculus operations of addition and scaling of functions.
- The set $R^{\mathbb{N}}$ of all real sequences under the usual Calculus operations of addition and scaling of sequences.
- The set $\mathfrak{C}\Big((0,1), \mathbb{R}^2\Big)$ of all continuous functions with initial space $(0,1]$ and a final space $\mathbb{R}^2$.

Notation 28.1.4

To make the notation less bracket heavy, let us agree on “the order of operations”:

> scalar multiplication $\cdot$ is performed first, and addition $+$ is performed thereafter.

Furthermore, the associativity of addition allows us to implement addition with more than two summands without a use of brackets.

Terminology 28.1.5

In order to draw further parallels between general linear spaces and $\mathbb{R}^n$, we shall call the additively neutral element $\mathbb{0}_{\boldsymbol{V}}$ of a linear space $\boldsymbol{V}$, its **null element**. Think of “NULL” as an abbreviation of “NeUtraLL”.

Some of the linear space properties are fundamental, while others can be derived from the fundamental ones and so are secondary. Here are some examples.

Theorem 28.1.6 ☞ Zero multiple equals the null element

If $\boldsymbol{W}$ is a linear space, then for every $W \in \boldsymbol{W}$:

$$0 \cdot W = \mathbb{0}_{\boldsymbol{W}} .$$

In particular, a linear space cannot have two distinct additively neutral elements.

Test Your Comprehension 28.1.7

Verify the last claim of Theorem 28.1.6.

Proof of Theorem 28.1.6. Let us write $W_\circ$ for $0 \cdot W$. Then

$$W_\circ + W_\circ = 0 \cdot W + 0 \cdot W = (0+0) \cdot W = 0 \cdot W = W_\circ .$$

Therefore

$$W_\circ = W_\circ + \mathbb{0}_{\boldsymbol{W}} = W_\circ + W_\circ + \neg W_\circ = W_\circ + \neg W_\circ = \mathbb{0}_{\boldsymbol{W}} . \qquad \blacksquare$$

Test Your Comprehension 28.1.8

Identify all of the operational properties of linear spaces that were used in the proof of Theorem 28.1.6.

Theorem 28.1.9 ☞ **Scaling the null element is pointless**

If $\boldsymbol{V}$ is a linear space, then for every $\alpha \in \mathbb{R}$:

$$\alpha \cdot \mathbb{0}_{\boldsymbol{V}} = \mathbb{0}_{\boldsymbol{V}}.$$

Proof of Theorem 28.1.9. We begin by showing that the claim holds true when $\alpha = 2$:

$$2 \cdot \mathbb{0}_{\boldsymbol{V}} = (1+1) \cdot \mathbb{0}_{\boldsymbol{V}} = 1 \cdot \mathbb{0}_{\boldsymbol{V}} + 1 \cdot \mathbb{0}_{\boldsymbol{V}} = \mathbb{0}_{\boldsymbol{V}} + \mathbb{0}_{\boldsymbol{V}} = \mathbb{0}_{\boldsymbol{V}}.$$

Now that this is done, we can argue the general case. We begin with the following observation.

$$\alpha \cdot \mathbb{0}_{\boldsymbol{V}} = \alpha \cdot \left(2 \cdot \mathbb{0}_{\boldsymbol{V}}\right) = (2\alpha) \cdot \mathbb{0}_{\boldsymbol{V}} = \alpha \cdot \mathbb{0}_{\boldsymbol{V}} + \alpha \cdot \mathbb{0}_{\boldsymbol{V}}.$$

If we write Z_o for $\alpha \cdot \mathbb{0}_{\boldsymbol{V}}$, we now have that

$$Z_o = Z_o + Z_o,$$

and therefore

$$\mathbb{0}_{\boldsymbol{V}} = \neg Z_o + Z_o = \neg Z_o + Z_o + Z_o = \mathbb{0}_{\boldsymbol{V}} + Z_o = Z_o,$$

which is the desired result. ∎

Theorem 28.1.10 ☞ **Uniqueness of additive antipodes**

In a linear space $\boldsymbol{Z}$ every element Z has a UNIQUE additively antipodal element, and that element equals $(-1) \cdot Z$.

Proof of Theorem 28.1.10. Let us begin by showing that $(-1) \cdot Z$ is an additive antipode of Z, and then show that no other element has this property.

$$\mathbb{0}_{\boldsymbol{Z}} = 0 \cdot Z = (-1+1) \cdot Z = (-1) \cdot Z + 1 \cdot Z = (-1) \cdot Z + Z.$$

Hence $(-1) \cdot Z$ is an additive antipode of Z. Let us say that Z_1 is also an additive antipode of Z. Then

$$Z_1 = \mathbb{0}_{\boldsymbol{Z}} + Z_1 = (-1) \cdot Z + Z + Z_1 = (-1) \cdot Z + \mathbb{0}_{\boldsymbol{Z}} = (-1) \cdot Z.$$

This shows that Z has no other additive antipodes. ∎

This is how the abstract game is played. Let us not dwell on it further, and proceed to the study of the higher level concepts.

28.2 Subspaces

Terminology 28.2.1

A subset $\boldsymbol{S}$ of a linear space $\boldsymbol{V}$ is said to be a **subspace** of $\boldsymbol{V}$ if it is *non-empty* and is **closed under addition and scaling**, in the sense that a sum of elements of $\boldsymbol{S}$ is again in $\boldsymbol{S}$, as is a scalar multiple of an element of $\boldsymbol{S}$.

It is easy to see that $\{\mathbb{0}_{\boldsymbol{V}}\}$ is a subspace of a linear space $\boldsymbol{V}$. This subspace is said to be **a trivial subspace** of $\boldsymbol{V}$.

Similarly, it is clear that every linear space is its own subspace. Subspaces of a linear space $\boldsymbol{V}$ that are not equal to $\boldsymbol{V}$ are said to be **proper subspaces**.

Test Your Comprehension 28.2.2 Subspaces are linear spaces

Every subspace of a linear space is a linear space in its own right, under the inherited operations of addition and scaling.

Test Your Comprehension 28.2.3 A subspace of a subspace is a subspace of the original space

If $\boldsymbol{Z}$ is a subspace of $\boldsymbol{X}$, which in turn is a subspace of $\boldsymbol{W}$, then $\boldsymbol{Z}$ is a subspace of $\boldsymbol{W}$.

Test Your Comprehension 28.2.4 A combined subspace criterion

Hint: Emulate the proof of Thm. 3.5.8.

A non-empty subset $\boldsymbol{S}$ of a linear space $\boldsymbol{V}$ is a subspace exactly when

$$\alpha \cdot X + Y \in \boldsymbol{S}, \text{ whenever } X, Y \in \boldsymbol{S} \text{ and } \alpha \in \mathbb{R}.$$

Exercise 28.2.5 Non-trivial linear spaces are infinite

Hint: Emulate ****??.

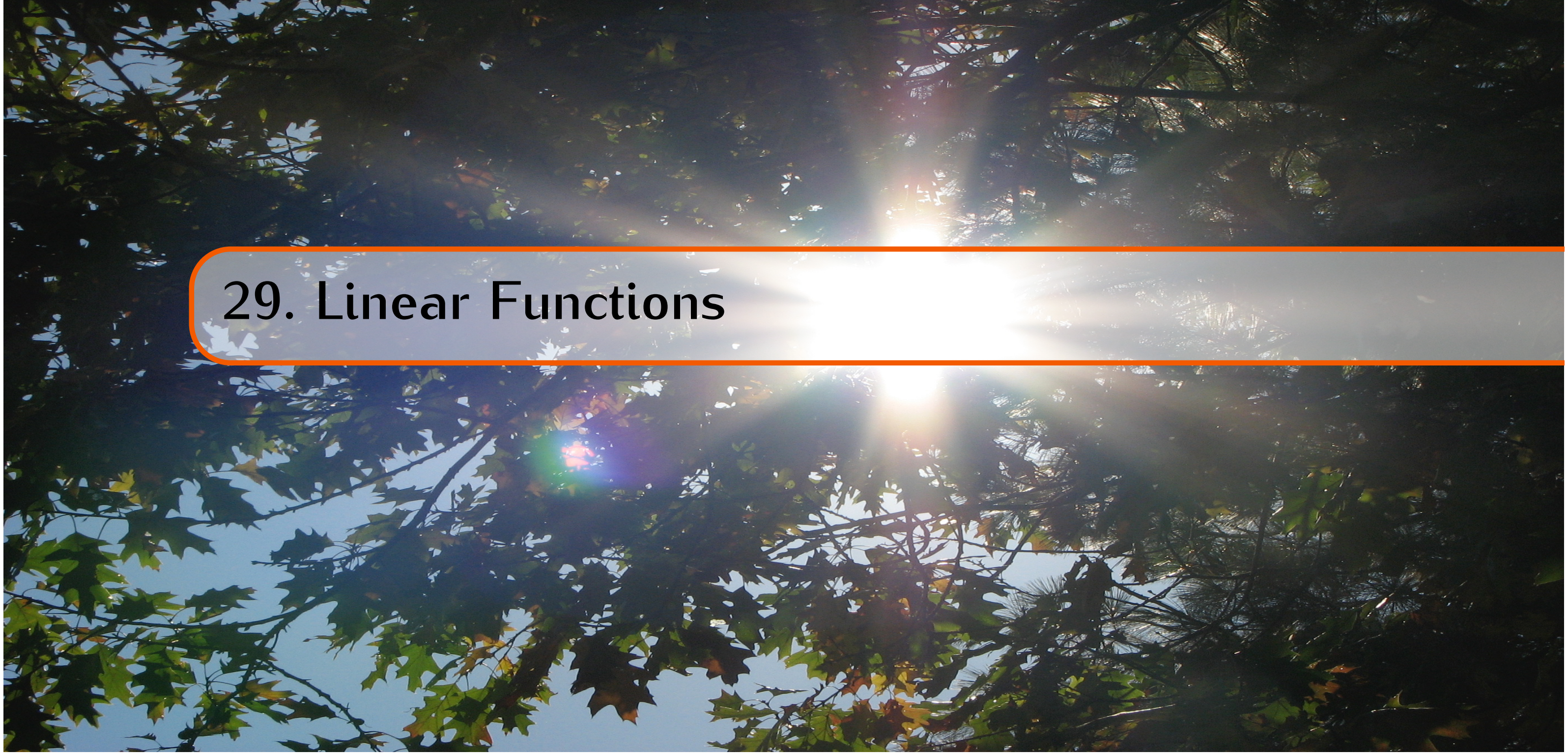
Every non-singleton linear space $\boldsymbol{V}$ is infinite (as a set).

Exercise 28.2.6

Here are some examples of subspaces of linear spaces.

- For any plane P and any line L, Υ^2_P and Υ^1_L are subspaces of Υ^3.
- Υ^1_L is a subspace of Υ^2_P exactly when L is parallel to a line that falls within P (in other words, exactly when L and P do not intersect).
- Υ^0 is a subspace of of every Υ^2_P and Υ^1_L.

- The set $\mathbb{T}_n$ of upper-triangular $n \times n$ matrices is a subspace of $\mathbb{M}_n$.
- The set $\mathbb{D}_n$ of diagonal $n \times n$ matrices is a subspace of $\mathbb{T}_n$, and consequently a subspace of $\mathbb{M}_n$.
- The set $\mathbb{S}_n$ of all symmetric $n \times n$ matrices is a subspace of $\mathbb{M}_n$.
- The set c_0 of all sequences that converge to zero is a subspace of $R^{\mathbb{N}}$.
- The set s of all summable sequences is a subspace of c_0, and is consequently a subspace of $R^{\mathbb{N}}$.
- The set ℓ^1 of all absolutely summable sequences is a subspace of s, and consequently – of c_0 and of $R^{\mathbb{N}}$.
- The set of all functions $f : (0, 1) \longrightarrow \mathbb{R}$ such that $f(\frac{3}{5}) = 0$ is a subspace of $R^{(0,1)}$.
- The set $\mathfrak{C}(0, 1)$ of all continuous real-valued functions with initial space $(0, 1)$ is a subspace of $R^{(0,1)}$.
- The set $\mathfrak{D}(0, 1)$ of all differentiable real-valued functions with initial space $(0, 1)$ is a subspace of $\mathfrak{C}(0, 1)$, and of $R^{(0,1)}$.
- The set $\mathfrak{C}^1(0, 1)$ of all continuously differentiable real-valued functions with initial space $(0, 1)$ is a subspace of $\mathfrak{D}(0, 1)$, $\mathfrak{C}(0, 1)$, and of $R^{(0,1)}$.
- The set of all differentiable functions $f : (0, 1) \longrightarrow \mathbb{R}$ such that $f'(x) + f(x) = 0$ is a subspace of $\mathfrak{C}^1(0, 1)$, and thus of $\mathfrak{D}(0, 1)$, $\mathfrak{C}(0, 1)$, and of $R^{(0,1)}$.
- The set $\mathfrak{C}^\infty(\mathbb{R})$ of all infinitely many times differentiable real-valued functions with initial space $\mathbb{R}$ is a subspace of $\mathfrak{C}^1(\mathbb{R})$, $\mathfrak{D}(\mathbb{R})$, $\mathfrak{C}(\mathbb{R})$, and of $R^{\mathbb{R}}$.
- The set $\mathbb{P}$ of polynomial functions is a subspace of $\mathfrak{C}^\infty(\mathbb{R})$, etc.
- The set $\mathbb{P}_{17}$ of all polynomial functions of degree at most 17 is a subspace of $\mathbb{P}$, and thus of ...



29. Linear Functions

Last modified on December 8, 2018

29.1 Linear Functions

Notation 29.1.1

Let us emphasize the fact that different linear spaces can be comprised of dissimilar objects, and with each space having its own notions of addition and scaling, the reader has to keep track of where the operations are taking place in each particular case.

To facilitate the process, we begin by writing $(\boldsymbol{V}, +, \cdot)$ to indicate a linear space, and by color-coding the $+$ and $\cdot$ signs for distinct linear spaces.

After a short while we shall abandon this practice and count on the reader's ability to discern distinct locations and operations from the context.

Terminology 29.1.2

A function $F : (\boldsymbol{W}, +, \cdot) \longrightarrow (\boldsymbol{Z}, +, \cdot)$ is said to be a **linear function** when it satisfies **the linearity conditions**:

- $F(W+V) = F(W)+F(V)$, for all $W, V \in \boldsymbol{W}$;
- $F(\alpha \cdot W) = \alpha \cdot F(W)$, for all $\alpha \in \mathbb{R}$ and $W \in \boldsymbol{W}$.

The leading condition can be described as saying that adding the inputs first and then applying the function produces the same outcome as applying the function to the individual inputs first and then adding the outputs. In this sense, it can be loosely* interpreted as stating that **the function distributes addition**.

In a similar fashion, the second condition can be loosely interpreted as stating that **the function commutes with scaling**.

*the two operations of addition take place in different linear spaces: the initial space and the final space.

Test Your Comprehension 29.1.3 ☞ **Equivalent conditions for linearity**

The following statements about a function $\mathcal{F} : (\boldsymbol{W}, +, \cdot) \longrightarrow (\boldsymbol{Z}, +, \cdot)$ are mutually equivalent.

1. $\mathcal{F}$ is a linear function.
2. $\mathcal{F}(a \cdot X + Y) = a \cdot \mathcal{F}(X) + \mathcal{F}(Y)$
   for all $a \in \mathbb{R}$ and X, Y in $\boldsymbol{W}$.
3. $\mathcal{F}(a \cdot X + b \cdot Y) = a \cdot \mathcal{F}(X) + b \cdot \mathcal{F}(Y)$
   for all $a, b \in \mathbb{R}$ and X, Y in $\boldsymbol{W}$.
4. $\mathcal{F}(a \cdot X + b \cdot Y + c \cdot V) = a \cdot \mathcal{F}(X) + b \cdot \mathcal{F}(Y) + c \cdot \mathcal{F}(V)$
   for all $a, b, c \in \mathbb{R}$ and X, Y, V in $\boldsymbol{W}$.
5. etc.

Hint: Mimic an argument used for Exercise 6.2.5.

In loose terms, $\mathcal{F}$ is linear exactly when it distributes over linear combinations.

Terminology 29.1.4

We shall refer to the equality (2) in TYC 29.1.3 as the **combined linearity condition**. Checking its validity for a given function $\mathcal{F}$ is often a quickest way of testing the linearity of $\mathcal{F}$.

Methods used in verifying the combined linearity condition for a given function depend very much on the linear spaces in question, and commonly involve mathematical tools explored in other courses, such as Calculus, for example.

Exercise 29.1.5

Argue that each of the following functions is linear. In each case make sure that you understand the definition of the function, including its initial and final spaces.

1. The identity function on any linear space.
2. The constantly $\mathbb{0}_{\boldsymbol{W}}$ function from a linear space $\boldsymbol{V}$ to a linear space $\boldsymbol{W}$.
3. A differentiation function $\mathcal{D} : \mathfrak{D}(0, 1) \longrightarrow R^{(0,1)}$, defined by

$$\mathcal{D}(f) := f'.$$

4. A differentiation function: $\Delta : \mathbb{P}_9 \longrightarrow \mathbb{P}_8$, defined by
$$\Delta(p) := p'.$$
5. An integration function $\mathcal{S} : \mathfrak{C}(0,1) \longrightarrow \mathfrak{D}(0,1)$, defined as follows: for each input function f the output function $\mathcal{S}(f)$ is described by the formula
$$\Big(\mathcal{S}(f)\Big)(z) := \int_{0.5}^{z} f.$$
6. The trace function $\mathcal{T} : \mathbb{M}_n \longrightarrow \mathbb{R}$, defined by
$$\mathcal{T}(\mathcal{A}) := \mathit{Trace}(\mathcal{A}).$$
7. An evaluation function $\mathcal{K} : R^{(0,1)} \longrightarrow \mathbb{R}$, defined by
$$\mathcal{K}(f) := f\left(\frac{1}{\sqrt{3}}\right).$$
8. A "shift in the variable" function $\Gamma : R^{(0,1)} \longrightarrow R^{(-\frac{2}{3},\frac{1}{3})}$, defined as follows: for each input function f the output function $\Gamma(f)$ is described by the formula
$$\Big(\Gamma(f)\Big)(\Box) := f\left(\Box + \frac{2}{3}\right).$$
9. Transposition $\Omega : \mathbb{M}_{5\times 16} \longrightarrow \mathbb{M}_{16\times 5}$, defined by
$$\Omega(\mathcal{B}) := \mathcal{B}^{T}.$$
10. A scaling function $\mathcal{F} : \mathfrak{D}(\mathbb{R}) \longrightarrow \mathfrak{D}(\mathbb{R})$, defined by
$$\mathcal{F}(g) := e^{\pi} g.$$
11. A "polynomial reversal" function $\Pi : \mathbb{P}_7 \longrightarrow \mathbb{P}_7$ defined by
$$\Pi(a_0 + a_1 x + a_2 x^2 + a_3 x^3 + \cdots + a_6 x^6 + a_7 x^7) := \\ a_7 + a_6 x + a_5 x^2 + a_4 x^3 + \cdots + a_1 x^6 + a_0 x^7.$$
12. A "polynomial creation" function: $\mathcal{C} : \mathbb{R}^5 \longrightarrow \mathbb{P}_4$, defined by
$$\mathcal{C}\begin{pmatrix}\alpha_1\\ \alpha_2\\ \alpha_3\\ \alpha_4\\ \alpha_5\end{pmatrix} := \alpha_1 + \alpha_2 t + \alpha_3 t^2 + \alpha_4 t^3 + \alpha_5 t^4.$$
13. A "mutiplication by cosine" function $\mathcal{M} : \mathbb{R}^{\mathbb{R}} \longrightarrow \mathbb{R}^{\mathbb{R}}$, defined by
$$\mathcal{M}(h) := h \cdot \cos.$$
14. A "composing with sine" function $\zeta : (0,1)^{[0,1]} \longrightarrow (0,1)^{\mathbb{R}}$, defined by
$$\zeta(g) := g \circ \sin.$$

Terminology 29.1.6

The function $\mathcal{F} : (\boldsymbol{W}, +, \cdot) \longrightarrow (\boldsymbol{Z}, +, \cdot)$ that sends every input to $\mathbb{O}_{\boldsymbol{W}}$, i.e. is **a constantly $\mathbb{O}_{\boldsymbol{W}}$ function**, is said to be **a null function** and is denoted by the symbol $\mathcal{O}_{\boldsymbol{W} \leftarrow \boldsymbol{V}}$.

In the case that $(\boldsymbol{W}, +, \cdot) = (\boldsymbol{Z}, +, \cdot)$, we will write $\mathcal{O}_{\boldsymbol{W}}$.

We will often drop off the subscript all together, and just write $\mathcal{O}$, when the notion being described is clear from the context.

One can play a game of abstraction to show that all linear functions have some properties in common. Since matrix functions are examples of linear functions, such properties will often remind the reader of the corresponding results about matrices presented earlier in the text. In many cases a proof of a general property can be obtained by emulating the proof of the property in the matrix case.

Hint: $\mathbb{O}_{\boldsymbol{V}} = 0 \cdot \mathbb{O}_{\boldsymbol{V}}$.

Exercise 29.1.7 ☞ **Linear functions map null elements to null elements**

For any $\mathcal{F} : \boldsymbol{V} \xrightarrow{\text{linear}} \boldsymbol{W}, \quad \mathcal{F}(\mathbb{O}_{\boldsymbol{V}}) = \mathbb{O}_{\boldsymbol{W}}$.

Exercise 29.1.8

Argue that each of the following functions is NOT linear. To do so you will need to come up with CONCRETE inputs (and scalars, if need be) that demonstrate a failure of the linearity conditions for the function, or a failure of the function to satisfy a property that all linear functions satisfy (for example: every linear function sends the neutral element to the neutral element).

1. A squaring function $\mathcal{F} : \mathbb{P} \longrightarrow \mathbb{P}$ defined by
$$\mathcal{F}(p) := p^2.$$
2. A composing function $\beta : \mathfrak{C}\Big((0,1), \mathbb{R}\Big) \longrightarrow \mathfrak{C}\Big((0,1), [-1,1]\Big)$ defined by
$$\beta(g) := \sin \circ g\,.$$
3. A function $\gamma : \mathfrak{D}(-1,1) \longrightarrow \mathfrak{D}(-1,1)$ defined by
$$\gamma(f) := e^f.$$
4. A function $\phi : \mathfrak{C}(-3,-1) \longrightarrow R^{(-3,-1)}$ which for each input function h produces the output function $\phi(h)$ defined by
$$\Big(\phi(h)\Big)(z) := \int_z^{-2} (5h+1)\,.$$
5. A function $\theta : \mathbb{M}_{9\times 5} \longrightarrow \mathbb{M}_5$ defined by
$$\theta(\mathcal{A}) := \mathcal{A}^T\mathcal{A}.$$

29.2 Operations On Functions With Linear Destination Spaces

29.2.1 — Scaling

Terminology 29.2.1

Given a function $\mathcal{F} : \Omega \longrightarrow (\boldsymbol{Z}, +, \cdot)$, and a scalar $\alpha \in \mathbb{R}$ we can form a new function $\mathcal{G} : \Omega \longrightarrow (\boldsymbol{Z}, +, \cdot)$ by declaring that

$$\mathcal{G}(\omega) := \alpha \cdot \mathcal{F}(\omega)$$

for all $\omega \in \Omega$. The function $\mathcal{G}$ is said to be **a scalar multiple of the function** $\mathcal{F}$, and is denoted by $\alpha \,\hat{\cdot}\, \mathcal{F}$.

Note that $\hat{\cdot}$ is an operation for the set $\boldsymbol{Z}^{\Omega}$, whereas $\cdot$ is an operation for $\boldsymbol{Z}$.

$$(\alpha \,\hat{\cdot}\, \mathcal{F})(\omega) := \alpha \cdot \mathcal{F}(\omega)$$

In other words, $\alpha \,\hat{\cdot}\, \mathcal{F}$ acts by performing $\mathcal{F}$ first, followed by the $\cdot$ -scaling of the output by α.

Compare this to the construction presented in Terminology 7.2.1.

Test Your Comprehension 29.2.2

Argue that for any $\mathcal{F} : \Omega \longrightarrow (\boldsymbol{Y}, +, \cdot)$ and $\alpha, \beta \in \mathbb{R}$,

$$\alpha \,\hat{\cdot}\, (\beta \,\hat{\cdot}\, \mathcal{F}) = (\alpha \cdot \beta) \,\hat{\cdot}\, \mathcal{F} = (\beta \cdot \alpha) \,\hat{\cdot}\, \mathcal{F} = \beta \,\hat{\cdot}\, (\alpha \,\hat{\cdot}\, \mathcal{F}) \,.$$

Hint: Mimic the argument used for TYC 7.2.3.

Test Your Comprehension 29.2.3

For any $\mathcal{F} : \Omega \longrightarrow (\boldsymbol{Y}, +, \cdot)$,

$$1 \,\hat{\cdot}\, \mathcal{F} = \mathcal{F}, \quad \text{and} \quad 0 \,\hat{\cdot}\, \mathcal{F} \text{ is the constantly } \mathbb{0}_{\boldsymbol{Y}} \text{ function.}$$

29.2.2 — Addition

Terminology 29.2.4

This time we start with two functions $\mathcal{F} : \Omega \longrightarrow (\boldsymbol{V}, +, \cdot)$ and $\mathcal{G} : \Omega \longrightarrow (\boldsymbol{V}, +, \cdot)$, whose final space is a linear space, and we form a new function $\mathcal{H} : \Omega \longrightarrow (\boldsymbol{V}, +, \cdot)$ by declaring that

$$\mathcal{H}(\omega) := \mathcal{F}(\omega) + \mathcal{G}(\omega), \quad \text{for all} \quad \omega \in \Omega \,.$$

This function $\mathcal{H}$ is said to be **the sum of functions $\mathcal{F}$ and $\mathcal{G}$**, and is denoted by $\mathcal{F} \hat{+} \mathcal{G}$. So,

$$(\mathcal{F} \hat{+} \mathcal{G})(\omega) := \mathcal{F}(\omega) + \mathcal{G}(\omega) \; .$$

In other words, $\mathcal{F} \hat{+} \mathcal{G}$ acts by applying $\mathcal{F}$ and $\mathcal{G}$ individually first (to the same given input), and then $+$ -adding their outputs.

Compare this to the construction presented in Terminology 7.3.1 in the case of matrix functions.

Again, $\hat{+}$ is an operation for the set $\boldsymbol{V}^{\Omega}$, whereas $+$ is an operation for $\boldsymbol{V}$.

Test Your Comprehension 29.2.5

For any $\mathcal{F} : \Omega \longrightarrow (\boldsymbol{Y}, +, \cdot)$,

$$\left(-1 \hat{\cdot} \mathcal{F} \right) \hat{+} \mathcal{F} \quad \text{is the constantly } \mathbb{0}_{\boldsymbol{Y}} \text{ function.}$$

Exercise 29.2.6 ☞ Functions into a linear space form a linear space

Given linear space $(\boldsymbol{W}, +, \cdot)$, and a set Ω, the space $\left(\boldsymbol{W}^{\Omega}, \hat{+}, \hat{\cdot}\right)$ is a linear space.*

*We have encountered this construction when we considered $\mathbb{R}^{(0,1)}$ and $\mathbb{R}^{\mathbb{N}}$ in Examples 28.1.3.

Example 29.2.7

The set $(\mathbb{R}^n)^{(0,1)}$ of all functions from the interval $(0, 1)$ to $\mathbb{R}^n$ becomes a linear space when we define operations addition and scaling for it in accordance with Terminology 29.2.1 and 29.2.4.

Comment 29.2.8

Based on the result given in Exercise 29.2.6, we can form linear combinations of functions acting from a given set to a given linear space.

We can even consider linear functions on the linear space $\left(\boldsymbol{W}^{\Omega}, \hat{+}, \hat{\cdot}\right)$ of such functions.

This may sound convoluted, but we have already encountered such a construction when we considered an evaluation function $\mathcal{K} : R^{(0,1)} \longrightarrow \mathbb{R}$, defined by

$$\mathcal{K}(f) := f\left(\frac{1}{\sqrt{3}}\right) \; ,$$

in Exercise 29.1.5.

Theorem 29.2.9 ☞ **Linear combinations of linear functions are linear**

The set $L(\boldsymbol{V}, \boldsymbol{W})$ of all linear functions acting from $(\boldsymbol{V}, +, \cdot)$ to $(\boldsymbol{W}, +, \cdot)$ is a subspace of the linear space $\left(\boldsymbol{W}^{\boldsymbol{V}}, \hat{+}, \hat{\cdot}\right)$.

In other words, in this context, a sum of two linear functions is another linear function, as is a scalar multiple of a linear function; i.e. a linear combination of linear functions is a linear function.

Proof of Theorem 29.2.9. By TYC 28.2.4, it is sufficient to verify that $\mathcal{H} := \alpha \hat{\cdot} \mathcal{F} \hat{+} \mathcal{G}$ is a linear function, whenever $\mathcal{F}$ and $\mathcal{G}$ are linear, and $\alpha \in \mathbb{R}$.

To this end, by TYC 29.1.3, it is sufficient to show that

$$\mathcal{H}\big(\gamma \cdot X + Y\big) = \gamma \cdot \mathcal{H}(X) + \mathcal{H}(Y) ,$$

for all $X, Y \in \boldsymbol{V}$, and $\gamma \in \mathbb{R}$.

To this end,

$$\mathcal{H}(X) = \Big(\alpha \hat{\cdot} \mathcal{F} \hat{+} \mathcal{G}\Big)(X) = \alpha \cdot \mathcal{F}(X) + \mathcal{G}(X) .$$

Similarly

$$\mathcal{H}(Y) = \alpha \cdot \mathcal{F}(Y) + \mathcal{G}(Y) .$$

Thus

$$\begin{aligned} \gamma \cdot \mathcal{H}(X) + \mathcal{H}(Y) &= \gamma \cdot \Big(\alpha \cdot \mathcal{F}(X) + \mathcal{G}(X)\Big) + \Big(\alpha \cdot \mathcal{F}(Y) + \mathcal{G}(Y)\Big) \\ &\overset{\text{algebra in } \boldsymbol{W}}{=} \alpha \cdot \Big(\gamma \cdot \mathcal{F}(X) + \mathcal{F}(Y)\Big) + \Big(\gamma \cdot \mathcal{G}(X) + \mathcal{G}(Y)\Big) \\ &\overset{\text{linearity of } \mathcal{F}, \mathcal{G}}{=} \alpha \cdot \mathcal{F}\big(\gamma \cdot X + Y\big) + \mathcal{G}\big(\gamma \cdot \mathcal{X} + \mathcal{Y}\big) \\ &= \mathcal{H}\big(\gamma \cdot X + Y\big) . \end{aligned}$$

■

Notation 29.2.10

At this time we end our diligent use of distinct symbols and color-coding (such as $+, \cdot, +, \cdot, \hat{+}, \hat{\cdot}$) to indicate operations on different linear spaces, and begin using symbols $+, \cdot$ universally for all linear spaces, including the types of spaces described in Exercise 29.2.6 and Theorem 29.2.9.

Furthermore, we will continue our previous practice of dropping "$\cdot$" off whenever this does not cause ambiguity.

29.2.3 — Composing Linear Functions

Hint: TYC 29.1.3.

Exercise 29.2.11 ☞ **Compositions of linear functions are linear**

If $\mathcal{F} : \boldsymbol{Z} \xrightarrow{\text{linear}} \boldsymbol{W}$, and $\mathcal{L} : \boldsymbol{W} \xrightarrow{\text{linear}} \boldsymbol{Y}$, then $\mathcal{L} \circ \mathcal{F} : \boldsymbol{Z} \xrightarrow{\text{linear}} \boldsymbol{Y}$.

Exercise 29.2.12 ☞ **Composition distributes (from either side) over linear combinations**

If $\mathcal{F}, \mathcal{G} : \boldsymbol{V} \xrightarrow{\text{linear}} \boldsymbol{W}$, $\mathcal{H} : \boldsymbol{W} \xrightarrow{\text{linear}} \boldsymbol{Z}$, $\mathcal{D} : \boldsymbol{Y} \xrightarrow{\text{linear}} \boldsymbol{V}$, then for any $a, b \in \mathbb{R}$,

$$\mathcal{H} \circ \Big(a \cdot \mathcal{F} + b \cdot \mathcal{G}\Big) = a \cdot \big(\mathcal{H} \circ \mathcal{F}\big) + b \cdot \big(\mathcal{H} \circ \mathcal{G}\big)$$

and

$$\Big(a \cdot \mathcal{F} + b \cdot \mathcal{G}\Big) \circ \mathcal{D} = a \cdot \big(\mathcal{F} \circ \mathcal{D}\big) + b \cdot \big(\mathcal{G} \circ \mathcal{D}\big) .$$

By taking $a = b = 1$, observe that *composition distributes over addition* (from either side).

By taking $\mathcal{G} = \mathcal{O}_{\boldsymbol{W} \leftarrow \boldsymbol{V}}$ and exchanging the roles of $\mathcal{F}$ and $\mathcal{H}$ as needed, argue that

$$\mathcal{H} \circ \big(a \cdot \mathcal{F}\big) = a \cdot \big(\mathcal{H} \circ \mathcal{F}\big) = \big(a \cdot \mathcal{H}\big) \circ \mathcal{F} .$$

Hint: Compare to Exc. 8.1.6.

In other words, *we can bring in a scalar into the composition* and attach it to any one of the functions involved. Alternatively, *we can pull scalar multiples out of the composition.*

Test Your Comprehension 29.2.13 ☞ **Inverses of linear functions are linear**

Hint: Look at the proof of Thm. 6.4.5.

The inverse of a bijective linear function is a (bijective) linear function.

Exercise 29.2.14 ☞ **Compositions of rotations in the plane**

Is a composition of rotations on Υ^2_P necessarily a rotation? *

*The corresponding question about rotations on Υ^3 is much harder, but we shall be able to deal with it later in the book.

29.3 Nullspaces And Ranges Of Linear Functions

Terminology 29.3.1

Generalizing the notion of a nullspace of a matrix, we define the **nullspace (a.k.a. kernel)** of a linear function $\mathcal{F} : (\boldsymbol{W}, +, \cdot) \longrightarrow (\boldsymbol{Z}, +, \cdot)$ to be the set of all inputs it annihilates*, namely

$$Nullspace\,(F) := \{ \; W \in \boldsymbol{W} \mid \mathcal{F}(W) = \mathbb{0}_{\boldsymbol{Z}} \; \} \, .$$

*As before, an input is **annihilated** iff it is mapped to the null element.

Test Your Comprehension 29.3.2

The following are equivalent for a function $\mathcal{F} : \boldsymbol{V} \xrightarrow{\text{linear}} \boldsymbol{W}$.

1. $\mathcal{F}$ is null.
2. Nullspace of $\mathcal{F}$ is $\boldsymbol{V}$.
3. Range of $\mathcal{F}$ is $\{\mathbb{0}_{\boldsymbol{W}}\}$.

Exercise 29.3.3

For any $\mathcal{F} : \boldsymbol{V} \xrightarrow{\text{linear}} \boldsymbol{W}$,

$Nullspace\,(\mathcal{F})$ is a subspace of $\boldsymbol{V}$, and

$Range\,(\mathcal{F})$ is a subspace of $\boldsymbol{W}$.

Exercise 29.3.4 ☞ **Nullspaces and injectivity**

The following are equivalent for any $\mathcal{F} : \boldsymbol{V} \xrightarrow{\text{linear}} \boldsymbol{W}$.

1. $\mathcal{F}$ is injective.
2. $Nullspace\,(\mathcal{F}) = \{\mathbb{0}_{\boldsymbol{V}}\}$.

Hint: Emulate Thm. 12.1.6.

Test Your Comprehension 29.3.5 ☞ **Nullspace of a composition**

If $\mathcal{F}, \mathcal{G}$ are linear functions and $\mathcal{F} \circ \mathcal{G}$ makes sense, then

$$Nullspace\,(\mathcal{G}) \subseteq Nullspace\,(\mathcal{F} \circ \mathcal{G}) \; .$$

In other words, if X is annihilated by $\mathcal{G}$, then it is annihilated by $\mathcal{F} \circ \mathcal{G}$.

Hint: Emulate TYC 12.1.13.

Exercise 29.3.6

If $\mathcal{F}$ is *injective* and $\mathcal{F} \circ \mathcal{G}$ makes sense, then

$$\mathit{Nullspace}\,(\mathcal{G}) = \mathit{Nullspace}\,(\mathcal{F} \circ \mathcal{G}) \ .$$

The intuitive idea here is that injective functions only annihilate the null tuples (TYC 29.3.4) and so are of little help in the business of annihilation.

Hint: Emulate TYC 12.1.13.

Exercise 29.3.7

Describe the nullspaces of the functions presented in Exercise 29.1.5.

Exercise 29.3.8

Describe the ranges of the functions presented in Exercise 29.1.5.

You may skip the function in part 3.

Hint: When trying to show that the outputs of $\mathcal{T}$ are polynomials of degree at most 5, you are arguing that for each polynomial p of degree at most 5, the formula $q(t) := p(t+1)$ defines a polynomial q (in t) of degree at most 5.
When considering injectivity, think about the kernel of $\mathcal{T}$, which consists of those polynomial functions $p \in \mathbb{P}_5$ for which $\mathcal{T}(p)$ is the constant(ly) zero polynomial. Keep in mind that a polynomial of degree $n > 0$ cannot have more than n roots.
When considering surjectivity, you will want to show that every polynomial q in $\mathbb{P}_5$ satisfies the identity $q(s) = p(s+1)$ for some polynomial $p \in \mathbb{P}_5$ and all $s \in \mathbb{R}$. Argue that this is the same identity as
$q(w-1) = p(w)$ for all $w \in \mathbb{R}$.
This should help you find the required p.

Exercise 29.3.9 ☞ Recentering Polynomials

Define a function $\mathcal{T}$ with the initial space $\mathbb{P}_5$ by declaring that for each input polynomial p the output is the function $\mathcal{T}(p)$ defined by

$$\Big(\mathcal{T}(p)\Big)(t) = p(t+1).$$

Argue that $\mathcal{T} : \mathbb{P}_5 \longrightarrow \mathbb{P}_5$ and that $\mathcal{T}$ is a linear bijection.

Infer that every polynomial (function) $p(x) = a_0 + a_1 x + a_2 x^2 + a_3 x^3 + \ldots + a_5 x^5$ can be expressed in exactly one way in the form

$$p(z) = b_0 + b_1(z-1) + b_2(z-1)^2 + \cdots + b_5(z-1)^5.$$

Exercise 29.3.10

Suppose that $\mathcal{F} : \boldsymbol{V} \xrightarrow{\text{linear}} \boldsymbol{W}$ and

$$\mathcal{F}(X_o) = Y_o .$$

Then

$$\{\ X_o + Z \mid Z \in \mathit{Nullspace}(\mathcal{F})\ \} \text{ is the set of ALL inputs that } \mathcal{F} \text{ sends to the output } Y_o .^*$$

In other words,

$$\mathcal{F}(X) = Y_o \iff X = X_o + Z, \quad \text{for some } Z \in \mathit{Nullspace}(\mathcal{F})$$

$$\iff X - X_o \in \mathit{Nullspace}(\mathcal{F}) .$$

Hint: Emulate Thm. 12.1.7

*If $\mathcal{F}$ is not injective, then $\mathit{Nullspace}(\mathcal{F})$ is an infinite set (Exc. 28.2.5), and so there are infinitely many different choices for Z. In that case the given set of inputs is infinite too.

29.4 Atrices

In our study of linear functions acting from $\mathbb{R}^m$ to $\mathbb{R}^n$, we relied heavily on such functions being matrix functions (Thm. 6.2.1), and hence being represented by tables of numbers. This latter representation was a consequence of the original definition (Def. 6.1.1), which stated that a matrix function is a function generated by a list of tuples in the final space $\mathbb{R}^n$, and it acts by creating a linear combination of these generating tuples using the entries of an input as coefficients.

Our next step is to show that these ideas can be applied to the study of linear functions ("atrices") acting from $\mathbb{R}^m$ to a general linear space $\boldsymbol{V}$.

The concept of atrices enables one to develop analogues of matricial results in a more general setting of linear spaces by simply emulating the proofs that were given for the matrix case. Consequently we are able to introduce concepts such a linear independence and spans in linear spaces by mimicking the development of these concepts in $\mathbb{R}^n$.

For this reason much of the material is presented in the form of TYC's and Exercises for the reader, who should be prepared to emulate the results of the earlier chapters, and thus has a natural opportunity to review the previous material.

Definition 29.4.1

Given elements $V_1, V_2, \ldots, V_m$ of a linear space $\boldsymbol{V}$, consider a function $f : \mathbb{R}^m \longrightarrow \boldsymbol{V}$ defined by

$$f\begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_m \end{pmatrix} := a_1 V_1 + a_2 V_2 + \ldots + a_m V_m \ .$$

Motivated by matricial notation and terminology, we denote f by

$$\begin{bmatrix} V_1 & V_2 & \cdots & V_m \end{bmatrix},$$

and shall refer to such an f as an **atrix function**, or an **atrix** for short. We will say that $V_1, V_2, \ldots, V_m$ are its **columns**. The columns of f are elements of $\boldsymbol{V}$, and consequently may not look like "columns" at all (see Examples 29.4.2 and 29.4.3). This let us say that "*an atrix looks like a matrix except its columns are not tuples but elements of* $\boldsymbol{V}$".

If $\boldsymbol{V}$ happens to be some $\mathbb{R}^n$, then of course, f is a matrix function and our notation coincides with the original matricial notation (Notation 6.1.4).

Clearly, a matrix is a particular type of an atrix, but not every atrix is a matrix, because not every linear space is an $\mathbb{R}^n$.

Example 29.4.2

For example, if $\boldsymbol{Z}$ is the linear space $\mathfrak{C}(0,1)$, then

$$\begin{bmatrix} e^{\square} & \sin\square & \square^2 - 2\square + 3 & 5 \end{bmatrix}$$

is an example of an atrix which maps $\mathbb{R}^4$ to $\mathfrak{C}(0,1)$, and has functions $e^{\square}$, $\sin\square$, $\square^2 - 2\square + 3$ and 5 as its columns. These are, of course, objects in $\mathfrak{C}(0,1)$. Here

$$\begin{bmatrix} e^{\square} & \sin\square & \square^2 - 2\square + 3 & 5 \end{bmatrix}\begin{pmatrix} 9 \\ -2 \\ \pi \\ \frac{3}{8} \end{pmatrix} =$$

$$= 9e^{\square} - 2\sin\square + \pi\cdot\square^2 - 2\pi\cdot\square + 3\pi + \frac{15}{8} \quad \in \mathfrak{C}(0,1)$$

Example 29.4.3

Similarly, the atrix

$$\begin{bmatrix} \uparrow & \searrow & \longleftarrow \end{bmatrix} : \mathbb{R}^3 \longrightarrow \mathfrak{G}^2,$$

is the function defined by

$$\begin{bmatrix} \uparrow & \searrow & \longleftarrow \end{bmatrix} \begin{pmatrix} a_1 \\ a_2 \\ a_3 \end{pmatrix} = a_1 \cdot \uparrow \; + a_2 \cdot \searrow \; + a_3 \cdot \longleftarrow \; ,$$

where $\mathfrak{G}^2$ stands for the linear space of planar geometric vectors. Here $\searrow$ is the second column of the atrix.

Test Your Comprehension 29.4.4 ☞ **Columns of an atrix are images of the standard basis tupples**

If $f : \mathbb{R}^n \longrightarrow \boldsymbol{Z}$ is an atrix function, then

$$f = \begin{bmatrix} f(E_1) & f(E_2) & \dots & f(E_m) \end{bmatrix} .^{*}$$

Hint: Emulate Thm. 6.1.10.

* $E_1, E_2, \dots, E_m$ is the standard coordinate system of $\mathbb{R}^m$.

Test Your Comprehension 29.4.5

A nullspace of an attrix contains a standard basis tuple if and only if one its columns is a null element.

Test Your Comprehension 29.4.6 ☞ **Range of an atrix is the span of its columns**

The range of an atrix $\mathcal{F} : \mathbb{R}^n \longrightarrow \boldsymbol{V}$ is the set of all elements of $\boldsymbol{V}$ that can be expressed as a linear combination of the columns of $\mathcal{F}$.

Terminology 29.4.7

Atrix $\mathcal{O}_{\boldsymbol{V} \leftarrow \mathbb{R}^m}$ is said to be a **null atrix**. Recall that $\mathcal{O}_{\boldsymbol{V} \leftarrow \mathbb{R}^m}$ stands for the linear function from $\mathbb{R}^m$ to $\boldsymbol{V}$ which maps every m-tuple to the null element $\mathbb{O}_{\boldsymbol{V}}$ of $\boldsymbol{V}$.

Test Your Comprehension 29.4.8 ☞ **Characterizations of null atrices**

The following are equivalent for an atrix $\mathcal{B} : \mathbb{R}^m \longrightarrow \boldsymbol{V}$.

1. $\mathcal{B}$ is a null atrix.

2. Every column of $\mathcal{B}$ is null (i.e. is $\mathbb{0}_{\boldsymbol{V}}$).

3. The range of $\mathcal{B}$ is the singleton set $\{\mathbb{0}_{\boldsymbol{V}}\}$.

4. The nullspace of $\mathcal{B}$ is $\mathbb{R}^m$.

29.4.1 — Atrices As Linear Functions

Matrices are exactly the linear functions from some $\mathbb{R}^m$ to some $\mathbb{R}^n$, and atrices turn out to be exactly the linear functions from some $\mathbb{R}^m$ to some linear space, which may or may not be an $\mathbb{R}^n$.

⇩

Exercise 29.4.9 ☞ $\mathbb{R}^n \xrightarrow{\text{linear}} \boldsymbol{V} \Longleftrightarrow \mathbb{R}^n \xrightarrow{\text{attrix}} \boldsymbol{V}$

Hint: Emulate Thm. 6.2.1.

For a function $f : \mathbb{R}^n \longrightarrow \boldsymbol{V}$, the following claims are equivalent.

1. f is a linear function.

2. f is an atrix function.

Therefore "the land of atrices" contains "the land of matrices", and is part of the bigger "land of general linear functions". Atrices have the same initial spaces as matrices, but their final spaces are as general as those of the general linear functions.

Of course, atrices act from $\mathbb{R}^n$'s to the general linear spaces, and their role as the connectors between spaces we understand well and those that are less familiar, will prove to be of utmost importance.

Test Your Comprehension 29.4.10

If an atrix $\mathcal{A}$ is bijective/invertible, its inverse is a linear function, but is an atrix only if $\mathcal{A}$ is a matrix.

29.4.2 — Combining Atrices

Atrices can be scaled and added in the same fashion as matrices, via the scaling and/or addition of their columns.

⇩

Test Your Comprehension 29.4.11 ☞ **Linear combinations of atrices**

Argue that a linear combination of atrices $F, G : \mathbb{R}^m \longrightarrow \boldsymbol{V}$ is an atrix by showing that

$$\alpha \cdot \begin{bmatrix} V_1 & V_2 & \cdots & V_m \end{bmatrix} + \beta \cdot \begin{bmatrix} Z_1 & Z_2 & \cdots & Z_m \end{bmatrix}$$

$$= \begin{bmatrix} \alpha V_1 + \beta Z_1 & \alpha V_2 + \beta Z_2 & \cdots & \alpha V_m + \beta Z_m \end{bmatrix}.$$

Because of the asymmetry of the initial space of an atrix being some $\mathbb{R}^n$ and the final space being some linear space (commonly not an $\mathbb{R}^m$), two atrices can be composed only when one of them (the one going first) is a matrix.

⇩

Test Your Comprehension 29.4.12 ☞ **Compositions of atrices**

Argue that a composition $\mathcal{F} \circ \mathcal{G}$ of two atrix functions does NOT makes sense when $\mathcal{G}$ is NOT a matrix.

By Exercise 29.2.11, a composition of linear functions is a linear function. In particular, if $\mathcal{A} : \mathbb{R}^m \longrightarrow \mathbb{R}^n$ is a matrix, and $f : \mathbb{R}^n \longrightarrow \boldsymbol{V}$ is an atrix, then $f \circ \mathcal{A} : \mathbb{R}^m \longrightarrow \boldsymbol{V}$ is a linear function, and therefore an atrix (Exc 29.4.9).

⇩

Test Your Comprehension 29.4.13 ☞ **Attrix ∘ Matrix**

If $\mathcal{A} : \mathbb{R}^m \longrightarrow \mathbb{R}^n$ is a matrix $\begin{bmatrix} C_1 & C_2 & \cdots & C_m \end{bmatrix}$, and $f : \mathbb{R}^n \longrightarrow \boldsymbol{V}$ is an atrix, then

$$f \circ \mathcal{A} = \begin{bmatrix} f(C_1) & f(C_2) & \cdots & f(C_m) \end{bmatrix}.$$

Hint: Emulate Thm. 8.1.7.

INSERT PICTURE

Exercise 29.4.14 ☞ **Range inclusion factorization for atrices**

The following claims are equivalent for atrices $\mathcal{F} : \mathbb{R}^m \longrightarrow \boldsymbol{V}$ and $\mathcal{G} : \mathbb{R}^k \longrightarrow \boldsymbol{V}$.

1. $\mathit{Range}(\mathcal{F}) \subseteq \mathit{Range}(\mathcal{G})$.

2. $\mathcal{F} = \mathcal{G} \circ \mathcal{C}$, for some $\mathcal{C} \in \mathbb{M}_{k \times m}$.

Hint: Emulate Thm. 13.1.2.

29.4.3 — Manupulating Columns Of Atrices

Comment 29.4.15

Since atrices generally do not have rows (so that, for example, we do not define transposition for atrices the way this was done for matrices), we focus on generalizing to the atrix setting the matricial results dealing with columns, and we leave those that dealt with rows behind (for the time being).

Exercise 29.4.16 **Columns and injectivity**

The following statements are equivalent for an atrix $\mathcal{A} : \mathbb{R}^m \longrightarrow \boldsymbol{V}$.

1. $\mathcal{A}$ is NOT injective.

2. A non-trivial* linear combination of the columns of $\mathcal{A}$ equals the null element $\mathbb{0}_{\boldsymbol{V}}$.

3. Either $\mathcal{A} = \left[\mathbb{0}_{\boldsymbol{V}}\right]$ or at least one of the columns of $\mathcal{A}$ is a linear combination of some other columns.

4. Either the first column of $\mathcal{A}$ is $\mathbb{0}_{\boldsymbol{V}}$, or at least one of the columns of $\mathcal{A}$ is a linear combination of some of the *preceding* columns of $\mathcal{A}$.

Hint: Emulate Thms. 12.2.3 and 12.2.5.

*A **non-trivial linear combination** linear combination is one where not all coefficients are zero.

Test Your Comprehension 29.4.17

An atrix with a single column is injective exactly when that column is not a null element.

Terminology 29.4.18

There are three types of **(elementary) column operations for atrices**. These replicate the elementary column operations on matrices.

Swap Columns: Swap two columns of an atrix, leaving all other columns as they were.

Scale a Column: Scale a column of an atrix by a NON-ZERO scalar.

Adjust a Column: Add to a given column of an atrix a NON-ZERO multiple of another column.

Theorem 29.4.19 ☞ **Elementary column operations for atrices**

Performing an elementary column operation on an atrix $\mathcal{F}$ amounts to composing it with an appropriate elementary matrix $\mathcal{E}$ to form $\mathcal{F} \circ \mathcal{E}$.

Here are the details:

1. To swap the i-th and the j-th columns of $\mathcal{F}$: form $\mathcal{F} \circ \overset{[i]\leftrightarrow[j]}{\mathcal{E}}$.
2. To scale the j-th column of $\mathcal{F}$ by $\alpha \neq 0$: form $\mathcal{F} \circ \overset{\alpha\cdot[j]}{\mathcal{E}}$.
3. To adjust the j-th column of $\mathcal{F}$ by adding to it α times the i-th column: form $\mathcal{F} \circ \overset{[i] \leftarrow\!+\, \alpha\cdot[j]}{\mathcal{E}}$. (Note the index reversal.)

Proof of Theorem 29.4.19. Let $\mathcal{F}$ be the atrix $\begin{bmatrix} V_1 & V_2 & V_3 & V_4 & V_5 \end{bmatrix}$. Then

$$\begin{aligned}
\mathcal{F} \circ \overset{[2]\leftrightarrow[5]}{\mathcal{E}} &\overset{\text{Thm. 10.1.3}}{=} \mathcal{F} \circ \begin{bmatrix} E_1 & E_5 & E_3 & E_4 & E_2 \end{bmatrix} \\
&= \begin{bmatrix} \mathcal{F}(E_1) & \mathcal{F}(E_5) & \mathcal{F}(E_3) & \mathcal{F}(E_4) & \mathcal{F}(E_2) \end{bmatrix} \\
&= \begin{bmatrix} V_1 & V_5 & V_3 & V_4 & V_2 \end{bmatrix}.
\end{aligned}$$

The proof can be converted to that for a general case by using symbolic subscripts and ellipses.

We leave the proofs of the other two claims as an exercise for the reader (Exc. 29.4.20). ■

Exercise 29.4.20

Prove the last two claims of Theorem 29.4.19.

Test Your Comprehension 29.4.21 ☞ **Elementary column operations for atrices do not affect the jectivity and do not change the range**

Performing an elementary column operation on an atrix $\mathcal{A}$ produces an atrix with the same range and the same jectivity as $\mathcal{A}$.

Hint: Compare to Observations 10.2.9 and 10.2.10.

Exercise 29.4.22 ☞ **Creating null columns via column operations**

If a column of an atrix $\mathcal{A} : \mathbb{R}^m \longrightarrow \boldsymbol{V}$ is a linear combination of some of the other columns of $\mathcal{A}$, then by performing a sequence of column adjustments we can turn that column into a $\mathbb{0}_{\boldsymbol{V}}$.

Hint: Emulate Thm. 14.1.2

29.4.4 — Column Insertion/Deletion And Atrix Ranges

Hint: Emulate TYC 10.2.10.

Test Your Comprehension 29.4.23 ☞ **Elementary column operations do not affect the range**

Performing elementary *column* operations on an atrix produces an atrix with the same range.

In particular, rearranging the order in which the columns of an atrix appear has no bearing on the range of the atrix.

Hint: Emulate Exc. 14.1.1.

Exercise 29.4.24 ☞ **Inserting or deleting null columns does not alter the range of an atrix**

An atrix produced from an atrix $\mathcal{A} : \mathbb{R}^m \longrightarrow \boldsymbol{V}$ by inserting or deleting null columns $\mathbb{O}_{\boldsymbol{V}}$ has the same range as $\mathcal{A}$.

Hint: Emulate Cor. 14.1.3.

Test Your Comprehension 29.4.25 ☞ **Deleting columns without changing the range of an atrix**

If a column of an atrix $\mathcal{A}$ is a linear combination of some other columns of $\mathcal{A}$, then its deletion produces an atrix with the same range as $\mathcal{A}$.

Hint: Emulate Thm. 14.1.4.

Exercise 29.4.26 ☞ **Slimming down to an injective atrix with the same range**

Given a non-null atrix $\mathcal{A}$, by deleting some (may be none) of the columns of $\mathcal{A}$ it is always possible to arrive at an *injective* atrix that has the same range as $\mathcal{A}$.

Exercise 29.4.27 ☞ **Inserting columns without changing the range of an atrix**

Suppose that an atrix $\mathcal{B}$ is obtained from an atrix $\mathcal{A}$ via an insertion of some additional columns. Then the following statements are equivalent.

Hint: Emulate Exc. 14.2.1.

1. $\mathit{Range}\,(\mathcal{B}) = \mathit{Range}\,(\mathcal{A})$.
2. All of the inserted columns came from the range of $\mathcal{A}$.

29.4.5 — Column Insertion/Deletion And Surjectivity

Test Your Comprehension 29.4.28 **Column insertion cannot destroy surjectivity**

Hint: Emulate TYC 14.2.2.

Inserting columns into a surjective atrix produces a surjective atrix.

Test Your Comprehension 29.4.29 **Surjective atrix = a widening of an invertible atrix**

The following statements are equivalent for an atrix $\mathcal{A}$.

1. $\mathcal{A}$ is surjective.
2. $\mathcal{A}$ can be obtained by inserting some additional columns into an invertible atrix.
3. By deleting some of the columns of $\mathcal{A}$ it is possible to arrive at an invertible atrix.

Hint: Emulate TYC. 14.2.3.

29.4.6 — Column Insertion/Deletion And Injectivity

Test Your Comprehension 29.4.30 **Column deletion cannot destroy injectivity**

Hint: Emulate Exc. 14.1.8

Deleting some (but not all) columns from an injective atrix (with more than one column) produces another injective atrix.

Exercise 29.4.31 **Inserting columns into an atrix without creating/destroying injectivity**

If $Y \in \boldsymbol{V}$ is not in the range of a matrix $\mathcal{A} : \mathbb{R}^m \longrightarrow \boldsymbol{V}$, then inserting Y into $\mathcal{A}$ as an additional column does not create or destroy injectivity.

Hint: Emulate Thm. 14.2.4.

In other words, the new atrix is injective if and only if $\mathcal{A}$ is injective.

Comment 29.4.32

One of the results about matrices (Thm. 14.2.6) states that an injective matrix is a narrowing of an invertible matrix, in the sense that it can be obtained by deleting some columns from an invertible atrix. *This result is no longer true in the land of atrices.*

The reason for this is that some linear spaces $\boldsymbol{V}$ are so big that there exist no invertible atrices with such a $\boldsymbol{V}$ as the final space. On the other hand there are always injective atrices with such a $\boldsymbol{V}$ as a final space.

Hint: Consider atrices with a single column.

Test Your Comprehension 29.4.33

Show that for every non-singleton linear space $\boldsymbol{V}$ and any $\mathbb{R}^n$, there is an injective atrix $\mathcal{F} : \mathbb{R}^n \longrightarrow \boldsymbol{V}$.

30. Linear Independence, Spans and Bases

Last modified on December 8, 2018

30.1 Linear Independence In Linear Spaces

Terminology 30.1.1

A list $X_1, X_2, X_3, \ldots, X_m$ of elements of a linear space $\boldsymbol{V}$ is said to be **linearly independent** exactly when the atrix $\begin{bmatrix} X_1 & X_2 & X_3 & \ldots & X_m \end{bmatrix}$ is injective.

When the nullspace of the atrix $\begin{bmatrix} X_1 & X_2 & X_3 & \ldots & X_m \end{bmatrix}$ is non-trivial (i.e. the atrix is not injective), we say that the list $X_1, X_2, X_3, \ldots, X_m$ is **linearly dependent**.

Since rearranging the order in which the columns appear in an atrix amounts to performing a number of column swaps, such rearrangement does not affect the jectivity (TYC 29.4.21). This shows that linear (in)dependence is neither created nor destroyed by a change in the order in which the objects are listed. We say that the concept of linear (in)dependence is **order-independent**.

In particular, we often say that $X_1, X_2, X_3, \ldots, X_m$ are **(collectively) linearly (in)dependent**, when we want to indicate that they form a linearly (in)dependent list.

Test Your Comprehension 30.1.2

A linearly independent list cannot contain null elements.

Let us restate some of the conditions equivalent to the injectivity of an atrix (see Exc. 29.4.16) in the terminology of linear independence for the reader's convenience.

Synopsis 30.1.3

The following statements about a list $X_1, X_2, X_3, \ldots, X_m$ of elements of a linear space $\boldsymbol{V}$ are equivalent.

Terminology: $X_1, X_2, X_3, \ldots, X_m$ are linearly independent.

Injectivity: $\begin{bmatrix} X_1 & X_2 & X_3 & \ldots & X_m \end{bmatrix}$ is injective; i.e. every element of $\boldsymbol{V}$ can be expressed in *at most one way** as a linear combination of $X_1, X_2, X_3, \ldots, X_m$.

Null Linear Combinations are Trivial: The only linear combination of $X_1, X_2, X_3, \ldots, X_m$ that equals $\mathbb{O}_{\boldsymbol{V}}$ is the trivial linear combination.

No Linear Combinations of Others: None of $X_1, X_2, X_3, \ldots, X_m$ is the null element $\mathbb{O}_{\boldsymbol{V}}$, and none are a linear combination of some of the others.

No Linear Combinations of Preceding Tuples: $X_1 \neq \mathbb{O}_{\boldsymbol{V}}$, and no X_i is a linear combination of those preceding it on the list.

*"at most one" includes the possibility of none at all.

Comment 30.1.4

Obviously one obtains a list of conditions equivalent to linear dependence of the list $X_1, X_2, X_3, \ldots, X_m$ by negating the statements given in Synthesis 30.1.3.

Test Your Comprehension 30.1.5

The singleton list is linearly independent exactly when its sole entry is not a null element.

Hint: TYC 29.4.30.

Test Your Comprehension 30.1.6

A sublist of a linearly independent list is also linearly independent.

Test Your Comprehension 30.1.7 ☞ **List operations that neither create nor destroy linear independence**

None of the following operations on a list of elements of a linear space $\boldsymbol{V}$ creates or destroys linear independence*.

1. Inserting an element of $\boldsymbol{V}$ that is NOT a linear combination of the elements on the original list.

2. Scaling one of the columns by a non-zero scalar.

3. Rearranging the order in which the elements appear on the list.

4. Adding to an element on the list a multiple of another element on the list.

---

*... in the sense that the resulting list is linearly independent if and only if the original one is.

Hint: Exc. 29.4.31 and TYC 29.4.21.

Test Your Comprehension 30.1.8 ☞ **Injective linear functions neither create nor destroy linear independence**

For $\mathcal{S} : \boldsymbol{W} \xrightarrow[\text{inj}]{\text{linear}} \boldsymbol{V}$, the following claims about a list $X_1, X_2, X_3, \ldots, X_m$ in $\boldsymbol{W}$ are equivalent.

1. $X_1, X_2, X_3, \ldots, X_m$ are linearly independent.

2. $\mathcal{S}\left(X_1\right), \mathcal{S}\left(X_2\right), \mathcal{S}\left(X_3\right), \ldots, \mathcal{S}\left(X_m\right)$ are linearly independent.

Hint: Emulate Exc. 18.1.10.

Example 30.1.9

Consider polynomials

$$\begin{aligned} p_0(x) &= 1; \\ p_1(x) &= x; \\ p_2(x) &= x^2; \\ p_3(x) &= x^3; \\ &\ etc. \end{aligned}$$

Let us argue that for any k, the polynomials $p_0, \quad p_1, \quad p_2, \quad \ldots p_k$ form a linearly independent subset of the linear space $\mathfrak{C}^\infty(\mathbb{R})$.

To this end we show that in order to express the neutral object in $\mathfrak{C}^\infty(\mathbb{R})$, namely the constantly zero function $\mathcal{O}$, as a linear combination of these polynomials, one MUST coefficients that are all zero.

This is easy to verify if $k = 0$, since the equality $a_0 p_0 = \mathcal{O}$ (of functions) leads to

$$0 = \mathcal{O}(1) = a_0 p_0(1) = a_0.$$

If it were possible to express $\mathcal{O}$ as a non-trivial linear combination of our polynomials for some $k > 0$, there would be a smallest such k. Let us call it k_{min}, and express it as $k_{min} = k_0 + 1$, where $k_0 \geq 0$.

The minimality of k_{min} implies that the only way of expressing $\mathcal{O}$ as a linear combination of $p_0, \; p_1, \; p_2, \; \dots p_{k_0}$ is through the use of only zero coefficients. Let us mark this statement by a ★.

Now, we are supposing that for some a_i's, not all zero, we have:

$$0 = \mathcal{O}(x) = a_0 p_0(x) + a_1 p_1(x) + a_2 p_2(x) + \dots + a_{k_0} p_{k_0}(x) + a_{k_0+1} p_{k_0+1}(x)$$

$$= a_0 + a_1 x + a_2 x^2 + a_3 x^3 + \dots + a_{k_0} x^{k_0} + a_{k_0+1} x^{k_0+1}, \tag{30.1}$$

for all $x \in \mathbb{R}$. After differentiating we arrive at the equality

$$\mathcal{O}(x) = 0 = a_1 + 2a_2 x + 3a_3 x^2 + \dots + k_0 a_{k_0} x^{k_0-1} + \left(k_0 + 1\right) a_{k_0+1} x^{k_0}$$

$$= a_1 p_0(x) + 2a_2 p_1(x) + 3a_3 p_2(x) + \dots + \left(k_0 + 1\right) a_{k_0+1} p_{k_0}(x),$$

for all $x \in \mathbb{R}$. By the statement ★, it follows that

$$\begin{aligned} a_1 &= 0 \\ 2a_2 &= 0 \\ 3a_3 &= 0 \\ &\vdots \\ \left(k_0 + 1\right) a_{k_0+1} &= 0. \end{aligned}$$

This gives

$$a_1 = a_2 = \cdots = a_{k_0+1} = 0,$$

and the original equation (30.1) reduces to the equality

$$0 = \mathcal{O} = a_0 p_0.$$

As we have seen, this equality leads to $a_0 = 0$, and thus contradicts the assumption that the a_i's in (30.1) are not all zero.

Hence no such k_{min} can exist, and thus for all k the only way to express $\mathcal{O}$ as a linear combination of $p_0, \; p_1, \; p_2, \; \dots p_k$ is to use only zero coefficients.

Comment 30.1.10

One consequence of the result of Example 30.1.9 is that, in stark contrast to the properties of $\mathbb{R}^n$, there are arbitrarily long linearly independent lists in $\mathfrak{C}^\infty(\mathbb{R})$. A linearly independent list in $\mathbb{R}^n$ has no more than n entries (TYC 18.1.7).

Theorem 30.1.11

Argue that functions

$$\sin(x), \quad \sin(2x), \quad \sin(3x), \quad \ldots, \quad \sin(17x)$$

are linearly independent elements of the linear space $\mathfrak{C}(0,1]$ of the continuous real-valued functions on the interval $(0,1]$.

Proof of Theorem 30.1.11. ■

30.2 Spans In Linear Spaces

Terminology 30.2.1

The range of an atrix $\mathcal{A} : \mathbb{R}^n \longrightarrow \boldsymbol{V}$ is the set of all elements of $\boldsymbol{V}$ that can be expressed as a linear combination of the columns of $\mathcal{A}$. We state this more concisely by saying that the range of $\mathcal{A}$ is **the (linear) span** of its columns.

In general, **the (linear) span** $\mathit{Span}\left(X_1, X_2, \ldots, X_m\right)$ of a list $X_1, X_2, \ldots, X_m$ of elements of $\boldsymbol{V}$ is the range of the atrix $\begin{bmatrix} X_1 & X_2 & \ldots & X_m \end{bmatrix}$.

So, $\mathit{Span}\left(X_1, X_2, \ldots, X_m\right)$ is the set of all elements of $\boldsymbol{V}$ that can be expressed as a linear combination of $X_1, X_2, \ldots, X_m$ in at least one way.

We commonly drop off the word “linear” and just talk about **the span**.

The order in which the elements are listed has no bearing on the span of the list (TYC 29.4.21). This can be seen directly, since the operation of addition in $\boldsymbol{V}$ is commutative and associative, and so it is irrelevant in which order the summands appear in a linear combination. In accordance with Terminology 30.1.1 we say that the concept of a span in $\boldsymbol{V}$ is **order-independent**.

When the span of a list in $\boldsymbol{V}$ is all of $\boldsymbol{V}$, we say that **the list spans $\boldsymbol{V}$**. Alternatively, since the concept of span is order-independent, we say that the elements of the list **(collectively) span $\boldsymbol{V}$**.

Example 30.2.2

Polynomials $p_0, p_1, p_2, p_3, \ldots, p_{15}$ defined in Example 30.1.9 span $\mathbb{P}_{15}$.

Theorem 30.2.3

$\mathcal{A} : \mathbb{R}^n \xrightarrow{\text{linear}} \mathbb{P}$ are never surjective.

Proof of Theorem 30.2.3. Given $\mathcal{A} : \mathbb{R}^n \xrightarrow{\text{linear}} \mathbb{P}$, $\mathit{Range}(\mathcal{A})$ is the span of the columns of $\mathcal{A}$, each of which is a polynomial. Thus $\mathit{Range}(\mathcal{A})$ is the span of polynomials. Among these polynomials, there is (at least) one of highest degree; say degree k. Thus $\mathit{Range}(\mathcal{A})$ is the span of n polynomials of degree at most k.

A linear combination of polynomials of degree at most k produces a polynomial of degree at most k. Thus all polynomials in $\mathit{Range}(\mathcal{A})$ have degree at most k. Therefore

$$\mathit{Range}(\mathcal{A}) \neq \mathbb{P} . \qquad \blacksquare$$

Hint: Exc. 29.3.3.

Test Your Comprehension 30.2.4 ☞ **Spans are subspaces**

A span of a list of elements of a linear space $\boldsymbol{V}$ is a subspace of $\boldsymbol{V}$.

Hint: Emulate TYC 18.2.5.

Test Your Comprehension 30.2.5

If $X_1, X_2, \ldots, X_{36} \in \boldsymbol{V}$ then

$$\mathit{Span}\left(X_1, X_2, \ldots, X_{27}\right) \subseteq \mathit{Span}\left(X_1, X_2, \ldots, X_{36}\right) .$$

Test Your Comprehension 30.2.6

Inserting additional elements into a list that spans $\boldsymbol{V}$ produces another list that spans $\boldsymbol{V}$.

Test Your Comprehension 30.2.7 ☞ **List operations that do not alter the span**

None of the following operations on a list of elements of a linear space $\boldsymbol{V}$ alters the span of the list.

1. Including or removing* $\mathbb{0}_{\boldsymbol{V}}$.

2. Removing an element that is a linear combination of other elements of the list.

3. Inserting an element that is a linear combination of the existing elements on the list.

4. Scaling one of the elements on the list by a non-zero scalar.

5. Adding to an element on the list a scalar multiple of another element on the list.

*as long as it is not the only element of the list

Hint: Emulate TYC 18.2.7. Consult the section on column insertion/deletion and atrix ranges, as well as the results about the effects of column operations on atrix ranges.

Test Your Comprehension 30.2.8 ☞ Reducing a list to a linearly independent list with the same span

If not all elements on a list are $\mathbb{0}_{\boldsymbol{V}}$, then by removing some of the elements from the list we can arrive at a linearly independent list that has the same span as the original list.

Hint: Emulate TYC 18.2.9.

Test Your Comprehension 30.2.9 ☞ All linear functions map lists that span their initial space to the lists that span their range

If $X_1, X_2, \ldots, X_k$ span $\boldsymbol{W}$, and $\mathcal{A} : \boldsymbol{W} \xrightarrow{\text{linear}} \boldsymbol{V}$, then $\mathcal{A}(X_1), \mathcal{A}(X_2), \ldots, \mathcal{A}(X_m)$ span the range of $\mathcal{A}$.

Hint: Emulate Exc. 18.2.11

Exercise 30.2.10 ☞ Invertible linear functions map spanning lists to spanning lists

If $\mathcal{A} : \boldsymbol{W} \xrightarrow{\text{linear}} \boldsymbol{V}$ is invertible (i.e. bijective), then the following claims about a list $X_1, X_2, \ldots, X_k$ in $\boldsymbol{W}$ are equivalent.

1. $X_1, X_2, \ldots, X_k$ span $\boldsymbol{W}$.

2. $\mathcal{A}\left(X_1\right), \mathcal{A}\left(X_2\right), \ldots, \mathcal{A}\left(X_m\right)$ span $\boldsymbol{V}$.

30.3 Coordinate Systems (a.k.a. Bases)

Terminology 30.3.1

A list $X_1, X_2, \ldots, X_m$ of elements of a linear space $\boldsymbol{V}$ is said to be **a coordinate system (a.k.a. a basis) of $\boldsymbol{V}$** if every element of $\boldsymbol{V}$ can be expressed IN EXACTLY ONE WAY* as a linear combination of $X_1, X_2, \ldots, X_m$.

In other words, for each element $V \in \boldsymbol{V}$ there is a unique m-tuple

$(\alpha_1, \alpha_2, \ldots, \alpha_m)$ such that

$$V = \alpha_1 X_1 + \alpha_2 X_2 + \cdots + \alpha_m X_m \ .$$

*... apart from the order in which $X_1, X_2, \ldots, X_m$ appear in the linear combination expression.

Test Your Comprehension 30.3.2 ☞ **"Is a basis"="spans & is linearly independent"**

A list of elements of a linear space $\boldsymbol{V}$ is a coordinate system of $\boldsymbol{V}$ exactly when the list spans $\boldsymbol{V}$ and is linearly independent.

Test Your Comprehension 30.3.3

A singleton linear space has no coordinate systems.

Test Your Comprehension 30.3.4

Reordering a coordinate system of a linear space $\boldsymbol{V}$ produces another coordinate system of $\boldsymbol{V}$.

Test Your Comprehension 30.3.5 ☞ **Coordinate systems correspond to the bijective atrices**

A list $X_1, X_2, \ldots, X_m$ of elements of a linear space $\boldsymbol{V}$ is a coordinate system of $\boldsymbol{V}$ exactly when

1. $\begin{bmatrix} X_1 & X_2 & \ldots & X_m \end{bmatrix}$ is injective;
2. $Range\begin{bmatrix} X_1 & X_2 & \ldots & X_m \end{bmatrix} = \boldsymbol{V}$.

In other words, exactly when $\begin{bmatrix} X_1 & X_2 & \ldots & X_m \end{bmatrix}$ is a bijective/invertible atrix.

Comment 30.3.6

As we have observed in Theorem 30.2.3, *not every linear space is a range of a bijective atrix*. Combining this with TYC 30.3.5, we see that NOT every linear space $\boldsymbol{V}$ has a list $X_1, X_2, \ldots, X_n$ of elements that is a coordinate system for $\boldsymbol{V}$. For example, $\mathbb{P}$ does not (no matter what $n \in \mathbb{N}$ is chosen).

Those linear spaces that do* are said to be **finite-dimensional linear spaces**, and *we shall agree to include the singleton linear spaces into this category as well.*

Linear spaces that are not finite-dimensional are said to be **infinite-dimensional**.

*i.e. the linear spaces that are ranges of bijective atrices.

Exercise 30.3.7 ☞ **A linear function is completely determined by its action on a basis**

If $X_1, X_2, \ldots, X_m$ is a coordinate system of $\boldsymbol{V}$, and $Y_1, Y_2, \ldots, Y_m$ is any list of elements of $\boldsymbol{W}$, then there exists EXACTLY ONE linear function $\mathcal{L} : \boldsymbol{V} \longrightarrow \boldsymbol{W}$ such that

$$\begin{aligned} \mathcal{L}\left(X_1\right) &= Y_1 \\ \mathcal{L}\left(X_2\right) &= Y_2 \\ &\vdots \\ \mathcal{L}\left(X_m\right) &= Y_m \ . \end{aligned}$$

Hint: Emulate Thm. 18.3.14.

Test Your Comprehension 30.3.8 ☞ **Bijective linear functions map bases to bases**

If $\mathcal{A} : \boldsymbol{W} \xrightarrow{\text{linear}} \boldsymbol{V}$ is *invertible (i.e. bijective)*, then the following claims about a list $X_1, X_2, \ldots, X_m$ in $\boldsymbol{W}$ are equivalent.

1. $X_1, X_2, \ldots, X_m$ form a coordinate system of $\boldsymbol{W}$.
2. $\mathcal{A}\left(X_1\right), \mathcal{A}\left(X_2\right), \ldots, \mathcal{A}\left(X_m\right)$ form a coordinate system of $\boldsymbol{V}$.

Hint: Emulate TYC 18.3.12.

Test Your Comprehension 30.3.9 ☞ **Operations on bases that produce bases**

The following operations performed on a coordinate system of a linear space $\boldsymbol{V}$ produce yet again a coordinate system.

1. Changing the order of the list.
2. Scaling one of the elements on the list by a non-zero scalar.
3. Adding to an element on the list a scalar multiple of another element on the list.

Hint: Emulate TYC 18.3.6.

30.4 Linear Bijections And Isomorphic Spaces

Terminology 30.4.1

Linear space $\boldsymbol{V}$ is said to be **isomorphic*** to a linear space $\boldsymbol{W}$ if there exists a linear bijection $\mathcal{F} : \boldsymbol{V} \longrightarrow \boldsymbol{W}$. In that case we write

$$\boldsymbol{V} \simeq \boldsymbol{W} .$$

It is also common to refer to linear bijections as **(linear) isomorphisms**, with the term "linear" commonly left implicit. This way, $\boldsymbol{V}$ is isomorphic to $\boldsymbol{W}$ if there is an isomorphism from $\boldsymbol{V}$ to $\boldsymbol{W}$.

*In Ancient Greek, "isos" meant "equal", and "morphe" meant "form".

Test Your Comprehension 30.4.2

A non-zero scalar multiple of an isomorphism is another isomorphism, as is the inverse of an isomorphism.

Test Your Comprehension 30.4.3 ☞ **A composition of isomorphisms is an isomorphism**

If $\mathcal{F} : \boldsymbol{V} \longrightarrow \boldsymbol{W}$ and $\mathcal{G} : \boldsymbol{W} \longrightarrow \boldsymbol{Z}$ are isomorphisms, then so is $\mathcal{G} \circ \mathcal{F}$.

There is a technical reason why we do not just say that $\approx$ is an equivalence relation. The issue is that the collection of objects to which $\approx$ pertains, namely the collection of all linear spaces, is too broad (in a certain sense), and consequently exhibits an anomalous behavior. An interested reader should consult a text on the Theory of Sets.
Were we to focus only on subsets of a given linear space, $\approx$ is a bona fide equivalence relation on such a collection.

Exercise 30.4.4 ☞ **$\approx$ behaves like an equivalence relation**

Reflexivity: Every linear space is isomorphic to itself.

Symmetry: If $\boldsymbol{V}$ is isomorphic to $\boldsymbol{W}$, then $\boldsymbol{W}$ is isomorphic to $\boldsymbol{V}$.

Transitivity: If $\boldsymbol{V}$ is isomorphic to $\boldsymbol{W}$, and $\boldsymbol{W}$ is isomorphic to $\boldsymbol{Z}$, then $\boldsymbol{V}$ is isomorphic to $\boldsymbol{Z}$.

Below we collect some of the results which show that isomorphic linear spaces can be thought of as "parallel universes" or "re-labeled copies", in so far as the properties of one translate into analogous properties of the other (via an isomorphism between them).

For a visual analogy, the reader should imagine two parallel but distinct planes in our physical 3−space. The two are different objects, and a point in one never lies in the other. Yet there are obvious ways to identify one plane and its properties with the other. INSERT PICTURE

It is a crucially important point that, apart from a trivial case, there are always infinitely many different isomorphisms between two isomorphic linear spaces (TYC 30.4.2, and *****). In particular there are infinitely many different ways to translate the properties of one space into the properties of the other.

Synopsis 30.4.5 ☞ **Isomorphisms and isomorphic spaces**

Suppose that $\mathcal{F} : \boldsymbol{V} \longrightarrow \boldsymbol{W}$ is an isomorphism. Then each of the following holds.

Isomorphisms preserve linear independence: $V_1, V_2, \ldots, V_n$ is a linearly independent list in $\boldsymbol{V}$ if and only if $\mathcal{F}\left(V_1\right), \mathcal{F}\left(V_2\right), \ldots, \mathcal{F}\left(V_n\right)$ is a linearly independent list in $\boldsymbol{W}$.

Isomorphisms preserve spanning lists: $V_1, V_2, \ldots, V_n$ span $\boldsymbol{V}$ if and only if $\mathcal{F}\left(V_1\right), \mathcal{F}\left(V_2\right), \ldots, \mathcal{F}\left(V_n\right)$ span $\boldsymbol{W}$.

Isomorphisms preserve bases: $V_1, V_2, \ldots, V_n$ is a coordinate system of $\boldsymbol{V}$ if and only if $\mathcal{F}\left(V_1\right), \mathcal{F}\left(V_2\right), \ldots, \mathcal{F}\left(V_n\right)$ is a coordinate system of $\boldsymbol{W}$.

See TYC's 30.1.8, 30.3.8 and Exc. 30.2.10.

Exercise 30.4.6 ☞ **Isomorphic spaces have the same dimensionality**

Suppose that $\boldsymbol{V}$ and $\boldsymbol{W}$ are isomorphic linear spaces. Then either $\boldsymbol{V}$ and $\boldsymbol{W}$ are both finite-dimensional, or they are both infinite-dimensional.

Hint: Argue that if one of $\boldsymbol{V}$, $\boldsymbol{W}$ is finite-dimensional, then so is the other. TYC 30.3.8 can be helpful here.

Example 30.4.7 ☞ **Coordinate systems of $\mathbb{P}_3$**

As we know (see Ex. 30.1.9), the list $1, \quad x, \quad x^2, \quad x^3$ is a coordinate system of $\mathbb{P}_3$. In other words,

$$\mathcal{A} := \begin{bmatrix} 1 & x & x^2 & x^3 \end{bmatrix},$$

is an isomorphism from $\mathbb{R}^4$ to $\mathbb{P}_3$.

Do the polynomials

$$1 - 3x + 4x^2, \quad 3 - 2x + 7x^2 - 5x^3, \quad 7 + x^2 - 3x^3, \quad 6 + 3x - 8x^2 - 9x^3$$

form a coordinate system of $\mathbb{P}_3$ as well?

Let us call these polynomials P_1, P_2, P_3, P_4, for short, and note that it is easy to express each one of these as a linear combination of the polynomials $1, \quad x, \quad x^2, \quad x^3$. For example,

$$P_2(x) = 3 \cdot \left(1\right) + (-2) \cdot \left(x\right) + 7 \cdot \left(x^2\right) + (-5) \cdot \left(x^3\right).$$

This can be restated as

$$P_2 = \mathcal{A}\begin{pmatrix} 3 \\ -2 \\ 7 \\ -5 \end{pmatrix}.$$

In a similar fashion we observe that

$$P_1 = \mathcal{A}\begin{pmatrix} 1 \\ 3 \\ 4 \\ 0 \end{pmatrix}, P_3 = \mathcal{A}\begin{pmatrix} 7 \\ 0 \\ 1 \\ -3 \end{pmatrix}, \quad \text{and} \quad P_4 = \mathcal{A}\begin{pmatrix} 6 \\ 3 \\ -8 \\ -9 \end{pmatrix}.$$

Since isomorphisms preserve coordinate systems (TYC 30.3.8), we see that P_1, P_2, P_3, P_4 is a coordinate system of $\mathbb{P}_3$, exactly when

$$\begin{pmatrix}1\\3\\4\\0\end{pmatrix}, \begin{pmatrix}3\\-2\\7\\-5\end{pmatrix}, \begin{pmatrix}7\\0\\1\\-3\end{pmatrix}, \begin{pmatrix}6\\3\\-8\\-9\end{pmatrix}$$

form a coordinate system of $\mathbb{R}^4$. To test the latter we simply have to test whether the matrix

$$\begin{bmatrix}1 & 3 & 7 & 6\\ 3 & -2 & 0 & 3\\ 4 & 7 & 1 & -8\\ 0 & -5 & -3 & -9\end{bmatrix}$$

is invertible, which has surely become an easy task for the reader by now.

Exercise 30.4.8 ☞ **Testing for linear independence, spanning, and being a basis of $\mathbb{P}_k$**

Develop a concrete algorithm one could use to discern whether a given list of 17 polynomials

1. is linearly independent;
2. spans $\mathbb{P}_{12}$;
3. is a coordinate system of $\mathbb{P}_{16}$.

Hint: The ideas of Example 30.4.7 can be helpful here.

30.5 Additional Exercises

Exercise 30.5.1 ☞ **Linear functions cannot create linear independence**

If $\mathcal{F} : \boldsymbol{W} \xrightarrow{\text{linear}} \boldsymbol{V}$ and a list $X_1, X_2, X_3, \ldots, X_{14}$ of elements of $\boldsymbol{W}$ is such that

$$\mathcal{A}(X_1), \mathcal{A}(X_2), \mathcal{A}(X_3), \ldots, \mathcal{A}(X_{14}) \text{ are linearly independent,}$$

then

$$X_1, X_2, X_3, \ldots, X_{14} \text{ are linearly independent.}$$

Hint: Compare to Exc. 12.2.6.

Exercise 30.5.2 ☞ **Injective linear functions map bases of their initial space to bases of their range**

If $\mathcal{A} : \boldsymbol{V} \xrightarrow{\text{linear}} \boldsymbol{W}$ is *injective*, and $X_1, X_2, \ldots, X_m$ is a coordinate system of $\boldsymbol{V}$, then

$$\mathcal{A}(X_1), \mathcal{A}(X_2), \ldots, \mathcal{A}(X_n) \text{ is a coordinate system of the range of } \mathcal{A}.$$

Hint: Emulate Exc. 18.3.11.

31. Finite-Dimensional Linear Spaces

Last modified on December 8, 2018

31.1 Dimension

The following exercise shows that the finite-dimensional linear spaces are exactly those that are "parallel universes" of various $\mathbb{R}^n$, and they enjoy many analogous properties. The proof of Theorem 31.1.4 offers the first glimpse of this paradigm.

Later we shall show that linear functions between such spaces can be represented by (and hence studied via the theory of) matrices (in many different ways).

Exercise 31.1.1 ☞ $\mathbb{R}^m \simeq \mathbb{R}^n \iff m = n$

If $m \neq n$, then $\mathbb{R}^m$ is NOT isomorphic to $\mathbb{R}^n$.

Hint: What type of a function would an isomorphism from $\mathbb{R}^m$ to $\mathbb{R}^n$ be?

Test Your Comprehension 31.1.2 ☞ **Atrices and isomorphisms to/from $\mathbb{R}^n$**

Isomorphisms $\mathcal{F} : \mathbb{R}^n \longrightarrow \boldsymbol{V}$ are bijective atrices, and isomorphisms $\mathcal{G} : \boldsymbol{W} \longrightarrow \mathbb{R}^m$ are inverses of bijective atrices.

Exercise 31.1.3 ☞ **Bases and isomorphisms to/from $\mathbb{R}^n$**

The following claims are equivalent for a non-singleton linear space $\boldsymbol{V}$.

1. $\boldsymbol{V}$ has a coordinate system with n elements.
2. $\boldsymbol{V}$ is isomorphic to $\mathbb{R}^n$.
3. $\boldsymbol{V}$ is isomorphic to a linear space that has a coordinate system with n elements.

Hint: TYC's 30.3.5 and 31.1.2, Excs. 29.4.9 and 30.4.4, and Syn. 30.4.5.

Theorem 31.1.4 ☞ **Coordinate systems come in one size**

If one coordinate system of a linear space $\boldsymbol{V}$ has n elements, then every coordinate system of $\boldsymbol{V}$ has n elements.*

*A coordinate system, being a linearly independent list, has no duplicate elements.

Proof of Theorem 31.1.4. Suppose that $X_1, X_2, \ldots, X_n$ and $Y_1, Y_2, \ldots, Y_m$ are coordinate systems of $\boldsymbol{V}$. By Exc. 31.1.3, $\boldsymbol{V}$ is isomorphic to $\mathbb{R}^n$, and to $\mathbb{R}^m$. By transitivity of $\simeq$, $\mathbb{R}^m$ is isomorphic to $\mathbb{R}^n$, and therefore $m = n$, by Exc. 31.1.1. ■

Terminology 31.1.5

The common size of all coordinate systems of a non-singleton finite-dimensional linear space $\boldsymbol{V}$ is said to be the **dimension** of $\boldsymbol{V}$, and is denoted by

$$\dim \boldsymbol{V} \ .$$

The singleton linear spaces have **dimension zero**, as a convention.

Test Your Comprehension 31.1.6

Hint: Exc. 31.1.3.

A linear space is isomorphic to an
n-dimensional linear space exactly when it is itself n-dimensional.

Test Your Comprehension 31.1.7

The following are equivalent for a non-singleton linear space $\boldsymbol{V}$.

1. $\dim \boldsymbol{V} = n$.

2. $\boldsymbol{V} \simeq \mathbb{R}^n$.

Test Your Comprehension 31.1.8 ☞ **For finite-dimensional spaces: “isomorphic” = “equidimensional”**

The following claims are equivalent for finite-dimensional spaces $\boldsymbol{V}$ and $\boldsymbol{W}$.

1. $\boldsymbol{V} \simeq \boldsymbol{W}$.

2. $\dim \boldsymbol{V} = \dim \boldsymbol{W}$.

Exercise 31.1.9

Suppose that for any $a, b \in \mathbb{R}$, the nullspace of $\mathcal{T} : \mathfrak{D}(-1,1) \xrightarrow{\text{linear}} R^{(-1,1)}$ contains a unique function f satisfying the conditions

- $f(0) = a$,
- $f'(0) = b$.

Argue that $\dim\left(\mathit{Nullspace}\,(\mathcal{T})\right) = 2$.

$R^{(-1,1)}$ is the linear space of all real-valued functions on the interval $(-1,1)$. $\mathfrak{D}(-1,1)$ is a subspace of $R^{(-1,1)}$ that consists of the differentiable functions.

Hint: Consider a new function $\mathcal{G} : \mathit{Nullspace}\,(\mathcal{T}) \longrightarrow \mathbb{R}^2$ defined by $\mathcal{G}(f) := \begin{pmatrix} f(0) \\ f'(0) \end{pmatrix}$. Show that $\mathcal{G}$ is a linear bijection. Then make use of TYC 31.1.6.

Theorem 31.1.10 ☞ **"Linearly independent"="part of a basis"; "spaning"="contains a basis"**

Suppose that $\boldsymbol{V}$ is a *non-singleton finite-dimensional* linear space. Then

1. the linearly independent lists in $\boldsymbol{V}$ are exactly those that are contained in coordinate systems (as sublists);
2. the lists that span $\boldsymbol{V}$ are exactly those that contain coordinate systems (as sublists).

Proof of Theorem 31.1.10.

1. We already know (TYC 30.1.6) that a sublist of a linearly independent list is linearly independent. All that we need to show is that every linearly independent list is contained in a coordinate system.

   Synopsis of the proof: Our strategy is to use an isomorphism from $\boldsymbol{V}$ to $\mathbb{R}^n$ to map our linearly independent list in $\boldsymbol{V}$ to a linearly independent list in $\mathbb{R}^n$, which, as we already know, can be enlarged to a coordinate system there.
   When we map this coordinate system back to $\boldsymbol{V}$ via the inverse of our isomorphism, we obtained a coordinate system of $\boldsymbol{V}$ that contains our original list.

   Suppose that $X_1, X_2, \ldots, X_k$ is a linearly independent list in an n-dimensional linear space $\boldsymbol{V}$. BY TYC 31.1.7, there is an isomorphism $\mathcal{F} : \boldsymbol{V} \longrightarrow \mathbb{R}^n$. Then

   $$\mathcal{F}\left(X_1\right), \mathcal{F}\left(X_2\right), \ldots, \mathcal{F}\left(X_k\right)$$

   is a linearly independent list in $\mathbb{R}^n$ (TYC 30.1.8 and Syn. 30.4.5).
   In particular, $k \le n$ and this list can be extended to a coordinate system

   $$\mathcal{F}\left(X_1\right), \mathcal{F}\left(X_2\right), \ldots, \mathcal{F}\left(X_k\right), Y_{k+1}, \ldots, Y_n$$

of $\mathbb{R}^n$, with the understanding that no Y's are added if $k = n$. Since $\mathcal{F}^{-1} : \mathbb{R}^n \longrightarrow \boldsymbol{V}$ is also an isomorphism (TYC 30.4.2), by TYC 30.3.8

$$\mathcal{F}^{-1}\left(\mathcal{F}\left(X_1\right)\right), \mathcal{F}^{-1}\left(\mathcal{F}\left(X_2\right)\right), \ldots, \mathcal{F}^{-1}\left(\mathcal{F}\left(X_k\right)\right), \mathcal{F}^{-1}\left(Y_{k+1}\right), \ldots, \mathcal{F}^{-1}\left(Y_n\right)$$

is a coordinate system of $\boldsymbol{V}$. This list can be rewritten as

$$X_1, X_2, \ldots, X_k, \mathcal{F}^{-1}\left(Y_{k+1}\right), \ldots, \mathcal{F}^{-1}\left(Y_n\right) ,$$

and so is a desired coordinate system of $\boldsymbol{V}$ that contains our original list as a sublist.

2. If $Z_1, Z_2, \ldots, Z_m$ spans $\boldsymbol{V}$, then this list must contain a non-null element of $\boldsymbol{V}$, since $\boldsymbol{V} \neq \{\mathbb{0}_{\boldsymbol{V}}\}$. Therefore, by TYC 30.2.8, we can remove some elements from our list to arrive at a sublist that is linearly independent and still spans $\boldsymbol{V}$. This sublist is a coordinate system of $\boldsymbol{V}$ (TYC 30.3.2). ■

Test Your Comprehension 31.1.11 ☞ **Sizes of linearly independent and spanning sets**

Suppose that $\boldsymbol{V}$ is an n-dimensional linear space. Then it has the following properties.

1. A linearly independent list in $\boldsymbol{V}$ cannot contain more than n elements.

2. A linearly independent list in $\boldsymbol{V}$ is a coordinate system exactly when it has n elements.

3. A list that spans $\boldsymbol{V}$ must contain at least n distinct elements.

4. A list that spans $\boldsymbol{V}$ is a coordinate system of $\boldsymbol{V}$ exactly when it has n elements.

Theorem 31.1.12 ☞ **Infinite-dimensionality conditions**

The following statements are equivalent for a non-singleton linear space $\boldsymbol{V}$.

1. $\boldsymbol{V}$ is *infinite*-dimensional.

2. Every linearly independent list in $\boldsymbol{V}$ can be enlarged to a strictly longer linearly independent set in $\boldsymbol{V}$.

3. Every linearly independent list in $\boldsymbol{V}$ can be enlarged to an arbitrarily long (finite) linearly independent set in $\boldsymbol{V}$.

4. There are arbitrarily long (finite) linearly independent lists in $\boldsymbol{V}$.

5. There are linearly independent lists in $\boldsymbol{V}$ of any (finite) length.

6. No list of finitely many elements of $\boldsymbol{V}$ spans $\boldsymbol{V}$.

Proof of Theorem 31.1.12.

$[\mathbf{1.} \Longrightarrow \mathbf{2.}]$ **:** Suppose that $\boldsymbol{V}$ is NOT finite-dimensional (and in particular $\boldsymbol{V}$ is not a singleton space). Can it be that under this hypothesis there exists a linearly independent list

$$X_1, X_2, \ldots, X_n$$

in $\boldsymbol{V}$ that cannot be extended to a strictly longer linearly independent list?

If that were the case and the span of this list were not all of $\boldsymbol{V}$, then some $Y \in \boldsymbol{V}$ would not be a linear combination of the elements on the list. Consequently

$$X_1, X_2, \ldots, X_n, Y$$

would be a strictly longer linearly independent list (TYC 30.1.7) in $\boldsymbol{V}$, contradicting the presumed non-extendability of the original list.

Thus it would have to be true that $X_1, X_2, \ldots, X_n$ spans $\boldsymbol{V}$, and hence is a coordinate system of $\boldsymbol{V}$ (TYC 30.3.2). This would contradict the hypothesis that $\boldsymbol{V}$ is not finite-dimensional.

Therefore it must be that there do not exists non-extendible linearly independent lists in $\boldsymbol{V}$.

$[\mathbf{2.} \Longrightarrow \mathbf{3.} \Longrightarrow \mathbf{4.} \Longrightarrow \mathbf{5.}]$ **:** TYC 31.1.13 below.

$[\mathbf{5.} \Longrightarrow \mathbf{1.}]$ **:** Suppose that there are linearly independent lists in $\boldsymbol{V}$ of any (finite) length. In particular $\boldsymbol{V}$ is not a singleton space. Can it be that $\boldsymbol{V}$ is finite dimensional? No, because were it so, no linearly independent list in $\boldsymbol{V}$ would have more elements than the dimension of $\boldsymbol{V}$ (TYC 31.1.11).

$[\mathbf{1.} \Longrightarrow \mathbf{6.}]$ **:** Suppose that $\boldsymbol{V}$ is NOT finite-dimensional. Then $\boldsymbol{V} \neq \{\mathbb{0}_{\boldsymbol{V}}\}$.

The proof of part 2. of Theorem 31.1.10 shows that if a finite list of elements of $\boldsymbol{V}$ spanned $\boldsymbol{V}$ then $\boldsymbol{V}$ would be finite-dimensional. Thus no finite list of elements of $\boldsymbol{V}$ spans $\boldsymbol{V}$.

$[\mathbf{6.} \Longrightarrow \mathbf{1.}]$ **:** TYC 31.1.13 below. ■

Test Your Comprehension 31.1.13

1. Verify the validity of the implications 2. $\Longrightarrow$ 3. $\Longrightarrow$ 4. $\Longrightarrow$ 5. of Theorem 31.1.12.

Hint: Sublists of linearly independent lists are linearly independent (TYC 30.1.6).

2. Mimic the proof of the implication 5. $\Longrightarrow$ 1. to show that the implication 6. $\Longrightarrow$ 1. holds in Theorem 31.1.12.

Exercise 31.1.14 ☞ **(Strictly) Bigger spaces have (strictly) bigger dimensions**

Hint: Emulate Thm. 18.3.26

If $\boldsymbol{W}$ is a subspace of a finite-dimensional linear space $\boldsymbol{V}$, then $\boldsymbol{W}$ is finite-dimensional, and

$$dim(\boldsymbol{W}) \leq dim(\boldsymbol{V}),$$

where the equality of dimensions holds exactly when $\boldsymbol{W} = \boldsymbol{V}$.

Test Your Comprehension 31.1.15

Hint: Subspaces are linear spaces.

If $\boldsymbol{W}$ and $\boldsymbol{V}$ are subspaces of a linear space $\boldsymbol{Z}$, and $\boldsymbol{W} \subseteq \boldsymbol{V}$, then $dim(\boldsymbol{W}) \leq dim(\boldsymbol{V})$, and the equality of dimensions holds exactly when $\boldsymbol{W} = \boldsymbol{V}$.

Exercise 31.1.16 ☞ **A basis of the range via enlarging a basis of the nullspace (to that of the initial space)**

Suppose that

1. $\boldsymbol{V}$ is a finite-dimensional linear space,
2. $\mathcal{F} : \boldsymbol{V} \longrightarrow \boldsymbol{W}$ is a *non-injective non-null* linear function, and
3. $X_1, X_2, \ldots, X_k$ is a coordinate system of the nullspace of $\mathcal{F}$.

Then for ANY enlargement of $X_1, X_2, \ldots, X_k$ to a coordinate system

$$X_1, X_2, \ldots, X_k, Y_{k+1}, Y_{k+2}, \ldots, Y_m \text{ of } \boldsymbol{V},$$

$\mathcal{F}\left(Y_{k+1}\right), \mathcal{F}\left(Y_{k+2}\right), \ldots, \mathcal{F}\left(Y_m\right)$ is a coordinate system of the range of $\mathcal{F}$.

Test Your Comprehension 31.1.17 ☞ **Rank-Nullity Theorem**

Suppose that $\boldsymbol{V}$ is a finite-dimensional linear space, and that $\mathcal{F} : \boldsymbol{V} \xrightarrow{\text{linear}} \boldsymbol{W}$. Then $Range(\mathcal{F})$ is a finite-dimensional, and

$$\dim(Range(\mathcal{F})) + \dim(Nullspace(\mathcal{F})) = \dim \boldsymbol{V}.$$

Terminology 31.1.18

When the nullspace of a linear function $\mathcal{F}$ is finite-dimensional, its dimension is said to be **the nullity** of $\mathcal{F}$, and we say that $\mathcal{F}$ has **finite nullity**. When the nullspace is not finite-dimensional, we say that $\mathcal{F}$ has **infinite nullity**.

Similarly, when the range of a linear function $\mathcal{F}$ is finite-dimensional, its dimension is said to be **the rank** of $\mathcal{F}$, and we say that $\mathcal{F}$ has **finite rank**. When the range is not finite-dimensional, we say that $\mathcal{F}$ has **infinite rank**.

In this terminology Rank-Nullity Theorem (TYC 31.1.17) can be restated as follows.

Rank-Nullity Theorem (restated)

A linear function whose initial space is finite-dimensional has finite rank and finite nullity, and the sum of the rank and the nullity equals the dimension of the initial space.

In fact we can strengthen Rank-Nullity Theorem by proving that for linear functions finiteness of rank and of nullity entails the finite-dimensionality of the initial space. This is achieved by establishing a variant of Exercise 31.1.16.

Exercise 31.1.19

1. Suppose that $\mathcal{F} : \boldsymbol{V} \longrightarrow \boldsymbol{W}$ is a *non-injective non-null* linear function, and $X_1, X_2, \ldots, X_k$ is a coordinate system of the nullspace of $\mathcal{F}$.

   Then for ANY enlargement of $X_1, X_2, \ldots, X_k$ to a linearly independent list $X_1, X_2, \ldots, X_k, Y_{k+1}, Y_{k+2}, \ldots, Y_{k+m}$ in $\boldsymbol{V}$,

   $$\mathcal{F}\left(Y_{k+1}\right), \mathcal{F}\left(Y_{k+2}\right), \ldots, \mathcal{F}\left(Y_{k+m}\right)$$

   is a linearly independent list in the range of $\mathcal{F}$.

2. State and prove the corresponding statement for the case of an injective $\mathcal{F}$.

Hint:
1. Emulate the second part of the proof of Thm. 19.1.4.
2. TYC 30.1.8 can be useful here.

Theorem 31.1.20 A stronger Rank-Nullity Theorem

The following claims are equivalent for a linear function $\mathcal{F} : \boldsymbol{V} \xrightarrow{\text{linear}} \boldsymbol{W}$.

1. $\mathcal{F}$ has finite rank and finite nullity.
2. $\boldsymbol{V}$ is finite-dimensional.

When these conditions hold,

$$\mathit{Rank}\,(\mathcal{F}) + \mathit{Nullity}\,(\mathcal{F}) = \dim \boldsymbol{V}\ .$$

Proof of Theorem 31.1.20. In view of TYC 31.1.17 we only need to verify the implication 1. $\Longrightarrow$ 2. Suppose that $\mathcal{F}$ has finite rank (r) and finite nullity (n).

Case 1: $\mathcal{F}$ is not injective (i.e. $n > 0$).

Let $X_1, X_2, \ldots, X_n$ be a coordinate system of the nullspace of $\mathcal{F}$.

If $\boldsymbol{V}$ were infinite-dimensional, then (Thm. 31.1.12) we would be able to enlarge $X_1, X_2, \ldots, X_n$ to a linearly independent set

$$X_1, X_2, \ldots, X_n, Y_{n+1}, \ldots, Y_{n+m} \ ,$$

with as large of an m as we wish. But then

$$\mathcal{F}\left(Y_{n+1}\right), \ldots, \mathcal{F}\left(Y_{n+m}\right)$$

is a linearly independent list of m elements in the range of $\mathcal{F}$ (TYC 31.1.19), with m being as large as we wish. Yet this implies that the range of $\mathcal{F}$ is not finite-dimensional (Thm. 31.1.12), contradicting our hypothesis. Thus $\boldsymbol{V}$ must be finite-dimensional.

Case 2: $\mathcal{F}$ is injective (i.e. $n = 0$).

We leave this case as an Excercise 31.1.21 for the reader. ■

Exercise 31.1.21

Establish Case 2. in the proof of the implication 1. $\Longrightarrow$ 2. in Theorem 31.1.20.

Exercise 31.1.22

Why sould one not expect to be able to make conclusions about dimensionality of the final space of $\mathcal{F}$ under the set-up of Theorem 31.1.20?

31.2 Coordinatization

Terminology 31.2.1

If the list $V_1, V_2, \ldots, V_n$ is a coordinate system of a linear space $\boldsymbol{V}$, then each element Z of $\boldsymbol{V}$ can be expressed as a linear combination of $V_1, V_2, \ldots, V_n$ in exactly one way.

The unique n-tuple $(\alpha_1, \alpha_2, \ldots, \alpha_n)$ such that

$$Z = \alpha_1 V_1 + \alpha_2 V_2 + \cdots + \alpha_n V_n$$

is said to be the **coordinate tuple of $\mathcal{Z}$ with respect to this coordinate system**.

This coordinate tuple can be considered to be the uniquely identifying address of $\mathcal{Z}$ in $\boldsymbol{V}$, just as pair of numbers can be used to identify a vector.

INSERT PICTURE AND DESCRIPTION OF A GEOMETRIC ANALOGUE

Comment 31.2.2

It should be noted that constructing a Z that has given coordinates $(\alpha_1, \alpha_2, \ldots, \alpha_n)$ with respect to a given coordinate system $V_1, V_2, \ldots, V_n$ is very easy: this Z equals the linear combination of $V_1, V_2, \ldots, V_n$ with coordinates $(\alpha_1, \alpha_2, \ldots, \alpha_n)$ serving as coefficients:

$$Z = \alpha_1 V_1 + \alpha_2 V_2 + \cdots + \alpha_n V_n = \begin{bmatrix} V_1 & V_2 & \cdots & V_m \end{bmatrix} \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_m \end{pmatrix}.$$

The reverse task is much harder, as it amounts to "resolving Z with respect to the coordinate system $V_1, V_2, \ldots, V_n$", i.e. finding which multiples of $V_1, V_2, \ldots, V_n$ will add up to Z.

INSERT PICTURE AND DESCRIPTION OF A GEOMETRIC ANALOGUE

Terminology 31.2.3

As we know (TYC 30.3.5), coordinate systems of a finite-dimensional linear space $\boldsymbol{V}$ correspond to bijective atrices $\mathcal{A}$ mapping into $\boldsymbol{V}$.

We shall say that an atrix $\mathcal{A} : \mathbb{R}^n \xrightarrow{\text{linear}} \boldsymbol{V}$ **implements a coordinate system** of a linear space $\boldsymbol{V}$, whenever $\mathcal{A}$ is an isomorphism.

Test Your Comprehension 31.2.4 ☞ **Inverse of a bijective atrix outputs the coordinates**

Suppose that $\mathcal{A} := \begin{bmatrix} V_1 & V_2 & \cdots & V_m \end{bmatrix}$ implements a coordinate system of $\boldsymbol{V}$. Then

$$Z = \alpha_1 V_1 + \alpha_2 V_2 + \cdots + \alpha_m V_m \iff \mathcal{A}^{-1}(Z) = \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_m \end{pmatrix}$$

Example 31.2.5

In Example 30.4.7, we presented a method of constructing all possible coordinate systems for $\mathbb{P}_2$.