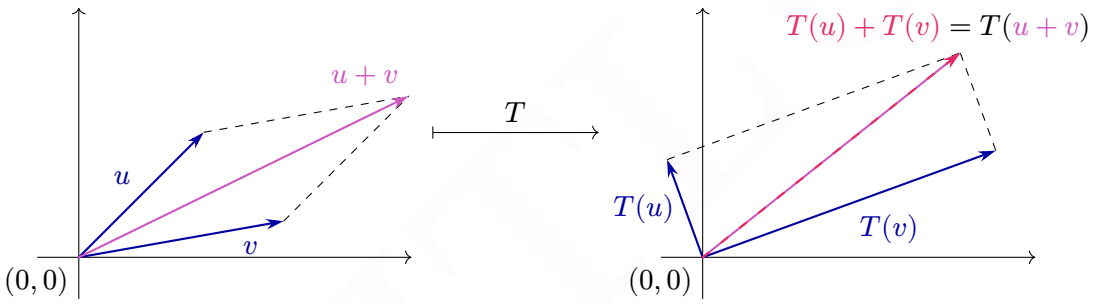
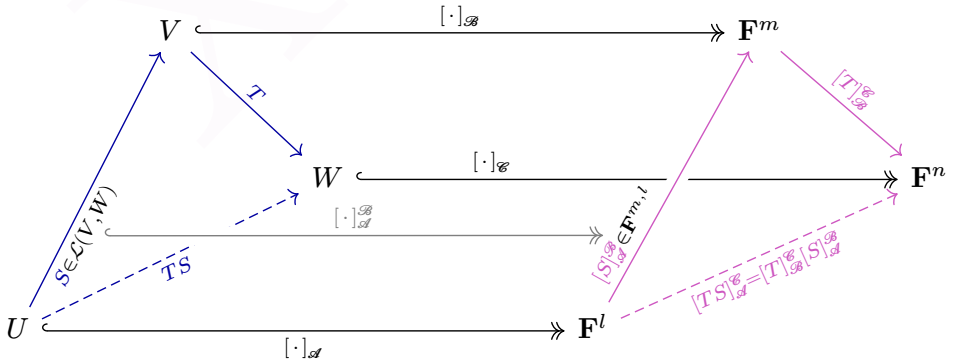
Advanced Linear Algebra

Lecture notes for MTH107 2025–2026

Paul-Henry Leemann





March 3, 2026

Foreword

These notes are a work in progress. They are still plenty of typos (and hopefully few mistakes). If you see some, please let me know by email or directly via learning mall and I will correct them.

Things might be presented in a slightly different way than what was done in class, or in a different order.

To go further

In these notes, you will see a few black boxes like this one. These are meant for the interested reader that wants to know more and can be skipped without harm. They are not necessarily be meant to be read in a first reading, but are here to provide more details if you come back to read these notes in the future.
The content that is written inside these "To go further" boxes will **NOT** be in the exam.

Theorem 0.1.

Blue boxes are for theorems.

Definition 0.2.

Green boxes are for definitions.

Standing assumption

Yellow boxes are for standing assumptions for chapters.

Remark 0.3.

Red boxes are for remarks.
Some passages are designed to forewarn the readers against serious errors, where they risk falling; these passages are indicated in the margin with the "dangerous bend" sign.

I am indebted to Hang Chen for his careful proofreading of this manuscript. Pietro Sgobba, Luca Demangos, Yanlin He, Yifan Chen, Gaoming Zhang, Yu Lu, Ziheng Yu, Jiahe Hai, Lyutong Lu, Qinfan Song and Haopeng Yang also contributed to significantly reduce the number of typos. These notes would not have been the same without their comments. The above list is likely not exhaustive and I apologise to those I have omitted.

Contents

Symbols

$\mathbf{N}$	natural integers including 0: $\mathbf{N} = \{0, 1, 2, \dots\}$
$\mathbf{Z}$	relative integers: $\mathbf{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$
$\mathbf{Q}$	rational numbers: $\mathbf{Q} = \left\{ \frac{p}{q} \;\middle|\; p, q \in \mathbf{Z}, q \neq 0 \right\}$
$\mathbf{R}$	real numbers
$\mathbf{C}$	complex numbers: $\mathbf{C} = \{a + b\mathrm{i} \mid a, b \in \mathbf{R}, \mathrm{i}^2 = -1\}$
$\mathbf{F}$	field (for example: $\mathbf{Q}$, $\mathbf{R}$ or $\mathbf{C}$)

Table 1: Important sets.

α, A	alpha	ν, N	nu
β, B	beta	ξ, Ξ	xi
γ, Γ	gamma	o, O	omicron
δ, Δ	delta	π, Π	pi
ε, E	epsilon	ρ, P	rho
ζ, Z	zeta	σ, Σ	sigma
η, H	eta	τ, T	tau
θ, Θ	theta	υ, Υ	upsilon
ι, I	iota	φ, Φ	phi
κ, K	kappa	χ, X	chi
λ, Λ	lambda	ψ, Ψ	psi
μ, M	mu	ω, Ω	omega

Table 2: Greek letters. Except for Σ and Π (to denote respectively sums and products), we will not use the capital greek letters, only their lower case versions.

1 Reminders about sets and functions

In this chapter we will see a few reminders about sets and functions (also called maps). These notions should be familiar to you, at least naively, but maybe not in a formal way.

1.1 Sets

Set theory is one of the cornerstones of modern mathematics, and algebraic objects are often defined as sets with some extra-structure on them. Modern set theory is an axiomatic theory that might seem impressive at first sight, and which is indeed complex. Hopefully for us, we will not need the full strength of set theory and a *naive* set theory will be enough for our project to understand vector spaces.

Let us fix a few notations as well as some important concepts. Heuristically, a *set* is a collection of object. We write $x \in X$ to say that x is an **element** of the **set** X, or that x **is in (belongs to)** X. By definition, two sets X and Y are equal if and only if they have the same elements. In formula:

$$(X = Y) \iff [\forall x : x \in X \iff x \in Y].$$

We use the notation $\{x\}$ to describe the set consisting of exactly the element x, and more generally $\{x_1, \dots, x_n\}$ for the set containing the elements x_1 to x_n.

One important point to remember, is that sets are unordered collections and cannot contain multiple copies of the same elements. So $\{1, 2\} = \{2, 1\}$ and if we add 1 to the set $\{1, 2\}$, we still have $\{1, 2\}$.

Sets can contain any mathematical object, not only numbers. For example, $\{f : x \mapsto 2x, \pi, 1, y, \mathbf{N}\}$ (where f is a function from $\mathbf{R}$ to $\mathbf{R}$) is a perfectly well-defined set. Sets can even contains other sets! For example, $\{1, \{a, b, c\}\}$ has two elements: 1 and the set $\{a, b, c\}$ (which itself has 3 elements).

There exists a specific set with no-elements: the **empty set**

$$\varnothing := \{\ \}.$$

Remark 1.1.1.

The notation $x := y$ means that we are defining the left-hand side has being equal to the right hand side. In particular, the symbol $:=$ can only be used if the left-hand side of it was not already defined.

Definition 1.1.2.

If a set X is finite, we define its **cardinality** $\#X = |X|$ to be its number of elements.

The empty set is the only set with 0 elements.

If we are given two sets, we can compare them. We say that X is a **subset** of Y if every element of Y also belongs to Y:

$$(X \subseteq Y) \iff (\forall x : x \in X \implies x \in Y).$$

One easily shows that for any sets X, Y and Z one have

1. $X \subseteq X$; (reflexivity)
2. $X = Y$ if and only if both $X \subseteq Y$ and $Y \subseteq X$; (antisymmetry)
3. If both $X \subseteq Y$ and $Y \subseteq Z$, then $X \subseteq Z$. (transitivity)

So $\subseteq$ is what we call an **order relation**. The empty set has the particularity to be contained in every set: $\varnothing \subseteq X$ for any set X. In other words, $\varnothing$ is the smallest element for the relation $\subseteq$.

To go further

In view of the above, it is natural to ask: does there exist a set V containing all sets? Equivalently, does there exists a biggest elements for the relation $\subseteq$? A first guess would be to define V has the "collection" of all sets.[a] Sadly, this does not work as V is too big to be a set. The proof of this is done by contradiction, but needs a bit more of formal set theory to be carried out.

[a] V is called a von Neumann universe, which is named after John von Neumann (1903–1957).

Not only can we compare sets, we can also make operations on them. Given two sets X and Y, we can construct their **intersection** $X \cap Y$ which is the set containing exactly the elements that are both in X and in Y:

$$(x \in X \cap Y) \iff (x \in X \text{ and } x \in Y).$$

We can also construct the **union** $X \cup Y$ which is the set containing all elements of X and all elements of Y:

$$(x \in X \cup Y) \iff (x \in X \text{ or } x \in Y).$$

Union and intersection are conveniently represented by Venn diagrams.[1] See Figure 1.1

Example 1.1.3. Let $X = \{0, 2, 4, 6, \dots\}$ be the set of even integers and let $Y = \{0, 3, 6, 9, \dots\}$ be the set of non-negative multiple of 3. Then $X \cap Y = \{0, 6, 12, \dots\}$ is the set of non-negative multiple of 6, while $X \cup Y = \{0, 2, 3, 4, 6, 8, 9, 10, 12, 14, \dots\}$.

[1] From the mathematician John Venn (1834–1923).

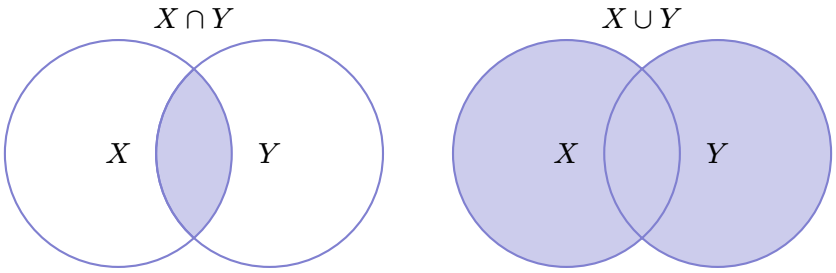


Figure 1.1: Intersection and union of two sets.

Exercise 1.1.4. Let $X = \{1, x, f\}$ and let $Y = \{\pi, \{1\}, 1, x\}$. Write the elements of $X \cup Y$ and of $X \cap Y$.

Remark 1.1.5.

For any sets X and Y we always have $X \cap Y \subseteq X \subseteq X \cup Y$.

It is useful to be able to construct new sets from old ones. An easy way to do this, is to start with two sets X and Y and construct the new set $\{X, Y\}$ whose elements are exactly X and Y. One can of course repeat this construction for any finite numbers of sets. That is start with X_1, ..., X_n to construct $\{X_1, \dots, X_n\}$.

Another powerful way to construct a new set is to start with a set X and with a "property" $\varphi(x)$ that can be true or false of its elements and to look at the subset of X containing all elements x such that $\varphi(x)$ is true. This new set is denoted by $\{x \in X \mid \varphi(x)\}$.

$$(y \in \{x \in X \mid \varphi(x)\}) \iff (y \in X \text{ and } \varphi(y) \text{ is true}).$$

For example,

$$\{n \in \mathbf{N} \mid \exists a \in \mathbf{N} : a^2 = n\} = \{0, 1, 4, 9, 16, 25, \dots\}$$

is the set of squares of integers.

Another useful way to produce new sets is the product operations. Before introducing it, we need a new notation. (x, y) represents an ordered pair. The most important property of ordered pairs is that

$$((x, y) = (a, b)) \iff (x = a \text{ and } y = b).$$

So $(x, y) \neq (y, x)$, unless $x = y$.

Definition 1.1.6.

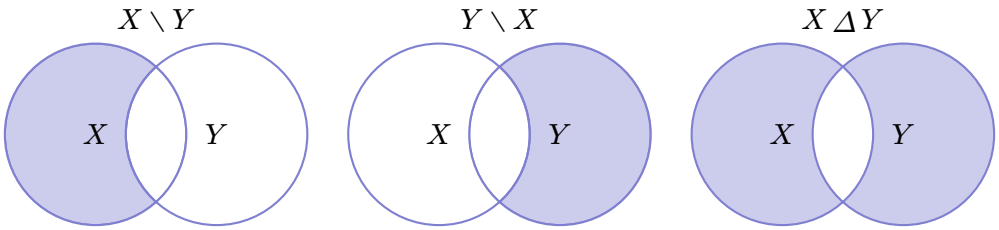
Let X and Y be two sets. Their **product** (also called **Cartesian product**[2]) is the set

$$X \times Y := \{(x, y) \mid x \in X, y \in Y\}.$$

[2]Named in honour of René Descartes (1596–1650).

To go further

Other operations on the sets X and Y are possible: X **minus** Y: $X \setminus Y := \{x \in X \mid x \notin Y\}$, $Y \setminus X$ and the **symmetric difference** $X \Delta Y := (X \setminus Y) \cup (Y \setminus X)$.



By looking at the Venn's diagram of X and Y, we see that we have $2^3 = 8$ possibilities for the result of an operation on X and Y. These 8 possibilities are realised by $\varnothing$, X, Y, $X \cup Y$, $X \cap Y$, $X \setminus Y$, $Y \setminus X$ and $X \Delta Y$. So our list of operations on two sets is exhaustive.

1.2 Functions

Now that we have a rough idea of what is a set, it is time to understand what is a function between two sets.

Definition 1.2.1.

Let X and Y be two sets. A **function**, or **map**, f from X to Y is a procedure that attribute to every element $x \in X$ a unique element $f(x) \in Y$. The set X is the **domain** of f and Y is its **codomain**.
The subset

$$\begin{aligned} \mathrm{Im}(f) = f(X) &:= \{f(x) \mid x \in X\} \\ &= \{y \in Y \mid \exists x \in X : f(x) = y\} \subseteq Y \end{aligned}$$

is called the **image** (or **range**) of f.

To denote a function f, we often use one of the following notations

$$\begin{aligned} f : X &\longrightarrow Y \\ x &\longmapsto f(x) \end{aligned} \qquad \text{or} \qquad \begin{aligned} X &\overset{f}{\longrightarrow} Y \\ x &\longmapsto f(x). \end{aligned}$$

To save vertical space, one also write $f : X \to Y, x \mapsto f(x)$ for the above function. We can also represent a function f by a picture. For example, for $X = \{1, 2, 3, 4\}$ and $Y = \{a, b, c\}$.

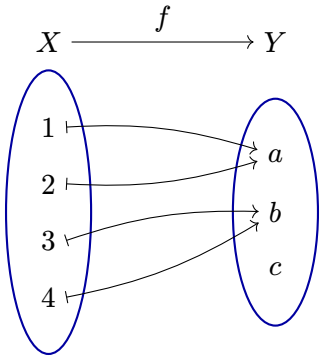


Figure 1.2: The function $f\colon X \to Y$ defined by $f(1) = f(2) = a$ and $f(3) = f(4) = b$. No element of X is sent onto c.

Remark 1.2.2.

A function $f\colon X \to Y$ is defined by 3 things: its domain X, its codomain Y and by what it does on elements of X. That is, two functions f and g are equals if they have the same domain X, the same codomain Y and if for all $x \in X$ one have $f(x) = g(x)$.

For example, the functions $f_1\colon \mathbf{R} \to \mathbf{R}, x \mapsto x^2$, $f_2\colon \mathbf{R}_{\geq 0} \to \mathbf{R}, x \mapsto x^2$, $f_3\colon \mathbf{R} \to \mathbf{R}_{\geq 0}, x \mapsto x^2$ and $f_4\colon \mathbf{R}_{\geq 0} \to \mathbf{R}_{\geq 0}, x \mapsto x^2$ are not equal because they do not have the same domain and codomain. This is very important and has real consequences. Indeed, f_4 is bijective, f_3 is surjective but not injective, f_2 is injective but not surjective and f_1 is neither injective nor surjective. See Definition 1.2.11 for a formal definition of injectivity, surjectivity and bijectivity.

As we have seen, sets cannot contain multiple copies of the same element. If we want to allow for repetition, we need to use families, or lists, which we can describe using functions.

Definition 1.2.3.

Let X be a set. A **family** of elements $(x_\alpha)_{\alpha \in I}$ of X is a function $\alpha \mapsto x_\alpha$ from a set I (called the index set) to X. If $I = \{1, \dots, m\}$ then this is simply the ordered list $(x_1, \dots, x_m)$.

Observe that in a family $(x_\alpha)_{\alpha \in I}$, the x_α are not necessarily distinct. Whenever the x_α are pairwise distinct, we sometimes identify $(x_\alpha)_{\alpha \in I}$ and the set $\{x_\alpha\}_{\alpha \in I} \subseteq X$. We will often make the slight abuse of notation and say that x is an element of the family $(x_\alpha)_{\alpha \in I}$ to mean that there exists an index $\alpha \in I$ such that $x = x_\alpha$.

If $X \subseteq Y$, then we have a special function called the **inclusion** defined by

$$\begin{aligned} \iota\colon X &\hookrightarrow Y \\ x &\longmapsto \iota(x) := x. \end{aligned}$$

Since the empty set is a subset of every set X, we always have a function $\iota\colon \varnothing \hookrightarrow X$.

If $f\colon Y \to Z$ is a function and $X \subseteq Y$ is a subset of Y, then f is also defined on X. We can therefore define the **restriction** of f to X as the function

$$\begin{aligned} f|_X\colon X &\longrightarrow Z \\ x &\longmapsto f|_X(x) := f(x). \end{aligned}$$

The only difference between $f\colon Y \to Z$ and $f|_X\colon X \to Z$ is that they do not have the same domain.

Example 1.2.4. The function

$$\begin{aligned} f\colon \mathbf{Z} &\longrightarrow \mathbf{R} \\ n &\longmapsto 2n \end{aligned}$$

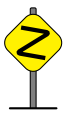
is the multiplication by 2 on relative integers. So $f(13) = 26$. Observe that the domain of f is $\mathbf{Z}$. In particular, $f(0.5)$ and $f(\pi)$ are not defined! The function

$$\begin{aligned} g\colon \mathbf{R}_{\geq 0} &\longrightarrow \mathbf{R} \\ x &\longmapsto 2x \end{aligned}$$

is also the multiplication by 2 (same "rule" as f) but is this time defined on all non-negative real numbers. So $g(\pi)$ is well-defined, but not $g(-2)$. If we define

$$\begin{aligned} h\colon \mathbf{R} &\longrightarrow \mathbf{R} \\ x &\longmapsto 2x, \end{aligned}$$

then we have $f = h|_{\mathbf{Z}}$ as well as $g = h|_{\mathbf{R}_{\geq 0}}$.



Remark 1.2.5.

In general a function does not need to be described by a nice rule as in the above examples and can be an arbitrary assignment.

Definition 1.2.6.

Given two functions $X \xrightarrow{f} Y$ and $Y \xrightarrow{g} Z$ we can define their **composition** $g \circ f$ as the function

$$\begin{aligned} g \circ f\colon X &\longrightarrow Z \\ x &\longmapsto (g \circ f)(x) := g(f(x)). \end{aligned}$$

We can summarise this by saying that the following diagram commutes

$$X \xrightarrow{f} Y \xrightarrow{g} Z, \qquad X \xrightarrow{g \circ f} Z.$$

Restriction of a function can also be described in term of composition of function. See the following commutative diagram.

$$\begin{array}{ccc} Y & \xrightarrow{f} & Z. \\ {\scriptstyle\iota}\uparrow & \nearrow_{f|_X} & \\ X & & \end{array}$$

In other words, we have $f|_X = f \circ \iota$ where $\iota \colon X \hookrightarrow Y$ is the inclusion function.

Remark 1.2.7.

Commutative diagrams are important tools of algebra. They allow us to easily visualise equalities between functions.
A diagram is a directed graph of sets and functions between them. A diagram is said to be commutative if for any two sets X and Y, any two directed paths p and q from X to Y are equal: $p = q$. For example, in the above diagram there are two paths $f \circ i$ and $f|_X$ from X to Z. For any other two choices of sets D, E in $\{X, Y, Z\}$ there is at most one path from D to E. So this specific diagram is commutative if and only if $f \circ i = f|_X$.

Observe that $g \circ f$ is defined only if the codomain of f is equal to the domain of g. In practice, if the codomain Y' of f is contained in the domain Y of g we will sometimes make a slight abuse of notation and write $g \circ f$ for $g|_{Y'} \circ f = g \circ \iota \circ f$:

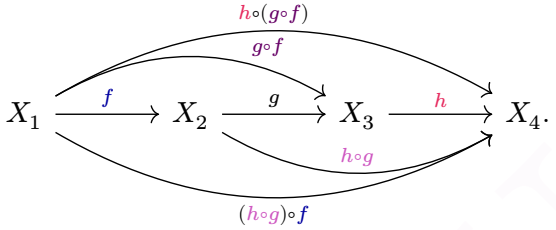
$$X \xrightarrow{f} Y' \subseteq Y \xrightarrow{g} Z \quad = \quad X \xrightarrow{f} Y' \xhookrightarrow{\iota} Y \xrightarrow{g} Z.$$

Remark 1.2.8.

Be careful about the order: $(g \circ f)(x) = g(f(x))$ means we first apply f to x and then we apply g to $f(x)$.
This is especially important as the composition of functions is not commutative. Firstly, the fact that $g \circ f$ is well defined does not imply that $f \circ g$ is. Indeed, let $f \colon \mathbf{R}^2 \to \mathbf{R}, (x, y) \mapsto x$ be the projection onto the first coordinate and let $g \colon \mathbf{R} \to \mathbf{R}, x \mapsto 2x$ be the multiplication by 2. Then $g \circ f \colon \mathbf{R}^2 \to \mathbf{R}, (x, y) \mapsto 2x$, but $f \circ g$ is not defined.
Secondly, even if both $g \circ f$ and $f \circ g$ are well-defined they do not need to have the same domains and codomain. For example, let f be as above and let $h \colon \mathbf{R} \to \mathbf{R}^2, x \mapsto (x, x)$ be the diagonal embedding. Then $h \circ f \colon \mathbf{R}^2 \to \mathbf{R}^2, (x, y) \mapsto (x, x)$ while $f \circ h \colon \mathbf{R} \to \mathbf{R}, x \mapsto x$.
Finally, even when $g \circ f$ and $f \circ g$ are well-defined and share the same domain and codomain they do not need to commute. For example, let g be the multiplication

by 2 as above and let $k\colon \mathbf{R} \to \mathbf{R}, x \mapsto x+1$. Then both $g\circ k$ and $k\circ g$ are functions from $\mathbf{R}$ to itself. However, $(g\circ k)(x) = 2(x+1) = 2x+2$ while $(k\circ g)(x) = 2x+1$.

The composition of function is associative: $(h\circ g)\circ f$ is defined if and only if $h\circ(g\circ f)$ is defined, in which case they are equal. Indeed, both $((h\circ g)\circ f)(x)$ and $(h\circ(g\circ f))(x)$ are equal to $(h(g(f(x))))$. When $(h\circ g)\circ f$ (equivalently $h\circ(g\circ f)$) is defined, we simply write $h\circ g\circ f$ for it. Associativity of composition of functions is equivalent to the commutativity of the following diagram:



Definition 1.2.9.

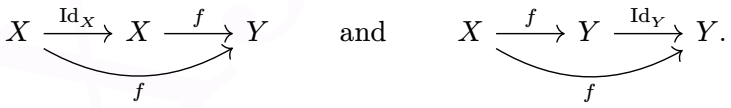
For any set X we have a special function, the **identity function** $\mathrm{Id}_X\colon X \to X$ that does nothing: $\mathrm{Id}_X(x) = x$ for every $x \in X$.

The identities functions are identities for the composition of functions as demonstrated in the following lemma.

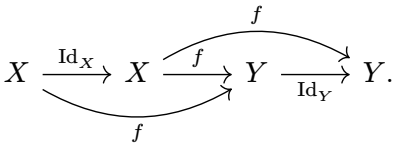
Lemma 1.2.10. *For every function $f\colon X \to Y$ we have $f\circ \mathrm{Id}_X = f = \mathrm{Id}_Y \circ f$.*

Proof. Let x be any element in X. Then $(f\circ \mathrm{Id}_X)(x) = f(\mathrm{Id}_X(x)) = f(x)$ while $(\mathrm{Id}_Y \circ f)(x) = \mathrm{Id}_Y(f(x)) = f(x)$. □

Lemma 1.2.10 is equivalent to say the following two diagrams are commutative:



We can even summarise the two equalities $f\circ \mathrm{Id}_X = f = \mathrm{Id}_Y \circ f$ in a single commutative diagram:



The following are important properties that a function can possess or not.

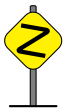
Definition 1.2.11.

Let $f\colon X \to Y$ be a function. It is **injective** (or **one-to-one**) if for every $x_1 \neq x_2$ in X we have $f(x_1) \neq f(x_2)$. This is equivalent to say that if $f(x_1) = f(x_2)$ then $x_1 = x_2$. Equivalently, for every $y \in Y$, there exists at most one $x \in X$ such that $f(x) = y$. We usually use the notation $f\colon X \hookrightarrow Y$ for injective functions.
The function f is **surjective** (or **onto**) if for every $y \in Y$ there exists at least one $x \in X$ with $f(x) = y$. Such an x is called a **preimage** of y. We usually use the notation $f\colon X \twoheadrightarrow Y$ for surjective functions.
Finally, the function f is **bijective** if it is both injective and surjective. This is equivalent to say that for every $y \in Y$ there exists a unique $x \in X$ such that $f(x) = y$. To denote a bijective function, we naturally use the notation $f\colon X \xhookrightarrow{\sim} Y$.
We write $X \simeq Y$ to say that there exists a bijection between X and Y, without having to specify the function.

An injective function is sometimes called an **embedding**. If X is a subset of Y, then the inclusion function $\iota\colon X \hookrightarrow Y$ is injective.

Definition 1.2.12.

A function $f\colon X \to Y$ is **invertible** if there exists a function $g\colon Y \to X$ such that $g \circ f = \mathrm{Id}_X$ and $f \circ g = \mathrm{Id}_Y$. Such a function g is called an **inverse** and is written f^{-1}.



Remark 1.2.13.

For g to be an inverse of g both equalities $g \circ f = \mathrm{Id}_X$ and $f \circ g = \mathrm{Id}_Y$ need to be satisfied.

Example 1.2.14. Let $f\colon \mathbf{R}^2 \to \mathbf{R}, (x, y) \mapsto x$ and $h\colon \mathbf{R} \to \mathbf{R}^2, x \mapsto (x, x)$ be the maps from Remark 1.2.8. Then $f \circ h = \mathrm{Id}_{\mathbf{R}}$ but $h \circ f \neq \mathrm{Id}_{\mathbf{R}^2}$. So h is not the inverse of f.

Inverses satisfies the following useful properties.

Lemma 1.2.15. *If $f\colon X \to Y$ is invertible, then*

1. *f has a unique inverse;*
2. *$(f^{-1})^{-1} = f$;*
3. *If $f\colon X \to Y$ and $g\colon Y \to Z$ are two invertible functions, then $g \circ f\colon X \to Z$ is invertible with inverse $(g \circ f)^{-1} = f^{-1} \circ g^{-1}\colon Z \to X$.*

Proof. Suppose that $g, h\colon Y \to X$ are two inverses for f. Then $g \circ f \circ h$ is a well defined function from Y to Y and we have

$$g = g \circ \mathrm{Id}_X = g \circ f \circ h = \mathrm{Id}_Y \circ h = h.$$

The second statement directly follows from the definition.

The last statement is a straightforward verification: $(g\circ f)\circ(f^{-1}\circ g^{-1}) = g\circ \mathrm{Id}_X \circ g^{-1} = g\circ g^{-1} = \mathrm{Id}_Z$ and similarly $(f^{-1}\circ g^{-1})\circ(g\circ f) = \mathrm{Id}_X$. □

Whenever there exists an invertible function $f\colon X \to Y$ we consider them similar as sets, as any "set property" that is true for X is also true for Y and vice-versa. For example, $\{1\}$ and $\{2\}$ are not equal (they do not have the same elements), but they behave similarly for any set property (they both have exactly one element, if Z is a set then there exists an injection $Z \hookrightarrow X$ if and only if there exists an injection $Z \hookrightarrow Y$,...).

In view of the above, invertible functions are fundamental and it is important to understand them. Luckily, it turns out that they are nothing more than bijections.

Theorem 1.2.16.

A function $f\colon X \to Y$ is a bijection if and only if is invertible.

Proof. "⇒"By bijectivity of f, one can define a function $g\colon Y \to X$ by

$$g(y) \coloneqq \text{the unique } x \text{ such that } f(x) = y.$$

This directly implies $(f\circ g)(y) = y$ for all $y \in Y$ and $(g\circ f)(x) = x$ for all $x \in X$, so g is the inverse for f.

"⇐"Let y be any element of Y. Then $f^{-1}(y)$ belongs to X and $f((f^{-1}(y)) = y$, proving surjectivity of f. Now, let x_1 and x_2 be two elements of X such that $f(x_1) = f(x_2)$. By applying f^{-1} on both sides we obtain $x_1 = (f^{-1}\circ f)(x_1) = (f^{-1}\circ f)(x_2) = x_2$, proving injectivity of f. □

For finite sets, we have a useful characterisation of bijectivity.

Lemma 1.2.17. *Let X and Y be two finite sets with the same cardinality $\#X = \#Y$, and let $f\colon X \to Y$ be any function. The following are equivalent:*

I. f is bijective;

II. f is injective;

III. f is surjective.

Proof. By definition f is bijective if and only if it is both injective and surjective. So all we have to do is to show the equivalence of II and III.

Let $f\colon X \to Y$ be any function between any sets. For any $y \in Y$, define $S(y) \coloneqq \{x \in X \mid f(x) = y\}$, the preimage of y ($S(y)$ is empty if y is not in the image of f). We have $\bigcup_{y\in Y} S(y) = X$, because every element of X is mapped to some element of y. Moreover, since f is a function, $S(y)\cap S(y') = \varnothing$ if $y \neq y'$ (every element has a unique image). So the union is a disjoint union: $\bigsqcup_{y\in Y} S(y) = X$ Let $N(y) = \#S(y)$, so $N(y)$ is the number of elements in X that are mapped to y. By the above, $\sum_{y\in Y} N(y) = \#X$.

Surjectivity of f is equivalent to $N(y) \geq 1$ for all $y \in Y$, while injectivity is equivalent to $N(y) \leq 1$ for all $y \in Y$.

If $\#X = \#Y$, then $\sum_{y\in Y} N(y) = \#Y$. So $N(y) \geq 1$ for all $y \in Y$ if and only if they are all 1, if and only if $N(y) \leq 1$ for all $y \in Y$. □

Remark 1.2.18.

Lemma 1.2.17 does not hold for infinite sets. For example, the function $s\colon n \mapsto n+1$ from $\mathbf{N}$ to itself is injective but not surjective. The function $p\colon \mathbf{N} \to \mathbf{N}$ defined by $p(0) = 0$ and $p(n) = n-1$ if $n \geq 1$ is surjective but not injective.

If the codomain of a function f coincides with its domain, we can compose f with itself.

Definition 1.2.19.

Let $f\colon X \to X$ be a function whose codomain is equal to codomain. For $k \in \mathbf{N}$ positive we define

$$f^k := \underbrace{f \circ \cdots \circ f}_{k \text{ times}}.$$

This is still a function from X to X. We also define $f^0 := \mathrm{Id}_X$.

It follows from associativity that for m and n in N we have $(f^m)^n = f^{m+n} = f^{n+m} = (f^n)^m$.

If f is an invertible function, it is unclear how to define f^{-2}. We can choose to define it as $(f^{-1})^2$ (the square of the inverse of f) or as $(f^2)^{-1}$ (the inverse of f^2). Luckily these two quantities are equal.

Lemma 1.2.20. *Let $f\colon X \to X$ be an invertible function and let $g = f^{-1}$ be its inverse. Then for any integer k, the function g^k is the inverse of f^k.*

Proof. The proof is by induction.

The property is true for $k = 0$ (as both f^0 and g^0 are equal to Id_X) and for $k = 1$ (by definition).

Now, suppose that $k \geq 2$ and that the proof property is true holds at $k-1$. Then $g^k f^k = g^{k-1} g f f^{k-1} = g^{k-1}\,\mathrm{Id}_X\, f^{k-1} = g^{k-1} f^{k-1} = \mathrm{Id}_X$. Similarly, $f^k g^k = \mathrm{Id}_X$. So g^k is the inverse of f^k. □

Definition 1.2.21.

Let $f\colon X \to X$ be an invertible function whose codomain is equal to codomain. For $k \in \mathbf{N}$ positive we define

$$f^{-k} := (f^{-1})^k = (f^k)^{-1}.$$

Corollary 1.2.22. *Let $f\colon X \to X$ be a function whose codomain is equal to its domain. Then*

1. $\forall m, n \in \mathbf{N} : (f^m)^n = f^{m\cdot n}$;

2. *If f is invertible, then $\forall m, n \in \mathbf{Z} : (f^m)^n = f^{m \cdot n}$;*

Since functions from X to Y play an important role, we gave a name to the set of all such functions.

Definition 1.2.23.

If X and Y are two sets, then we define

$$Y^X := \{f \mid f \colon X \to Y \text{ is a function}\}$$

to be the set of all functions from X to Y.

The notation comes from the fact that if X and Y are finite sets, then $\#(Y^X) = (\#Y)^{(\#X)}$.

To go further

The notation Y^X is one of the reasons for the convention $0^0 = 1$. Indeed, we have $0 = \#\varnothing$ and there is a unique function from $\varnothing$ to $\varnothing$ (the empty function that does nothing). So $\#(\varnothing^\varnothing) = 1$ and we want this to be equal to $(\#\varnothing)^{(\#\varnothing)} = 0^0$.

2 Vector spaces

The aim of this chapter is to define vector spaces and start the study of their properties. We will start with reminders on $\mathbf{R}^2$ and $\mathbf{R}^3$, generalise to $\mathbf{R}^n$ and finally see the definition of an abstract vector space.

2.1 First examples

Before introducing the abstract definition of a vector space, we review some examples from high-school and introduce some straightforward generalisations of them.

2.1.1 $\mathbf{R}^n$ as a vector space

You probably already now the spaces

$$\mathbf{R}^2 := \left\{ \begin{bmatrix} x \\ y \end{bmatrix} \,\middle|\, x, y \in \mathbf{R} \right\} \qquad \text{and} \qquad \mathbf{R}^3 := \left\{ \begin{bmatrix} x \\ y \\ z \end{bmatrix} \,\middle|\, x, y, z \in \mathbf{R} \right\}.$$

It is natural to generalise this construction for any $n \in \mathbf{N}$:

$$\mathbf{R}^n := \left\{ \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix} \,\middle|\, x_i \in \mathbf{R} \text{ for } i \in \{1, \dots, n\} \right\}.$$

In order to save space, we will sometimes use the notation $[x, y]^\mathsf{T} := \begin{bmatrix} x \\ y \end{bmatrix}$ and similarly for elements of $\mathbf{R}^3$ and $\mathbf{R}^n$.

Remark 2.1.1 (On the notation of vectors)**.**

Some people prefer to use parenthesis instead of brackets and write $\binom{x}{y}$ for $\begin{bmatrix} x \\ y \end{bmatrix}$.
It is also possible to use the horizontal (list) notation $\{(x, y) \mid x, y \in \mathbf{R}\}$ for $\mathbf{R}^2$.
The horizontal notation (x, y) and the vertical notation $\begin{bmatrix} x \\ y \end{bmatrix}$ are of course equivalent and both notations have their merits.
The vertical notation is useful for the matrix-vector product and is often used in geometry. The horizontal notation agrees with Definition 1.1.6 (Cartesian product) and with the notations for the forthcoming generalisations $\mathbf{R}^{(\mathbf{N})}$ and $\mathbf{R}^S$, see Examples 2.2.9 and 2.2.10. We will usually use the vertical notation $\begin{bmatrix} x \\ y \end{bmatrix} = [x, y]^\mathsf{T}$, but we might also use the horizontal one when more appropriate.

Observe that $\mathbf{R}^1 \simeq \mathbf{R}$, while $\mathbf{R}^0$ has only one element (the empty list). To simplify the notation, we will sometimes simply write x to denote the element $[x_1, x_2, \dots, x_n]^\mathsf{T} \in \mathbf{R}^n$, and we will call such an element $x \in \mathbf{R}^n$ a **vector**. Some authors use the notation $\vec{x}$ or $\boldsymbol{x}$ (a boldface x) for the vector x.

So far, $\mathbf{R}^n$ is just a set. To make it more interesting, we will endow it with some operations. Given two elements $[x_1, x_2, \dots, x_n]^\mathsf{T}$ and $[y_1, y_2, \dots, y_n]^\mathsf{T}$ in $\mathbf{R}^n$ we define their **addition** by

$$\begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} +_{\mathbf{R}^n} \begin{bmatrix} y_1 \\ \vdots \\ y_n \end{bmatrix} := \begin{bmatrix} x_1 + y_1 \\ \vdots \\ x_n + y_n \end{bmatrix},$$

Where the $+$ on the right hand side is the usual addition of real numbers.

Now, if $[x_1, x_2, \dots, x_n]^\mathsf{T}$ is an element of $\mathbf{R}^n$ and $\lambda \in \mathbf{R}$ is a real number, we define the **scalar multiplication** by

$$\lambda \cdot_{\mathbf{R}^n} \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} := \begin{bmatrix} \lambda x_1 \\ \vdots \\ \lambda x_n \end{bmatrix},$$

where the λx_i are the usual multiplication of real numbers. Be careful that we only defined $\lambda \cdot_{\mathbf{R}^n} [x_1, x_2, \dots, x_n]^\mathsf{T}$ and that $[x_1, x_2, \dots, x_n]^\mathsf{T} \cdot_{\mathbf{R}^n} \lambda$ is not defined.

Remark 2.1.2.

In practice, we will often simply write $+$ instead of $+_{\mathbf{R}^n}$ and $\cdot$ instead of $\cdot_{\mathbf{R}^n}$. We will even often simply omit $\cdot$ and simply write $\lambda[x_1, x_2, \dots, x_n]^\mathsf{T}$ for $\lambda \cdot_{\mathbf{R}^n} [x_1, x_2, \dots, x_n]^\mathsf{T}$.

The operations $+$ and $\cdot$ we just defined on $\mathbf{R}^n$ generalise the familiar operations on $\mathbf{R}$, $\mathbf{R}^2$ and $\mathbf{R}^3$.

For $n \in \{1, 2, 3\}$ we can interpret geometrically vectors of $\mathbf{R}^n$ as arrow in the Cartesian line/plane/space. As demonstrated in Figure 2.1, we use $\{(x, y) \mid x, y \in \mathbf{R}\}$ for the Cartesian plane. A dot at coordinate (x, y) represents a point in $\{(x, y) \mid x, y \in \mathbf{R}\}$. A vector $\begin{bmatrix} x \\ y \end{bmatrix}$ is represented by an arrow from the origin $(0, 0)$ to the point (x, y), see Figure 2.1.

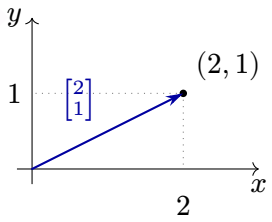


Figure 2.1: Representation of the vector $\begin{bmatrix} 2 \\ 1 \end{bmatrix}$ as an arrow from $(0, 0)$ to $(2, 1)$.

With this representation, one can interpret geometrically the operation $+$ and $\cdot$, see Figure 2.2. For $\lambda \cdot v$, simply take the arrow representing v and multiply its length by λ. In particular, if $\lambda < 0$, then λv goes in the opposite direction as v. For $v + w$, we complete

the parallelogram formed by the arrow representing v and w and take the diagonal arrow from $(0,0)$ to the newly created vertex of the parallelogram.

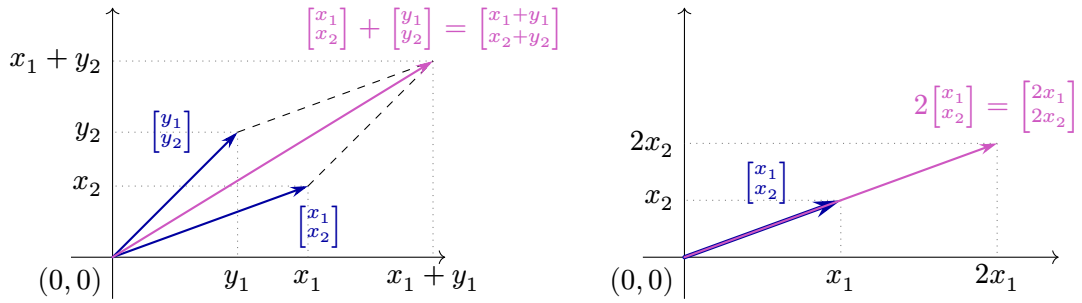


Figure 2.2: Addition and scalar multiplication (by 2) $\mathbf{R}^2$.

For $n \geq 4$, we cannot draw pictures anymore and it is thus not possible to visualise vectors in the real world. But this does not mean that we cannot use $\mathbf{R}^n$ with $n \geq 4$ to solve real world problems. For example, modern machine learning use $n \geq 1000$ ($n = 2048$ for ChatGPT 3).

We have constructed $(\mathbf{R}^n, +, \cdot) = (\mathbf{R}^n, +_{\mathbf{R}^n}, \cdot_{\mathbf{R}^n})$. The operations $+$ and $\cdot$ satisfy some useful properties that turns $\mathbf{R}^n$ into a **real vector space**.[1]

Proposition 2.1.3. *The following properties hold for* $(\mathbf{R}^n, +, \cdot)$.

1. $\forall x, y, z \in \mathbf{R}^n : (x + y) + z = x + (y + z)$; *(associativity of $+$)*
2. $\exists 0_{\mathbf{R}^n} \in \mathbf{R}^n, \forall x \in \mathbf{R}^n : 0_{\mathbf{R}^n} + x = x$; *(existence of a neutral element for $+$)*
3. $\forall x \in \mathbf{R}^n, \exists x' \in \mathbf{R}^n : x + x' = 0_{\mathbf{R}^n}$; *(existence of an inverse for $+$)*
4. $\forall x, y \in \mathbf{R}^n : x + y = y + x$; *(commutativity of $+$)*
5. $\forall x \in \mathbf{R}^n : 1 \cdot x = x$; *($1 \in \mathbf{R}$ is the left identity for $\cdot$)*
6. $\forall \lambda, \mu \in \mathbf{R}, \forall x \in \mathbf{R}^n : (\lambda\mu) \cdot x = \lambda \cdot (\mu \cdot x)$; *(compatibility of multiplication)*
7. $\forall \lambda, \mu \in \mathbf{R}, \forall x \in \mathbf{R}^n : (\lambda +_{\mathbf{R}} \mu) \cdot x = \lambda \cdot x +_{\mathbf{R}^n} \mu \cdot x$; *(right distributivity)*
8. $\forall \lambda \in \mathbf{R}, \forall x, y \in \mathbf{R}^n : \lambda \cdot (x +_{\mathbf{R}^n} y) = \lambda \cdot x +_{\mathbf{R}^n} \lambda \cdot y$. *(left distributivity)*

Proof. Let $0_{\mathbf{R}^n} := [0, 0, \dots, 0]^\mathsf{T}$ and for $x = [x_1, \dots, x_n]^\mathsf{T} \in \mathbf{R}^n$ let $x' := [-x_1, \dots, -x_n]^\mathsf{T}$. Then the proof of the properties are just easy (but fastidious) verification. We will just verify the first property and leave the verification of the other ones to the reader.

So let $x = [x_1, \dots, x_n]^\mathsf{T} \in \mathbf{R}^n$ and $y = [y_1, \dots, y_n]^\mathsf{T} \in \mathbf{R}^n$ be two vectors. We have

$$x + y = \begin{bmatrix} x_1 + y_1 \\ \vdots \\ x_n + y_n \end{bmatrix} = \begin{bmatrix} y_1 + x_1 \\ \vdots \\ y_n + x_n \end{bmatrix} = y + x,$$

[1] We will formally define vector spaces in Definition 2.2.2.

where the first and third equalities are by definition, and the second equality is the commutativity of the addition in $\mathbf{R}$. □

We will usually write 0 for $0_{\mathbf{R}^n}$ and $-x$ for the element x' in Item 3.

Remark 2.1.4.

One important moral of Proposition 2.1.3 is that the operations $+_{\mathbf{R}^n}$ and $\cdot_{\mathbf{R}^n}$ behave well with respect to the usual addition and multiplication on $\mathbf{R}$. This is what allows us to safely drop the index $\mathbf{R}^n$ and write $+$ instead of $+_{\mathbf{R}^n}$.

2.1.2 Getting complex: $\mathbf{C}^n$

Recall that the field of **complex numbers** is defined by

$$\mathbf{C} := \{a + b\mathrm{i} \mid a, b \in \mathbf{R}\},$$

where i is a symbol not in $\mathbf{R}$. One can define addition and multiplication of complex numbers by:

$$(a + b\mathrm{i}) +_{\mathbf{C}} (c + d\mathrm{i}) := (a + c) + (b + d)\mathrm{i}$$
$$(a + b\mathrm{i}) \cdot_{\mathbf{C}} (c + d\mathrm{i}) := (ac - bd) + (bc + ad)\mathrm{i}.$$

As usual, we will usually drop the index $\mathbf{C}$ and simply write $+$ and $\cdot$, or even simply $(a + b\mathrm{i})(c + d\mathrm{i})$ for the multiplication. By definition of the multiplication, we have $\mathrm{i}^2 = -1 + 0 = -1$.

To go further

The addition of complex numbers is done component-by-component and is quite natural. It correspond to the addition of vectors in $\mathbf{R}^2$. The definition of multiplication might seem a bit bizarre at first sight. It has two justifications.
The first justification is the existence of a square root of -1. Indeed, if we impose the relation $\mathrm{i}^2 = -1$, and want $\cdot_{\mathbf{C}}$ to be distributive over the addition, then $(a + b\mathrm{i})(c + d\mathrm{i}) = ac + bd(\mathrm{i}^2) + bc\mathrm{i} + ad\mathrm{i} = (ac - bd) + (bc + ad)\mathrm{i}$. One can later verify that $(\mathbf{C}, +, \cdot)$ is a field, see Appendix 2.1.
The second justification is to start with $\mathbf{R}^2$ and try to define a multiplication on vector that generalises the scalar multiplication λv and behave "nicely", that is that turns $(\mathbf{R}^2, +, \cdot)$ into a field. It turns out that the only way to do this is to define the multiplication as we did. This is known as the Frobenius[a] Theorem. If $n \geq 3$, then it is not possible to define such a nice multiplication on $\mathbf{R}^n$. But, see Subsection 2.2.1 …

[a] Ferdinand Georg Frobenius (1849–1917).

Given $m \in \mathbf{N}$, we define $\mathbf{C}^m := \{[z_1, \dots, z_m]^\mathsf{T} \mid z_j \in \mathbf{C} \text{ for } j \in \{1, \dots, m\}\}$. Elements of $\mathbf{C}^m$ are also called (complex) **vectors**. It is then possible to define $+_{\mathbf{C}^m}$ the addition of vectors and $\cdot_{\mathbf{C}^m}$ the scalar multiplication of a vector by a complex number $\lambda \in \mathbf{C}$

similarly to what we did for $+_{\mathbf{R}^m}$ and $\cdot_{\mathbf{R}^m}$. These operations turn $(\mathbf{C}^m, +_{\mathbf{C}^m}, \cdot_{\mathbf{C}^m})$ into a **complex vector space**.[2] That is, $(\mathbf{C}^m, +_{\mathbf{C}^m}, \cdot_{\mathbf{C}^m})$ satisfies Proposition 2.1.3, except with all instances of $\mathbf{R}$ replaced by $\mathbf{C}$.

2.2 Definition and first properties

We will now generalise the previous examples and give an abstract definition of vector spaces. We will then investigate a few properties that directly follows from the definition.

2.2.1 Abstract vector spaces

Most of the results we will learn are common to $\mathbf{R}$ and $\mathbf{C}$. We will therefore use a unified notation and write $\mathbf{F}$ for either of them. The letter $\mathbf{F}$ stands for **field**, which intuitively is a set where we can "add" and "multiply" elements, but also "substract" or "divide" (except by 0) them and where these operations are subject to some axioms which ensure that they behave similarly to $\mathbf{R}$ and $\mathbf{C}$. In particular, in a field addition and multiplication are commutative and we always have a "0" element ($0 + x = x$ and $0x = 0$ for all $x \in \mathbf{F}$) and a "1" element ($1x = x$ for all $x \in \mathbf{F}$). For example, $(\mathbf{R}, +, \cdot)$ and $(\mathbf{C}, +, \cdot)$ are fields, but $(\mathbf{Q}, +, \cdot)$ is also a field.

Example 2.2.1. The following are NOT fields: $(\mathbf{Z}, +, \cdot)$ (we cannot divide 2 by 3), $(\mathbf{R}_{\geq 0}, +, \cdot)$ (we cannot substract 7 from 5).

The vector space $(\mathbf{R}^3, +, \cdot)$ is NOT a field. Indeed, one can naively try to define the multiplication component-wise by $[x_1, x_2, x_3]^\mathsf{T}[y_1, y_2, y_3]^\mathsf{T} = [x_1y_1, x_2y_2, x_3y_3]^\mathsf{T}$, but then it is not possible to divide by (the non-zero element) $[1, 0, 0]^\mathsf{T}$.

To go further

The interested reader can find the formal definition as well as a few elementary properties of fields in Appendix 2.1.

Given a field $\mathbf{F}$, one can mimic the construction of $(\mathbf{R}^n, +, \cdot)$ and $(\mathbf{C}^n, +, \cdot)$ and construct $(\mathbf{F}^n, +_{\mathbf{F}^n}, \cdot_{\mathbf{F}^n})$ which will satisfy Proposition 2.1.3, except with all instances of $\mathbf{R}$ replaced by $\mathbf{F}$.

As we have seen, Proposition 2.1.3 is satisfied by all of $(\mathbf{R}^n, +, \cdot)$, $(\mathbf{C}^n, +, \cdot)$ and $(\mathbf{F}^n, +_{\mathbf{F}^n}, \cdot_{\mathbf{F}^n})$. We will use it to define an abstract vector space.

Definition 2.2.2.

Let $\mathbf{F} = (\mathbf{F}, +_\mathbf{F}, \cdot_\mathbf{F})$ be a field (for example, $\mathbf{R}$ or $\mathbf{C}$). A **$\mathbf{F}$-vector space** (or simply a **vector space**) is a set V endowed with two operations:

$$+_V : V \times V \longrightarrow V \qquad \cdot_V : \mathbf{F} \times V \longrightarrow V$$
$$(v, w) \longmapsto v +_V w \qquad (\lambda, v) \longmapsto \lambda \cdot_V v,$$

[2] We will formally define vector spaces in Definition 2.2.2.

satisfying the analog of Proposition 2.1.3. Formally, $(V, +_v, \cdot_V)$ is an $\mathbf{F}$-vector space if the following axioms are true:

(1) $\forall u, v, w \in V : (u +_V v) +_V w = u +_V (v +_V w)$; (associativity of $+_V$)

(2) $\exists 0_V \in V, \forall v \in V : 0_V +_V v = v$; (neutral element for $+_V$)

(3) $\forall v \in V, \exists v' \in V : v +_V v' = 0_V$; (inverse for $+_V$)

(4) $\forall u, v \in V : v +_V v = v +_V u$; (commutativity of $+_V$)

(5) $\forall v \in V : 1_{\mathbf{F}} \cdot_V v = v$; ($1_{\mathbf{F}} \in \mathbf{F}$ is the left identity for $\cdot_V$)

(6) $\forall \lambda, \mu \in \mathbf{F}, \forall v \in V : (\lambda \cdot_{\mathbf{F}} \mu) \cdot_V v = \lambda \cdot_V (\mu \cdot_V v)$; (compatibility of $\cdot$)

(7) $\forall \lambda, \mu \in \mathbf{F}, \forall v \in V : (\lambda +_{\mathbf{F}} \mu) \cdot_V v = \lambda \cdot_V v +_V \mu \cdot_V v$; (right distributivity)

(8) $\forall \lambda \in \mathbf{F}, \forall v, w \in V : \lambda \cdot_V (v +_V w) = \lambda \cdot_V v +_V \lambda \cdot_V w$. (left distributivity)

Elements of V are called **vectors** (or **points**) and elements of $\mathbf{F}$ are called scalars **scalars**. We say that $+_V$ is an **addition** and $\cdot_V$ a **scalar multiplication**.

As usual, we will respectively write $+$, $\cdot$ (or simply λv), 0 and $-v$ instead of $+_V$, $\cdot_V$, 0_V and v' from Axiom (4). When $+$ and $\cdot$ are clear from context, we will write V instead of $(V, +, \cdot)$.

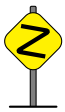
We will usually write $v - w$ for $v + (-w)$, $u + v + w$ for $u + (v + w) = u + (v + w)$ and $\lambda\mu v$ for $(\lambda\mu)v = \lambda(\mu v)$.

To go further

The fact that $(V, +_V)$ satisfies Properties (1) to (4) means that it is a **commutative group**. Commutative groups, and more generally groups, are very important objects of abstract algebra.

Definition 2.2.2 might seem quite abstract, but it is its strength. Indeed, this allows us to treat, in a unified way, many examples coming from various branches of mathematics as the space of polynomials, the space of (continuous) functions from $\mathbf{R}$ to $\mathbf{R}$, the space of solutions of a given ordinary differential equation and many others.

Remark 2.2.3.



The base field $\mathbf{F}$ matters! Indeed, $V = \mathbf{R}$ is a $\mathbf{R}$-vector space, but not a $\mathbf{C}$-vector space. On the other hand, $V = \mathbf{C}$ is both a $\mathbf{R}$-vector space and a $\mathbf{C}$-vector space. However, will see later (Remark 2.4.42) that $\mathbf{C}$ has "$\mathbf{R}$-dimension" 2 but "$\mathbf{C}$-dimension" 1.

In order to better understand the abstract definition of a vector space, we will now present many examples.

Example 2.2.4. For any field $\mathbf{F}$, the set $\{0\}$ is an $\mathbf{F}$-vector space. It has only one element, 0 and we have $0+0=0$ and $\lambda 0 = 0$ for all $\lambda \in \mathbf{F}$.

Example 2.2.5. If $\mathbf{F}$ is a field and $n \in \mathbf{N}$ a non-negative integer, then $\mathbf{F}^n$ is an $\mathbf{F}$-vector space (with $\mathbf{F}^0 \cong \{0\}$).[3]

Example 2.2.6. Let V and W be two $\mathbf{F}$-vector spaces. Define $+$ and $\cdot$ component-wise on $V \times W$:

$$(v_1, w_1) + (v_2, w_2) := (v_1 + v_2, w_1 + w_2)$$
$$\lambda \cdot (v, w) := (\lambda v, \lambda w).$$

Then $(V \times W, +, \cdot)$ is an $\mathbf{F}$-vector space, is called the **product** of V and W. We sometimes write $V \oplus W$ for this space, in which case we call it the **direct sum**.

We have $\mathbf{F}^n \times \mathbf{F}^m \cong \mathbf{F}^{n+m}$.

Example 2.2.7. For $\mathbf{F}$ a field, let $\mathbf{F}^{\mathbf{N}} := \{(x_0, x_1, \dots) \mid x_i \in \mathbf{F} \text{ for } i \in \mathbf{N}\}$ be the set of infinite sequences of elements of $\mathbf{F}$, with addition and scalar multiplication defined component-wise:

$$(x_0, x_1, \dots) +_{\mathbf{F}^{\mathbf{N}}} (y_0, y_1, \dots) := (x_0 + y_0, x_1 + y_1, \dots),$$
$$\lambda \cdot_{\mathbf{F}^{\mathbf{N}}} (x_0, x_1, \dots) := (\lambda x_0, \lambda x_1, \dots).$$

Then $(\mathbf{F}^{\mathbf{N}}, +, \cdot)$ is an $\mathbf{F}$-vector space.

Remark 2.2.8.

Some authors use the notation $\mathbf{F}^\infty$ for $\mathbf{F}^{\mathbf{N}}$. However, other authors use $\mathbf{F}^\infty$ for $\mathbf{F}^{(\mathbf{N})}$ from Example 2.2.10. These two spaces, $\mathbf{F}^{\mathbf{N}}$ and $\mathbf{F}^{(\mathbf{N})}$, are very different and should not be confused.

Example 2.2.9. Let S be a set and let $\mathbf{F}$ be a field. Recall that $\mathbf{F}^S = \{f : S \to \mathbf{F}\}$ is the set of functions from S to $\mathbf{F}$. We can endow $\mathbf{F}^S$ with point-wise addition and scalar multiplication. That is, for $f, g \in \mathbf{F}^S$ and $\lambda \in \mathbf{F}$, the functions $f +_{\mathbf{F}^S} g$ and $\lambda \cdot_{\mathbf{F}^S} f$ are defined by

$$(f +_{\mathbf{F}^S} g)(s) := f(s) +_{\mathbf{F}} g(s),$$
$$(\lambda \cdot_{\mathbf{F}^S} f)(s) := \lambda f(s)$$

for every $s \in S$. Then $(\mathbf{F}^S, +, \cdot)$ is an $\mathbf{F}$-vector space. We also use the notation $\prod_S \mathbf{F}$ for this space and call it the **product** of copies of $\mathbf{F}$.

Proof. Let us verify some of the axioms. For example, we need to prove the equality $f + g = g + f$. We know that two functions are equal if and only if their values agree on

[3] $\mathbf{F}^0 \cong \{0\}$ means that the spaces $\mathbf{F}^0$ and $\{0\}$ are isomorphic, see Definition 3.1.40. Intuitively, it means that they are similar as vector spaces.

every element of the domain. For every $s \in S$, we have

$$\begin{aligned}(f+g)(s) &= f(s)+g(s) && \text{(definition of } +_{\mathbf{F}^S}\text{)}\\ &= g(s)+f(s) && \text{(commutativity of } +_{\mathbf{F}}\text{)}\\ &= (g+f)(s) && \text{(definition of } {}_{\mathbf{F}^S}\text{)}\end{aligned}$$

and hence $f+g=g+f$.

Let $0_{\mathbf{F}^S}\colon S \to \mathbf{F}$ be the constant function 0, that is $0(s)=0_{\mathbf{F}}$ for all $s \in S$. One easily verify that for any $s \in S$ one has $(f+0_{\mathbf{F}^S})(s) = f(s)+0 = f(s)$, so $0_{\mathbf{F}^S}$ is the zero element of $\mathbf{F}^S$.

For $f \in \mathbf{F}^S$, define $-f\colon S \to \mathbf{F}$ by $(-f)(s) := -_{\mathbf{F}}(f(s))$. One can then check that for every $s \in S$ we have

$$(f+(-f))(s) = f(s)+-f(s) = 0$$

and so $f+(-f)=0_{\mathbf{F}^S}$. The (elementary but fastidious) verification of the other 5 axioms is left to the reader. □

If S is finite, then $\mathbf{F}^S \cong \mathbf{F}^{\#S}$. In particular, $\mathbf{F}^{\varnothing} \cong \{0\}$. If S is countable (for example, $S=\{1,2,\dots,\}$), then $\mathbf{F}^S \cong \mathbf{F}^{\mathbf{N}}$.

Vector spaces of the form $\mathbf{F}^S$ include all examples we have seen so far. But not all vector spaces are of this form.

Example 2.2.10. For $\mathbf{F}$ a field, let $\mathbf{F}^{(\mathbf{N})} := \{(x_0,x_1,\dots) \mid \forall j \in \mathbf{N} : x_j \in \mathbf{F}, x_j = 0 \text{ for all but finitely many } j\}$ be the set of finitely supported infinite sequences of elements of $\mathbf{F}$, with addition and scalar multiplication defined component-wise. Then $\mathbf{F}^{(\mathbf{N})}$ is an $\mathbf{F}$-vector space.

Another important example is the space of polynomials. Let us recall its definition.

Definition 2.2.11.

Let $\mathbf{F}$ be a field. A **polynomial (with coefficient in $\mathbf{F}$)** is an expression of the form

$$p = p(x) := a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$$

where $n \in \mathbf{N}$ is an integer and x is a formal variable. The $a_i \in \mathbf{F}$ are called the **coefficients** of p.

If $p(x) = a_0+a_1x+\cdots+a_nx^n$ with $a_n \neq 0$, we define its **degree** $\deg(p)$ to be n.

We set the degree of the polynomial 0 to be $\deg(0) := -\infty$.

We write $\mathcal{P}(\mathbf{F})$ for the set of polynomials with coefficients in $\mathbf{F}$. For a fixed $n \in \mathbf{N} \cup \{-\infty\}$, we write $\mathcal{P}(\mathbf{F})_n$ for the set of polynomials of degree at most n.

To simplify the writing, we usually omit the component a_ix^i with 0 coefficient $a_i=0$. In particular, we make the identification $a_0+\cdots+a_nx^n+0x^{n+1}+\cdots+0x^{n+m} = a_0+\cdots+a_nx^n$. That is, we can erase trailing zeroes. For example, we write $1+2x^2$ for $1+0x+2x^2$. Let $p(x)=a_0+\cdots+a_mx^m$ and $q(x)=b_0+\cdots+b_nx^n$ be two polynomials with $a_m \neq 0$ and $b_n \neq 0$. They are equal if and only if $m=n$ and $a_i=b_i$ for all i. One can add polynomials

and multiply them by a scalar component-wise. For example $(1+2x+x^2)+(2+3x^2) = 3+2x+4x^2$ and $2(1+2x+x^2) = 2+4x+2x^2$. It is also possible to multiply two polynomials together, but we will not make use of this.

Example 2.2.12. The set $\mathcal{P}(\mathbf{F})$ endowed with polynomials addition and with multiplication by scalars is an $\mathbf{F}$-vector space. For n in $\{-\infty\} \cup \mathbf{N}$, the set $\mathcal{P}(\mathbf{F})_n$ is also a vector space. We have $\mathcal{P}(\mathbf{F})_{-\infty} \cong \{0\}$, $\mathcal{P}(\mathbf{F})_0 \cong \mathbf{F}$ and more generally $\mathcal{P}(\mathbf{F})_n \cong \mathbf{F}^{n+1}$. Finally, $\mathcal{P}(\mathbf{F}) \cong \mathbf{F}^{(\mathbf{N})}$.

To go further

Using ideas from Examples 2.2.9 and 2.2.10, one can build the following example. Let S be a set and let $\mathbf{F}$ be a field. Let $\mathbf{F}^{(S)} := \{f\colon S \to \mathbf{F} \mid f(s) = 0 \text{ for all but finitely many } s\}$ be the set of functions from S to $\mathbf{F}$ that are 0 almost everywhere. Then $\mathbf{F}^{(S)}$ is a subset of $\mathbf{F}^S$ and we can look at the restriction of $+_{\mathbf{F}^S}$ and $\lambda_{\mathbf{F}^S}$ to it. Endowed with these operations $\mathbf{F}^{(S)}$ is an $\mathbf{F}$-vector space. Some authors use the notation $(\mathbf{F}^S)_0$ for $\mathbf{F}^{(S)}$. We also use the notation $\bigoplus_S \mathbf{F}$ for this space and call it the **direct sum** of copies of $\mathbf{F}$. If S is finite, then the direct sum and the product agrees: $\bigoplus_S \mathbf{F} = \prod_S \mathbf{F}$.

It turns out that every $\mathbf{F}$-vector space V is isomorphic to $\mathbf{F}^{(S)}$ for some S. See the Infinite dimensional spaces box on page 71.

To go further

If $(V_\alpha)_{\alpha\in I}$ is a family of $\mathbf{F}$-vector spaces, then it is possible to define their product $\prod_{\alpha\in I} V_\alpha = \{(v_\alpha)_{\alpha\in I} \mid \forall \alpha \in I : v_\alpha \in V_\alpha\}$. One then define their direct sum $\bigoplus_{\alpha\in I} V_\alpha$ as the subset of $\prod_{\alpha\in I} V_\alpha$ consisting of elements $(v_\alpha)_{\alpha\in I}$ that are 0 for all but finitely many α. Both $\prod_{\alpha\in I} V_\alpha$ and $\bigoplus_{\alpha\in I} V_\alpha$ are $\mathbf{F}$-vector spaces.

2.2.2 General properties of vector spaces

Let V be a vector space over a field $\mathbf{F}$. Using only the definition (the 8 axioms) we will prove some general properties of V.

Lemma 2.2.13. *Let V be a vector space. The zero (additive identity of V) is unique. That is, there exists a unique $0 \in V$ such that for every v we have $0 + v = v$.*

Proof. Suppose 0 and $0'$ are two additive identities in V. We need to prove they are equal. We have

$$\begin{aligned} 0' &= 0 + 0' && \text{(0 is a zero)} \\ &= 0' + 0 && \text{(commutativity of } +\text{)} \\ &= 0. && \text{($0'$ is a zero)} \end{aligned}$$

So any two additive identities are equal, or equivalently there exists a unique additive identity. □

Lemma 2.2.14. *Let V be a vector space. For every $v \in V$ the additive inverse is unique.*

Proof. Suppose w and w' are two additive inverses of v. Then

$$w = 0 + w = (v + w') + w = v + (w' + w) = v + (w + w') = (v + w) + w' = 0 + w' = w',$$

where we used that 0 is the additive identity that w' is an inverse of v, associativity, commutativity, associativity once again, that w is an inverse of v and finally that 0 is the additive identity. □

In the above proof, we have detailed every step explicitly. However, using commutativity and associativity, it is fine to directly write the shorter $(v + w') + w = (v + w) + w'$.

Lemma 2.2.15. *Let v and w be two elements of a vector space. If $v + w = v$, then $w = 0$.*

Proof. $w = v + w - v = v - v = 0$. □

The previous lemma might seem to be a repetition of Lemma 2.2.14. This is not the case, as we only suppose that w behaves like 0 for one vector v, but a priori not necessarily for all vectors of V.

Lemma 2.2.16. *Let V be an $\mathbf{F}$-vector space. For every $v \in V$ and every $\lambda \in \mathbf{F}$ we have:*

1. $0_{\mathbf{F}} \cdot v = 0_V$;
2. $\lambda \cdot 0_V = 0_V$;
3. $\lambda v = 0$ *if and only if* $\lambda = 0_{\mathbf{F}}$ *or* $v = 0_V$.

Proof. For teh first equality, we have $0_{\mathbf{F}} \cdot v = (0_{\mathbf{F}} + 0_{\mathbf{F}}) \cdot v = 0_{\mathbf{F}} \cdot v + 0_{\mathbf{F}} \cdot v$. By subtracting $0_{\mathbf{F}} \cdot v$ on both sides we obtain $0_V = 0_{\mathbf{F}} \cdot v$.

The proof of the second equality is similar, except that this time we use left distributivity instead of right distributivity. We have $\lambda \cdot 0_V = \lambda \cdot (0_V + 0_V) = \lambda \cdot 0_V + \lambda \cdot 0_V$. By subtracting $\lambda \cdot 0_V$ on both sides we obtain $0_V = \lambda \cdot 0_V$.

Finally, we already know that the condition $\lambda = 0$ or $v = 0$ is sufficient for $\lambda v = 0$. We now prove the necessity. Suppose that $\lambda \neq 0$. We need to show that $v = 0$. Then, since $\mathbf{F}$ is a field, there exists λ^{-1} such that $\lambda^{-1}\lambda = 1$. By multiplying both sides of the equation by it we obtain $\lambda^{-1} \cdot (\lambda \cdot v) = \lambda^{-1} \cdot 0 = 0$. So we have

$$0 = (\lambda^{-1}\lambda) \cdot v = 1 \cdot v = v.$$ □

Lemma 2.2.17 (Tutorial 2, Question 1.)**.** *For every $v \in V$ we have $(-1) \cdot v = -v$, where -1 is the additive inverse of 1 in $\mathbf{F}$ and $-v$ the additive inverse of v in V.*

2.3 Subspaces and operations on them

In this section we introduce subspaces: the subsets of a vector space that are themselves vector spaces. We will also investigate some operations on them.

2.3.1 Subspaces of a vector space

Sets have subsets, and vector spaces have subspaces. Intuitively, a subspace is a subset that is also a vector space itself. Studying subspaces of a vector space V helps us to understand V and can also produce new interesting examples.

Before seing the formal definition, let us look at some examples. For now, these are just informal examples and we will come back to them later.

Example 2.3.1. Let $V = \mathbf{R}$. Then V has only two subspaces: $\mathbf{R}$ and $\{0\}$.

Example 2.3.2. Let $V = \mathbf{R}^2$. Then the subspaces are $\mathbf{R}^2$, the lines containing the origin (see the left part of Figure 2.3) and $\left\{\begin{bmatrix}0\\0\end{bmatrix}\right\}$ (the zero vector).

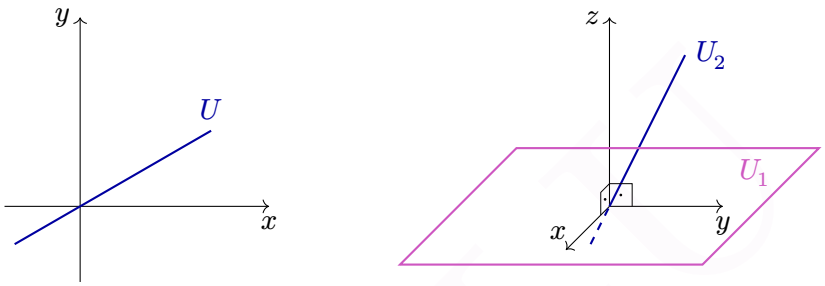


Figure 2.3: On the left: a line containing the origin in $\mathbf{R}^2$. On the right: a plane and a line containing the origin in $\mathbf{R}^3$.

Example 2.3.3. Let $V = \mathbf{R}^3$. Then the subspaces are $\mathbf{R}^3$, the planes containing the origin, the lines containing the origin (see the right part of Figure 2.3) and $\{[0,0,0]^\mathsf{T}\}$ (the zero vector).

Definition 2.3.4.

Let $(V, +, \cdot)$ be a vector space and let $U \subseteq V$ be a subset. Then U is a **subspace of** V if $(U, +, \cdot)$ is itself a vector space.

Remark 2.3.5.

We have

$$+_V \colon V \times V \longrightarrow V, \qquad \cdot_V \colon \mathbf{F} \times V \longrightarrow V.$$

If U is a subset of V, then $U \times U$ is a subset of $V \times V$ and $\mathbf{F} \times U$ is a subset of $\mathbf{F} \times V$. We therefore have the operations

$$+_V\big|_{U\times U} \colon U \times U \longrightarrow V, \qquad \cdot_V\big|_{\mathbf{F}\times U} \colon \mathbf{F} \times U \longrightarrow V.$$

When we say that $(U, +, \cdot)$ is a vector space, this means that the images $\operatorname{Im}(+_V|_{U\times U})$ and $\operatorname{Im}(\cdot_V|_{\mathbf{F}\times U})$ are both contained in U and that

$(U, +_V|_{U\times U}, \cdot_V|_{\mathbf{F}\times U})$ satisfies the 8 axioms of a vector space.

The following simple result directly follows from the definition of a subspace.

Lemma 2.3.6. *Let W be a vector space, $V \subseteq W$ be a subspace and $X \subseteq V$ be a subset. Then X is a subspace of V if and only if it is a subspace of W.*

Let us use Definition 2.3.4 to show that some subsets are not subspaces.

Example 2.3.7. Let $V = \mathbf{R}$ and let $X = \{x\} \subseteq V$ consist of exactly one point. Then X is a subspace if and only if $x = 0$. On one hand, it is clear that $\{0\}$ is a subspace. On the other hand, we want $+$ to be an internal operation, so $x + x = 2x$ should be an element of X. But this is possible if and only if $2x = x$, that is if and only if $x = 0$.

Example 2.3.8. Let $V = \mathbf{R}^2$ and let $X_1 = \left\{\begin{bmatrix} x \\ 1 \end{bmatrix} \mid x \in \mathbf{R}\right\}$, $X_2 = \left\{\begin{bmatrix} x \\ x \end{bmatrix} \mid x \in \mathbf{R}_{\geq 0}\right\}$ and $X_3 = \left\{\begin{bmatrix} x \\ x \end{bmatrix} \mid x \in \mathbf{R}\right\} \cup \left\{\begin{bmatrix} x \\ -x \end{bmatrix} \mid x \in \mathbf{R}\right\}$ be three subsets of V. Then X_1 is not a subspace as it does not contain 0_V. X_2 is not a subspace as $\cdot$ is not an internal operation. Indeed, the vector $\begin{bmatrix} 1 \\ 1 \end{bmatrix}$ belongs to X_2, but $\begin{bmatrix} -1 \\ -1 \end{bmatrix} = -1\begin{bmatrix} 1 \\ 1 \end{bmatrix}$ does not. Finally, X_3 is not a subspace as $+$ is not an internal operation: both $\begin{bmatrix} 1 \\ 1 \end{bmatrix}$ and $\begin{bmatrix} -1 \\ 1 \end{bmatrix}$ are in X_3, but their sum $\begin{bmatrix} 0 \\ 2 \end{bmatrix}$ is not.

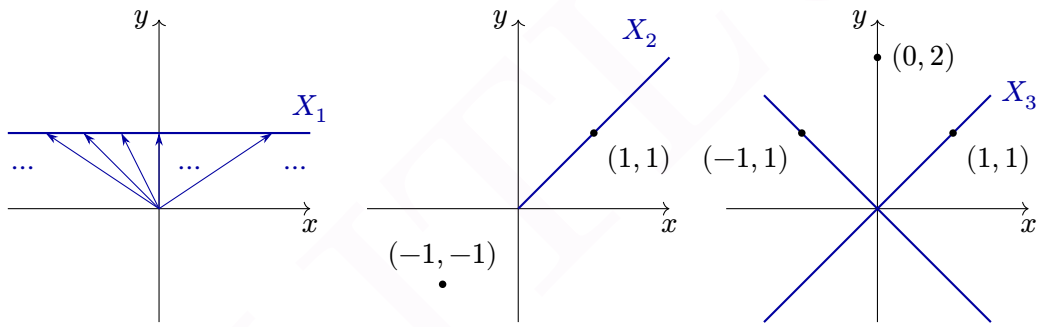


Figure 2.4: Subsets of $\mathbf{R}^2$ that are not subspaces. On the left, both the subset X_1 (the line) and its elements (the arrows) are represented.

Example 2.3.9. For every $m \leq n$, the set $\mathcal{P}(\mathbf{F})_m$ of polynomials of degree at most m is a subspace of $\mathcal{P}(\mathbf{F})_n$. They are both subspaces of $\mathcal{P}(\mathbf{F})$

Remark 2.3.10.

When talking about a subspace, we need to stat clearly of which vector space it is a subspace. We also need $\mathbf{F}$ to be explicit, as it does matter.

Example 2.3.11. Let $V = \mathbf{C}$ be viewed as a complex vector space. Then $U = \mathbf{R} \subseteq V$ is not a subspace. Indeed, 1 belongs to U, but $\mathrm{i} = \mathrm{i} \cdot 1$ does not.

However, if we decide to view $V = \mathbf{C}$ as a real vector space, then one can check that U is a subspace.

Definition 2.3.4 has the advantage of being natural: a *subspace* is a *sub*set that is also a vector *space* (for the restriction to U of the operations of V). The disadvantage of Definition 2.3.4 is that it is impractical: we need to check that $+$ and $\cdot$ are internal operations and that they satisfy the 8 axioms of a vector space. Luckily, we can use the following simple criteria to decide if a subset is a subspace.

Proposition 2.3.12. *Let V be an $\mathbf{F}$-vector space and let $X \subseteq V$ be a subset. Then the following are equivalent:*

I. X is a subspace;

II. The following three conditions hold:

1. $0_V \in X$, *(X contains 0)*
2. $\forall x, y \in X : x + y \in X$, *($+$ is an internal operation)*
3. $\forall \lambda \in \mathbf{F}, \forall x \in X : \lambda x \in X$; *($\cdot$ is an internal operation)*

III. The following two conditions hold:

1. $0_V \in X$,
2'. $\forall \lambda \in \mathbf{F}, \forall x, y \in X : \lambda x + y \in X$.

Proof. "I $\implies$ II" If X is a subspace, then both the image of $+$ and $\cdot$ are contained in X by definition. Moreover, since X is a vector space, it contains at least one element: 0_X, the zero element for $+_X = +|_{X\times X}$. So $0_V = 0_{\mathbf{F}} \cdot 0_X$ is also in X. Moreover, it follows from unicity of the zero element that $0_X = 0_V$.

"II $\implies$ I" Suppose that Properties 1 to 3 hold. Then we have a set X with two operations, $+ : X \times X \to X$ and $\cdot : \mathbf{F} \times X \to X$ (the restrictions of $+_V$ and $\cdot_V$) and an element 0_V. For every $x \in X$, we have $x \in V$ and thus $0_V + x = x$. That is, 0_V is a zero element for $+ = +_X$. There also exists an element $-x \in V$ such that $x + (-x) = 0_V = 0_X$. Since $-x = -1 \cdot x$ it belongs to X by 3. It remains to check the 6 other axioms of the definition of a vector space. They all follow from the fact that V is a vector space and that $+$ and $\cdot$ are the restrictions of $+_V$ and $\cdot_V$. For example, for all x and y in X, we have $x, y \in V$. Therefore, $x +_X y = x +_V y = y +_V x = y +_X x$, where the second equality is the commutativity of $+_V$.

"II $\implies$ III" Applying first 3 to λ and x and then 2 to λx and y gives 2'.

"III $\implies$ II" Property 3 follows from putting $\lambda = 1$ in 2', while if 1 holds, then 2 follows from using $y = 0$ in 2'. □

All three conditions of Proposition 2.3.12.II are important. The first one is basically equivalent to X being non-empty, see Remark 2.3.13. In Example 2.3.8, the subset X_2 is closed under addition, but not under scalar multiplication. The subset X_3 is closed under scalar multiplication, but not under addition.

While the three conditions of Proposition 2.3.12.II are conceptually important, using Proposition 2.3.12.III allows for shorter proofs as we can check together that X is closed under addition and scalar multiplication.

Remark 2.3.13.

Given either condition 3 or 2', Condition 1 is equivalent to the fact that X is not empty. Indeed, suppose X is not empty, therefore there exists $x \in X$. Then if condition 3 holds, taking $\lambda = 0$ we have and $0x = 0$ in X. If it is condition 2' that holds, then taking $\lambda = -1$ and $y = x$ we have $(-1)x + x = 0$ in X.

Remark 2.3.14.

When checking that X is a subspace of V, you should not forget the "hidden condition" 0: X is a subset of V. For example, $\mathbf{R}$ is not a subspace of $\mathbf{R}^2$, but $\left\{\begin{bmatrix} x \\ 0 \end{bmatrix} \mid x \in \mathbf{R}\right\}$ is (and so are $\left\{\begin{bmatrix} 0 \\ x \end{bmatrix} \mid x \in \mathbf{R}\right\}$ or $\left\{\begin{bmatrix} 3x \\ -2x \end{bmatrix} \mid x \in \mathbf{R}\right\}$).

Using Proposition 2.3.12, it is easy to provide plenty of examples and counter-examples of subspaces.

Example 2.3.15. Let V be a vector space. Then

1. $\varnothing$ is NOT a subspace;
2. $\{0_V\}$ is a subspace;
3. V is a subspace.

For the first assertion, 0_V does not belong to $\varnothing$. For the second assertion, $0 + 0 = 0$ and $\lambda 0 = 0$, so (the restrictions of) $+$ and $\cdot$ are internal operations on $\{0_V\}$. The last assertion is tautologic.[4]

Example 2.3.16. Let $b \in \mathbf{F}$ and define $X := \{[x_1, x_2, x_3, x_4]^\mathsf{T} \in \mathbf{F}^4 \mid x_3 = 5x_4 + b\}$. Then X is a subspace of $\mathbf{F}^4$ if and only if $b = 0_\mathbf{F}$.

Proof. "$\Rightarrow$" If X is a subspace, then $[0, 0, 0, 0]^\mathsf{T} = 0_{\mathbf{F}^4} \in X$ and so $b = 0$.

"$\Leftarrow$" Suppose that $b = 0$. Then $0_{\mathbf{F}^4}$ belongs to X. If $[x_1, x_2, x_3, x_4]^\mathsf{T}$ and $[y_1, y_2, y_3, y_4]^\mathsf{T}$ are in X, then both $x_3 = 5x_4$ and $y_3 = 5y_4$. So for any scalar λ we have

$$\lambda[x_1, x_2, x_3, x_4]^\mathsf{T} + [y_1, y_2, y_3, y_4]^\mathsf{T} = [\lambda x_1 + y_1, \lambda x_2 + y_2, \lambda x_3 + y_3, \lambda x_4 + y_4]^\mathsf{T}$$

in X since $\lambda x_3 + y_3 = \lambda 5x_4 + 5y_4 = 5(\lambda x_4 + y_4)$. □

Example 2.3.17. $\mathcal{P}(\mathbf{F})_m$ is a subspace of $\mathcal{P}(\mathbf{F})_n$ if and only if $m \leq n$ (so if and only if $\mathcal{P}(\mathbf{F})_m \subseteq \mathcal{P}(\mathbf{F})_n$). All the $\mathcal{P}(\mathbf{F})_m$ are subspaces of $\mathcal{P}(\mathbf{F})$.

We therefore have an infinite chain of subspaces:

$$\{0\} = \mathcal{P}(\mathbf{F})_{-\infty} \subsetneq \mathcal{P}(\mathbf{F})_0 \subsetneq \mathcal{P}(\mathbf{F})_1 \subsetneq \cdots \subsetneq \mathcal{P}(\mathbf{F})_n \subsetneq \cdots \subsetneq \mathcal{P}(\mathbf{F}).$$

Example 2.3.18. The set $\mathcal{C}^0([0,1]) := \{f \colon [0,1] \to \mathbf{R} \mid f \text{ continuous}\}$ of continuous functions from $[0, 1]$ to $\mathbf{R}$ is a subspace of $\mathbf{R}^{[0,1]}$.

[4] A tautology is a statement that is trivially true, by the fact of repeating essentially two times the same thing. It comes from ancient greek ταυτολογία: identical logic.

Proof. Recall that f is continuous at x_0 if and only if $\lim_{x\to x_0} f(x) = f(x_0)$. The constant zero function $0_{\mathbf{R}^{[0,1]}}$ is the zero element of $\mathbf{R}^{[0,1]}$. This is a continuous function and hence belongs to $\mathcal{C}^0([0,1])$. Indeed, for every $x_0 \in [0,1]$ we have $\lim_{x\to x_0} 0_{\mathbf{R}^{[0,1]}}(x) = 0 = 0_{\mathbf{R}^{[0,1]}}(x_0)$.

Let f and g be two elements of $\mathcal{C}^0([0,1])$. Then for every scalar λ and any $x_0 \in [0,1]$ we have

$$(\lambda f + g)(x_0) = \lambda f(x_0) + g(x_0) = \lambda \lim_{x\to x_0} f(x) + \lim_{x\to x_0} g(x) = \lim_{x\to x_0} (\lambda f + g)(x)$$

and thus $\lambda f + g$ is in $\mathcal{C}^0([0,1])$. □

Example 2.3.19. The set $\mathcal{C}^1(\mathbf{R}) \coloneqq \{f \colon \mathbf{R} \to \mathbf{R} \mid f \text{ differentiable and } f' \text{ continuous}\}$ of functions from $\mathbf{R}$ to itself that are differentiable and have a continuous first derivative, is a subspace of $\mathbf{R}^{\mathbf{R}}$. Actually, we have $\mathcal{C}^1(\mathbf{R}) \subsetneq \mathcal{C}^0(\mathbf{R}) \subsetneq \mathbf{R}^{\mathbf{R}}$, with each member a subspace in the next one.

Proof. We just need to check that the 0 function is differentiable, that the sum of two differentiable functions is differentiable and that the scalar product of scalar and a differentiable function is still differentiable. These are standard and easy results from analysis and we will not write down their proof here. □

Example 2.3.20. More generally, for every integer n, one can define $\mathcal{C}^m(\mathbf{R}) \coloneqq \{f \colon \mathbf{R} \to \mathbf{R} \mid f^{(n)} \text{ exists and is continuous}\}$ of functions from $\mathbf{R}$ to itself that are n times differentiable and have a continuous n^{th} derivative. We also define $\mathcal{C}^\infty(\mathbf{R}) \coloneqq \{f \colon \mathbf{R} \to \mathbf{R} \mid \forall n \in \mathbf{N} : f^{(n)} \text{ exists}\}$ the space of **smooth real functions**. We then have an infinite chain of subspaces

$$\mathcal{C}^\infty(\mathbf{R}) \subsetneq \cdots \subsetneq \mathcal{C}^n(\mathbf{R}) \subsetneq \cdots \subsetneq \mathcal{C}^1(\mathbf{R}) \subsetneq \mathcal{C}^0(\mathbf{R}) \subsetneq \mathbf{R}^{\mathbf{R}}$$

Example 2.3.21. Let b be any real number. Then the set $X \coloneqq \{f \in \mathcal{C}^1((0,3)) \mid f'(2) = b\}$ is a subspace of $\mathcal{C}^1((0,3))$ if and only if $b = 0$.

Proof. We have 0 in X if and only if $b = 0'(2) = 0$. So, $b = 0$ is a necessary condition for X to be a vector space.

It remains to show that if $b = 0$, then X is closed under addition and scalar multiplication. Let f and g be two elements of X and let $\lambda \in \mathbf{R}$ be a scalar. Then

$$(\lambda f + g)'(2) = \lambda f'(2) + g'(2) = \lambda 0 + 0 = 0.$$

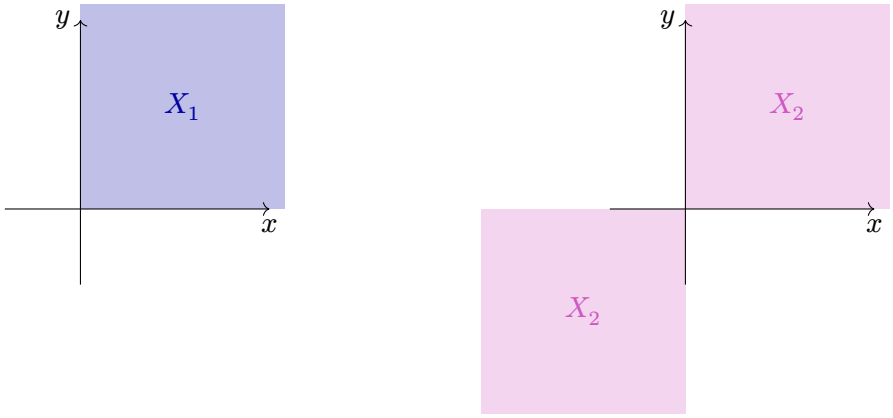
So $\lambda f + g$ is in X. □

Example 2.3.22. The set $U \coloneqq \{(x_0, x_1, \dots) \in \mathbf{R}^{\mathbf{N}} \mid \lim_{i\to\infty} x_i = 0\}$ is a subspace of $\mathbf{R}^{\mathbf{N}}$. We even have $\mathbf{R}^{(\mathbf{N})} \subsetneq U \subsetneq \mathbf{R}^{\mathbf{N}}$, with each member a subspace in the next one.

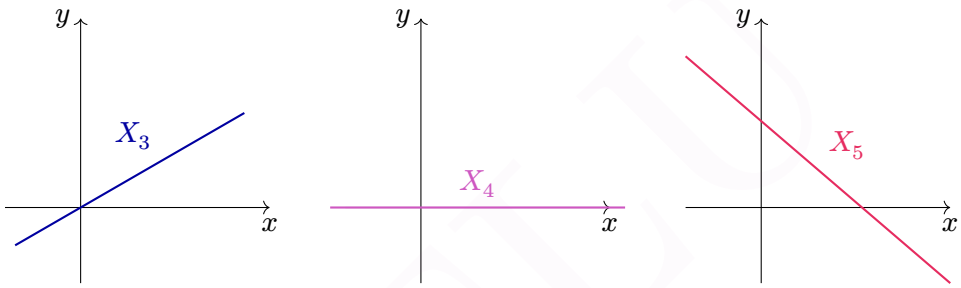
The proof is left as an exercise to the reader.

Exercise 2.3.23. Which of the following are subspaces of $\mathbf{R}^2$? Consider that the figures extend in an obvious way to the infinity. For example, $X_1 = \{\left[\begin{smallmatrix} x \\ y \end{smallmatrix}\right] \in \mathbf{R}^2 \mid x, y \geq 0\}$ and $X_1 = \{\left[\begin{smallmatrix} x \\ y \end{smallmatrix}\right] \in \mathbf{R}^2 \mid xy \geq 0\}$.

a.



b.



Solution. a. X_1 is not a subspace as $(1,1)$ belongs to X_1, but $-1 \cdot (1,1) = (-1,-1)$ does not. X_2 is not a subspace despite being closed under scalar multiplication. Indeed both $(2,1)$ and $(-1,-2)$ are in X_2, but $(2,1)+(-1,-2) = (1,-1)$ is not.

b. X_3 and X_4 are lines containing the origin and so are subspaces. X_5 does not contain $(0,0)$ and therefore is not a subspace.

□

2.3.2 Sums of subspaces

Recall that if $X \subseteq Z$ and $Y \subseteq Z$ are two subsets, then $X \cup Y$ is again a subset of Z. Furthermore, $X \cup Y$ is the smallest subset of Z containing both X and Y.

Question 2.3.24. What about subspaces $U, W \subseteq V$ of a vector space? Is $U \cup W$ also a subspace?

Answer. The answer is no in general. For example, let $V = \mathbf{R}^2$ and let $U_x = \left\{ \begin{bmatrix} x \\ 0 \end{bmatrix} \mid x \in \mathbf{R} \right\}$ be the x-axis and $U_y = \left\{ \begin{bmatrix} 0 \\ y \end{bmatrix} \mid y \in \mathbf{R} \right\}$ be the y-axis. Then both $\begin{bmatrix} 1 \\ 0 \end{bmatrix}$ and $\begin{bmatrix} 0 \\ 1 \end{bmatrix}$ belong to $U \cup W$, but their sum $\begin{bmatrix} 1 \\ 0 \end{bmatrix} + \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \end{bmatrix}$ does not. So $U_x \cup U_y$ is not a subspace. ■

Exercise 2.3.25. Let V be a vector space and let $U, W \subseteq V$ be two subspaces. Show that $U \cup W$ is a subspace if and only if either $U \subseteq W$ or $W \subseteq U$.

Solution. If $U \subseteq W$, then $U \cup W = W$ is a subspace. The situation is similar if $W \subseteq U$.

Suppose now that $U \not\subseteq W$ and $W \not\subseteq U$. This is equivalent to the simultaneous existence of some $u \in U \setminus W$ and some $w \in W \setminus U$. We have both u and w in $U \cup W$, but we claim that $u + w$ is not in $U \cup W$. Indeed, suppose that $u + w = u' \in U$. Then $w = -u + u'$ is also in U which is a contradiction. Similarly, $u + w$ cannot belong to W. □

We have seen that $U \cup W$ is not the smallest subspace of V containing both U and V. Does such a subspace exist? If yes, how can we construct it?

Definition 2.3.26.

Let V be a vector space and let X_1, X_2, ..., X_n be non-empty subsets of V. Their **sum** is the subset

$$\sum_{i=1}^{n} X_i = X_1 + X_2 + \cdots + X_n := \{v_1 + v_2 + \cdots + v_n \mid \forall i \in \{1, \dots, n\} : v_i \in X_i\}.$$

Remark 2.3.27.

The operation $\sum_{i=1}^{n} X_i$ is defined only if all the X_i are subsets of the same vector space V.

The sum of subsets satisfies some elementary but useful properties.

Lemma 2.3.28. *Let V be vector space and let X, Y be non-empty subsets of V. Then*

1. $X + Y = Y + X$;
2. $X + \{0\} = X$;
3. $X + V = V$.

Proof. The proof is left as an exercise to the reader. See Tutorial 2, Question 6 for the first equality. □

We have geometric examples of sum of subsets.

Example 2.3.29. Let $X := \{[x, 0, 0]^\mathsf{T} \mid x \in [0, 1]\}$, $Y := \{[0, y, 0]^\mathsf{T} \mid y \in [0, 1]\}$ and $Z := \{[0, 0, z]^\mathsf{T} \mid z \in [0, 1]\}$ be initial segment of size 1 of the x, y and z-axes in $\mathbf{R}^3$. Then $X + Y = \{[x, y, 0]^\mathsf{T} \mid x, y \in [0, 1]\}$, $X + Z = \{[x, 0, z]^\mathsf{T} \mid x, z \in [0, 1]\}$ and $Y + Z = \{[0, y, z]^\mathsf{T} \mid y, z \in [0, 1]\}$. We also have $X + Y + Z = \{[x, y, z]^\mathsf{T} \mid x, y, z \in [0, 1]\}$, a cube of size 1, see Figure 2.5.

Finally, we present an algebraic example.

Example 2.3.30. Let $U := \{[x, x, z, z]^\mathsf{T} \mid x, z \in \mathbf{F}\}$ and $W := \{[x, x, x, t]^\mathsf{T} \mid x, t \in \mathbf{F}\}$ be two subspaces of $\mathbf{F}^4$. Then $U + W = \{[x, x, z, t]^\mathsf{T} \mid x, z, t \in \mathbf{F}\} =: Z$.

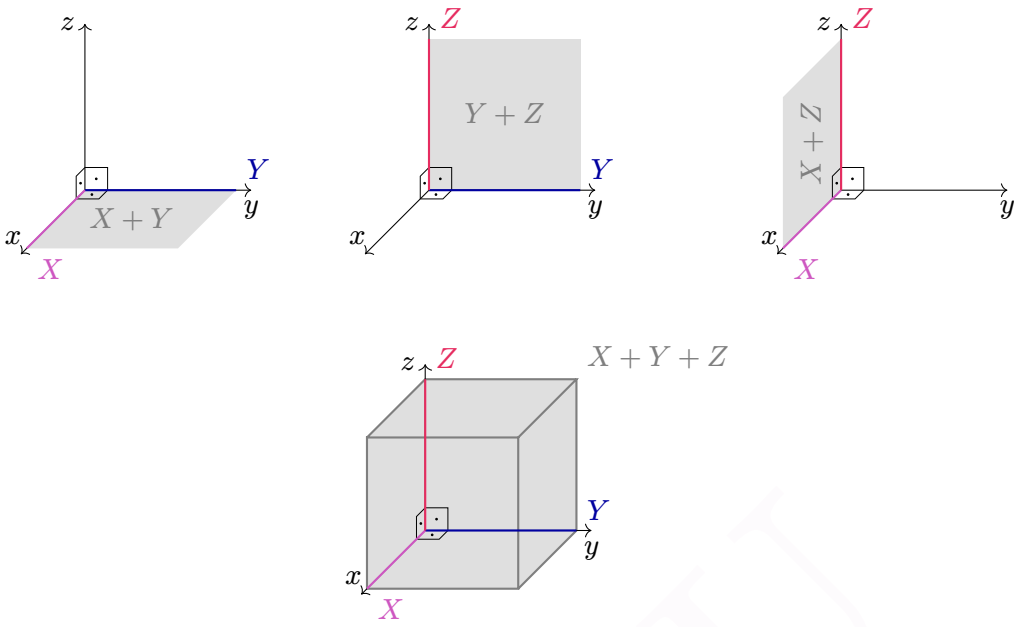


Figure 2.5: Sum of some subsets of $\mathbf{R}^3$.

Indeed, we have

$$\begin{aligned} U + W &= \{[a, a, b, b]^\mathsf{T} \mid a, b \in \mathbf{F}\} + \{[c, c, c, d]^\mathsf{T} \mid c, d \in \mathbf{F}\} \\ &= \{[a + c, a + c, b + c, b + d]^\mathsf{T} \mid a, b, c, d \in \mathbf{F}\}. \end{aligned}$$

By letting $x := a + c$, $z := b + c$, $t := b + d$, we have $U + W \subseteq Z$. For the inclusion $Z \subseteq U + W$, we need to solve

$$\begin{cases} a + c = x \\ b + c = y \\ b + d = z \end{cases}$$

for a, b, c and d in $\mathbf{F}$. One possible solution is to take $b = 0$, $d = z$, $c = y$ and $a = x - y$.

To go further

It is possible to define the sum of an infinite family of *subspaces*. The trick to define an infinite sum is that we look only at combinations containing finitely many non-zero vectors. Formally speaking, if $(U_\alpha)_{\alpha \in I}$ is a non-empty family of subspaces of a vector space V, we can defined its sum:

$$\sum_{\alpha \in I} U_\alpha := \left\{ \sum_{\alpha \in I} u_\alpha \;\middle|\; \forall \alpha \in I : u_\alpha \in U_\alpha \text{ and } u_\alpha = 0 \text{ for all but finitely many } \alpha \right\}.$$

Observe that the sum of infinitely many subsets is well-defined only if all the U_α contain 0, which is the case if they are subspaces.

We have defined the sum of general subsets of a vector space. The following result shows that the sum of subspaces is particularly interesting.

Theorem 2.3.31.

Let V be a vector space and let $(U_\alpha)_{\alpha\in I}$ be a non-empty family of subspaces. Then the sum $\sum_{\alpha\in I} U_\alpha$ is the smallest subspace of V containing all the U_α.

Proof. We will write the proof for a finite family of subspaces $(U_1, \dots, U_n)$, the general case is similar. We need to prove three things:

1. $U := U_1 + \cdots + U_n$ is a subspace;
2. U contains all the U_i;
3. U is the smallest: if another subspace W contains all the U_i, then $U \subseteq W$.

We have $0_V \in U_1 \subseteq U$, so U contains 0_V. Now let u and v be two elements of U and let λ be a scalar. By definition, there exists $u_i, v_i \in U$ such that $u = u_1 + \cdots + u_n$ and $v = v_1 + \cdots + v_n$. We have

$$\begin{aligned}\lambda u + v &= \lambda(u_1 + \cdots + u_n) + v_1 + \cdots + v_n \\ &= (\lambda u_1 + v_1) + \cdots + (\lambda u_i + v_i)\end{aligned}$$

with the $\lambda u_i + v_i \in U_i$. This finishes the proof that U is a subspace.

For every $u_i \in U_i$, we have $u_i = 0 + \cdots + 0 + u_i + 0 + \cdots + 0 \in U$ since 0 belongs to all the U_i. We conclude that U contains U_i.

Finally, let W be a subspace containing all the U_i and let u be an element of U. There exists $u_i \in U_i \subseteq W$ such that $u = u_1 + \cdots + u_n$. But then u is a sum of elements of W and hence still in W. So $U \subseteq W$ and thus U is the smallest subspace of V containing all the U_i. □

Inspired by Theorem 2.3.31 and because $\{0\}$ is the smallest subspace containing $\varnothing$, we define a sum over an empty family to be the $\{0\}$ subspace: $\sum_{\alpha\in\varnothing} U_\alpha := \{0\}$. We also define an empty sum of vectors to be the 0 vector: $\sum_{\alpha\in\varnothing} v_\alpha := 0$.

Before introducing our next definition, let us see one last example of the sum of subspaces.

Example 2.3.32. Let $U = \{[x, y, 0]^\mathsf{T} \mid x, y \in \mathbf{F}\}$ and $W = \{[0, y, z]^\mathsf{T} \mid y, z \in \mathbf{F}\}$. These are two subspaces of $\mathbf{F}^3$ and we have $U + W = \mathbf{F}^3$.

In the above example, intuitively (see Definition 2.4.39 for a formal definition) both U and W are of dimension 2, while $\mathbf{F}^3$ is of dimension 3. So we have the sum of two subspaces of dimension 2 being equal to a space of dimension 3, not $2+2=4$. The above "dimension problem" is due to the fact that $U \cap W = \{[0, y, 0]^\mathsf{T} \mid y \in \mathbf{F}\}$ is of dimension

1.[5] Actually, the problem steams from the fact that $[1,1,1]^\mathsf{T} \in \mathbf{F}^3$ can be written in two different ways:

$$[1,1,1]^\mathsf{T} = [1,1,0]^\mathsf{T} + [0,0,1]^\mathsf{T} \quad \text{but also} \quad [1,1,1]^\mathsf{T} = [1,0,0]^\mathsf{T} + [0,1,1]^\mathsf{T}.$$

In order to overcome the above problem, we introduce a new definition.

Definition 2.3.33.

Let V be a vector space and let U_1,..., U_n be subspaces. The sum $U = U_1 + \cdots + U_n$ is **direct** if for any $u \in U$ there exists a unique way to decompose u as $u = u_1 + \cdots + u_n$ with $u_i \in U_i$. In this case, we write $U_1 \oplus U_2 \oplus \cdots \oplus U_n$ for U.

To go further

It is not a coincidence if the name and the notation for the direct sum of subspaces $U_1 \oplus U_2$ are identical to the ones for the direct sum of vector spaces of Example 2.2.6. The former is sometimes called the inner or internal direct sum while the later is called the external direct sum.
If U and V are two $\mathbf{F}$-vector spaces, then $\tilde{U} := \{(u,0) \mid u \in U\}$ is a subspace of $U \oplus V$, which is a copy of U. We similarly have a copy $\tilde{V}$ of V inside $U \oplus V$. One easily verify that $\tilde{U} + \tilde{V}$ is an internal direct sum, equal to the whole space. That is, the external direct sum $U \oplus V$ is equal to the internal direct sum $\tilde{U} \oplus \tilde{V}$.

To go further

One can of course define direct sums for an arbitrary family $(U_\alpha)_{\alpha \in I}$ of subspaces. In this context, the sum $U = \sum_{\alpha \in I} U_\alpha$ is direct, written $\bigoplus_{\alpha \in I} U_\alpha$, if for any $u \in U$ there exists a unique way to decompose u as $u = \sum_{\alpha \in I} u_\alpha$ with the $u_\alpha \in U_\alpha$ (and with $u_\alpha = 0$ for all but finitely many α).

Remark 2.3.34.

The notation $U = U_1 \oplus U_2$ means two things. Firstly, that $U = U_1 + U_2$ and secondly that for every $u \in U$ the decomposition $u = u_1 + u_2$ is unique.

As an example, the sum $U + W = \mathbf{F}^3$ of Example 2.3.32 is not direct.

Example 2.3.35. Let $U_{x,y} = \{[x,y,0]^\mathsf{T} \mid x,y \in \mathbf{F}\}$ and $U_z = \{[0,0,z]^\mathsf{T} \mid z \in \mathbf{F}\}$. Then $\mathbf{F}^3 = U_{x,y} \oplus U_z$. It is trivial that $U_{x,y} + U_z = \mathbf{F}^3$, it hence only remains to prove that the sum is direct. Let $v = [a,b,c]^\mathsf{T}$ be any element of $\mathbf{F}^3$ and let $v = u + w \in U_{x,y} + U_z$ be a decomposition with $u \in U_{x,y}$ and $w \in U_z$. So $u = [x,y,0]^\mathsf{T}$ and $w = [0,0,z]^\mathsf{T}$ for some x, y and z in $\mathbf{F}$. Since $v = u + w$ we have $[a,b,c]^\mathsf{T} = [x+0, y+0, 0+z]^\mathsf{T}$ and we conclude that $x = a$, $y = b$ and $z = c$. That is, both u and w are uniquely determined by v, which proves that the sum is direct.

[5] We will see in Theorem 2.4.51 that the correct formula for the dimension of $\mathbf{R}^3$ in this example is $3 = 2 + 2 - 1$.

Example 2.3.36. Let n be a positive integer. For each i in $\{1, \dots, n\}$, let $U_i \subseteq \mathbf{F}^n$ be the subspace

$$U_i = \left\{ \begin{array}{c|c} 1 & 0 \\ \vdots & \vdots \\ i-1 & 0 \\ i & x \\ i+1 & 0 \\ \vdots & \vdots \\ n & 0 \end{array} \;\middle|\; x \in \mathbf{F} \right\} \subseteq \mathbf{F}^n$$

(all non i-coordinates are 0). Finally, let $W = \{[x, \dots, x]^\mathsf{T} \mid x \in \mathbf{F}\} \subseteq \mathbf{F}^n$ be the diagonal subspace. Then $\mathbf{F}^n = U_1 \oplus \cdots \oplus U_n = U_1 \oplus \cdots \oplus U_{n-1} \oplus W$.

The proof of first equality is easy and left to the reader. So let v be any element of $\mathbf{F}^n$. That is $v = [x_1, \dots, x_n]^\mathsf{T}$ for some $x_i \in \mathbf{F}$ (uniquely determined by v). Then

$$v = [x_1 - x_n, 0, \dots, 0]^\mathsf{T} + [0, x_2 - x_n, 0, \dots, 0]^\mathsf{T} + \cdots + [0, \dots, 0, x_{n-1} - x_n, 0]^\mathsf{T} + [x_n, \dots, x_n]^\mathsf{T}$$

is in $U_1 + \cdots + U_{n-1} + W$ and so $\mathbf{F}^n = U_1 + \cdots + U_{n-1} + W$. Finally, let $v = u_1 + \cdots + u_{n-1} + w$ be any decomposition with the $u_i \in U_i$ and $w \in W$. Since the n^{th} coordinate of all u_i is 0, we necessarily have $w = [x_n, \dots, x_n]^\mathsf{T}$. Therefore,

$$v - w = [x_1 - x_n, \dots, x_{n-1} - x_n, 0]^\mathsf{T} = u_1 + \cdots + u_{n-1}.$$

Since the i^{th} coordinate of u_j is 0 if $i \neq j$, we conclude that $u_i = [0, \dots, 0, x_i - x_n, 0, \dots, 0]^\mathsf{T}$. We have just proved that the decomposition is unique and thus that the sum is direct.

Example 2.3.37. Let $U_{x,y} = \{[x, y, 0]^\mathsf{T} \mid x, y \in \mathbf{F}\}$, $W = \{[0, y, y]^\mathsf{T} \mid y \in \mathbf{F}\}$ and $U_z = \{[0, 0, z]^\mathsf{T} \mid z \in \mathbf{F}\}$ be three subspaces of $\mathbf{F}^3$. Then $\mathbf{F}^3 = U_{x,y} + W + U_z$ is not a direct sum.

Indeed, the decomposition of 0 is not unique:

$$\begin{aligned} [0, 0, 0]^\mathsf{T} &= [0, 0, 0]^\mathsf{T} + [0, 0, 0]^\mathsf{T} + [0, 0, 0]^\mathsf{T} \\ &= [0, 1, 0]^\mathsf{T} + [0, -1, -1]^\mathsf{T} + [0, 0, 1]^\mathsf{T}. \end{aligned}$$

As the above example suggests, there is an easy criterion to check if a sum is direct.

Theorem 2.3.38.

Let V be a vector space and let $(U_\alpha)_{\alpha \in I}$ be a family of subspaces. Then $\sum_{\alpha \in I} U_\alpha$ is a direct sum if and only if whenever $0 = \sum_{\alpha \in I} u_\alpha$ then all the u_α are 0. That is, the sum is direct if and only if there exists a unique way to decompose 0.

Proof. We will prove the theorem for a finite family $(U_1, \cdots, U_n)$ of subspaces. The general case is similar.

"⇒" If the sum is direct, then any vector, and in particular 0, admits a unique decomposition.

"⇐" Suppose that the decomposition of 0 is unique and let $v \in U_1 + \cdots + U_n$. Let

$$u_1 + \cdots + u_n = v = u_1' + \cdots + u_n'$$

be two decomposition of v, so $u_i, u_i' \in U_i$ for all i. We need to show that these two decompositions are in fact the same, that is that $u_i = u_i'$ for all i. By subtracting the u_i' on both sides, we obtain

$$0 = (u_1 - u_1') + \cdots + (u_n - u_n')$$

with $u_i - u_i' \in U_i$ for all i. By unicity of the decomposition of 0, we conclude that $u_i - u_i' = 0$ and hence that $u_i = u_i'$ as desired. □

It follows from Theorem 2.3.38 that if two of the U_α are equal and not $\{0\}$, then the sum is not direct. Indeed, in this case we can write $0 = u - u$ for $u \in U_\alpha = U_\beta$ for $\alpha \neq \beta$.

Exercise 2.3.39. Let V be a vector space and let U_1, U_2 and W be subspaces. Are the following assertions true? If yes, prove them. If no, provide a counterexample.

a. If $U_1 + W = U_2 + W$, then $U_1 = U_2$;

b. If $U_1 \oplus W = U_2 \oplus W$, then $U_1 = U_2$.

Solution. Both assertions are incorrect. For example, let $U_x = \left\{ \begin{bmatrix} x \\ 0 \end{bmatrix} \mid x \in \mathbf{R} \right\}$, $U_y = \left\{ \begin{bmatrix} 0 \\ y \end{bmatrix} \mid y \in \mathbf{R} \right\}$ and $W = \left\{ \begin{bmatrix} z \\ z \end{bmatrix} \mid z \in \mathbf{R} \right\}$ be the x-axis, y-axis and the diagonal in $\mathbf{R}^2$. Then $U_1 \oplus W = \mathbf{R}^2 = U_2 \oplus W$ but $U_1 \neq U_2$. Observe that this is simply Example 2.3.36 for $n = 2$. □

Definition 2.3.40.

Let V be a vector space and let U be a subspace. A **complementary subspace** of U is a subspace $W \subseteq V$ such that $U \oplus W = V$.

We will see later in Theorem 2.4.48 that a subspace U always admits at least one complementary subspace. However, as we have just seen, in general a complementary subspace is not unique.

Exercise 2.3.41. Let $U = \{[x, y, x+y, x-y, 2x]^\mathsf{T} \mid x, y \in \mathbf{F}\} \subseteq \mathbf{F}^5$. Find a complementary subspace for U.

Solution. Intuitively, the first and second coordinates of U are free, but not the other ones. So one can guess that $W = \{[0, 0, z, s, t]^\mathsf{T} \mid z, s, t \in \mathbf{F}^5\}$. Let us prove that formally. Let v be any element of $\mathbf{F}^5$, so $v = [a, b, c, d, e]^\mathsf{T}$. We need to solve the following for $x, y, z, s, t \in \mathbf{F}$.

$$\begin{bmatrix} a \\ b \\ c \\ d \\ e \end{bmatrix} = \begin{bmatrix} x \\ y \\ x+y \\ x-y \\ 2x \end{bmatrix} + \begin{bmatrix} 0 \\ 0 \\ z \\ s \\ t \end{bmatrix} = \begin{bmatrix} x \\ y \\ z+x+y \\ s+x-y \\ t+2x \end{bmatrix}.$$

We immediately have $x = a$ and $y = b$. This implies $z = c - x - y$, $s = d - x + y$ and $t = e - 2x$, so if a solution exists it is unique. One easily verify that the above is indeed a solution and so that v admits a unique decomposition as $v = u + w$ with $u \in U$ and $w \in W$. That is, $\mathbf{F}^5 = U \oplus W$. □

2.3.3 Intersection of subspaces

If X and Y are subsets of Z, then both $X \cap Y$ and $X \cup Y$ are subsets of Z. We have seen that for subspaces U and W of a vector space $U \cup W$ is not a subspace of V, which pushed us to define the sum $U + W$. But what about the intersection?

Lemma 2.3.42. *Let V be a vector space and let $(U_\alpha)_{\alpha \in I}$ be a non-empty family of subspaces. Then the intersection $\bigcap_{\alpha \in I} U_\alpha$ is the biggest subspace of V contained in all the U_α.*

Proof. If $(U_\alpha)_{\alpha \in I} = \{U\}$ has exactly one element, then $\bigcap_{\alpha \in I} U = U$ and the statement is trivially true. Let us now treat the case $(U_\alpha)_{\alpha \in I} = \{U_1, U_2\}$. We already know that $U_1 \cap U_2$ is the biggest *subset* of V contained both U_1 and U_2. It only remains to prove that it is a subspace. This is left as an exercise to the reader. Hint: do not forget to use Proposition 2.3.12.

If $(U_\alpha)_{\alpha \in I}$ is a finite family, then repeated application of the statement for two subspaces proves the result. For a general, possibly infinite, family of subspaces, one can directly prove the statement in a similar fashion to the two subspaces case. □

For subsets, we have the notion of disjoint union $X \sqcup Y$, meaning that we look at $X \cup Y$ while asserting that the intersection $X \cap Y$ is empty. Heuristically, the sum of subspaces is similar to the union of subsets. This motivates us to find a result relating the direct sum $U \oplus W$ and the intersection $U \cap W$. In this case, $U \cap W$ is never empty as it always contains 0. But we can still ask the intersection to be "as small as possible", that is to be equal to $\{0\}$.

Theorem 2.3.43.

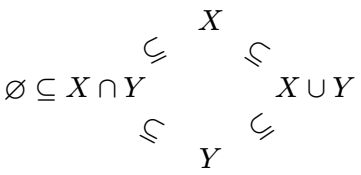
Let V be a vector space and let U_1 and U_2 be two subspaces. Then $U_1 + U_2$ is a direct sum if and only if $U_1 \cap U_2 = \{0\}$.

Proof. We will use Theorem 2.3.38.

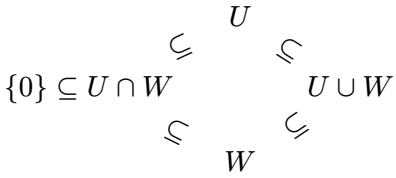
"⇒" Let v be an element of the intersection. Then v belongs both to U_1 and U_2 and so we have the following decomposition $0 = v + (-v)$, which implies that $v = 0$.

"⇐" Suppose that $0 = u_1 + u_2$ is a decomposition with $u_i \in U_i$ for $i \in \{1, 2\}$. Then $u_1 = -u_2$ is in $U_1 \cap U_2$ and hence equal to 0. We conclude that $u_1 = u_2 = 0$ and so the sum is direct. □

Figure 2.6 summarise the situation for subsets and subspaces.



Subsets. $\varnothing$ is the smallest subset of Y. $X \cup Y$ is the smallest subset of Z containing both X and Y. The union $X \cup Y$ is a disjoint union $X \sqcup Y$ if and only if $X \cap Y = \varnothing$.



Subspaces. $\{0\}$ is the smallest subspace of V. $U+W$ is the smallest subspace of V containing both U and W. The sum $U+W$ is a direct sum $U \oplus W$ if and only if $U \cap W = \{0\}$.

Figure 2.6: Comparaisons between subsets X and Y of a set Z and subspaces U and W of a vector space V. The intersection $X \cap Y$ ($U \cap W$) is the biggest subset (subspace), of Z (of V), contained both in X and Y (U and W).

Remark 2.3.44.

Be careful when trying to generalise Theorem 2.3.43 to the sum of more than two subspaces. The correct statement is that the sum $\sum_{\alpha \in I} U_\alpha$ is direct if and only if for all $\alpha \neq \beta$ we have $U_\alpha \cap U_\beta = \{0\}$. In particular, it is not enough that $\bigcap_{\alpha \in I} U_\alpha = \{0\}$, see the next example. This is similar to the situation for sets.

Example 2.3.45. Let $U_{x,y} := \{[x,y,0]^\mathsf{T} \in \mathbf{F}^3 | x, y \in \mathbf{F}\}$, $U_{x,z} := \{[x,0,z]^\mathsf{T} \in \mathbf{F}^3 | x, z \in \mathbf{F}\}$ and $U_{y,z} := \{[0,y,z]^\mathsf{T} \in \mathbf{F}^3 \,|\, y, z \in \mathbf{F}\}$ be three subspaces of $\mathbf{F}^3$. Then $U_{x,y} \cap U_{x,z} \cap U_{y,z} = \{0\}$, but the sum $U_{x,y} + U_{x,z} + U_{y,z}$ is not direct as $0 = [1,1,0]^\mathsf{T} + [-1,0,0]^\mathsf{T} + [0,-1,0]^\mathsf{T}$.

2.4 Span, linear independence and bases

It is well-known that any vector of $\mathbf{R}^2$ can be uniquely written as $\lambda \begin{bmatrix}1\\0\end{bmatrix} + \mu \begin{bmatrix}0\\1\end{bmatrix}$, where λ and μ are real numbers. The family $\left(\begin{bmatrix}1\\0\end{bmatrix}, \begin{bmatrix}0\\1\end{bmatrix}\right)$ is called the (standard) basis of $\mathbf{R}^2$. While it is easy to generalise this to $\mathbf{F}^n$, the generalisation to an abstract vector space requires more work. This is the subject of this section.

2.4.1 Linear combinations and span

In the previous sections, we sometimes used combination of vectors of the form $\lambda v + \mu u$. Such combinations play an important role in the theory of vector spaces, and thus deserve a specific name.

Definition 2.4.1.

Let V be an $\mathbf{F}$-vector space. A **linear combination** of the vectors $v_1, \ldots, v_n$ is any vector of the form

$$\lambda_1 v_1 + \cdots + \lambda_n v_n$$

where each $\lambda_i \in \mathbf{F}$ is a scalar.
By definition, 0 is the only linear combination of no vectors.

Example 2.4.2. All the vectors 0, v_1, $v_1 + v_2$, $2v_1 - 3v_2$ are linear combinations of v_1 and v_2.

Example 2.4.3. The vector $[17, -4, 2]^\mathsf{T} \in \mathbf{F}^3$ is a linear combination of $v = [2, 1, -3]^\mathsf{T}$ and $w = [1, -2, 4]^\mathsf{T}$ while $[17, -4, 5]^\mathsf{T}$ is not. In order to show that, we need to find λ and μ such that $[17, -4, 2]^\mathsf{T} = \lambda[2, 1, -3]^\mathsf{T} + \mu[1, -2, 4]^\mathsf{T}$. That is, we need to solve the linear system

$$\begin{bmatrix} 17 \\ -4 \\ 2 \end{bmatrix} = \begin{bmatrix} 2 & 1 \\ 1 & -2 \\ -3 & 4 \end{bmatrix} \begin{bmatrix} \lambda \\ \mu \end{bmatrix}.$$

Using row operations: $r_1 \mapsto r_1 - 2r_2$ and $r_3 \mapsto r_3 + 3r_2$ gives the following system

$$\begin{bmatrix} 25 \\ -4 \\ -10 \end{bmatrix} = \begin{bmatrix} 0 & 5 \\ 1 & -2 \\ 0 & -2 \end{bmatrix} \begin{bmatrix} \lambda \\ \mu \end{bmatrix}.$$

This system admits the solution $\mu = 5$ and $\lambda = 6$, so $[17, -4, 2]^\mathsf{T} = 6v + 5w$ is indeed a linear combination of v and w. The corresponding system for $[17, -4, 5]^\mathsf{T}$ has no solutions, and therefore $[17, -4, 5]^\mathsf{T}$ is not a linear combination of v and w.

Example 2.4.4. The function $\sin(x + \pi/4)$ is a linear combination of $\sin(x)$ and $\cos(x) \in \mathbf{R}^\mathbf{R}$. Indeed, $\sin(x + \pi/4) = \sqrt{2}/2 \sin(x) + \sqrt{2}/2 \cos(x)$.

The linear combination of vectors is an easy way to create new vectors from know ones. It is natural to collect all such vectors.

Definition 2.4.5.

Let v_1, ..., v_n be vectors in an $\mathbf{F}$-vector space V. Their **span** is the subset

$$\operatorname{span}_\mathbf{F}(v_1, \dots, v_n) := \{\lambda_1 v_1 + \cdots + \lambda_n v_n \mid \forall i : \lambda_i \in \mathbf{F}\} \subseteq V.$$

We also define $\operatorname{span}(\,) = \operatorname{span}(\varnothing) := \{0_V\}$.
If $\operatorname{span}(v_1, \dots, v_n) = V$, we say that $(v_1, \dots, v_n)$ spans V, or that V is spanned by $(v_1, \dots, v_n)$, or also that $(v_1, \dots, v_n)$ is a spanning family for V.

Observe that the span does not really depend on the family $(v_1, \dots, v_m)$, but only on the corresponding subset $\{v_1, \dots, v_m\} \subseteq V$ of vectors.

Remark 2.4.6.

In practice, we will often drop the subscript and simply write $\operatorname{span}(v_1, \dots, v_n)$. However, $\mathbf{F}$ does matter! For example, let $\mathbf{C}$ be viewed as a $\mathbf{C}$-vector space. Then

$\operatorname{span}_{\mathbf{C}}(1) = \mathbf{C}$. But we can also view $\mathbf{C}$ as a $\mathbf{R}$-vector space. In this case we have $\operatorname{span}_{\mathbf{R}}(1) = \{a + 0i \mid a \in \mathbf{R}\} \subsetneq \mathbf{C}$.

Example 2.4.7. The space $\mathbf{F}^n$ is spanned by $e_1 = [1, 0, \dots, 0]^\mathsf{T}$, $e_2 = [0, 1, 0, \dots, 0]^\mathsf{T}$,..., $e_n = [0, \dots, 0, 1]^\mathsf{T}$. Indeed, every $[x_1, \dots, x_n]^\mathsf{T}$ in $\mathbf{F}^n$ can be written as $[x_1, \dots, x_n]^\mathsf{T} = x_1[1, 0, \dots, 0]^\mathsf{T} + \cdots + x_n[0, \dots, 0, 1]^\mathsf{T}$.

Example 2.4.8. Let S be a finite set. For every $s \in S$, define $\chi_s \colon S \to \mathbf{F}$ to be the characteristic function of s:

$$\chi_s(t) = \begin{cases} 1 & \text{if } t = s, \\ 0 & \text{otherwise.} \end{cases}$$

Then $\mathbf{F}^S$ is spanned by $\{\chi_s \mid s \in S\}$: for any $f \in \mathbf{F}^S$ we have $f = \sum_{s \in S} f(s)\chi_s$ where the $f(s) \in \mathbf{F}$ are scalars. Indeed, since we are dealing with functions, the equality $f = \sum_{s \in S} f(s)\chi_s$ is true if and only if for every $t \in S$ the values of both sides agree when evaluated at t. But we have

$$\left(\sum_{s \in S} f(s)\chi_s\right)(t) = \sum_{s \in S}(f(s)\chi_s(t)) = 0 + \cdots + 0 + f(t)1 + 0 + \cdots + 0 = f(t).$$

To go further

The span of a finite family of vectors is the subset of all linear combination of these vectors. One can also define linear combination of infinitely many vectors and span of an arbitrary family of vectors. The trick is that in a linear combination of an infinite family of vectors, we ask that almost all coefficients (that is all but finitely many) to be 0. Formally, if $(v_\alpha)_{\alpha \in I}$ is a possibly infinite family of vectors of V, then

$$\operatorname{span}((v_\alpha)_{\alpha \in I}) := \left\{ \sum_{\alpha \in I} \lambda_\alpha v_\alpha \;\middle|\; \lambda_\alpha = 0 \text{ for all but finitely many } \alpha \right\}.$$

We have $\operatorname{span}((v_\alpha)_{\alpha \in I}) = \bigcup_{J \subseteq I \text{ finite}} \operatorname{span}((v_\alpha)_{\alpha \in J})$.
With this general notion of spanning family, one can generalise Example 2.4.8. Let S be any set.

> *For every $s \in S$, define $\chi_s \colon S \to \mathbf{F}$ to be the characteristic function of s. Then the direct sum $\mathbf{F}^{(S)} = \bigoplus_S \mathbf{F}$ is spanned by $\{\chi_s \mid s \in S\}$.*

Be careful that the product $\prod_S \mathbf{F}$ is not spanned by $\{\chi_s \mid s \in S\}$. Indeed, $\operatorname{span}(\{\chi_s \mid s \in S\})$ consists of linear combinations of finitely many of the χ_s. In particular, any function in $\operatorname{span}(\{\chi_s \mid s \in S\})$ has value 0 for all but finitely many s. So the constant function $\mathbf{1} : S \to \mathbf{F}, s \mapsto 1$ is in $\prod_S \mathbf{F}$ but not in $\operatorname{span}(\{\chi_s \mid s \in S\})$.

Span is important because of the following result.

Theorem 2.4.9.

Let V be a vector space and let $(v_\alpha)_{\alpha\in I}$ be a family of vectors of V. Then $\operatorname{span}((v_\alpha)_{\alpha\in I})$ is the smallest subspace of V containing all the v_α.

Proof. We will prove the theorem for a finite family $(v_1, \dots, v_n)$ of vectors. The general statement follows from $\operatorname{span}((v_\alpha)_{\alpha\in I}) = \bigcup_{J\subseteq I \text{ finite}} \operatorname{span}((v_\alpha)_{\alpha\in J})$.

We need to prove three things. Firstly that $\operatorname{span}(v_1, \dots, v_n)$ is a subspace, secondly that it contains all the v_i and finally that it is the smallest such space. If $n = 0$ (that is if the family is empty), then $\operatorname{span}(\varnothing) = \{0\}$ by definition, is the smallest subspace of V and hence the result holds. We can therefore assume in the following that $n \geq 1$.

We have $0 = 0v_1 + \cdots + 0v_n \in \operatorname{span}(v_1, \dots, v_n)$. If v and w are two vectors in $\operatorname{span}(v_1, \dots, v_n)$ and $\lambda \in \mathbf{F}$ is a scalar, there exists $\lambda_i, \mu_i \in \mathbf{F}$ such that

$$\begin{aligned}\lambda v + w &= \lambda(\lambda_1 v_1 + \cdots + \lambda_n v_n) + (\mu_1 v_1 + \cdots + \mu_n v_n) \\ &= (\lambda\lambda_1 + \mu_1)v_1 + \cdots + (\lambda\lambda_n + \mu_n)v_n \in \operatorname{span}(v_1, \dots, v_n).\end{aligned}$$

We conclude that $\operatorname{span}(v_1, \dots, v_n)$ is a subspace.

For any v_i we have $v_i = 0v_1 + \cdots + 0v_{i-1} + 1v_i + 0 + \cdots + 0v_n \in \operatorname{span}(v_1, \dots, v_n)$, so $\operatorname{span}(v_1, \dots, v_n)$ contains all the v_j.

Finally, suppose that U is a subspace containing all the v_i. We want to show that U also contains $\operatorname{span}(v_1, \dots, v_n)$. Let $v = \lambda_1 v_1 + \cdots + \lambda_n v_n$ be an arbitrary element of $\operatorname{span}(v_1, \dots, v_n)$. By assumption, the v_i belong to W. But W being a subspace, it is closed under scalar multiplication and under addition. It therefore contains v, which finishes the proof of a finite family $v_1, \dots, v_n$ of vectors. □

Corollary 2.4.10. *Let V be a vector space and let $(U_\alpha)_{\alpha\in I}$ be a family of subspaces. Then $\sum_{\alpha\in I} U_\alpha = \operatorname{span}(\bigcup_{\alpha\in I} U_\alpha)$.*

Proof. If the family is empty, then both $\sum_{\alpha\in\varnothing} U_\alpha$ and $\operatorname{span}(\bigcup_{\alpha\in\varnothing} U_\alpha)$ are equal to $\{0\}$ by definition.

If the family is non-empty, both $\sum_{\alpha\in I} U_\alpha$ (Theorem 2.3.31) and $\operatorname{span}(\bigcup_{\alpha\in I} U_\alpha)$ (Theorem 2.4.9) are both the smallest subspace of V containing all the U_α for all $\alpha \in I$. They are hence equal. □

2.4.2 Linear independence

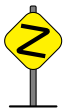
Consider the following example: $V = \mathbf{R}^2$ and $v_1 = \begin{bmatrix}1\\0\end{bmatrix}$, $v_2 = \begin{bmatrix}0\\1\end{bmatrix}$, $v_3 = \begin{bmatrix}1\\1\end{bmatrix}$. Then $V = \operatorname{span}(v_1, v_2)$ and $0\cdot v_1 + 0\cdot v_2 = 0$ is the only way to write 0 as a linear combination of v_1 and v_2. We also have $V = \operatorname{span}(v_1, v_2, v_3)$, but for every $\lambda \in \mathbf{R}$ we have $\lambda v_1 + \lambda v_2 - \lambda v_3 = 0$. We have here a phenomenon similar to what happens with sums and direct sums. Indeed, if we let $U_x := \operatorname{span}(v_1) = \left\{\begin{bmatrix}x\\0\end{bmatrix} \mid x \in \mathbf{R}\right\}$, $U_y := \operatorname{span}(v_2) = \left\{\begin{bmatrix}0\\y\end{bmatrix} \mid y \in \mathbf{R}\right\}$ and $W := \operatorname{span}(v_3) = \left\{\begin{bmatrix}x\\x\end{bmatrix} \mid x \in \mathbf{R}\right\}$ then $V = U_x \oplus U_y = U_x + U_y + W$, with the first sum direct but the second one not. We would like to have a criterion on the vectors similar to the criterion for direct sums for subspaces. This is provided by the next definition.

Definition 2.4.11.

Let v_1, ..., v_m be vectors in an $\mathbf{F}$-vector space V. They are **linearly independent** if the vector equation $\lambda_1 v_1 + \cdots + \lambda_m v_m = 0$ has a unique solution $\lambda_1 = \cdots = \lambda_m = 0$.
A non-linearly independent family of vectors is called **linearly dependent**. That is, v_1,..., v_m are linearly dependent if and only if $\lambda_1 v_1 + \cdots + \lambda_m v_m = 0$ admits a non-trivial solution (with one of the $\lambda_i \neq 0$).
By definition, the empty set $\varnothing$ is linearly independent.

If two of the v_i are identical, then the family $(v_1, \ldots, v_m)$ is linearly dependent.

Remark 2.4.12.



Once again, $\mathbf{F}$ does matter! For example, let $\mathbf{C}$ be viewed as a $\mathbf{C}$-vector space. Then the family $(1, \mathrm{i})$ is linearly dependent over $\mathbf{C}$ as $0 = \mathrm{i}\cdot 1 - 1\cdot \mathrm{i}$. But we can also view $\mathbf{C}$ as a $\mathbf{R}$-vector space. In this case the family $(1, \mathrm{i})$ is linearly independent over $\mathbf{R}$ as $0 = \lambda + \mathrm{i}\mu$ does not admit non-trivial real solutions.

To go further

An arbitrary (possibly infinite) family $(v_\alpha)_{\alpha \in I}$ of vectors is **linearly independent** if the vector equation $\sum_{\alpha \in I} \lambda_\alpha v_\alpha = 0$ (with all but finitely many $\lambda_\alpha = 0$) has a unique solution: $\lambda_\alpha = 0$ for all $\alpha \in I$. A non linearly independent family is **linearly dependent**.
The family $(v_\alpha)_{\alpha \in I}$ is linearly independent if and only if every finite subfamily is linearly independent. It is linearly dependent if and only if there exists a finite subfamily that is linearly dependent.

Let us investigate some easy consequences of this definition.

Lemma 2.4.13. *1. Any family of vectors containing* 0 *is linearly dependent;*

2. A single vector v is linearly independent if and only if $v \neq 0$;

3. Two vectors $v, w \in V$ are linearly independent if and only if both $v \notin \mathrm{span}(w)$ and $w \notin \mathrm{span}(v)$. If $v \neq 0$, then v and w are linearly independent if and only if $v \notin \mathrm{span}(w)$.

Proof. "1" One can always write $0 = 1 \cdot 0 + 0 \cdot v_1 + \cdots + 0 \cdot v_m$.
"2" This follows from the fact that $0 = \lambda v$ if and only if $\lambda = 0$ or $v = 0$.
"3" If v is in $\mathrm{span}(w)$, then $v = \mu w$ for some $\mu \in \mathbf{R}$. Then the equation $0 = \lambda_1 v + \lambda_2 w = (\mu\lambda_1 + \lambda_2)w$ has the non-trivial solution $\lambda_1 = 1$ and $\lambda_2 = -\mu$. So (v, w) is linearly dependent. If w is in $\mathrm{span}(v)$ a symmetric argument also shows that (v, w) is linearly dependent.
The equation $0 = \lambda_1 v + \lambda_2 w$ is equivalent to $\lambda_1 v = -\lambda_2 w$. If (v, w) is linearly dependent, then at least one of λ_1 or λ_2 is non-zero. If $\lambda_1 \neq 0$, then $v = -\lambda_1^{-1}\lambda_2 w$ is

in span(w). Similarly, if $\lambda_2 \neq 0$, then v is in span(w). We can hence conclude that the linear dependence of (v, w) implies that $v \in \text{span}(w)$ or $w \in \text{span}(v)$

Finally, suppose that $v \neq 0$ and that (v, w) is linearly dependent, so $\lambda_1 v = -\lambda_2 w$ for some $(\lambda_1, \lambda_2) \neq (0, 0)$. We claim that $\lambda_2 \neq 0$. Indeed, otherwise we would have $\lambda_1 v = 0$ forcing $\lambda_1 = 0$, which is absurd. From $\lambda_2 \neq 0$, w conclude as above that v is in span(w) We conclude from $\lambda v = -\mu w$ that both λ and μ are not 0. □

Observe that without the hypothesis $v \neq 0$ it is not enough to check only one of the condition $v \notin \text{span}(w)$ and $w \notin \text{span}(v)$. Indeed, if $v \neq 0$ and $w = 0$, then we have $v \notin \text{span}(w)$, but (v, w) is a linearly dependent family as it contains 0.

We now see more examples of linear dependence/independence.

Example 2.4.14. The vectors $[2, 3, 1]^\mathsf{T}$, $[1, -1, 2]^\mathsf{T}$ and $[17, 3, c]^\mathsf{T}$ in $\mathbf{F}^3$ are linearly dependent if and only if

$$\begin{bmatrix} 2 & 1 & 7 \\ 3 & -1 & 3 \\ 1 & 2 & c \end{bmatrix} \begin{bmatrix} \lambda_1 \\ \lambda_2 \\ \lambda_3 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}$$

has a non trivial solution. That is if and only if

$$\det \begin{bmatrix} 2 & 1 & 7 \\ 3 & -1 & 3 \\ 1 & 2 & c \end{bmatrix} = 0,$$

which is true if and only if $c = 8$.

Example 2.4.15. Let $(u_\alpha)_{\alpha \in I}$ be a family of vectors in a vector space V. Suppose that there exists $\alpha_0 \in I$ such that that v_{α_0} belongs to span$((u_\alpha)_{\alpha \in I \setminus \alpha_0})$. Then $(u_\alpha)_{\alpha \in I}$ is linearly dependent.

Let us show this for a finite family $(v_1, v_2, \dots, v_m)$. Without loss of generality, one can suppose that $v_1 \in \text{span}(v_2, \dots, v_m)$. By hypothesis we have $v_1 = \lambda_2 v_2 + \cdots + \lambda_m v_m$. This directly implies that $0 = (-1) \cdot v_1 + \lambda_2 v_2 + \cdots + \lambda_m v_m$ and so $(v_1, v_2, \dots, v_m)$ is linearly dependent.

An attentive reader might have observed that the definitions of linear independence (Definition 2.4.11) and of direct sum (Definition 2.3.33) are similar. Indeed, these two concepts are related and the following result follows directly from the definitions.

Proposition 2.4.16. *Let $(v_\alpha)_{\alpha \in I}$ be a family of non-zero vectors in a vector space V. Then the following are equivalent:*

I. $(v_\alpha)_{\alpha \in I}$ is linearly independent;

II. The sum $\sum_{\alpha \in I} \text{span}(v_\alpha)$ is direct.

As another interesting result linking linear independence and spanning, we have

Lemma 2.4.17. *A family $(v_\alpha)_{\alpha \in I}$ is linearly independent if and only if any vector v in* span$((v_\alpha)_{\alpha \in I})$ *can uniquely be written as a combination of the v_αs.*

Proof. We will prove the theorem for a finite family $(v_1, \dots, v_m)$ of vectors. The general proof is similar.

"$\Leftarrow$" Suppose that $(v_1, \dots, v_n)$ is linearly independent and let $v = \lambda_1 v_1 + \cdots + \lambda_m v_m = \mu_1 v_1 + \cdots + \mu_m v_m$ be two decompositions of v as a linear combination of the v_is. Then $0 = v - v = (\lambda_1 - \mu_1)v_1 + \cdots + (\lambda_m - \mu_m)v_m$ and so $\lambda_i = \mu_i$ for all $i \in \{1, \dots, m\}$, proving unicity of the decomposition.

"$\Rightarrow$" Since 0 belongs to the span of the v_is, the equation $0 = \lambda_1 v_1 + \cdots + \lambda_m v_m$ has a unique solution by assumption. This implies that all the λ_is are necessarily 0, proving the linear independence of the family $(v_1, \dots, v_m)$. □

2.4.3 Bases

We can finally formally define the fundamental notion of this section: the basis of a vector space.

Definition 2.4.18.

A **basis** of an $\mathbf{F}$-vector space V is a family $(v_\alpha)_{\alpha \in I}$ of vectors that is both linearly independent and spanning.

Remark 2.4.19.

The field $\mathbf{F}$ does matter if we want to check that a family of vectors is a basis (that is: is both linearly independent and spanning). For example, let $\mathbf{C}$ be viewed as a $\mathbf{C}$-vector space. Then the family 1 is a basis, but $(1, i)$ is not. But we can also view $\mathbf{C}$ as a $\mathbf{R}$-vector space, in which case $(1, i)$ is a basis, but 1 is not.

Remark 2.4.20.

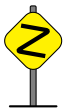
We explicitly require that a basis is a family of vectors, not simply a set. If it is finite, then it is simply a m-tuple $(v_1, \dots, v_m)$ for some $m \in \mathbf{N}$. In particular, in $\mathbf{R}^2$ the two families $(\begin{bmatrix}1\\0\end{bmatrix}, \begin{bmatrix}0\\1\end{bmatrix})$ and $(\begin{bmatrix}0\\1\end{bmatrix}, \begin{bmatrix}1\\0\end{bmatrix})$ are different bases even if they have the same elements.

We already have seen some examples of bases.

Example 2.4.21. The family $(e_1 := [1, 0, \dots, 0]^\mathsf{T}, \dots, e_m := [0, \dots, 0, 1]^\mathsf{T})$ is a basis of $\mathbf{F}^m$. It is called the **standard basis of $\mathbf{F}^m$**.

Example 2.4.22. The family $(1, x, \dots, x^m)$ is a basis of $\mathcal{P}(\mathbf{F})_m$. It is called the **standard basis of $\mathcal{P}(\mathbf{F})_m$**. The family $(1, x, \dots, x^m, \dots)$ is a basis of $\mathcal{P}(\mathbf{F})$. It is called the **standard basis of $\mathcal{P}(\mathbf{F})$**.

Example 2.4.23. The emptyset $\varnothing$ is the only basis of $\{0\}$. It is a basis because $\operatorname{span}(\varnothing) = \{0\}$. It is the only basis because (0) is a linearly dependent list.



Remark 2.4.24.

In general, even if a basis exists it is not unique (even up to permutation of the elements). Indeed, if a basis of an $\mathbf{F}$-vector space has at least two elements v_1 and v_2, then replacing v_2 by $v_1 + v_2$ gives a new basis.

Example 2.4.25. The bases of $\mathbf{F}$ are exactly the non-zero elements. Indeed, (x) is linearly independent if and only if $x \neq 0$. Moreover, any $y \in \mathbf{F}$ can be written as $y = (yx^{-1}) \cdot x$ with $yx^{-1} \in \mathbf{F}$, so $\operatorname{span}(x) = \mathbf{F}$. Finally, any family of $\mathbf{F}$ with at least 2 elements is linearly dependent by the same argument as above.

To go further

Let V be a vector space with a basis with exactly one element. By the forthcoming Corollary 2.4.27 this means that $V \cong \mathbf{F}$. So any element of $\mathbf{F} \setminus \{0\}$ is a basis as we have just seen. This means that if $\mathbf{F}$ has at least 3 elements, then V has at least 2 bases. However, if $\mathbf{F} = \mathbf{F}_2 = \{0, 1\}$ is the 2 elements field $\mathbf{F}_2$ from Example 2.2, then V has also 2 elements and hence a unique basis.
To summarise, the only vector spaces that admit a unique basis are: $\{0\}$ (any $\mathbf{F}$) and $\mathbf{F}_2$ (as an $\mathbf{F}_2$-vector space).

We have a first equivalent characterisation of bases.

Lemma 2.4.26. *Let $(v_\alpha)_{\alpha \in I}$ be a family of vectors in a vector space V. Then the following are equivalent;*

I. $(v_\alpha)_{\alpha \in I}$ is a basis of V;

II. Every vector $v \in V$ can uniquely be written as a linear combination of elements of $(v_\alpha)_{\alpha \in I}$.

Proof. On one hand, the set of vectors that can be written as a linear combination of elements of $(v_\alpha)_{\alpha \in I}$ is by definition $\operatorname{span}((v_\alpha)_{\alpha \in I})$. This holds for every vector of V if and only if $(v_\alpha)_{\alpha \in I}$ is spanning.

On the other hand, every vector in $\operatorname{span}((v_\alpha)_{\alpha \in I})$ can uniquely be written as a linear combination if and only if the family $(v_\alpha)_{\alpha \in I}$ is linearly independent. □

Corollary 2.4.27. *Let V be an $\mathbf{F}$-vector space. Suppose that V admits a finite basis $(v_1, \dots, v_m)$. Then the map*

$$[\,\cdot\,]_{\mathscr{B}} \colon V \longrightarrow \mathbf{F}^m$$
$$v = \sum_{i=1}^{m} \lambda_i v_i \longmapsto [v]_{\mathscr{B}} := [\lambda_1, \dots, \lambda_m]^{\mathsf{T}}$$

is a well-defined bijection. We will see in Corollary 3.1.49 than it is a fact an isomorphism of vector spaces.

Definition 2.4.28.

Let $(v_\alpha)_{\alpha\in I}$ be a basis of a vector space V and let $v \in V$ be a vector. By Lemma 2.4.26, there exists a unique way to write $v = \sum_{\alpha\in I} \lambda_\alpha v_\alpha$ (with all but finitely many $\lambda_\alpha = 0$). The λ_α are called the **coordinates** of v in the basis $(v_\alpha)_{\alpha\in I}$.

Exercise 2.4.29. The family $\left(\begin{bmatrix}2\\1\end{bmatrix}, \begin{bmatrix}1\\3\end{bmatrix}\right)$ is a basis of $\mathbf{R}^2$. What are the coordinates of $\begin{bmatrix}1\\0\end{bmatrix}$ in this basis?

Solution. To solve this, we need to find λ and μ solutions to

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

The unique solution to this system is given by $\lambda = 3/5$ and $\mu = -1/5$. □

We now give another characterisation of bases.

Theorem 2.4.30.

Let $(v_\alpha)_{\alpha\in I}$ be a family of vectors in a vector space V. Then the following are equivalent;

I. $(v_\alpha)_{\alpha\in I}$ is a basis of V;

II. $(v_\alpha)_{\alpha\in I}$ is a maximal linearly independent family;

III. $(v_\alpha)_{\alpha\in I}$ is a minimal spanning family;

IV. Every vector $v \in V$ can uniquely be written as a linear combination of elements of $(v_\alpha)_{\alpha\in I}$.

Proof. To simplify the notation, let us write $\mathscr{B} := (v_\alpha)_{\alpha\in I}$.

"I $\iff$ IV" is Lemma 2.4.26.

"I $\implies$ II" By hypothesis, $\mathscr{B}$ is both linearly independent and spanning. We claim that it is is maximal among linearly independent family: if a family $\mathscr{C}$ of vectors V contains both $\mathscr{B}$ and a vector v not in $\mathscr{B}$, then it is not linearly independent. Indeed $v = \sum_{\alpha\in I} \lambda_\alpha v_\alpha$ (with all but finitely many $\lambda_\alpha = 0$), so $0 = (-1)v + \sum_{\alpha\in I} \lambda_\alpha v_\alpha$ is a linear dependence relation.

"I $\implies$ III" As above $\mathscr{B}$ is both linearly independent and spanning. We claim that it is minimal among spanning family: any proper subfamily $\mathscr{A}$ of it is not spanning. Suppose that was not the case. Then there exists $\mathscr{A} \subsetneq \mathscr{B}$ spanning, and linearly independent as it is included in $\mathscr{B}$. But by the above $\mathscr{A}$ is a maximal linearly independent family, contradicting the linear independence of $\mathscr{B}$.

"II $\implies$ I" Suppose that $\mathscr{B}$ is a maximal linearly independent family. We need to prove it is spanning. Let v be any element in V. If v is already in $\mathscr{B}$ then it is in $\mathrm{span}(\mathscr{B})$.

Otherwise, the subset $\mathscr{B} \cup \{v\}$ is not linearly independent and therefore there exists λ and λ_α (with all but finitely many $\lambda_\alpha = 0$) not all 0 such that

$$\lambda v + \sum_{\alpha \in I} \lambda_\alpha v_\alpha = 0.$$

But $\lambda \neq 0$ as this would contradict the linear independence of $\mathscr{B}$. We conclude that $v = -\sum_{\alpha \in I} \lambda^{-1} \lambda_\alpha v_\alpha$ is in $\operatorname{span}(\mathscr{B})$.

"III $\implies$ I" Suppose that $\mathscr{B}$ is a minimal spanning family. We need to prove it is linearly independent. Let $(\lambda_\alpha)_{\alpha \in I}$ be scalars (with all but finitely many $\lambda_\alpha = 0$) such that

$$0 = \sum_{\alpha \in I} \lambda_\alpha v_\alpha.$$

We need to prove that they are all 0. Suppose by contradiction that there exists α_0 such that $\lambda_{\alpha_0} \neq 0$. This would implies that $v_{\alpha_0} = -\lambda_{\alpha_0}^{-1} \sum_{\alpha \in I \setminus \{\alpha_0\}} \lambda_\alpha v_\alpha$. But then $\operatorname{span}(\mathscr{B} \setminus v_{\alpha_0}) = \operatorname{span}(\mathscr{B}) = V$ contradicting the minimality of $\mathscr{B}$. □

Remark 2.4.31.

In this subsection we have obtained some interesting result about bases. However, we still have not yet proved that bases exist. This will be the subject of the next subsection.

2.4.4 Finite dimensional vector spaces

Our aim in this subsection is to define the dimension of a vector space. In order to do that, we first need to define what it means to be finite dimensional.

Definition 2.4.32.

A vector space V is said to be **finite dimensional** (or of **finite type**) if it has a finite spanning set. Otherwise it is **infinite dimensional**.

Example 2.4.33. The vector space $\mathbf{F}^m$ is finite dimensional, as its standard basis is a spanning family with m elements.

Example 2.4.34. The vector space $\mathcal{P}(\mathbf{F})$ of polynomials is infinite dimensional. Indeed, let p_1, ..., p_m be a finite set of polynomial. Let $d := \max\{\deg(p_i)\}$ be their maximal degree. Then any polynomial in $\operatorname{span}(p_1, \dots, p_m)$ has degree at most d. We conclude that $\operatorname{span}(p_1, \dots, p_m) \subseteq \mathcal{P}(\mathbf{F})_d \subsetneq \mathcal{P}(\mathbf{F})$ and thus that there exists no finite spanning set in $\mathcal{P}(\mathbf{F})$.

We can now prove the most important theorem of this section.

Theorem 2.4.35.

Every finite dimensional vector space V has a finite basis.

Proof. Let $(v_1, \dots, v_m)$ be a finite spanning family. Since this family is finite, it contains a minimal spanning subfamily $\mathscr{B}$, which is a basis by Theorem 2.4.30. □

We have seen in Lemma 2.4.13 and Example 2.4.15 that there exists some relation between span and linear independence. This relationship is quite important and we have the following converse of Example 2.4.15.

Lemma 2.4.36 (Linear dependence lemma)**.** *Let $(v_1, \dots, v_m)$ be a linearly* dependent *family of vectors in a vector space V. Then there exists $i \in \{1, \dots, m\}$ such that*

1. *v_i belongs to $\operatorname{span}(v_1, \dots, v_{i-1})$;*
2. *$\operatorname{span}(v_1, \dots, v_m) = \operatorname{span}(v_1, \dots, v_{i-1}, v_{i+1}, \dots, v_m)$ (we can remove v_i without changing the span).*

Proof. We start by proving the first assertion. By hypothesis, there exists $(\lambda_1, \dots, \lambda_m) \in \mathbf{F}^m$ with at least one non-zero λ_j such that $0 = \lambda_1 v_1 + \cdots + \lambda_m v_m$. Let $i := \max\{i \mid \lambda_j \neq 0\}$ be the biggest index such that $\lambda_i \neq 0$. Since λ_i is not 0, we can divide both sides by it to obtain

$$0 = \lambda_i^{-1}\lambda_1 v_1 + \cdots + \lambda_i^{-1}\lambda_{i-1} v_{i-1} + v_i + 0 \cdot v_{i+1} + \cdots 0 \cdot v_m$$

by maximality of i. So $v_i = (-\lambda_i^{-1}\lambda_1)v_1 + \cdots + (-\lambda_i^{-1}\lambda_{i-1})v_{i-1}$ is in $\operatorname{span}(v_1, \dots, v_{i-1})$.

For the second assertion, it is clear that the right hand side is contained in the left hand side. For the other inclusion, let v be any element of $\operatorname{span}(v_1, \dots, v_m)$. Then there exist μ_1, …, μ_m such that

$$\begin{aligned} v &= \mu_1 v_1 + \cdots + \mu_m v_m \\ &= \mu_1 v_1 + \cdots + \mu_{i-1} v_{i-1} + \mu_i(-\lambda_i^{-1}\lambda_1 v_1 - \cdots - \lambda_i^{-1}\lambda_{i-1} v_{i-1}) + \mu_{i+1} v_{i+1} + \cdots \mu_m v_m \\ &= (\mu_1 - \mu_i\lambda_i^{-1}\lambda_1)v_1 + \cdots + (\mu_{i-1} - \mu_i\lambda_i^{-1}\lambda_{i-1})v_{i-1} + \mu_{i+1} v_{i+1} + \cdots + \mu_m v_m. \end{aligned}$$

So v belongs to $\operatorname{span}(v_1, \dots, v_{i-1}, v_{i+1}, \dots, v_m)$, which finishes the proof. □

Using this lemma, we can prove the following important result.[6]

Theorem 2.4.37 (Grassmann's exchange lemma)**.**

Let V be a vector space. Let $(v_1, \dots, v_m)$ be a finite linearly independent family and let $(w_\alpha)_{\alpha \in I}$ be a (possibly infinite) spanning family. Then $m \leq \#I$.
Moreover, if $I = \{1, \dots, n\}$, there exists a renumbering of the w_is such that $(v_1, \dots, v_m, w_{m+1}, \dots, w_n)$ is spanning.

Proof. We will prove the theorem for a finite spanning family$(w_1, \dots, w_n)$. The general proof is similar. Consider the family $(v_1, w_1, \dots, w_n)$. Since v_1 is in $V = \operatorname{span}(w_1, \dots, w_n)$, the above family is linearly dependent. Moreover, $v_1 \neq 0$ since it belongs to a linearly

[6] Named after Hermann Günther Grassmann (1809–1877).

independent family. So $v_1 \notin \operatorname{span}(\varnothing)$. By Lemma 2.4.36, there exists i_1 such that $V = \operatorname{span}(v_1, w_1, \dots, w_n) = \operatorname{span}(v_1, w_1, \dots, w_{i_1-1}, w_{i_1+1}, \dots, w_n)$.

Now, consider the family $(v_1, v_2, w_1, \dots, w_{i-1}, w_{i+1}, \dots, w_n)$. This family is linearly dependent and $v_2 \notin \operatorname{span}(v_1)$ by linear independence. So there exists i_2 such that $V = \operatorname{span}(v_1, v_2, w_1, \dots, \psi_{i_1}, \dots, \psi_{i_2}, \dots, w_n)$.[7] By repeating this process, we find distinct i_1 to i_m such that we can replace w_{i_j} by v_j in $(w_1, \dots, w_n)$ and still have a spanning family. Since all the i_j are distinct, we conclude that $m \leq n$. □

The above theorem is: finite linearly independent family of vectors are shorter than finite spanning ones. We have an immediate but extremely important corollary of it.

Corollary 2.4.38. *Let V be a finite dimensional vector space. Then all its bases have the same number of elements.*

Proof. By Theorem 2.4.35 V admits a finite basis $\mathscr{B}$ with m elements. Let $\mathscr{B}'$ be any other basis. Since $\mathscr{B}'$ is linearly independent and $\mathscr{B}$ is spanning, $\mathscr{B}'$ has at most m elements by Theorem 2.4.37, it is hence a finite basis. By exchanging the roles of $\mathscr{B}$ and $\mathscr{B}'$, we see that $\mathscr{B}'$ has at least, and thus exactly, m elements. □

We can now finally state the main definition of this subsection.

Definition 2.4.39.

Let V be a finite dimensional $\mathbf{F}$-vector space. Its **dimension** $\dim_{\mathbf{F}}(V)$ is the number of elements in any of it's bases.

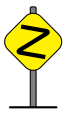
Observe that if a vector space V is finite dimensional, then its dimension $\dim_{\mathbf{F}}(V)$ is finite.

Example 2.4.40. For any field $\mathbf{F}$, the space $\{0\}$ is the only $\mathbf{F}$-vector space of dimension 0.

Example 2.4.41. We have $\dim_{\mathbf{F}}(\mathbf{F}^m) = m$ and $\dim_{\mathbf{F}}(\mathcal{P}(\mathbf{F})_m) = m + 1$. Indeed, the standard basis of $\mathbf{F}^m$ has m elements, while the standard basis of $\mathcal{P}(\mathbf{F})_m$ has $m + 1$ elements, see Examples 2.4.21 and 2.4.22.

5

Remark 2.4.42.



We will often drop the subscript $\mathbf{F}$ and simply write $\dim(V)$. However, $\mathbf{F}$ does matter. For example $\dim_{\mathbf{C}}(\mathbf{C}) = 1$ while $\dim_{\mathbf{R}}(\mathbf{C}) = 2$.

The next result might naively seem trivially true. However, its proof is far to be trivial.

[7] $(v_1, v_2, w_1, \dots, \psi_{i_1}, \dots, \psi_{i_2}, \dots, w_n)$ is the list $(v_1, \dots, v_m, w_1, \dots, w_n)$ with w_{i_1} and w_{i_2} removed.

Theorem 2.4.43.

Let U be a subspace of a finite dimensional vector space V. Then $\dim(U) \leq \dim(V)$. In particular, every subspace of a finite dimensional vector space is also finite dimensional.

Proof. We do not know yet that U is finite dimensional. So we would like to prove the theorem without assuming the existence of a basis. What we will do is show that U has at least one maximal linearly independent family $\mathscr{B}$, which will be a basis by Theorem 2.4.30.

Every linearly independent family of vectors of U is also a linearly independent family of vectors of V. By consequence, every such family has at most $\dim(V)$ elements by Theorem 2.4.37. We conclude that any linearly independent family $\mathscr{A}$ of vectors of U is contained in a maximal linearly independent family $\mathscr{B}$ of vectors of U. To conclude the proof it is hence enough to show that U has at least one linearly independent family $\mathscr{A}$ of vectors. One can always take $\mathscr{A} = \varnothing$ to be the empty family. □

To conclude this subsection, we present to important consequences of Grassmann's exchange lemma.

Corollary 2.4.44. *Let V be a vector space of dimension m. Then*

1. *Any linearly independent family of m vectors is a basis;*
2. *Any spanning family of m vectors is a basis.*

Proof. This is a direct consequence of Theorems 2.4.30 and 2.4.37. □

Corollary 2.4.45. *Let U be a subspace of a finite dimensional vector space V. Then $\dim(U) = \dim(V)$ if and only if $U = V$.*

Proof. The proof is left as an exercise to the reader. □

Tutorial 3, Question 2.

Corollary 2.4.46. *Let V be a finite dimensional vector space. Then any linearly independent family can be completed into a basis of V.*

Proof. Let $(v_1, \dots, v_m)$ be a linearly independent family and let $(w_1, \dots, w_n)$ be a basis of V. Applying Theorem 2.4.37 we obtain a family $(v_1, \dots, v_m, w_{i_1}, \dots, w_{i_r})$ that is both linearly independent and spanning. □

Corollary 2.4.47. *Let V be a vector space of dimension n and let U be a subspace of dimension m. Then every basis $(u_1, \dots, u_m)$ of U can be completed into a basis $(u_1, \dots, u_m, v_{m+1}, \dots, v_n)$ of V.*

Proof. If $(u_1, \dots, u_l)$ is a basis of U it is linearly independent. It can hence be completed to a basis of V by the previous corollary. □

Infinite dimensional vector spaces

The proofs of Theorems 2.4.35 and 2.4.37 and Corollary 2.4.38 only work for finite dimensional vector spaces. The results however remain true for infinite dimensional vector spaces, under one extra-technical set-theoric assumption called (AC), see Appendix 1.2. That is, if we assume (AC), then the following hold.

> *Every vector space has a basis, and any two of its bases have the same cardinality. Moreover, a linearly independent family is of smaller cardinality than a spanning family.*

We can use this to define the dimension of V to be the cardinality of any of its bases. With this notion, a vector space V is finite dimensional if and only if its dimension is finite. With this general notion of dimension, we still have (see Theorem 2.4.43 and Corollary 2.4.47)

> *If U is a subspace of a (possibly infinite dimensional) vector space V, then* $\dim(U) \leq \dim(V)$. *Moreover, any basis of U can be completed into a basis of V.*

However, Corollaries 2.4.44 and 2.4.45 are not true for infinite dimensional vector spaces. Indeed, if $U \subseteq \mathbf{F}^{(\mathbf{N})}$ is the subspace of sequences with a 0 in the first coordinate, then $\dim(U) = \dim(\mathbf{F}^{(\mathbf{N})})$, but U is a proper subspace of $\mathbf{F}^{(\mathbf{N})}$.

To go further

The cardinality of a vector space can be computed from its dimension.

> *Let V be an $\mathbf{F}$ vector space. Then*
>
> $$\#V = \begin{cases} 1 & \text{if } V = \{0\}, \\ \#\mathbf{F}^{\dim(V)} & \text{if both } \mathbf{F} \text{ and } \dim(V) \text{ are finite}, \\ \max(\dim(V), \#\mathbf{F}) & \text{otherwise.} \end{cases}$$

Let us prove this statement. If $\dim(V)$ is finite, it follows from the forthcoming Corollary 3.1.49 that $V \cong \mathbf{F}^{\dim(V)}$ has $\#\mathbf{F}^{\dim(V)}$ elements. This formula is true regardless of the cardinality of $\mathbf{F}$.
Let $\mathscr{B}$ be a basis of V. For a set S, write $\mathscr{P}_{\text{fin}}(S)$ for the set of its finite subsets. We have two injective maps

$$\begin{aligned} \mathbf{F} \times \mathscr{B} &\longrightarrow V & V &\longrightarrow \mathscr{P}_{\text{fin}}(\mathbf{F} \times \mathscr{B}) \\ (\lambda, v) &\longmapsto \lambda v & v = \sum_{i=1}^{m} \lambda_i v_i &\longmapsto \{(\lambda_1, v_1), \dots, (\lambda_m, v_m)\}. \end{aligned}$$

This shows that $\#F \times \dim(V) = \#\mathbf{F} \times \#\mathscr{B} = \#(\mathbf{F} \times \mathscr{B}) \leq \#V \leq \#\mathscr{P}_{\text{fin}}(\mathbf{F} \times \mathscr{B})$. Since $\mathbf{F}$ has at least two elements (0 and 1), the left inequality gives $2\dim(V) \leq \#V$.

If $V \neq \{0\}$, we also have $\#\mathbf{F} \leq \#V$ and thus $\max(2\dim(V), \#\mathbf{F}) \leq \#V$. Suppose now that at least one of $\#\mathbf{F}$ or $\dim(V)$ is infinite and that $V \neq \{0\}$ (so both $\#\mathbf{F}$ and $\dim(V)$ are not 0). Then $\mathbf{F} \times \mathscr{B}$ is infinite and by cardinal arithmetic we have $\max(\dim(V), \mathbf{F}) = \#\mathbf{F} \times \#\mathscr{B} = \#\mathscr{P}_{\text{fin}}(\mathbf{F} \times \mathscr{B}) \geq \#V$ as desired. It remains to show the inequality $\#V \leq \max(\dim(V), \#\mathbf{F})$.

2.4.5 Sums of subspaces and dimension

Recall from Definition 2.3.40 that if U is a subspace of V, a complementary subspace for U is a subspace $W \subseteq V$ such that $U \oplus W = V$. Using bases, we will show that such a W always exists.

Theorem 2.4.48.

Let U be a subspace of a vector space V. Then there exists a complementary subspace W. That is, there exists W such that $U \oplus W = V$.

Proof. We give the proof only for finite dimensional vector spaces, but the result remains true in general. Let $(u_1, \dots, u_l)$ be a basis of U and complete it to $(u_1, \dots, u_l, v_{l+1} \dots, v_m)$ a basis of V. Let $W := \text{span}(v_{l+1}, \dots, v_m)$. We claim that $U \oplus W = V$.

On one hand, it is clear that $U + W \supseteq \text{span}(u_1, \dots, u_l, v_{l+1} \dots, v_m) = V$ and so that $U + W = V$. On the other hand, if v belongs to $U \cap W$, there exists λ_i such that

$$0 = v - v = (\lambda_1 u_1 + \cdots + \lambda_l u_l) - (\lambda_{l+1} v_{l+1} + \cdots + \lambda_m v_m).$$

By linear independence we conclude that all the λ_i are zero and thus that $v = \lambda_1 u_1 + \cdots + \lambda_l u_l = 0$. We have just proved that $U \cap W = \{0\}$ and so the sum is direct. □

Remark 2.4.49.

Such a W is not unique in general, see Example 2.3.36. However both $\{0\}$ and V itself have a unique direct complement (which is respectively V and $\{0\}$).

It turns out that having a unique complement characterise 0 and V.

Proposition 2.4.50. *Let $U \subseteq V$ be a subspace of a vector space. Then U admits a unique complement if and only if $U = \{0\}$ or $U = V$.*

Proof. "⇒" If $U = V$, then $V + W = V$ for all subspaces W. Moreover, $W = \{0\}$ is the only subspace such that $V \cap W = \{0\}$, so $\{0\}$ is the only direct complement of V. This also implies that V is a direct complement of $\{0\}$. Finally, if $U = \{0\}$ then $W = V$ is the only subspace such that $U + W = V$. So V is the only direct complement of $\{0\}$.

"⇐" This direction is more difficult and we will skip it. But see the next "To go further" box for details. □

To go further

We will now give a proof of

If $U \subseteq V$ admits a unique direct complement then $U = \{0\}$ or $U = V$.

Proof. We will prove it for finite dimensional vector spaces, but the general proof is similar.
Let $\{0\} \subsetneq U \subsetneq V$ be a subspace that is neither $\{0\}$ nor V and let W_1 be a direct complement of U. We want to build another direct complement $W_2 \neq W_1$ of U. On one hand, since $U \neq \{0\}$ it has a non-empty basis $(u_1, \dots, u_m)$. On the other hand, since $U \neq V$ the subspace W is not $\{0\}$. In particular W has a non-empty basis $(w_1, \dots, w_n)$. Define $W_2 := \mathrm{span}(u_1 + w_1, w_2, \dots, w_n)$. We claim that $W_2 \neq W_1$ and that it is another direct complement of U.
Firstly, $W_2 \neq W_1$. Indeed, if $W_2 \subseteq W_1$, then W_1 contains both w_1 and $u_1 + w_1$. This would implies that $0 \neq u_1 = (u_1 + w_1) - u_1$ is in $U \cap W_1$ which contradicts the fact that $U \oplus W_1$ is a direct sum.
One can also show that W_2 does not contains u_1. Indeed, if it was the case then W_2 would also contains w_1 and hence $w_1 = \lambda_1(u_1 + w_1) + \lambda_2 w_2 + \cdots + \lambda_n w_n$ for some scalars λ_i. We cannot have $\lambda_1 = 0$ as this would contradict the linear independence of $(w_1, \dots, w_n)$. But $\lambda_1 \neq 0$ implies that u_1 is in W_1 which is absurd.
Secondly, let $v \in U \cap W_2$. Then there exists scalars $(\lambda_i)_{i=1}^n$ such that $v = \lambda_1(u_1 + w_1) + \lambda_2 w_2 + \dots + \lambda_n w_n \in U \cap W_2$. But then $v - \lambda_1 u_1 = \lambda_1 w_1 + \lambda_2 w_2 + \dots + \lambda_n w_n$ is in $U \cap W_1 = \{0\}$. So $\lambda_1 u_1 = v$ is in $U \cap W_2$. This means that either $v = 0$ as desired or that $u_1 = \lambda_1^{-1} v \in W_2$. We just proved that the second possibility cannot happen. This finish the proof that $U + W_2 = U \oplus W_2$ is a direct sum.
It remains to show that $U + W_2 = V$. Let $v \in V = U + W_1$ be any vector in V. Then there exists scalars $(\mu_j)_{j=1}^m$ and $(\lambda_i)_{i=1}^n$ such that

$$\begin{aligned} v &= \mu_1 u_1 + \cdots + \mu_m u_m + \lambda_1 w_1 + \cdots + \lambda_n w_n \\ &= (\mu_1 - \lambda) u_1 + \mu_2 u_2 + \cdots + \mu_m u_m + \lambda_1(u_1 + w_1) + \lambda_2 w_2 \cdots + \lambda_n w_n, \end{aligned}$$

showing that $V \subseteq U \oplus W_2$. □

Recall that if A and B are two finite subsets of C we have the inclusion-exclusion formula: $\#(A \cup B) = \#A + \#B - \#(A \cap B)$. We have a similar result for subspaces of vector spaces, where the cardinality of a subset is replaced by the dimension of a subspace.

Theorem 2.4.51.

Let V be a vector space and let U and W be two finite dimensional subspaces. Then we have

$$\dim(U + W) = \dim(U) + \dim(W) - \dim(U \cap W).$$

Proof. To prove results about dimension of vector spaces, it is usually useful to use bases. So let $(v_1, \dots, v_m)$ be a basis of the finite dimensional vector space $U \cap W$, so $\dim(U \cap W) = m$. We can extend it to $(v_1, \dots, v_m, u_1, \dots, u_k)$ a basis of U, but also to $(v_1, \dots, v_m, w_1, \dots, w_l)$ a basis of W, so $\dim(U) = m + k$ and $\dim(W) = m + l$. We claim that $(v_1, \dots, v_m, u_1, \dots, u_k, w_1, \dots, w_m)$ is a basis of $U + W$. This will imply that $\dim(U + W) = m + k + l = (m + k) + (m + l) - m$.

The family $(v_1, \dots, v_m, u_1, \dots, u_k)$ spans U while the family $(v_1, \dots, v_m, w_1, \dots, w_l)$ spans W. So the family $(v_1, \dots, v_m, u_1, \dots, u_k, v_1, \dots, v_m, w_1, \dots, w_l)$ spans $U + W$ and so does $(v_1, \dots, v_m, u_1, \dots, u_k, w_1, \dots, w_m)$, where we just removed the repeated vectors.

In order to finish the proof, we need to show that $(v_1, \dots, v_m, u_1, \dots, u_k, w_1, \dots, w_m)$ is linearly independent. Let λ_i, μ_i and γ_i be scalars such that

$$0 = \lambda_1 v_1 + \cdots + \lambda_m v_m + \mu_1 u_1 + \cdots + \mu_k u_k + \gamma_1 w_1 + \cdots + \gamma_l w_l.$$

Then the element

$$v := -(\gamma_1 w_1 + \cdots + \gamma_l w_l) = \lambda_1 v_1 + \cdots + \lambda_m v_m + \mu_1 u_1 + \cdots + \mu_k u_k$$

is in $W \cap U$. That is, there exists β_i such that $v = \beta_1 v_1 + \cdots + \beta_m v_m$. We have

$$0 = v - v = (\lambda_1 - \beta_1) v_1 + \cdots + (\lambda_m - \beta_m) v_m + \mu_1 u_1 + \cdots + \mu_k u_k.$$

Using the linear independence of $(v_1, \dots, v_m, u_1, \dots, u_k)$ we obtain that all the coefficients are 0 and in particular that $\mu_i = 0$ for all i. We conclude that

$$v = -(\gamma_1 w_1 + \cdots + \gamma_l w_l) = \lambda_1 v_1 + \cdots + \lambda_m v_m.$$

Writing $0 = v - v$ and using the linear independence of $(v_1, \dots, v_m, w_1, \dots, w_l)$ we obtain that all the λ_i and γ_i are 0, which finishes the proof of the linear independence of $(v_1, \dots, v_m, u_1, \dots, u_k, w_1, \dots, w_m)$. □

Corollary 2.4.52. *Let V be a finite dimensional vector space and let $U_1 + \cdots + U_k$ be a sum of subspaces. Then the following are equivalent:*

I. The sum is direct;

II. $\dim(U_1 \oplus \cdots \oplus U_k) = \dim(U_1) + \cdots + \dim(U_k)$.

Proof. If $k = 1$, there is nothing to prove. The case $k = 2$ is a simple application of the Theorem, since $U_1 \cap U_2 = \{0\}$ if and only if the sum $U_1 + U_2$ is direct. The case $k \geq 3$ is done by induction. □

Infinite dimensional vector spaces

For a general vector space V, we still have the formula

$$\dim(U + W) + \dim(U \cap W) = \dim(U) + \dim(W).$$

However, this is not really interesting as for infinite dimensional vector spaces,

$\dim(U)+\dim(W) = \max\{\dim(U), \dim(W)\}$. More generally, using bases, one can show

$$\dim\Big(\bigoplus_{\alpha\in I} U_\alpha\Big) = \sum_{\alpha\in I} \dim(U_\alpha).$$

But to understand the above expression we need to make sense of infinite sums of infinite cardinals, which goes beyond this course.

3 Linear maps

Standing assumption

In this chapter, we will fix an arbitrary field $\mathbf{F}$. In particular, when talking about multiple vector spaces, U, V, W, etc. we will always assume that they are vector spaces over the same field.

In the previous chapter, we have defined vector spaces and started the study of their structure (subspaces, bases, …). In this chapter we will see how to connect vector spaces by maps that preserve their structures.

3.1 Linear maps, kernels and images

In this section, we will define a linear map as a map $T : V \to W$ that "preserves the vector space structure". A prominent example of such maps is given by matrix multiplications. We will then define two subspaces associated with T. The first one, $\mathrm{Im}(T) \subseteq W$ is simply the image of T and related to surjectivity, similarly to what happens with maps between sets. The second subspace $\ker(T) \subseteq V$ is related to injectivity and does not have an equivalence in the realm of functions between sets.

3.1.1 Definition and first properties

Before defining linear maps between vector spaces, let us shortly recall the situation for sets from Chapter 1. Sets do not have structure. We are therefore interested in any maps $f : A \longrightarrow B$ without restrictions. Bijections are specially important maps and whenever there exists a bijection $A \xhookrightarrow{\sim} B$ we consider A and B identical as sets. Moreover, we have $A \simeq B$ if and only if $\#A = \#B$.

Contrary to sets, vector spaces do have structure, namely the addition and scalar multiplication. So we are interested in maps between vector spaces that do "preserve" this structure. Here is an example that shows why bijections are not the correct tools to use for vector spaces. There exists a bijection between $\mathbf{R}$ and $\mathbf{R}^2$, so they are identical as sets. However, as real vector spaces $\mathbf{R}$ and $\mathbf{R}^2$ are quite different (for example, they do not have the same dimension) and thus should not be identified as vector spaces. Actually, there even exists a bijection between $\mathbf{R}$ and $\mathbf{R}^{(\mathbf{N})}$ while one is of dimension 1 and the dimension of other is infinite.

Definition 3.1.1.

Let V and W be two vector spaces over the same field $\mathbf{F}$. A map $T\colon V \longrightarrow W$ is a **$\mathbf{F}$-linear map** (or **$\mathbf{F}$-linear transformation**, or simply **linear map** or **linear transformation**) if it satisfies the following two conditions:

(1) $\forall u, v \in V : T(u +_V v) = T(u) +_W T(v)$ (additivity);

(2) $\forall v \in V, \lambda \in \mathbf{F} : T(\lambda \cdot_V v) = \lambda \cdot_W T(v)$ (homogeneity).

We will sometimes write T_v or Tv for $T(v)$.
We write $\mathcal{L}(V, W)$ for the set of all linear maps from V to W:

$$\mathcal{L}(V, W) := \{T\colon V \longrightarrow W \mid T \text{ is linear}\}.$$

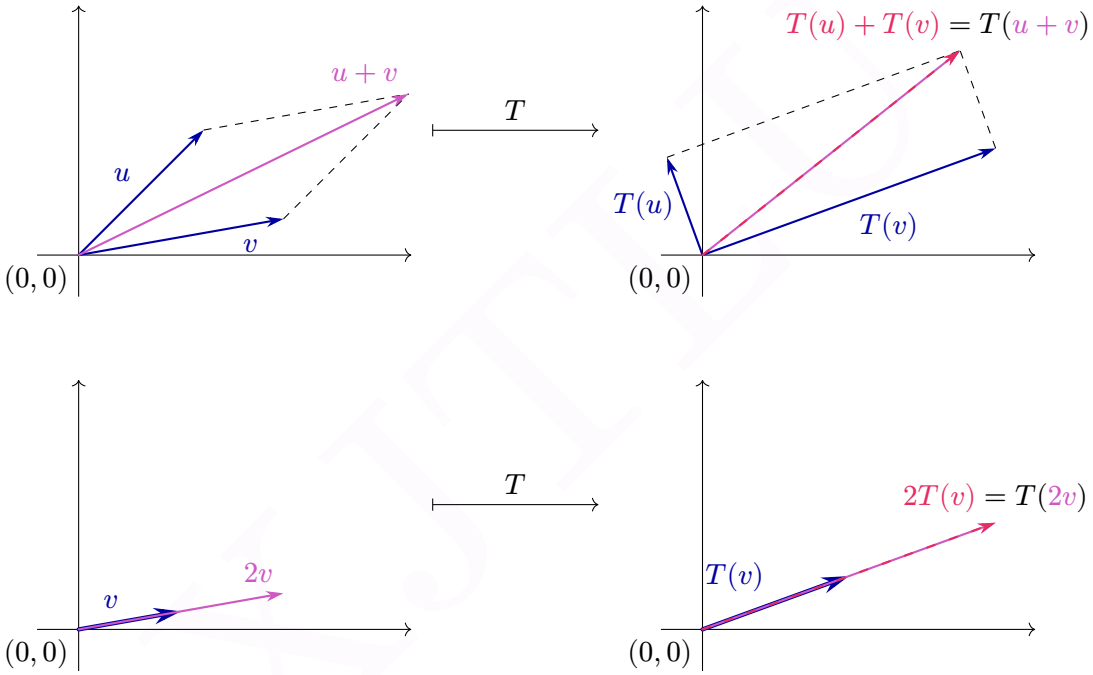
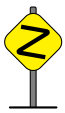


Figure 3.1: Effect of a linear map on addition and scalar multiplication of vectors in $\mathbf{R}^2$.

Remark 3.1.2.

When writing $T \in \mathcal{L}(V, W)$ we means two things. Firstly that V and W are two vector spaces over the same field. Secondly that T is a linear map from V to W.



Remark 3.1.3.

As usual, the base field $\mathbf{F}$ matters even if we will often not write it explicitly. For example, let $V = W = \mathbf{C}$. This is both a real vector space and a complex vector space. Let $T(z) = \overline{z}$ be the complex conjugate of z, that is $\overline{a + b\mathrm{i}} = a - b\mathrm{i}$. Then T is $\mathbf{R}$-linear, but not $\mathbf{C}$-linear, see Tutorial 4 Question 1.

The linear maps for which their domain and codomain coincide form an important and interesting family.

Definition 3.1.4.

If V is a vector space, $\mathcal{L}(V) := \mathcal{L}(V, V)$. An element $T \in \mathcal{L}(V)$ is called an **operator** on V.

A vector space does not only have an addition and a scalar multiplication, it also has a zero element and every vector has an additive inverse. We would like our maps to also "preserve" these operations. Luckily we have this for free.

Lemma 3.1.5. *For any linear map $T \in \mathcal{L}(V, W)$ we have*

1. $T(0_V) = 0_W$;
2. $\forall v \in V : T(-_V v) = -_W T(v)$.

Proof. We have $T(0_V) = T(0_V + 0_V) = T(0_V) + T(0_V)$. Subtracting $T(0_V)$ on both sides we obtain $T(0_V) = 0_W$.

The second assertion follows directly from the definition of linear map and the fact that $-v = (-1)v$. □

Using the above lemma, one can summarise the two properties of linear maps into one unique property. This is similar to what we did for subspaces.

Corollary 3.1.6. *Let V and W be two vector spaces over the same field. A map $T : V \to W$ is linear if and only if it satisfies the single condition*

$$\forall u, v \in V, \lambda \in \mathbf{F} : T(\lambda u + v) = \lambda T(u) + T(v).$$

Proof. If T is linear, then $T(\lambda u + v) = T(\lambda u) + T(v) = \lambda T(u) + T(v)$.

If the map T satisfies the condition, then $T(u + v) = T(1u + v) = T(u) + T(v)$ and $T(\lambda u) = T(\lambda u + 0) = \lambda T(u) + 0 = \lambda T(u)$. □

Let us now see a few examples of linear maps.

Example 3.1.7. If V and W are two vector spaces over the same field $\mathbf{F}$, one define the **zero map**

$$\begin{aligned} 0_{\mathcal{L}(V,W)} : V &\longrightarrow W \\ v &\longmapsto 0_W. \end{aligned}$$

This is a linear map. The verifications are straightforward and left to the reader. As usual, we will often drop the subscript and simply write 0 whenever V and W are clear from context.

The above example shows that if V and W are vector spaces *over the same field*, then $\mathcal{L}(V, W)$ is never empty.

Example 3.1.8. If V is a vector space, then the **identity map**

$$\begin{aligned} \mathrm{Id}_V \colon V &\longrightarrow V \\ v &\longmapsto v \end{aligned}$$

is a linear map. We will simply write Id if V is clear from context. But be careful: $\mathrm{Id}_{\mathbf{R}} \neq \mathrm{Id}_{\mathbf{R}^2}$!

It follows from the previous two examples that if $V \neq \{0\}$, then $\mathcal{L}(V)$ has at least two elements: $0 \neq \mathrm{Id}$. If $V = \{0\}$ then these two maps are the same.

Example 3.1.9 (Differentiation)**.** Define

$$\begin{aligned} D \colon \mathcal{P}(\mathbf{R}) &\longrightarrow \mathcal{P}(\mathbf{R}) \\ p &\longmapsto p', \end{aligned}$$

where p' is the derivative of the polynomial p. From calculus, we know $D(p+q) = D(p) + D(q)$ and $D(\lambda p) = \lambda D(p)$, so D is a linear map. One can also define D on the larger domain $\mathcal{C}^\infty(\mathbf{R}) := \{f \colon \mathbf{R} \to \mathbf{R} \mid f^{(n)} \text{ exists } \forall n\}$ (the space of infinitely many times differentiable real functions[1]) to itself. It is even possible to go complex and to define D on $\mathcal{P}(\mathbf{C})$ or on $\mathcal{C}^\infty(\mathbf{C})$.[2]

Observe that while we used the same letter D, we have 4 different linear maps. Indeed, these maps are respectively elements of $\mathcal{L}(\mathcal{P}(\mathbf{R}), \mathcal{P}(\mathbf{R}))$, $\mathcal{L}(\mathcal{C}^\infty(\mathbf{R}), \mathcal{C}^\infty(\mathbf{R}))$, $\mathcal{L}(\mathcal{P}(\mathbf{C}), \mathcal{P}(\mathbf{C}))$ and of $\mathcal{L}(\mathcal{C}^\infty(\mathbf{C}), \mathcal{C}^\infty(\mathbf{C}))$. We used the same letter for these different maps are they "do the same things". In fact, they are restrictions one of the other. For example, $\mathcal{P}(\mathbf{R})$ is a subspace of all the other 3 spaces and the D map on $\mathcal{P}(\mathbf{R})$ is the restriction of any of the other three D maps.

Example 3.1.10 (Definite integration)**.** Define

$$\begin{aligned} T \colon \mathcal{P}(\mathbf{R}) &\longrightarrow \mathbf{R} \\ p &\longmapsto \int_0^1 p(x)\,\mathrm{d}x. \end{aligned}$$

From calculus, we know that T is linear. This is still true if we replace the integration interval $[0, 1]$ by any fixed interval $[a, b]$ with $a < b$.

It is possible to extend T to $\{f \colon \mathbf{R} \to \mathbf{R} \mid f \text{ integrable on } [0, 1]\}$ and even to complex integrable functions.

Be careful, the differentiation map from the previous example is in $\mathcal{L}(\mathcal{P}(\mathbf{R}), \mathcal{P}(\mathbf{R}))$, but the definite integration map is in $\mathcal{L}(\mathcal{P}(\mathbf{R}), \mathbf{R})$.

[1] A real function that is infinitely many times differentiable is called a **smooth function**.

[2] $\mathcal{C}^\infty(\mathbf{C})$ is the space of **holomorphic functions**. See your analysis class for more details.

Example 3.1.11 (Backward shift)**.** Define

$$S\colon \mathbf{F}^{\mathbf{N}} \longrightarrow \mathbf{F}^{\mathbf{N}}$$
$$(x_0, x_1, x_2, \dots) \longmapsto (x_1, x_2, x_3 \dots).$$

One easily verify that S is linear.

Example 3.1.12 (Multiplication by x)**.** Define

$$T\colon \mathcal{P}(\mathbf{F}) \longrightarrow \mathcal{P}(\mathbf{F})$$
$$p(x) \longmapsto x \cdot p(x).$$

One easily checks that $T(\lambda p + q) = x(\lambda p + q) = \lambda xp + xq = \lambda T(p) + T(q)$ and so T is linear. The map T is sometimes called the *forward shift* as

$$T(a_0 + \cdots + a_n x^n) = a_0 x + \cdots + a_n x^{n+1} = 0 + a_{1-1}x + \cdots + a_{n-1}x^n + a_{(n+1)-1}x^{n+1}.$$

In other words, the sequence of coefficients $(a_0, \dots, a_n, 0, \dots)$ is sent to the sequence $(0, a_0, \dots, a_n, 0, \dots)$.

Observe that applying twice the map T is simply the multiplication by x^2. Indeed, $T(T(p(x))) = x^2 \cdot p(x)$.

Our next example is more concrete and might look familiar.

Example 3.1.13. The map

$$T\colon \mathbf{R}^3 \longrightarrow \mathbf{R}^2$$
$$\begin{bmatrix} x \\ y \\ z \end{bmatrix} \longmapsto \begin{bmatrix} 2x - y + 3z \\ 7x + 5y - 6z \end{bmatrix}$$

is a linear map: $T \in \mathcal{L}(\mathbf{R}^3, \mathbf{R}^2)$.

One can easily check that the above example corresponds to the left multiplication by the matrix $\begin{bmatrix} 2 & -1 & 3 \\ 7 & 5 & -6 \end{bmatrix}$. Actually, multiplication by a matrix is always a linear map as demonstrated in the following example.

Example 3.1.14. If a_{ij} belongs to $\mathbf{F}$ for $i \in \{1, \dots, m\}$ and $j \in \{1, \dots, n\}$, then the map

$$T\colon \mathbf{F}^n \longrightarrow \mathbf{F}^m$$
$$\begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} \longmapsto \begin{bmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{m1} & \cdots & a_{mn} \end{bmatrix} \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix}$$

is linear and belong to $\mathcal{L}(\mathbf{F}^n, \mathbf{F}^m)$. See Definition 3.2.5 for a reminder on matrix multiplication.

We will see in Subsection 3.2.2 that any linear map from $\mathbf{F}^n$ to $\mathbf{F}^m$ can be realised by a matrix multiplication.

The following theorem is important as it allows for easy construction of linear maps. Indeed, it says that in order to construct a linear map T from V to W we only need to decide the value of T on a basis of V.

Theorem 3.1.15.

Let V and W be two vector spaces. Suppose that $(v_\alpha)_{\alpha\in I}$ is a basis of V and let $(w_\alpha)_{\alpha\in I}$ be a list of arbitrary vectors (not necessarily distinct) in W. Then there exists a unique linear map $T \in \mathcal{L}(V,W)$ such that $T(v_\alpha) = w_\alpha$ for all α in I.

Proof. We will write the proof for a finite basis $\mathscr{B} = (v_1, \dots, v_m)$ of V (so for V finite dimensional), the general case being similar.

We start by proving the existence of such a linear map. Let v be any vector in V. Since $\mathscr{B}$ is a basis, there exists unique λ_js such that $v = \lambda_1 v_1 + \cdots + \lambda_m v_m$. We define T on v by $T(v) = \lambda_1 w_1 + \cdots + \lambda_m w_m \in W$. By existence of the λ_js each v has at least one image, and by unicity each v has exactly one image, so T is a well-defined map. It remains to check that T is linear. Let $v = \lambda_1 v_1 + \cdots + \lambda_m v_m$ and $u = \mu_1 v_1 + \cdots + \mu_m v_m$ be arbitrary vectors in V and let $\gamma \in \mathbf{F}$ be a scalar. Then

$$\begin{aligned} T(\gamma v + u) &= T((\gamma\lambda_1 + \mu_1)v_1 + \cdots + (\gamma\lambda_m + \mu_m)v_m) \\ &= (\gamma\lambda_1 + \mu_1)w_1 + \cdots + (\gamma\lambda_m + \mu_m)w_m \\ &= \gamma(\lambda_1 w_1 + \cdots + \lambda_m w_m) + (\mu_1 w_1 + \cdots + \mu_m w_m) \\ &= \gamma T(v) + T(u). \end{aligned}$$

For uniqueness, suppose that $S \in \mathcal{L}(V,W)$ is a linear map satisfying $S(v_i) = w_i$. Then for any $v = \lambda_1 v_1 + \cdots + \lambda_m v_m$ in V, we have

$$\begin{aligned} S(v) &= S(\lambda_1 v_1 + \cdots + \lambda_m v_m) \\ &= \lambda_1 S(v_1) + \cdots + \lambda_m S(v_m) \\ &= \lambda_1 w_1 + \cdots + \lambda_m w_m = T(v), \end{aligned}$$

where the second equality is the linearity of S. Since S and T agree on every elements of their domain V (and have the same codomain W), they are equal. □

The above theorem not only gives us an easy way to construct linear maps, it also allows us to easily check if two linear maps are equal. Instead of checking that $S, T \in \mathcal{L}(V,W)$ agree on all vectors of V, it is enough to check that they agree on a basis of V. In particular, if V is finite dimensional, then we only need to verify $\dim(V)$ (which is finite) many equalities, instead of verifying $\mathbf{F}^{\dim(V)}$ (which is infinite if $\mathbf{F}$ is infinite) of them.

As we defined it, $\mathcal{L}(V,W)$ is simply a set. We will endow it with an addition and a scalar multiplication in order to turn it into a vector space. This will be done in a similar fashion of what we did on $\mathbf{F}^S = \{f : S \to \mathbf{F}\}$.

Definition 3.1.16.

Let V and W be two $\mathbf{F}$-vector spaces, let S, T be two linear maps in $\mathcal{L}(V,W)$ and let $\lambda \in \mathbf{F}$ be a scalar. We define $S +_{\mathcal{L}(V,W)} T$ by $(S+T)(v) := S(v) + T(v)$ and $\lambda \cdot_{\mathcal{L}(V,W)} S$ by $(\lambda \cdot S)(v) := \lambda S(v)$ for every $v \in V$.

Theorem 3.1.17.

Let V and W be two $\mathbf{F}$-vector spaces. Then $(\mathcal{L}(V,W),+,\cdot)$ is an $\mathbf{F}$-vector space.

Proof. Firstly, we need to check that $S+T$ and λS are well defined. That is, we need to verify that they are indeed linear maps from V to W and not simply functions from V to W. This is elementary and left as an exercise to the reader.

Then, we have the zero map 0 in $(\mathcal{L}(V,W),+,\cdot)$. For all S we also have a map $-S$ defined by $(-S)(v) := -(S(v))$ for all $v \in V$. Once again, we let the reader verify that $-S$ is linear.

Finally, it remains to verify the 8 axioms of the definition of a vector space. This is elementary but fastidious and left as an exercise to the reader. □

Recall that we have the composition of maps $A \xrightarrow{f} B \xrightarrow{g} C$ (with $g \circ f : A \to C$). It turns out that the compositions of two linear maps is still linear.

Lemma 3.1.18. *Let $T \in \mathcal{L}(U,V)$ and $S \in \mathcal{L}(V,W)$ be two linear maps. Then the map $S \circ T : U \to W$ is linear.*

Proof. This is a straightforward verification, using $(S \circ T)(u) = S(T(u))$. □

Definition 3.1.19.

Let $T \in \mathcal{L}(U,V)$ and $S \in \mathcal{L}(V,W)$ be two linear maps. Then their **product** is $ST := S \circ T \in \mathcal{L}(U,W)$.

Remark 3.1.20.

As with general functions, the product of two linear maps $T \in \mathcal{L}(U,V)$ and $S \in \mathcal{L}(X,W)$ is not necessarily defined in general. It is defined only if $X = V$. In particular, the fact that ST is well defined ($V = X$) does not implies that TS is well-defined ($W = U$). Even if both ST and TS are defined, they do not necessarily have the same domains and codomains. Finally, even if they have the same domain and codomain they are not necessarily equal.
The examples given for general functions in Remark 1.2.8 were already linear maps and still apply.

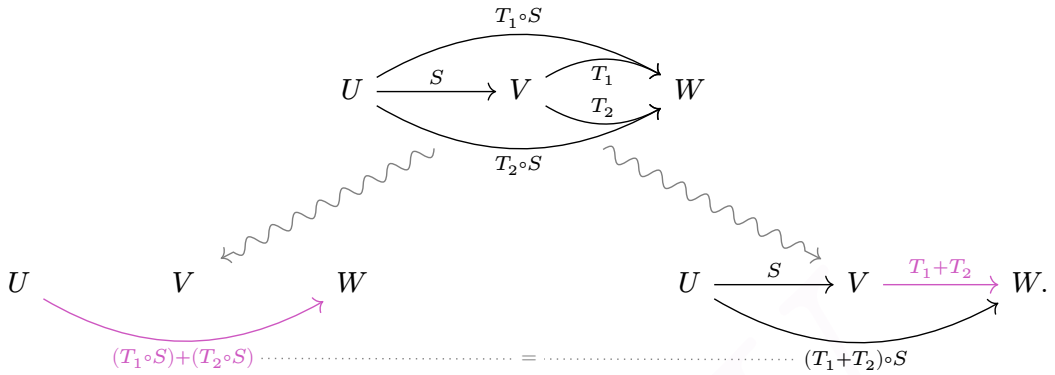
Products enjoy some nice properties.

Proposition 3.1.21.

1. *The product of linear maps is associative: $(T_3T_2)T_1 = T_3(T_2T_1)$. More precisely, the left-hand side of the equality is well-defined if and only if the right-hand side is, in which case they are equal.*
2. *The product of linear maps has identities: for all $T \in \mathcal{L}(V,W)$ we have $T\,\mathrm{Id}_V = T = \mathrm{Id}_W\,T$.*

3. *The product of linear maps is distributive over the addition:* $T(S_1+S_2) = TS_1+TS_2$ *and* $(T_1+T_2)S = T_1S+T_2S$ *for all* $S, S_1, S_2 \in \mathcal{L}(U,V)$ *and* $T, T_1, T_2 \in \mathcal{L}(V,W)$.

Before proving Proposition 3.1.21, let us show on diagrams the maps involved in $T(S_1+S_2) = TS_1+TS_2$. The situation for $(T_1+T_2)S = T_1S+T_2S$ is similar.



Proof of Proposition 3.1.21. The first and second assertion are true for any maps, not only for linear ones. See the discussion after Remark 1.2.8 for the first assertion and Lemma 1.2.10 for the second.

Let us prove the last assertion, namely the part $= T_1S + T_2S$ as the proof for $T(S_1 + S_2) = TS_1 + TS_2$ is similar. Let u be any vector in U. Then

$$\begin{aligned}((T_1+T_2)S))u &= (T_1+T_2)(Su)\\ &= T_1(Su)+T_2(Su)\\ &= (T_1S)u+(T_2S)u\\ &= (T_1S+T_2S)(u)\end{aligned}$$

and thus $(T_1+T_2)S = T_1S+T_2S$. □

3.1.2 Image and surjectivity

Any linear map $T \in \mathcal{L}(V,W)$ is a map, and therefore its **image**

$$\operatorname{Im}(T) = \{w \in W \mid \exists v \in V : w = T(v)\}$$

is a subset of W. The image of a linear map T is also called its **range**, and written $\operatorname{range}(T)$.

Images of linear maps are not only subsets of the codomain, but also subspaces.

Lemma 3.1.22. *If* $T \in \mathcal{L}(V,W)$, *then* $\operatorname{Im}(T)$ *is a subspace of* W.

Proof. We have $T(0) = 0$ and thus 0 belongs to $\operatorname{Im}(T)$. Let w_1, w_2 be two vectors in $\operatorname{Im}(T)$ and let $\lambda \in \mathbf{F}$ be a scalar. Then there exists v_1 and v_2 in V such that $T(v_1) = w_1$ and $T(v_2) = w_2$. Therefore $T(\lambda v_1 + v_2) = \lambda w_1 + w_2$, which proves that $\lambda w_1 + w_2$ is also in $\operatorname{Im}(T)$. This finishes the proof that $\operatorname{Im}(T)$ is a subspace. □

We have just seen that to any linear map $T \in \mathcal{L}(V, W)$ we can associate a subspace of W. It turns out that every subspace can be realised in this way.

Lemma 3.1.23. *Let $W \subseteq V$ be a subspace of the vector space V. Then there exists a linear map $T \in \mathcal{L}(V)$ such that $W = \mathrm{Im}(T)$.*

Proof. The proof is postponed to Proposition 3.3.4.

For the interested reader that would like to prove the proposition right now, here is a skeleton of the proof. Take any direct complement U of W so that $V = U \oplus W$ and define T to be the identity on W and the 0 map on U. □

The following trivial result links image and surjectivity.

Lemma 3.1.24. *A linear map $T \in \mathcal{L}(V, W)$ is surjective if and only if $\mathrm{Im}(T) = W$.*

Proof. This directly follows from the definition. □

One can therefore use $\mathrm{Im}(T)$ to quantify the default of surjectivity of T. The smaller $\mathrm{Im}(T)$ is, the further away T is to be surjective.

3.1.3 Kernel and injectivity

In the previous subsection, to any linear map $T \in \mathcal{L}(V, W)$ we associated a subspace of W and made a connection between this subspace and the surjectivity of T. In this subsection, we will associate a subspace of V to T and made a connection between this subspace and the injectivity of T.

Definition 3.1.25.

Let $T \in \mathcal{L}(V, W)$ be a linear map. We define its **kernel** (or **null space**) to be the subset

$$\ker(T) = \mathrm{null}(T) := \{v \in V \mid T(v) = 0\} \subseteq V.$$

While $\mathrm{Im}(T)$ was simply the set-theoretic image of T, we need the presence of a 0 to define $\ker(T)$. This explains why $\ker(T)$ has no analog for functions between sets.

The following result, dual to Lemma 3.1.22, justifies the name of null *space*.

Lemma 3.1.26. *If $T \in \mathcal{L}(V, W)$, then $\ker(T)$ is a subspace of V.*

Proof. By linearity $T(0) = 0$ and so $\ker(T)$ contains 0. Let u, v be two vectors in $\ker(T)$ and let $\lambda \in \mathbf{F}$ be a scalar. Then

$$T(\lambda u + v) = \lambda T(u) + T(v) = \lambda 0 + 0 = 0,$$

which proves that $\lambda u + v$ is also in $\ker(T)$. This finishes the proof that $\ker(T)$ is a subspace. □

We have just seen that we can associate a subspace to a linear map. It turns out that every subspace can be realised in this way, dually to Lemma 3.1.23.

Lemma 3.1.27. *Let $U \subseteq V$ be a subspace of the vector space V. Then there exists a linear map $T \in \mathcal{L}(V)$ such that $U = \ker(T)$.*

Proof. As with Lemma 3.1.23, the proof is postponed to Proposition 3.3.4.

The interested reader that would like to prove the lemma right now, can follow the same strategy as for Lemma 3.1.23. □

The image of a map was connected to surjectivity. It is no surprise that its kernel is connected to injectivity. While Lemma 3.1.24 was trivially true, this is not the case of the dual statement that requires a real proof.

Theorem 3.1.28.

A linear map $T \in \mathcal{L}(V, W)$ is injective if and only if $\ker(T) = \{0\}$.

Proof. "⇒" If v is in $\ker(T)$ we have $T(v) = 0 = T(0)$, which implies $v = 0$ by injectivity of T.

"⇐" Let u and v be two vectors in V such that $T(u) = T(v)$. We need to prove that $u = v$. We have $T(u - v) = T(u) - T(v) = 0$ so $u - v$ is in $\ker(T) = \{0\}$. We conclude that $u - v = 0$ and so that $u = v$ as desired. □

Heuristically, for $T \in \mathcal{L}(V, W)$ the kernel $\ker(T)$ is the subspace of V that is "compressed by T". The bigger it is, the further T is from being injective.

An injective linear maps is sometimes called an **embedding of vector spaces**.

We now go back to some examples of linear maps we have seen and compute their kernels and images.

Example 3.1.29. Let $0 \in \mathcal{L}(V, W)$ be the zero map. We have $\ker(0) = V$ and $\mathrm{Im}(0) = \{0\}$. We conclude that the zero map is injective if and only if $V = \{0\}$ and surjective if and only if $W = \{0\}$.

Example 3.1.30. Let $T \in \mathcal{L}(\mathcal{P}(\mathbf{R}), \mathcal{P}(\mathbf{R}))$ be the multiplication by x, that is $T(p(x)) = xp(x)$. Then its kernel $\ker(T)$ is the $\{0\}$ subspace while its image $\mathrm{Im}(T)$ is the subspace of polynomials with constant coefficient 0. We conclude that the map T is injective but not surjective.

Example 3.1.31. Let $D \in \mathcal{L}(\mathcal{P}(\mathbf{R}), \mathcal{P}(\mathbf{R}))$ be the differentiation map $D(p) = p'$ on polynomials. Then its kernel $\ker(D)$ is the subspace of constant polynomials while its image $\mathrm{Im}(D)$ is the whole space $\mathcal{P}(\mathbf{R})$. Indeed, if p is any polynomial, there exists an antiderivative q such that $q' = p$. We conclude that the differentiation map D is surjective but not injective.

Example 3.1.32. As we have seen, the differentiation map $D \in \mathcal{L}(\mathcal{P}(\mathbf{R}), \mathcal{P}(\mathbf{R}))$ is surjective. Similarly, the differentiation map $D \in \mathcal{L}(\mathcal{P}(\mathbf{R})_5, \mathcal{P}(\mathbf{R})_4)$ is surjective. However neither $D \in \mathcal{L}(\mathcal{P}(\mathbf{R})_5, \mathcal{P}(\mathbf{R})_5)$ nor $D \in \mathcal{L}(\mathcal{P}(\mathbf{R})_4, \mathcal{P}(\mathbf{R})_4)$ are surjective (the image of the first map does not contain x^5, while the image of the second map does not contain x^4). This example shows that both the domain and the codomain of a linear map are important for surjectivity.

3.1.4 Rank-nullity theorem

The aim of this subsection is to prove the Rank–nullity theorem, which is the fundamental theorem of linear maps.

Theorem 3.1.33 (Rank-nullity theorem)**.**

Let $T \in \mathcal{L}(V, W)$ be a linear map. Then

$$\dim(V) = \dim(\ker(T)) + \dim(\mathrm{Im}(T)).$$

In particular, if V is finite dimensional, then so is $\mathrm{Im}(T)$.

Proof. We will prove the theorem under the assumption that V is finite dimensional. The general proof is similar.

As always with dimension formula, the proof uses bases. More precisely, we will start with a basis for a subspace and then extend it to the whole space.

Let $(u_1, \dots, u_m)$ be a basis for $\ker(T)$ and extend it to a basis $\mathscr{B} := (u_1, \dots, u_m, v_1, \dots, v_n)$ of V. So $\dim((\ker(T)) = m$ and $\dim(V) = m + n$. We claim that $\mathscr{C} := (Tv_1, \dots, Tv_n)$ is a basis of $\mathrm{Im}(T)$. If the claim holds, then $\mathrm{Im}(T)$ has dimension n and we are done.

We now prove the claim. We need to prove three things: that $\mathscr{C} \subseteq \mathrm{Im}(T)$, that it is linearly independent and that it is spanning. It is trivial that $\mathscr{C} \subseteq \mathrm{Im}(T)$. We now prove linear independence. Suppose that there exists scalars $(\lambda_i)_{i=1}^n$ such that

$$0 = \lambda_1 T(v_1) + \cdots + \lambda_n T(v_n) = T(\lambda_1 v_1 + \cdots + \lambda_n v_n).$$

This implies that $\lambda_1 v_1 + \cdots + \lambda_n v_n$ is in $\ker(T)$ and so there exist scalars $(\mu_i)_{i=1}^m$ such that

$$\lambda_1 v_1 + \cdots + \lambda_n v_n = \mu_1 u_1 + \cdots + \mu_m u_m,$$

or equivalently such that

$$0 = \mu_1 u_1 + \cdots + \mu_m u_m - \lambda_1 v_1 - \cdots - \lambda_n v_n.$$

Since $\mathscr{B}$ is a basis, it is a linearly independent family and so all the λ_i (and the μ_j) are 0. This finishes the proof that $\mathscr{C}$ is linearly independent.

Finally, we prove that $\mathscr{C}$ spans $\mathrm{Im}(T)$. Let w be any element in $\mathrm{Im}(T)$. So there exists $v \in V$ such that $T(v) = w$. Using that $\mathscr{B}$ is spanning, there exists $(\lambda_i)_{i=1}^n$ and $(\mu_i)_{i=1}^m$ such that

$$v = \mu_1 u_1 + \cdots + \mu_m u_m + \lambda_1 v_1 + \cdots + \lambda_n v_n.$$

By applying T on both sides, we obtain

$$\begin{aligned} w = T(v) &= T(\mu_1 u_1 + \cdots + \mu_m u_m + \lambda_1 v_1 + \cdots + \lambda_n v_n) \\ &= \mu_1 T(u_1) + \cdots + \mu_m T(u_m) + \lambda_1 T(v_1) + \cdots + \lambda_n T(v_n) \\ &= \lambda_1 T(v_1) + \cdots + \lambda_n T(v_n), \end{aligned}$$

and so w is in $\mathrm{Im}(T)$, proving that $\mathscr{C}$ is spanning. □

To go further

The above proof shows a bit more than what was announced, namely:

Let $T \in \mathcal{L}(V, W)$ be a linear map. Then $V \cong \ker(T) \oplus \mathrm{Im}(T)$, meaning that V and $\ker(T) \oplus \mathrm{Im}(T)$ are "similar as vector spaces", see Definition 3.1.40.

The formula for dimension follows.

Infinite dimensional vector spaces

Both $V \cong \ker(T) \oplus \mathrm{Im}(T)$ and the dimension formula $\dim(V) = \dim(\ker(T)) + \dim(\mathrm{Im}(T))$ hold for an arbitrary, possibly infinite dimensional, vector space V. The proof relies on the possibility given by 2.4.47 to extend a basis of a subspace to a basis of the whole space. It therefore ultimately relies on the axiom of choice, see the Infinite dimensional spaces box on page 49.
But what does the equality $\dim(V) = \dim(\ker(T)) + \dim(\mathrm{Im}(T))$ really means of $\dim(V)$ is infinite? It means that at least one of $\ker(T)$ and $\mathrm{Im}(T)$ is infinite dimensional and that we have $\dim(V) = \max\{\dim(\ker(T)), \dim(\mathrm{Im}(T))\}$.

Theorem 3.1.33 has many important consequences and applications.

Proposition 3.1.34. *Let V and W be two vector spaces.*

1. *If $\dim(V) > \dim(W)$, then no linear map $T \in \mathcal{L}(V, W)$ is injective.*
2. *If $\dim(V) < \dim(W)$, then no linear map $T \in \mathcal{L}(V, W)$ is surjective.*

Proof. "1" We will prove this statement under the assumption that V (and hence also W) is finite dimensional. The proof for infinite dimensional vector spaces is way more complex and we will not see it.

Since $\mathrm{Im}(T)$ is a subspace of W, we have $\dim(\mathrm{Im}(T)) \leq \dim(W) < \dim(V)$. It follows from $\dim(V) = \dim(\ker(T)) + \dim(\mathrm{Im}(T))$ that $\dim(\ker(T)) > 1$ and so that T is not injective.

"2" By the rank-nullity theorem, we have $\dim(\mathrm{Im}(T)) \leq \dim(V) < \dim(W)$. Therefore, $\mathrm{Im}(T) \neq W$ is a proper subspace and T is not surjective. □

Example 3.1.35. There exists no surjective linear map $\mathbf{R} \to \mathbf{R}^2$ and no injective linear map $\mathbf{R}^2 \to \mathbf{R}$, even if there exists a bijection between $\mathbf{R}$ and $\mathbf{R}^2$. See the discussion at the beginning of Subsection 3.1.1.

Recall from Lemma 1.2.17 that if A and B are finite sets with the same cardinality, then a function $f : A \to B$ is injective if and only if it is surjective, if and only if it is bijective. A similar statement holds for finite dimensional vector spaces and linear maps.

Proposition 3.1.36. *Let V and W be finite dimensional vector spaces of the same dimension. For a linear map $T \in \mathcal{L}(V, W)$ the following are equivalent:*

I. T *is bijective;*

II. T *is injective;*

III. T *is surjective.*

Proof. On one hand, the map T is injective if and only if $\ker(T) = \{0\}$, if and only if $\dim(\ker(T)) = 0$. On the other hand, the map T is surjective if and only if $\mathrm{Im}(T) = W$, if and only if $\dim(\mathrm{Im}(T)) = \dim(W)$ by Corollary 2.4.45 (here we use that W is finite dimensional). The conclusion follows from the equality $\dim(W) = \dim(V) = \dim(\ker(T)) + \dim(\mathrm{Im}(T))$. □

Remark 3.1.37.

Proposition 3.1.36 is one of the few statements that are true for finite dimensional vector spaces but not true in general. See Example 3.1.31.

Here is a nice application of Proposition 3.1.36.

Exercise 3.1.38. Show that for all polynomial $q \in \mathcal{P}(\mathbf{R})$ there exists a polynomial $p \in \mathcal{P}(\mathbf{R})$ such that $\left((x^2+5x+7)p\right)'' = q$.

Solution. Let $m := \deg(q)$. Define

$$\begin{aligned} T\colon \mathcal{P}(\mathbf{R})_m &\longrightarrow \mathcal{P}(\mathbf{R})_m \\ p &\longmapsto \left((x^2+5x+7)p\right)''. \end{aligned}$$

The degree of $\left((x^2+5x+7)p\right)''$ is at most $(m+2)-2 = m$, so this map is well-defined. We claim that T is injective and thus surjective by Proposition 3.1.36. So there exists p such that $T(p) = q$.

It remains to prove the claim. Let $p_1 = a_0 + \cdots + a_m x^m$ and $p_2 = b_0 + \cdots + b_m x^m$ be two distinct polynomials of degree at most m. Since they are distinct, there exists $i \in \{1, \ldots, m\}$ such that $a_i \neq b_i$. Take i_0 to be minimal for this property. Then the coefficients of x^{i_0} in $T(p_1)$ and in $T(p_2)$ are not the same, showing that $T(p_1) \neq T(p_2)$ as desired. □

3.1.5 Application to linear systems

The study of general linear maps has important consequences for the solutions of linear systems of equations, as demonstrated below.

An **homogeneous system of linear equations** (with constant coefficients) is a system of the form

$$\begin{cases} a_{11}x_1 + \cdots + a_{1n}x_n &= 0 \\ \vdots & \\ a_{m1}x_1 + \cdots + a_{mn}x_n &= 0 \end{cases} \tag{3.1}$$

where for $i \in \{1, \dots, m\}$ and $j \in \{1, \dots, n\}$ the a_{ij} belong to $\mathbf{F}$ and the x_j are independent variables. The System (3.1) has m equations and n indeterminants. Such a system can be rephrased using the linear map

$$\begin{aligned} T \colon \mathbf{F}^n &\longrightarrow \mathbf{F}^m \\ \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} &\longmapsto \begin{bmatrix} a_{11}x_1 + \cdots + a_{1n}x_n \\ \vdots \\ a_{m1}x_1 + \cdots + a_{mn}x_n \end{bmatrix}. \end{aligned} \tag{3.2}$$

A vector $x = [x_1, \dots, x_n]^\mathsf{T}$ is a solution of (3.1) if and only if it belongs to $\ker(T)$.

As a direct corollary, we obtain that if $m < n$, then (3.1) has a non-trivial solution. Indeed, $\dim(\ker(T)) = \dim(\mathbf{F}^n) - \dim(\mathrm{Im}(T)) \geq n - m$.

An **inhomogeneous system of linear equations** (with constant coefficients) is a system of the form

$$\begin{cases} a_{11}x_1 + \cdots + a_{1n}x_n &= c_1 \\ \vdots & \\ a_{m1}x_1 + \cdots + a_{mn}x_n &= c_n \end{cases} \tag{3.3}$$

where for $i \in \{1, \dots, m\}$ and $j \in \{1, \dots, n\}$ the a_{ij} and c_i belong to $\mathbf{F}$, with at least one $c_i \neq 0$, and the x_j are independent variables. As before, such a system can be rephrased using the linear map T from (3.2). This time, x is a solution of the inhomogeneous system (3.3) if and only if $T(x) = c$, where $c = [c_1, \dots, c_m]^\mathsf{T}$.

We hence obtain that if $m > n$ there exists $0 \neq c \in \mathbf{F}^n$ such that (3.3) has no solution. Indeed, $\dim(\mathrm{Im}(T)) \leq \dim(\mathbf{F}^n) = n < m = \dim(\mathbf{F}^m)$, so $\mathrm{Im}(T) \subsetneq \mathbf{F}^m$.

Proposition 3.1.39. *Suppose $c \in \mathrm{Im}(T)$ and $x_p \in \mathbf{F}^n$ is a solution of (3.3). Then the solution sets of (3.3) is*

$$x_p + \ker(T) = \{x_p + y \mid y \in \ker(T)\}.$$

Proof. "$\subseteq$" For any x in $\mathbf{F}^n$ we always have $x = x_p + (x - x_p)$. Now, if x is a solution of (3.3), then $T(x) = c$ and thus $T(x - x_p) = 0$. That is $x - x_p$ is in $\ker(T)$ and we are done.

"$\supseteq$" If $x = x_p + y$ with $y \in \ker(T)$, then $T(x) = T(x_p) + T(y) = c + 0 = 0$. □

3.1.6 Isomorphisms of vector spaces

Recall that two sets A and B are considered similar if and only if there exist functions $f \colon A \to B$ and $g \colon A \to B$ that are the inverse of each other, meaning that $g \circ f = \mathrm{Id}_A$ and $f \circ g = \mathrm{Id}_B$. For sets, the existence of such a pair of functions f and g is equivalent to the existence of a bijective function $f \colon A \to B$.

Since any linear map $T \in \mathcal{L}(V, W)$ is a function, one can ask if it is invertible as a function, or not. That is, $T \in \mathcal{L}(V, W)$ is invertible if there exists a function (a priori not necessarily a linear map) $g \colon W \to V$ such that $g \circ T = \mathrm{Id}_V$ and $T \circ g = \mathrm{Id}_W$. In order to consider V and W "similar as vector spaces" we want an invertible linear map T such that the inverse is also a linear map. If such a T exists, anything in V can be transposed to W by T without loosing any information (and vice-versa from W to V by T^{-1}).

Definition 3.1.40.

A linear map $T \in \mathcal{L}(V, W)$ is an **isomorphism**[a] if it is invertible and its inverse T^{-1} is also linear. That is, $T \in \mathcal{L}(V, W)$ is an isomorphism if there exists $S \in \mathcal{L}(W, V)$ such that $ST = \mathrm{Id}_V$ and $TS = \mathrm{Id}_W$.
Two vector spaces V, W are **isomorphic** if there exists an isomorphism $T \in \mathcal{L}(V, W)$. In such case, we write $V \cong W$.

[a] Isomorphism comes from the ancient greek ἴσος μορφή, which roughly means *equal shape*.

We have a result similar to Theorem 1.2.16.

Theorem 3.1.41.

A linear map $T \in \mathcal{L}(V, W)$ is an isomorphism if and only if it is a bijection.

Proof. By Theorem 1.2.16, the map T is a bijection if and only if there exists a set-theoretic inverse function $T^{-1} : W \to V$. We hence need to prove that if T is linear, then its inverse map is also linear.

Let w_1 and w_2 be two vectors in W and let $\lambda \in \mathbf{F}$ be a scalar. Write $v_1 := T^{-1}(w_1)$ and $v_2 := T^{-1}(w_2)$. So $T(v_1) = w_1$ and $T(v_2) = w_2$. Then

$$\begin{aligned} T^{-1}(\lambda w_1 + w_2) &= T^{-1}(\lambda T(v_1) + T(v_2)) \\ &= T^{-1}(T(\lambda v_1 + v_2)) \\ &= (T^{-1}T)(\lambda v_1 + v_2) \\ &= \lambda v_1 + v_2 = \lambda T^{-1}(w_1) + T^{-1}(w_2), \end{aligned}$$

where we used linearity of T for the second equality. □

Using the above theorem one can easily exhibit examples of non-invertible linear maps.

Example 3.1.42. Let $T \in \mathcal{L}(\mathcal{P}(\mathbf{R}), \mathcal{P}(\mathbf{R}))$ be the multiplication by x $(T(p(x)) = xp(x))$ and let D
$in\mathcal{L}(\mathcal{P}(\mathbf{R}), \mathcal{P}(\mathbf{R}))$ be the differentiation operator $(D(p(x)) = p'(x))$. Neither D nor T is invertible, as D is not injective (but surjective) and T is not surjective (but injective). See Examples 3.1.30 and 3.1.31.

Other examples include the backward shift $T : (x_0, x_1, x_2, \dots) \mapsto (x_1, x_2, x_3 \dots)$ (Example 3.1.11) and the forward shift $S : (x_0, x_1, x_2, \dots) \mapsto (0, x_0, x_1, \dots)$ (see Example 3.1.12), both belonging to $\mathcal{L}(\mathbf{F}^{\mathbf{N}}, \mathbf{F}^{\mathbf{N}})$. Neither S nor T is invertible, as T is not injective (but surjective) and S is not surjective (but injective).

Isomorphism of vector spaces is an *equivalence relation* on the class of $\mathbf{F}$-vector spaces, meaning:

Theorem 3.1.43.

The following hold for all vector spaces U, V and W:

1. $V \cong V$; *(reflexivity)*
2. *If* $V \cong W$, *then* $W \cong V$; *(symmetry)*
3. *If both* $U \cong V$ *and* $V \cong W$, *then* $U \cong W$. *(transitivity)*

Proof. "1" The identity map $\mathrm{Id}_V \in \mathcal{L}(V)$ is an isomorphism.
"2" If $T \in \mathcal{L}(V,W)$ is an isomorphism from V to W, then $T^{-1} \in \mathcal{L}(W,V)$ is an isomorphism from W to V.
"3" Let $T \in \mathcal{L}(V,W)$ and $S \in \mathcal{L}(U,V)$ be isomorphism. Then $TS \in \mathcal{L}(U,W)$ is an isomorphism with inverse $S^{-1}T^{-1}$. □

We already know another equivalence relation: $A \simeq B$ (being in bijection) is an equivalence relation for sets. Other equivalence relations include: having the same absolute value for real numbers or having the same age for people.

We have said that two isomorphic vector spaces are similar as vector space. Here is a concrete application of this principle.

Lemma 3.1.44. *Let* $V \cong W$ *be two isomorphic vector spaces. Then* $\dim(V) = \dim(W)$.

Proof. This directly follows from the rank-nullity theorem. For $T \in \mathcal{L}(V,W)$ we have

$$\dim(V) = \dim(\ker(T)) + \dim(\mathrm{Im}(T)).$$

If T is an isomorphism, it is bijective and thus $\dim(\ker(T)) = 0$ and $\dim(\mathrm{Im}(T)) = \dim(W)$. □

One can alternatively derives the above Lemma from the following proposition.

Proposition 3.1.45. *Let* $T \in \mathcal{L}(V,W)$. *Then*

1. *If* T *is injective and* $\mathscr{B} = (v_\alpha)_{\alpha \in I}$ *is a linearly independent family (in* V*), then* $T(\mathscr{B}) = (Tv_\alpha)_{\alpha \in I}$ *is linearly independent (in* W*);*
2. *If* T *is surjective and* $\mathscr{B}$ *is a spanning family (in* V*), then* $T(\mathscr{B}) = (Tv_\alpha)_{\alpha \in I}$ *is spanning (in* W*);*
3. *If* T *is an isomorphism and* $\mathscr{B}$ *is a basis (of* V*), then* $T\mathscr{B}$ *is a basis (of* W*).*

Proof. "1" This is left as an exercise. Tutorial 4, Question 3
"2" Let w be any vector in W and let v be a preimage: $T(v) = w$. Since $\mathscr{B}$ is spanning, there exists $v_1, \dots, v_n \in \mathscr{B}$ and scalars $\lambda_1, \dots, \lambda_n \in \mathbf{F}$ such that $v = \lambda_1 v_1 + \cdots + \lambda_n v_n$. Applying T to both sides we obtain $w = \lambda_1 T(v_1) + \cdots + \lambda_n T(v_n)$, which shows that $T(\mathscr{B})$ is spanning.
"3" This directly follows from the two above properties. □

We know that two sets are in bijection if and only if they have the same cardinality (this follows from Theorem 1.2.16 for finite sets, and is the definition of cardinality for infinite sets). A similar result holds for vector spaces if we replace cardinality by dimension. That is, the converse of Lemma 3.1.44 holds.

Theorem 3.1.46.

Let V and W be two vector spaces. Then $V \cong W$ if and only if $\dim(V) = \dim(W)$.

Proof. By Lemma 3.1.44, $\dim(V) = \dim(W)$ is a necessary condition for V and W to be isomorphic. We hence need to show that it is also a sufficient condition.

Let $(v_\alpha)_{\alpha\in I}$ and $(w_\alpha)_{\alpha\in I}$ be respectively bases of V and W of the same cardinality. Let $T \in \mathcal{L}(V,W)$ be the unique linear map in $\mathcal{L}(V,W)$ such that $T(v_\alpha) = w_\alpha$ for all $\alpha \in I$ and let $S \in \mathcal{L}(W,V)$ be the unique linear map in $\mathcal{L}(W,V)$ such that $S(w_\alpha) = v_\alpha$ for all $\alpha \in I$. We claim that T is an isomorphism, with $T^{-1} = S$. It directly follows from the definition that for any $\alpha \in I$ we have $(ST)(v_\alpha) = v_\alpha = \mathrm{Id}_V(v_\alpha)$. Since ST and Id_V are two linear maps in $\mathcal{L}(V)$ that agree on a basis, they are identical: $ST = \mathrm{Id}_V$. Similarly we have $TS = \mathrm{Id}_W$ and so S and T are isomorphisms with $S = T^{-1}$. □

Kernels and Images are invariant by isomorphisms. More precisely, we have:

Lemma 3.1.47. *Let $T \in \mathcal{L}(V,W)$ be a linear map and let $S_1 \in \mathcal{L}(U_1,V)$ and $S_2 \in \mathcal{L}(W,U_2)$ be isomorphisms. Then*

1. $\ker(T) = \ker(S_2T)$,
2. $\mathrm{Im}(TS_1) = \mathrm{Im}(T)$.

Proof. A vector v is in the kernel of T if and only if $Tv = 0$, if and only if $(S_2Z)(v) = S_2(Tv) = 0$ since S_2 is an isomorphism.

A vector $w \in W$ is in $\mathrm{Im}(T)$ if and only if there exists $v \in V$ such that $Tv = w$. But any v in V can uniquely be written as S_1u for $u \in U$. So $w \in W$ is in $\mathrm{Im}(T)$ if and only if there exists $u = S_1^{-1}v \in U$ such that $w = Tv = T(S_1u) = (TS_1)u$. □

Definition 3.1.48.

Let V be a finite dimensional vector space with a given basis $\mathscr{B} = (v_1, \dots, v_m)$ (so $m = \dim(V)$). Let $\mathscr{E} = (e_1, \dots, e_m)$ be the standard basis of $\mathbf{F}^m$, that is $e_i = [0, \dots, 0, 1, 0, \dots, 0]^\mathsf{T}$ has a 1 in position i and 0 elsewhere. Define the map $[\,\cdot\,]_\mathscr{B} \in \mathcal{L}(V, \mathbf{F}^m)$ to be the unique linear map such that $[v_i]_\mathscr{B} = e_i$ for all $i \in \{1, \dots, m\}$.

$$[\,\cdot\,]_\mathscr{B} : V \longrightarrow \mathbf{F}^{\dim(V)}$$
$$v_i \longmapsto e_i.$$

The following is an important corollary of (the proof of) Theorem 3.1.46.

Corollary 3.1.49. *Let V be a finite dimensional vector space with a given basis $\mathscr{B}$. Then the map $[\,\cdot\,]_\mathscr{B} \in \mathcal{L}(V, \mathbf{F}^{\dim(V)})$ is an isomorphism.*

Infinite dimensional vector spaces

A statement similar to Corollary 3.1.49 is also true for infinite dimensional vector spaces, but we need to be careful about the details. Indeed, let V be an $\mathbf{F}$-vector space. Then it has a basis $\mathscr{B}$ of cardinality $\dim(V)$. We have two natural candidates to play the role of $\mathbf{F}^n$: the product $\prod_{\mathscr{B}} \mathbf{F} = \mathbf{F}^{\mathscr{B}}$ (the space of all functions from $\mathscr{B}$ to $\mathbf{F}$, see Subsection 2.2.1) and the direct sum $\bigoplus_{\mathscr{B}} \mathbf{F} = \mathbf{F}^{(\mathscr{B})}$ (the subspace of $\mathbf{F}^{\mathscr{B}}$ of functions that are 0 for all but finitely many $b \in \mathscr{B}$, see the Infinite dimensional spaces' box on page 71). Since $\operatorname{span}(\mathscr{B})$ consists of linear combinations of finitely many elements of $\mathscr{B}$ we have the following generalisation of Corollary 3.1.49.

Let V be an $\mathbf{F}$-vector space and let $\mathscr{B}$ be a basis of V. Then $V \cong \bigoplus_{\mathscr{B}} \mathbf{F} = \mathbf{F}^{(\mathscr{B})}$.

It follows from this result that $\dim(\bigoplus_{\mathscr{B}} \mathbf{F}) = \#\mathscr{B}$. However, for an infinite $\mathscr{B}$ we have $\dim(\prod_{\mathscr{B}} \mathbf{F}) = \#(\mathbf{F}^{\mathscr{B}}) = (\#\mathbf{F})^{\#\mathscr{B}} > \#\mathscr{B}$. The main idea is to use $\prod_{\mathscr{B}} \mathbf{F} \cong \mathbf{F}^{\mathscr{B}} =: V$ and to use the formula $\dim(V) \leq \#V = \max(\dim(V), \#\mathbf{F})$ of the To go further's box on page 49. It then remains to show that $\mathbf{F}^S$ admits a linearly independent family of size at least $\mathbf{F}$. A detailed proof is given in Jacobson, *Lectures in Abstract Algebra,* Volume 2, Chapter 9, § 5.

Example 3.1.50. Let $\mathcal{P}(\mathbf{F})_n$ the vector space of polynomial of degree at most n. Then $\dim \mathcal{P}(\mathbf{F})_n = n + 1$ and we have the standard basis: $\mathscr{B} = (1, x, \dots, x^n)$. Then

$$\begin{aligned} \mathcal{P}(\mathbf{F})_n &\longrightarrow \mathbf{F}^{n+1} \\ a_0 + \cdots + a_n x^n &\longmapsto [a_0, \dots, a_n]^{\mathsf{T}} \end{aligned}$$

is an isomorphism.

Similarly, let $\mathcal{P}(\mathbf{F})$ be the vector space of all polynomial and let $\mathscr{B} = (1, x, x^2, \dots)$ be the standard basis. Then

$$\begin{aligned} \mathcal{P}(\mathbf{F})_n &\longrightarrow \mathbf{F}^{(\mathbf{N})} = \bigoplus_{\mathbf{N}} \mathbf{F} \\ a_0 + \cdots + a_m x^m &\longmapsto (a_0, \dots, a_m, 0, \dots) \end{aligned}$$

is an isomorphism.

Theorem 3.1.46 is good news for us, as it means that in order to study an abstract vector space V we only need to find a basis $\mathscr{B}$ and then one can use the isomorphism $[\,\cdot\,]_{\mathscr{B}} \colon V \to \bigoplus_{\mathscr{B}} \mathbf{F}$. Moreover, if V is finite dimensional, then $\bigoplus_{\mathscr{B}} \mathbf{F} = \mathbf{F}^{\dim(V)}$. The bad news is that, has we have seen, in general basis are not unique. So if $\mathscr{B}$ and $\mathscr{C}$ are two different bases, then $[\,\cdot\,]_{\mathscr{B}}$ and $[\,\cdot\,]_{\mathscr{C}}$ are two different isomorphisms $V \xrightarrow{\cong} \bigoplus_{\mathscr{B}} \mathbf{F}$.

3.2 Matrices

Matrices play an important role in the theory of vector spaces. We will start this section by reviewing the definitions of matrices. We will later see in Subsection 3.2.2 that any linear map can be represented by a matrix.

3.2.1 The vector space of matrices

Recall the classical definition of matrices.

Definition 3.2.1.

For $\mathbf{F}$ a field and m, n two positive integers, we define

$$\mathbf{F}^{m,n} := \left\{ \begin{bmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,n} \\ a_{2,1} & a_{2,2} & \cdots & a_{2,n} \\ \vdots & \vdots & & \vdots \\ a_{m,1} & a_{m,2} & \cdots & a_{m,n} \end{bmatrix} \middle| \, a_{i,j} \in \mathbf{F} \text{ for } i \in \{1, \dots, m\}, j \in \{1, \dots, n\} \right\}$$

to be the set of $m \times n$ matrices with entries in $\mathbf{F}$.
When m and n are known, we often forget the subscripts and simply write $A = [a_{i,j}] \in \mathbf{F}^{m,n}$.
For $A[a_{i,j}]_{\substack{1 \leq i \leq m, \\ 1 \leq j \leq n}}, B = [b_{i,j}]_{\substack{1 \leq i \leq m, \\ 1 \leq j \leq n}} \in \mathbf{F}^{m,n}$ and $\lambda \in \mathbf{F}$ we define

$$A +_{\mathbf{F}^{m,n}} B := [a_{i,j} + b_{i,j}]_{\substack{1 \leq i \leq m, \\ 1 \leq j \leq n}} = \begin{bmatrix} a_{1,1} + b_{1,1} & \cdots & a_{1,n} + b_{1,n} \\ \vdots & \ddots & \vdots \\ a_{m,1} + b_{m,1} & \cdots & a_{m,n} + b_{m,n} \end{bmatrix}$$

and

$$\lambda \cdot_{\mathbf{F}^{m,n}} A := [\lambda a_{i,j}]_{\substack{1 \leq i \leq m, \\ 1 \leq j \leq n}} = \begin{bmatrix} \lambda a_{1,1} & \cdots & \lambda a_{1,n} \\ \vdots & \ddots & \vdots \\ \lambda a_{m,1} & \cdots & \lambda a_{m,n} \end{bmatrix}.$$

Finally, when $m = n$ we define the **identity matrix** $\mathrm{Id}_m \in \mathbf{F}^{m,m}$ to be the $m \times m$ matrix with 1 on the diagonal and 0 elsewhere.

Lemma 3.2.2. *$(\mathbf{F}^{m,n}, +, \cdot)$ is an $\mathbf{F}$–vector space.*

Proof. The zero and the additive inverse are respectively given by $[0]$ and $-[a_{i,j}] = [-a_{i,j}]$. The verification of the axioms of a vector space is an elementary but fastidious exercise left to the reader. □

For $i \in \{1, \dots, m\}$ and $j \in \{1, \dots, n\}$, let

$$E_{i,j} := \begin{array}{c} \\ 1 \\ \vdots \\ i-1 \\ i \\ i+1 \\ \vdots \\ n \end{array} \begin{array}{c} \begin{array}{ccccc} 1 & \cdots & j-1 & j & j+1 \cdots n \end{array} \\ \begin{bmatrix} 0 & \cdots & 0 & 0 & 0 \\ \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & \cdots & 0 & 0 & 0 \\ 0 & \cdots & 0 & 1 & 0 \\ 0 & \cdots & 0 & 0 & 0 \\ \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & \cdots & 0 & 0 & 0 \end{bmatrix} \end{array}$$

be the matrix with a 1 in th coordinate (i, j) and 0 everywhere else. The family $(E_{i,j})_{\substack{1 \le i \le m, \\ 1 \le j \le n}}$ is the **standard basis of $\mathbf{F}^{m,n}$**.

Proposition 3.2.3. *The standard basis of $\mathbf{F}^{m,n}$ is indeed a basis. As a consequence,* $\dim(\mathbf{F}^{m,n}) = m \cdot n$.

Proof. We need to prove that the family $(E_{i,j})_{\substack{1 \le i \le m, \\ 1 \le j \le n}}$ is both linearly independent and spanning.

Let $[a_{i,j}]$ be any matrix in $\mathbf{F}^{m,n}$. All the $a_{i,j}$ belongs to $\mathbf{F}$ and we have

$$[a_{i,j}] = \sum_{\substack{1 \le i \le m, \\ 1 \le j \le n}} a_{i,j} E_{i,j},$$

proving that the $E_{i,j}$a are spanning.

Suppose now that $[0] = \sum_{i,j} \lambda_{i,j} E_{i,j}$ with the $\lambda_{i,j} \in \mathbf{F}$. We have $[0] = \sum_{i,j} \lambda_{i,j} E_{i,j} = [\lambda_{i,j}]$. This implies that $\lambda_{i,j} = 0$ for all i and j, proving that the $E_{i,j}$ are linearly independent. □

Corollary 3.2.4. $\mathbf{F}^{m,n} \cong \mathbf{F}^{m \cdot n}$.

If $A \in \mathbf{F}^{m,n}$ and $B \in \mathbf{F}^{n,k}$, then we have a matrix multiplication and $AB \in \mathbf{F}^{m,k}$. We will see the general case later in Definition 3.2.26, but for now we will only need the specific case where $B \in \mathbf{F}^{n,1} \cong \mathbf{F}^n$ is a vector.

Definition 3.2.5.

Let $A \in \mathbf{F}^{m,n}$ be a matrix and $B \in \mathbf{F}^n$ be a vector. The **product** $A \cdot B$ is the vector of $\mathbf{F}^m$ defined by

$$\begin{bmatrix} a_{1,1} & \cdots & a_{1,n} \\ \vdots & & \vdots \\ a_{m,1} & \cdots & a_{m,n} \end{bmatrix} \begin{bmatrix} b_1 \\ \vdots \\ b_n \end{bmatrix} := \begin{bmatrix} a_{1,1}b_1 + \cdots + a_{1,n}b_n \\ \vdots \\ a_{m,1}b_1 + \cdots + a_{m,n}b_n \end{bmatrix}.$$

Lemma 3.2.6. *Let $A \in \mathbf{F}^{m,n}$. Left multiplication by A is a linear map from $\mathbf{F}^n$ to $\mathbf{F}^m$.*

Proof. The demonstration is elementary and left to the reader. □

Remark 3.2.7.

Be careful that a $m \times n$ matrix is a linear map from $\mathbf{F}^n$ to $\mathbf{F}^m$!

3.2.2 Matrix representation of linear maps

The concrete spaces $\mathbf{F}^n$ were our first examples of vector spaces. We have later seen in Corollary 3.1.49 that any abstract finite dimensional vector space V is isomorphic to $\mathbf{F}^{\dim(V)}$. More precisely, given a basis $\mathscr{B}$ of V, one can construct an explicit isomorphism $[\,\cdot\,]_{\mathscr{B}} \colon V \xrightarrow{\cong} \mathbf{F}^{\dim(V)}$. In the last subsection we saw that multiplication by a matrix $A \in \mathbf{F}^{m,n}$ is a concrete example of a linear map in $\mathcal{L}(\mathbf{F}^n, \mathbf{F}^m)$. In this subsection, we will see that all linear maps in $\mathcal{L}(\mathbf{F}^n, \mathbf{F}^m)$ are of this form. Moreover, given two finite dimensional abstract vector spaces and an abstract linear map $T \in \mathcal{L}(V, W)$ we will see how to represent T by a matrix in $\mathbf{F}^{\dim(W),\dim(V)}$. Such a matrix will depend on a choice of a basis of V and of a basis of W.

Recall that if W is a finite dimensional $\mathbf{F}$-vector space of dimension n and $\mathscr{C} = (w_1, \dots, w_n)$ is a basis of W we have an isomorphism

$$W \xrightarrow{[\cdot]_{\mathscr{C}}} \mathbf{F}^{\dim(W)}$$

$$w = \lambda_1 w_1 + \cdots + \lambda_n w_n \longmapsto [v]_{\mathscr{C}} = \begin{bmatrix} \lambda_1 \\ \vdots \\ \lambda_n \end{bmatrix}.$$

The situation for linear maps is similar, but slightly more complex as two abstract vector spaces are involved.

Definition 3.2.8.

Let V and W be two finite dimensional $\mathbf{F}$-vector spaces with given respective bases $\mathscr{B} = (v_1, \dots, v_m)$ and $\mathscr{C} = (w_1, \dots, w_n)$ of respective size $m = \dim(V)$ and $n = \dim(W)$. Let $T \in \mathcal{L}(V, W)$ be a linear map. Then for $j \in \{1, \dots, m\}$ we have

$$T(v_j) = a_{1,j} w_1 + a_{2,j} w_2 + \cdots + a_{n,j} w_n$$

for some $a_{i,j} \in \mathbf{F}$ ($i \in \{1, \dots, n\}$). These datas define a matrix

$$[T]^{\mathscr{C}}_{\mathscr{B}} := \begin{bmatrix} a_{1,1} & \cdots & a_{1,m} \\ \vdots & & \vdots \\ a_{n,1} & \cdots & a_{n,m} \end{bmatrix} \in \mathbf{F}^{n,m}$$

which is called the **matrix representation** (with respect to $\mathscr{B}$ and $\mathscr{C}$) of the linear map T. We hence have the **matrix representation map**

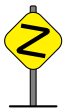
$$[\,\cdot\,]^{\mathscr{C}}_{\mathscr{B}} \colon \mathcal{L}(V, W) \longrightarrow \mathbf{F}^{\dim(W),\dim(V)}$$
$$T \longmapsto [T]^{\mathscr{C}}_{\mathscr{B}}.$$

Observe that since $\mathscr{C}$ is a basis, the decomposition $T(v_j) = a_{1,j}w_1 + a_{2,j}w_2 + \cdots + a_{n,j}w_n$ is unique, and hence $[T]_{\mathscr{B}}^{\mathscr{C}}$ is well-defined. The matrix $[T]_{\mathscr{B}}^{\mathscr{C}}$ from Definition 3.2.8 is a $n \times m$ matrix, and so left multiplication by $[T]_{\mathscr{B}}^{\mathscr{C}}$ is a linear map from $\mathbf{F}^m$ to $\mathbf{F}^n$. This is consistent with the fact that $T \in \mathcal{L}(V, W)$ and $V \cong \mathbf{F}^m$ and $W \cong \mathbf{F}^n$.

Remark 3.2.9.

Let V and W be two finite dimensional $\mathbf{F}$-vector spaces with given respective bases $\mathscr{B} = (v_1, \dots, v_m)$ and $\mathscr{C}$. Then the j^{th} column of $[T]_{\mathscr{B}}^{\mathscr{C}}$ is $[T(v_j)]_{\mathscr{C}}$.

Remark 3.2.10.



Be very careful about the fact that $[\,\cdot\,]_{\mathscr{B}}^{\mathscr{C}} \colon \mathcal{L}(V, W) \to \mathbf{F}^{\dim(W),\dim(V)}$ has domain $\mathcal{L}(V, W)$ but codomain $\mathbf{F}^{\dim(W),\dim(V)}$. The order of appearance of V and W is switched! So if $\dim(V) = m$ and $\dim(W) = n$ the codomain of $[\,\cdot\,]_{\mathscr{B}}^{\mathscr{C}}$ consists of the $n \times m$ matrices (but not the $m \times n$ matrices).

We start with some elementary examples.

Example 3.2.11. Let V be a vector space and let $\mathscr{B} = (v_1, \dots, v_n)$ be basis for V. Let $\mathrm{Id}_V \colon V \to V$ be the identity map. Then $\mathrm{Id}(v_1) = v_1$, so $[\mathrm{Id}(v_1)]_{\mathscr{B}} = [1, 0, \dots, 0]^{\mathsf{T}}$. Similarly, $[\mathrm{Id}(v_i)]_{\mathscr{B}}$ is the vector with a 1 in position i and 0 elsewhere. It follows that

$$[\mathrm{Id}_V]_{\mathscr{B}}^{\mathscr{B}} = \begin{bmatrix} 1 & & \\ & \ddots & \\ & & 1 \end{bmatrix} = \mathrm{Id}_n \in \mathbf{F}^{n,n} \tag{3.4}$$

is the identity matrix of $\mathbf{F}^{n,n}$. Indeed, $[\mathrm{Id}_V\, v]_{\mathscr{B}} = [\mathrm{Id}_V]_{\mathscr{B}}^{\mathscr{B}} [v]_{\mathscr{B}}$.

Remark 3.2.12.

The equation (3.4) does not depend on the choice of the basis $\mathscr{B}$!

The identity map is not the only one that can be represented by the identity matrix:

Example 3.2.13. Let V be a finite dimensional vector space with basis $\mathscr{B}$ and let $T \colon V \xrightarrow{\cong} W$ be an isomorphism. Then, by the Proposition 3.1.45 $\mathscr{C} := (Tv_1, \dots, Tv_n)$ is a basis and

$$[T]_{\mathscr{B}}^{\mathscr{C}} = \begin{bmatrix} 1 & & \\ & \ddots & \\ & & 1 \end{bmatrix} = \mathrm{Id}_n \in \mathbf{F}^{n,n}$$

is the identity matrix of $\mathbf{F}^{n,n}$.

Remark 3.2.14.

The above example shows that any isomorphisms between *finite dimensional* vector spaces can be represented by the identity matrix *if we chose bases appropriately.*

The converse of Example 3.2.13 holds, as demonstrated in the following exercise.

Exercise 3.2.15. Let V and W be two vector spaces of dimension n and let $T \in \mathcal{L}(V,W)$. Show that T is an isomorphism if and only if there exists bases $\mathscr{B}$ of V and $\mathscr{C}$ of W such that $[T]_{\mathscr{B}}^{\mathscr{C}}$ is the identity matrix of $\mathbf{F}^{n,n}$.

Solution. Let $T \in \mathcal{L}(V,W)$ be a linear map between finite dimensional vector spaces. Suppose that there exists bases $\mathscr{B} = (v_1, \dots, v_m$ of V and $\mathbf{C} = (w_1, \dots, w_m$ of W such that $[T]_{\mathscr{B}}^{\mathbf{C}}$ is the identity matrix. This implies in particular that $[T]_{\mathscr{B}}^{\mathbf{C}}$ is a square matrix and thus that $m = n$. By definition of $[T]_{\mathscr{B}}^{\mathbf{C}}$ we have $Tv_j = w_j$ for every j in $\{1, \dots, m\}$. Let $S \in \mathcal{L}(W,V)$ be the linear map defined by $Sw_j \coloneqq v_j$ for j in $\{1, \dots, m\}$. It is trivial to verify that S is the inverse of T. □

When writing $\left[\begin{smallmatrix} x \\ y \end{smallmatrix}\right] \in \mathbf{F}^2$, we already implicitly use the standard basis. The following example makes this explicit.

Example 3.2.16. Let $V = \mathbf{F}^n$ and let $\mathscr{E} = (e_1 = [1, 0, \dots, 0]^\mathsf{T}, \dots, e_n = [0, \dots, 0, 1]^\mathsf{T})$ be the standard basis. Then $[\,\cdot\,]_{\mathscr{E}} \colon V \to \mathbf{F}^n$ is the identity map $\mathrm{Id}_{\mathbf{F}^n}$. Indeed, for any $x = [x_1, \dots, x_n]^\mathsf{T}$ in V we have $x = \sum_{i=1}^n x_i e_i$, so $[x]_{\mathscr{E}} = [x_1, \dots, x_n]^\mathsf{T}$.

Example 3.2.17. Let $T \in \mathcal{L}(\mathbf{F}^2, \mathbf{F}^3)$ be the map $T\left[\begin{smallmatrix} x \\ y \end{smallmatrix}\right] = [x + 3y, 2x + 5y, 7x + 9y]^\mathsf{T}$ and let $\mathscr{E}^2$ and $\mathscr{E}^3$ be the standard bases of $\mathbf{F}^2$ and $\mathbf{F}^3$. By the above example, one have

$$[T]_{\mathscr{E}^2}^{\mathscr{E}^3} = \begin{bmatrix} 1 & 3 \\ 2 & 5 \\ 7 & 9 \end{bmatrix}.$$

Let us now modify a little bit this example. Let $\mathscr{C} = ([1, 0, 0]^\mathsf{T}, [0, 1, 0]^\mathsf{T}, [1, 1, 1]^\mathsf{T})$. This is a basis of $\mathbf{F}^3$. We have

$$T\begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \\ 2 \\ 7 \end{bmatrix} = -6\begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix} - 5\begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix} + 7\begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix} \quad \text{and} \quad T\begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 3 \\ 5 \\ 9 \end{bmatrix} = -6\begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix} - 4\begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix} + 9\begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix},$$

and thus

$$[T]_{\mathscr{E}^2}^{\mathscr{C}} = \begin{bmatrix} -6 & -6 \\ -5 & -4 \\ 7 & 9 \end{bmatrix}.$$

Finally, let $\mathscr{B} = ([1, 0]^\mathsf{T}, [1, 1]^\mathsf{T})$. This is a basis of $\mathbf{F}^2$. We have

$$T\begin{bmatrix} 1 \\ 0 \end{bmatrix} = -6\begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix} - 5\begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix} + 7\begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix} \quad \text{and} \quad T\begin{bmatrix} 1 \\ 1 \end{bmatrix} = \begin{bmatrix} 4 \\ 7 \\ 16 \end{bmatrix} = -12\begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix} - 9\begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix} + 16\begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix},$$

and thus

$$[T]_{\mathscr{B}}^{\mathscr{C}} = \begin{bmatrix} -6 & -12 \\ -5 & -9 \\ 7 & 16 \end{bmatrix}.$$

Example 3.2.18. Let $D \in \mathcal{L}(\mathcal{P}(\mathbf{R})_3, \mathcal{P}(\mathbf{R})_2)$ be the differentiation operator: $D(p) = p'$ and let $\mathscr{B} = (1, x, x^2, x^3)$ and $\mathscr{C} = (1, x, x^2)$ be the standard bases of $\mathcal{P}(\mathbf{R})_3$ and $\mathcal{P}(\mathbf{R})_2$. Then $D(1) = 0$, $D(x) = 1$, $D(x^2) = 2x$ and $D(x^3) = 3x^2$, which gives $[D(1)]_{\mathscr{C}} = [0,0,0]^\mathsf{T}$, $[D(x)]_{\mathscr{C}} = [1,0,0]^\mathsf{T}$, $[D(x^2)]_{\mathscr{C}} = [0,2,0]^\mathsf{T}$ and $[D(x^3)]_{\mathscr{C}} = [0,0,3]^\mathsf{T}$. Altogether, we have

$$[D]^{\mathscr{C}}_{\mathscr{B}} = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 3 \end{bmatrix}.$$

Example 3.2.19. Let V be the subspace of $\mathbf{R}^\mathbf{R}$ spanned by $(\sin(x), \cos(x))$. We claim that the functions cos and sin are linearly independent. Indeed, let a and b in $\mathbf{R}$ such that $a\sin + b\cos = 0$. In particular the equality $a\sin(x) + b\cos(x) = 0$ holds both for $x = 0$ and $x = \pi/2$ and we may deduce that $a = b = 0$.

By linear independence of sin and cos, the family $\mathscr{B} = (\sin(x), \cos(x))$ is a basis of V. If we fix $\theta \in \mathbf{R}$, the map $T_\theta \colon V \to V, f(x) \mapsto f(x+\theta)$ is a well-defined. Indeed, $T_\theta(\sin(x)) = \cos(\theta)\sin(x) + \sin(\theta)\cos(x) \in V$ and $T_\theta(\cos(x)) = -\sin(\theta)\sin(x) + \cos(\theta)\cos(x) \in V$ and thus the image of T_θ is contained in V. On can show that $T_\theta /$ is a linear map. It follows from the above computations that

$$[T_\theta]^{\mathscr{B}}_{\mathscr{B}} = \begin{bmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{bmatrix}.$$

Given finite dimensional vector spaces V and W, with bases $\mathscr{B}$ and $\mathscr{C}$, we have constructed a function $[\,\cdot\,]^{\mathscr{C}}_{\mathscr{B}} \colon \mathcal{L}(V,W) \to \mathbf{F}^{\dim(W),\dim(V)}$. Both $\mathcal{L}(V,W)$ and $\mathbf{F}^{\dim(W),\dim(V)}$ are not only sets, but vector spaces. We are thus not interested in merely the functions between them, but in the linear maps. It turns out that $[\,\cdot\,]^{\mathscr{C}}_{\mathscr{B}}$ is indeed a linear map, and even an isomorphism. This justifies the name of matrix *representation*.

Theorem 3.2.20.

Let V and W be finite dimensional $\mathbf{F}$-vector spaces, with given bases $\mathscr{B} = (v_1, \dots, v_m)$ and $\mathscr{C} = (w_1, \dots, w_n)$. Then the map $[\,\cdot\,]^{\mathscr{C}}_{\mathscr{B}} \colon \mathcal{L}(V,W) \to \mathbf{F}^{\dim(W),\dim(V)}$ is an isomorphism. Moreover, the inverse of $[\,\cdot\,]^{\mathscr{C}}_{\mathscr{B}}$ is given by the map

$$\begin{aligned} M^{\mathscr{C}}_{\mathscr{B}} \colon \mathbf{F}^{\dim(W),\dim(V)} &\longrightarrow \mathcal{L}(V,W) \\ [a_{i,j}] &\longmapsto (T \colon v_j \mapsto a_{1,j}w_1 + \cdots + a_{n,j}w_n). \end{aligned}$$

Proof. We need to prove three things: that $[\,\cdot\,]^{\mathscr{C}}_{\mathscr{B}}$ is linear, that the map $M^{\mathscr{C}}_{\mathscr{B}}$ sending $[a_{i,j}]$ to T is well-defined and that it is the inverse of $[\,\cdot\,]^{\mathscr{C}}_{\mathscr{B}}$.

Let S and T be in $\mathcal{L}(V,W)$ and λ be a scalar in $\mathbf{F}$. For every basis vector $v_j \in \mathscr{B}$ we have $(\lambda S + T)(v_j) = \lambda S(v_j) + T(v_j)$, which implies $[(\lambda S + T)(v_j)]_{\mathscr{C}} = \lambda[S(v_j)]_{\mathscr{C}} + [T(v_j)]_{\mathscr{C}}$. It follows that $[\lambda S + T]^{\mathscr{C}}_{\mathscr{B}} = \lambda[S]^{\mathscr{C}}_{\mathscr{B}} + [T]^{\mathscr{C}}_{\mathscr{B}}$, which proves linearity.

The map $T = M^{\mathscr{C}}_{\mathscr{B}}([a_{i,j}])$ in the statement of the theorem is defined only on $\mathscr{B}$. But there is a unique way to extend to it to a linear map in $\mathcal{L}(V,W)$, so $M^{\mathscr{C}}_{\mathscr{B}}$ is well-defined. It directly follows from the definition that $[T]^{\mathscr{C}}_{\mathscr{B}} = [a_{i,j}]$, proving $([\,\cdot\,]^{\mathscr{C}}_{\mathscr{B}})(M^{\mathscr{C}}_{\mathscr{B}}) = \mathrm{Id}_{\mathbf{F}^{n,m}}$. Another direct verification shows that $(M^{\mathscr{C}}_{\mathscr{B}})([\,\cdot\,]^{\mathscr{C}}_{\mathscr{B}}) = \mathrm{Id}_{\mathcal{L}(V,W)}$. □

Corollary 3.2.21. *Let V and W be two finite dimensional vector spaces. Then* $\dim(\mathcal{L}(V,W)) = \dim(V)\cdot\dim(W)$.

If $V = \mathbf{F}^m$ and $W = \mathbf{F}^n$, the map $([\,\cdot\,]_{\mathscr{B}}^{\mathscr{C}})^{-1}$ is simply the matrix multiplication:

Corollary 3.2.22. *Let $\mathscr{E}^n$ and $\mathscr{E}^m$ be the standard bases of $\mathbf{F}^n$ and $\mathbf{F}^m$. Define*

$$\begin{aligned} \mathrm{L}\colon \mathbf{F}^{n,m} &\longrightarrow \mathcal{L}(\mathbf{F}^m,\mathbf{F}^n) \\ A &\longmapsto (\mathrm{L}_A\colon v \mapsto Av). \end{aligned}$$

Then the maps $[\,\cdot\,]_{\mathscr{E}^m}^{\mathscr{E}^n}\colon \mathcal{L}(\mathbf{F}^m,\mathbf{F}^n)\to\mathbf{F}^{n,m}$ and $\mathrm{L}\colon \mathbf{F}^{n,m}\to\mathcal{L}(\mathbf{F}^m,\mathbf{F}^n)$ are isomorphisms of vector spaces, and one is the inverse of the other.

Proof. It is straightforward that in this case the map $M_{\mathscr{B}}^{\mathscr{C}}$ described in Theorem 3.2.20 coincides with multiplication by A on the left. □

We say that the matrix A represents the linear map L_A. Using this map we can translate the image and kernel of L_A into matrices properties.

Definition 3.2.23.

Let A be a $m\times n$ matrix. Define its **column space** $\mathrm{col}(A)$ to be the subspace of $\mathbf{F}^m$ spanned by its columns vectors. The **null space** $\mathrm{null}(A)$ is the subspace of $\mathbf{F}^n$ consisting of vectors v such that $Av = 0$.

Lemma 3.2.24. *Let A be a $m\times n$ matrix. Then* $\mathrm{null}(A) = \ker(\mathrm{L}_A)$ *and* $\mathrm{col}(A) = \mathrm{range}(\mathrm{L}_A)$.

Proof. The equality $\mathrm{null}(A) = \ker(\mathrm{L}_A)$ is immediate from the definitions.

Let e_j be the j^{th} vector in the standard basis of $\mathbf{F}^n$, so e_j has a 1 in coordinate j and 0 everywhere else. Let $w_j := [a_{i,j}]_{1\le i\le m}$ be the j^{th} column vector of A. Then $Ae_j = w_j$. This implies that all column vectors of A belongs to $\mathrm{range}(\mathrm{L}_A)$ and therefore that $\mathrm{col}(A)\subseteq\mathrm{range}(\mathrm{L}_A)$. For the other direction, let w be a vector in $\mathrm{range}(\mathrm{L}_A)$ and let v be a preimage: $Av = w$. Then there exists scalars such that $v = \sum_{j=1}^n \lambda_j e_j$ and $Av = \sum_{i=j}^n \lambda_j Ae_j = \sum_{j=1}^n w_j$ is in $\mathrm{col}(A)$, proving the inclusion $\mathrm{col}(A)\supseteq\mathrm{range}(\mathrm{L}_A)$. □

Given two finite dimensional vector spaces V and W with given respective basis $\mathscr{B}$ and $\mathscr{C}$, we have seen so fare the following three isomorphisms: $[\,\cdot\,]_{\mathscr{B}}\colon V\to\mathbf{F}^{\dim(V)}$, $[\,\cdot\,]_{\mathscr{C}}\colon W\to\mathbf{F}^{\dim(W)}$ and $[\,\cdot\,]_{\mathscr{B}}^{\mathscr{C}}\colon\mathcal{L}(V,W)\to\mathbf{F}^{\dim(W),\dim(V)}\cong\mathcal{L}(\mathbf{F}^{\dim(V)},\mathbf{F}^{\dim(W)})$. It is natural to ask if we have some sort of relation or compatibility between these three isomorphisms. We indeed have

Lemma 3.2.25. *Let V and W be finite dimensional vector spaces with given respective basis $\mathscr{B}$ and $\mathscr{C}$, and let $T\in\mathcal{L}(V,W)$ be a linear map. Then for every v in V we have*

$$[T(v)]_{\mathscr{C}} = [T]_{\mathscr{B}}^{\mathscr{C}}[v]_{\mathscr{B}}.$$

This result is equivalent to say that the following diagram commutes:

$$\begin{array}{ccc} V & \xrightarrow{T} & W \\ {\scriptstyle [\cdot]_{\mathscr{B}}}\downarrow & & \downarrow{\scriptstyle [\cdot]_{\mathscr{C}}} \\ \mathbf{F}^m & \xrightarrow[[T]^{\mathscr{C}}_{\mathscr{B}}]{} & \mathbf{F}^n \end{array} \qquad \begin{array}{ccc} v & \longmapsto & Tv \\ \downarrow & & \downarrow \\ [v]_{\mathscr{B}} & \longmapsto & [Tv]_{\mathscr{C}} = [T]^{\mathscr{C}}_{\mathscr{B}}[v]_{\mathscr{B}}. \end{array}$$

Proof. The proof consists at looking at the definitions of $[\,\cdot\,]_{\mathscr{B}}$, $[\,\cdot\,]_{\mathscr{C}}$ and $[\,\cdot\,]^{\mathscr{C}}_{\mathscr{B}}$. Let $(v_1, \dots, v_m) = \mathscr{B}$ and $(w_1, \dots, v_n) = \mathscr{C}$. Then for any $v \in V$ we have

$$[v]_{\mathscr{B}} = \begin{bmatrix} c_1 \\ \vdots \\ c_m \end{bmatrix} \iff v = c_1 v_1 + \cdots + c_m v_m.$$

and

$$[Tv]_{\mathscr{C}} = \begin{bmatrix} d_1 \\ \vdots \\ d_n \end{bmatrix} \iff Tv = d_1 w_1 + \cdots + d_n w_n.$$

Finally,

$$[T]^{\mathscr{C}}_{\mathscr{B}} = [a_{i,j}] \iff \forall i \in \{1, \dots, m\} : Tv_i = a_{1,i} w_1 + \cdots + a_{n,i} w_n.$$

Putting everything together we obtain

$$\begin{aligned} d_1 w_1 + \cdots + d_n w_n = Tv &= T(c_1 v_1 + \cdots + c_m v_m) \\ &= c_1 T(v_1) + \cdots + c_m T(v_m) \\ &= c_1(a_{1,1} w_1 + \cdots + a_{n,1} w_n) + \cdots + c_m(a_{1,m} w_1 + \cdots + a_{n,m} w_n). \end{aligned}$$

That is, for all $j \in \{1, \dots, n\}$ we have $d_j = c_1 a_{j,1} + \cdots + c_m a_{j,m}$. This it the same as the matrix-vector product

$$\begin{bmatrix} d_1 \\ \vdots \\ d_n \end{bmatrix} = \begin{bmatrix} a_{1,1} & \cdots & a_{1,m} \\ \vdots & & \vdots \\ a_{n,1} & \cdots & a_{n,m} \end{bmatrix} \begin{bmatrix} c_1 \\ \vdots \\ c_m \end{bmatrix},$$

and thus $[Tv]_{\mathscr{C}} = [T]^{\mathscr{C}}_{\mathscr{B}}[v]_{\mathscr{B}}$. □

3.2.3 Matrix product as composition of linear maps

We have seen in Definition 3.2.5 how to multiply a matrix and a vector. We now look at the general case.

Definition 3.2.26.

Let $A = [a_{i,j}] \in \mathbf{F}^{l,m}$ and $B = [b_{j,k}] \in \mathbf{F}^{m,n}$ be two matrices. Their **product** is the matrix

$$C = [c_{i,k}]_{\substack{0 \le i \le l \\ 0 \le k \le n}} = [a_{i,j}]_{\substack{0 \le i \le l \\ 0 \ne j \le m}} [b_{j,k}]_{\substack{0 \le j \le m \\ 0 \le k \le n}}$$

where for $i \in \{1, \dots, l\}$ and $k \in \{n, \dots,\}$ the coefficient $c_{i,k}$ of C is given by

$$c_{i,k} = \sum_{j=1}^{m} a_{i,j} b_{j,k}.$$

$$\begin{bmatrix} 金 \\ 木 \\ 水 \\ 土 \end{bmatrix} \begin{bmatrix} 金 & 木 & 水 & 土 \end{bmatrix} = \begin{bmatrix} 鋅 & 鉢 & 淦 & 釷 \\ 鉢 & 林 & 沐 & 杜 \\ 淦 & 沐 & 氷 & 汢 \\ 釷 & 杜 & 汢 & 圭 \end{bmatrix}$$

Figure 3.2: Product of a 4×1 matrix with a 1×4 matrix.

Remark 3.2.27.

In general, the product of $A \in \mathbf{F}^{l,m}$ and $B \in \mathbf{F}^{k,n}$ is not defined. It is defined only if $k = m$. Even when both AB and BA are defined, they are not equal in general.

The following are standard properties of the product of matrices.

Proposition 3.2.28. *The matrix product is a generalisation of the matrix-vector product. Moreover, we have*

1. $(AB)C$ *is defined if and only if* $A(BC)$ *is, in which case we have* $(AB)C = A(BC)$;
2. $A(B+C)$ *is defined if and only if* $AB+AC$ *is, in which case we have* $A(B+C) = AB+AC$;
3. $(A+B)C$ *is defined if and only if* $AC+BC$ *is, in which case we have* $(A+B)C = AC+BC$;
4. *If* $A \in \mathbf{F}^{m,n}$, *then* $\mathrm{Id}_m A = A = A \mathrm{Id}_n$.

Proof. These are all elementary, but tedious, verifications. The details are left to the reader. □

To go further

Associativity of the product means that the result of a sequence of product of matrices does not depend on the order of operation (provided that the order of the matrices is not changed). However, the *computational complexity* may depend dramatically on this order.
For example, if A, B and C are matrices of respective sizes 10×30, 30×5 and 5×60, then AB has size 10×5 and BC size 30×60. Therefore, computing $(AB)C$ needs $10 \cdot 30 \cdot 5 + 10 \cdot 5 \cdot 60 = 4500$ multiplications, while computing $A(BC)$ needs

$30 \cdot 5 \cdot 60 + 10 \cdot 30 \cdot 60 = 27\,000$ multiplications.
Multiplication algorithms used in practice have been designed for choosing the best order of products.

We have seen that $[\,\cdot\,]_{\mathscr{B}}^{\mathscr{C}}$ is an isomorphism. In particular, it is a linear map and thus preserves addition and multiplication. It turns out that it also preserve products.

Proposition 3.2.29. *Let U, V and W be finite dimensional $\mathbf{F}$-vector spaces with respective given bases $\mathscr{A}$, $\mathscr{B}$ and $\mathscr{C}$. Then for any $S \in \mathcal{L}(U,V)$ and $T \in \mathcal{L}(V,W)$ we have*

$$[TS]_{\mathscr{A}}^{\mathscr{C}} = [T]_{\mathscr{B}}^{\mathscr{C}}[S]_{\mathscr{A}}^{\mathscr{B}}.$$

Proof. The statement follows from an elementary by fastidious application of the definition of $[\,\cdot\,]_*^*$. The proof is somehow similar to what we did for Lemma 3.2.25.

An alternative proof by digram commutation is the following.

$$\begin{array}{ccccc} U & \xrightarrow{S} & V & \xrightarrow{T} & W \\ {\scriptstyle [\cdot]_{\mathscr{A}}}\downarrow & & {\scriptstyle [\cdot]_{\mathscr{B}}}\downarrow & & \downarrow{\scriptstyle [\cdot]_{\mathscr{C}}} \\ \mathbf{F}^l & \xrightarrow[[S]_{\mathscr{A}}^{\mathscr{B}}]{} & \mathbf{F}^m & \xrightarrow[[T]_{\mathscr{B}}^{\mathscr{C}}]{} & \mathbf{F}^n \end{array}$$

In the above diagram, the two exterior squares commute by Lemma 3.2.25. It follows that the whole rectangle is commuting.

In other words, for all $u \in U$ we have:

$$[TSu]_{\mathscr{C}} = [T(Su)]_{\mathscr{C}} = [T]_{\mathscr{B}}^{\mathscr{C}}[Su]_{\mathscr{B}} = [T]_{\mathscr{B}}^{\mathscr{C}}([S]_{\mathscr{A}}^{\mathscr{B}}[u]_{\mathscr{A}}) = ([T]_{\mathscr{B}}^{\mathscr{C}}[S]_{\mathscr{A}}^{\mathscr{B}})[u]_{\mathscr{A}},$$

where we applied Lemma 3.2.25 twice. Since we also have $[(TS)u]_{\mathscr{C}} = [TS]_{\mathscr{A}}^{\mathscr{C}}[u]_{\mathscr{A}}$, we conclude $[TS]_{\mathscr{A}}^{\mathscr{C}} = [T]_{\mathscr{B}}^{\mathscr{C}}[S]_{\mathscr{A}}^{\mathscr{B}}$.

□

Figure 3.3 summarises the results obtained up to now for the maps $[\,\cdot\,]_*^*$ and $[\,\cdot\,]_*$.

3.2.4 More on matrix representation

We have seen in the previous subsection that matrix representation behaves well with respect to products. It is no surprise that it also behaves well with respect to inverses.

Proposition 3.2.30. *Let V and W be two vector spaces of the same finite dimension n. Let $\mathscr{B}$ be a basis for V and let $\mathscr{C}$ be a basis for W. Let $T \in \mathcal{L}(V,W)$ be a linear map. Then T is invertible (as a linear map) if and only if $[T]_{\mathscr{B}}^{\mathscr{C}} \in \mathbf{F}^{n,n}$ is invertible (as a matrix).*

Moreover, if T is invertible, then $([T]_{\mathscr{B}}^{\mathscr{C}})^{-1} = [T^{-1}]_{\mathscr{C}}^{\mathscr{B}}$.

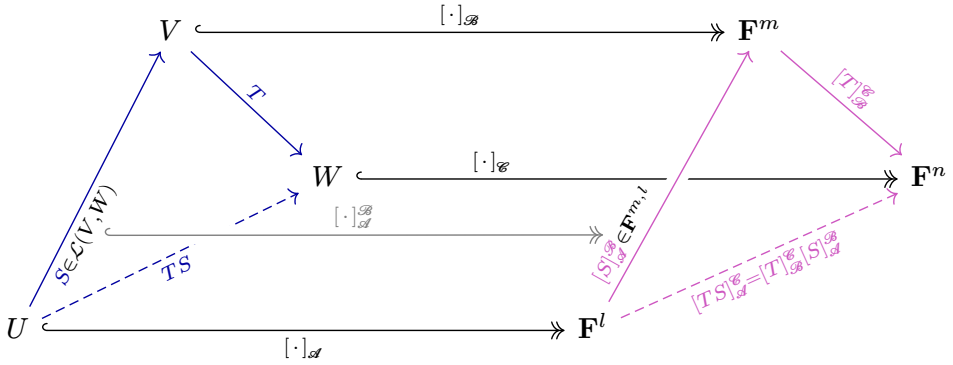


Figure 3.3: Let U, V and W be finite dimensional $\mathbf{F}$-vector spaces with respective given bases $\mathscr{A}$, $\mathscr{B}$ and $\mathscr{C}$ and of respective dimensions l, m and n. Then for any $S \in \mathcal{L}(U,V)$ and $T \in \mathcal{L}(V,W)$, their product TS is in $\mathcal{L}(U,W)$. This situation is depicted in the blue triangle on the left. Applying the isomorphisms $[\,\cdot\,]_*$ and $[\,\cdot\,]_*^*$ one obtains the purple triangle on the right. The whole diagram is commutative. For example, for any $u \in U$ one have $[TSu]_{\mathscr{C}} = [T]_{\mathscr{B}}^{\mathscr{C}}[S]_{\mathscr{A}}^{\mathscr{B}}[u]_{\mathscr{A}} = [TS]_{\mathscr{A}}^{\mathscr{C}}[u]_{\mathscr{A}}$.

Proof. "⇒" Suppose T is invertible, so $T^{-1} \in \mathcal{L}(W,V)$ exists. We will prove that $[T^{-1}]_{\mathscr{C}}^{\mathscr{B}}$ is the inverse matrix of $[T]_{\mathscr{B}}^{\mathscr{C}}$. We have

$$\begin{aligned} \mathrm{Id}_n &= [\mathrm{Id}_W]_{\mathscr{C}}^{\mathscr{C}} = [TT^{-1}]_{\mathscr{C}}^{\mathscr{C}} = [T]_{\mathscr{B}}^{\mathscr{C}}[T^{-1}]_{\mathscr{C}}^{\mathscr{B}} \\ \mathrm{Id}_n &= [\mathrm{Id}_V]_{\mathscr{B}}^{\mathscr{B}} = [T^{-1}T]_{\mathscr{C}}^{\mathscr{C}} = [T^{-1}]_{\mathscr{C}}^{\mathscr{B}}[T]_{\mathscr{B}}^{\mathscr{C}}. \end{aligned}$$

That is, $[T]_{\mathscr{B}}^{\mathscr{C}}$ is invertible and $\left([T]_{\mathscr{B}}^{\mathscr{C}}\right)^{-1} = [T^{-1}]_{\mathscr{C}}^{\mathscr{B}}$.

"⇐" Suppose $[T]_{\mathscr{B}}^{\mathscr{C}}$ is invertible. We will construct an inverse fot T. So let $\left([T]_{\mathscr{B}}^{\mathscr{C}}\right)^{-1} =: A = [a_{i,j}]$ and define $S \in \mathcal{L}(W,V)$ by $[S(w)]_{\mathscr{B}} := A[w]_{\mathscr{C}}$ for all $w \in \mathscr{C}$. That is, S is the unique linear map from W to V such that $S(w_i) = \sum_{j=1}^n a_{ij}v_j$. By construction, we have $[S]_{\mathscr{C}}^{\mathscr{B}} = [[S(w_1)]_{\mathscr{B}} \cdots [S(w_n)]_{\mathscr{B}}] = A$. So we conclude that $[ST]_{\mathscr{B}}^{\mathscr{B}} = \mathrm{Id}_V$. In particular, for any $1 \le i \le n$, we have $ST(v_i) = \mathrm{Id}_V(v_i)$ and hence $ST = \mathrm{Id}_V$. Similarly, $TS = \mathrm{Id}_W$. □

The case of $V = W$ and $T \in \mathcal{L}(V)$ an operator is particularly interesting, as we can talk about powers. Indeed, since T is a function whose domain and codomain V agree, for any $k \in \mathbf{N}$ positive the function

$$T^k := \underbrace{T \cdots T}_{k \text{ times}} \in \mathcal{L}(V)$$

is well-defined. This is composition of linear maps and therefore a linear map itself.

Proposition 3.2.31. *Let V be a finite dimensional space with basis $\mathscr{B}$ and let $T \in \mathcal{L}(V)$ be an operator. Then for $k \in \mathbf{N}$ we have*

$$[T^k]_{\mathscr{B}}^{\mathscr{B}} = \left([T]_{\mathscr{B}}^{\mathscr{B}}\right)^k.$$

Proof. The proof is by induction. If $k = 0$ or $k = 1$, this is obvious. Now, suppose that the formula holds for $k \geq 1$ and let us try to prove it for $(k+1) = k+1$. By the product formula

$$[T^{k+1}]_{\mathscr{B}}^{\mathscr{B}} = [T^k]_{\mathscr{B}}^{\mathscr{B}}[T]_{\mathscr{B}}^{\mathscr{B}} = \left([T]_{\mathscr{B}}^{\mathscr{B}}\right)^k [T]_{\mathscr{B}}^{\mathscr{B}} = \left([T]_{\mathscr{B}}^{\mathscr{B}}\right)^{k+1}.$$

□

By combining Propositions 3.2.30 and 3.2.31, for invertible $T \in \mathcal{L}(V)$ we have

$$[T^k]_{\mathscr{B}}^{\mathscr{B}} = \left([T]_{\mathscr{B}}^{\mathscr{B}}\right)^k$$

for all $k \in \mathbf{Z}$.

Exercise 3.2.32. Let $R_\theta \colon \mathbf{R}^2 \to \mathbf{R}^2$ be the map "rotation by angle θ", see Figure 3.4. Let $\mathscr{E} = \left(\begin{bmatrix}1\\0\end{bmatrix}, \begin{bmatrix}0\\1\end{bmatrix}\right)$ be the standard basis for $\mathbf{R}^2$. Prove that R_θ is a linear map and find $[R_\theta]_{\mathscr{E}}^{\mathscr{E}}$.

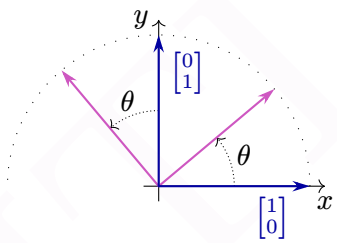


Figure 3.4: Rotation (in purple) of the standard basis vectors (in blue) by an angle θ.

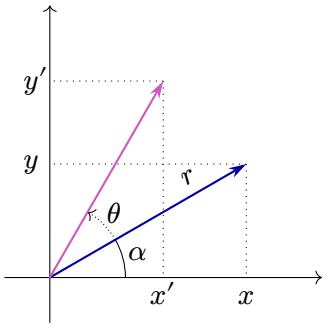
Solution. Let $\begin{bmatrix}x\\y\end{bmatrix}$ be a point in $\mathbf{R}^2$. Define $r := \sqrt{x^2+y^2}$ and $\begin{bmatrix}x'\\y'\end{bmatrix} := R_\theta \begin{bmatrix}x\\y\end{bmatrix}$. Finally, let α be the angle between $\begin{bmatrix}x\\y\end{bmatrix}$ and the x-axis. Then we have $\cos(\alpha) = \frac{x}{r}$ and $\sin(\alpha) = \frac{y}{r}$, while $\cos(\alpha+\theta) = \frac{x'}{r}$ and $\sin(\alpha+\theta) = \frac{y'}{r}$. We conclude that

$$R_\theta \begin{bmatrix}x\\y\end{bmatrix} = \begin{bmatrix}x'\\y'\end{bmatrix} = \begin{bmatrix}x\cos(\theta) - y\sin(\theta)\\ x\sin(\theta) + y\cos(\theta)\end{bmatrix}.$$

Using the above formula, one easily checks that R_θ is linear, and by computing the image of $\begin{bmatrix}1\\0\end{bmatrix}$ and $\begin{bmatrix}0\\1\end{bmatrix}$ we obtain

$$[R_\theta]_{\mathscr{E}}^{\mathscr{E}} = \begin{bmatrix}\cos(\theta) & -\sin(\theta)\\ \sin(\theta) & \cos(\theta)\end{bmatrix}. \tag{3.5}$$

□



$$\cos(\alpha) = \frac{x}{r}$$
$$\sin(\alpha) = \frac{y}{r}$$

Figure 3.5: A vector (in blue) and its image (in purple) by the rotation of an angle θ.

Remark 3.2.33.

The following facts can easily been seen geometrically (see Figure 3.6) but can also be shown using the formula for $[R_\theta]_{\mathscr{E}}^{\mathscr{E}}$.

1. $R_{\theta_1} R_{\theta_2} = R_{\theta_1+\theta_2}$;
2. R_θ is invertible and $(R_\theta)^{-1} = R_{-\theta}$;
3. for any $n \in \mathbf{Z}$ we have $(R_\theta)^n = R_{n\theta}$;
4. for any $k \in \mathbf{Z}$ we have $R_{2k\pi} = \mathrm{Id}_{\mathbf{R}^2}$.

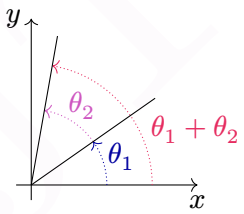


Figure 3.6: Angles addition.

Exercise 3.2.34. Let $S_1 : \mathbf{R}^2 \to \mathbf{R}^2$ be the reflexion along the x-axis, $S_2 : \mathbf{R}^2 \to \mathbf{R}^2$ the reflexion along the y-axis and let $\mathscr{E}$ be the standard basis. Find $[S_1]_{\mathscr{E}}^{\mathscr{E}}$ and $[S_2]_{\mathscr{E}}^{\mathscr{E}}$.

Solution.

We have $S_1 \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} x \\ -y \end{bmatrix}$ and $S_2 \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} -x \\ y \end{bmatrix}$ for any $\begin{bmatrix} x \\ y \end{bmatrix}$ in $\mathbf{R}^2$. Using these formulas, one easily shows that both S_1 and S_2 are linear maps.

By computing the image of the basis vectors, we obtain

$$[S_1]_{\mathscr{E}}^{\mathscr{E}} = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \qquad \text{and} \qquad [S_2]_{\mathscr{E}}^{\mathscr{E}} = \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}.$$

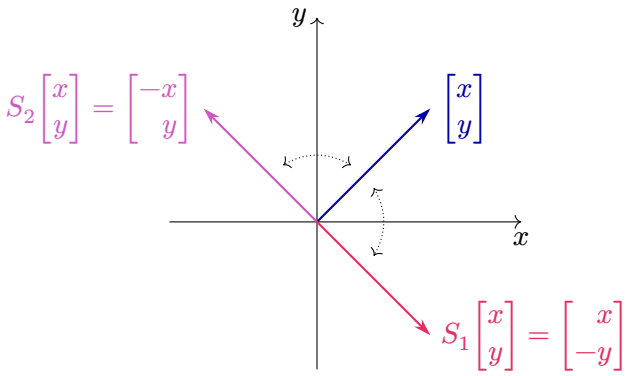


Figure 3.7: Mirror symmetries with respect to the x-axis (S_1) and the y-axis (S_2).

□

Observe that we the notations from the previous exercises, we have $[S_1S_2]_{\mathscr{E}}^{\mathscr{E}} = [S_2S_1]_{\mathscr{E}}^{\mathscr{E}} = [R_\pi]_{\mathscr{E}}^{\mathscr{E}}$. Since two linear maps are equal if and only have the same matrix representation, we have $S_1S_2 = S_2S_1 = R_\pi$. We also have $S_1^2 = S_2^2 = (S_1S_2)^2 = \mathrm{Id}_{\mathbf{R}^2}$.

See Tutorial 6, question 5 for more details.

Exercise 3.2.35. Let $T \in \mathcal{L}(V)$. Suppose that there exists $v \in V$ and $n \in \mathbf{N}_{\geq 1}$ such that $T^n v = 0$, but $T^{n-1}v \neq 0$.

1. Prove that $\mathscr{B} := (v, Tv, \dots, T^{n-1}v)$ is linearly independent.
2. Let $U := \mathrm{span}(\mathscr{B})$ (so $\mathscr{B}$ is a basis for U). Prove that for any $u \in U$, its image Tu is still in U.
3. Let $T|_U : U \to U$ be the restriction of T to U. Find $[(T|_U)^k]_{\mathscr{B}}^{\mathscr{B}}$ for $k \in \mathbf{N}_{\geq 1}$.

Solution. 1. Observe that if $m \geq n$, then $T^m v = T^{m-n}T^n v = T^{m-n}0 = 0$. Suppose we can write

$$0_V = \sum_{i=0}^{n-1} \lambda_i T^i v = \lambda_0 v + \lambda_1 Tv + \cdots + \lambda_{n-1}T^{n-1}v. \tag{3.6}$$

We want to show that all the λ_i are 0. By applying T^{n-1} to both sides of (3.6), we obtain $0_V = \lambda_0 T^{n-1}v + \lambda_2 0 + \cdots + \lambda_{n-1}0$. But this implies that $\lambda_0 = 0$. We can then apply T^{n-2} to both sides of (3.6) to obtain that $\lambda_1 = 0$. By repeating this process, we obtain that all the λ_i are 0 as desired.

2. For an element $u \in U$ we have $u = \lambda_0 v + \cdots + \lambda_{n-1}T^{n-1}v$, so

$$T(u) = \lambda_0 Tv + \cdots + \lambda_{n-2}T^{n-1}v + \underbrace{\lambda_{n-1}T^n v}_{=0}$$

is also in U.

3. We have $T|_U(T^i v) = T^{i+1}v$, so

$$[T|_U]_{\mathscr{B}}^{\mathscr{B}} = \begin{array}{c} 1 \\ 2 \\ 3 \\ \vdots \\ n \end{array}\!\!\begin{bmatrix} 0 & \cdots & \cdots & 0 \\ 1 & \ddots & & \vdots \\ 0 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & 1 \;\; 0 \end{bmatrix}.$$

Similarly, $T|_U{}^k(T^i v) = T^{k+i}v$ and

$$[T|_U{}^k]_{\mathscr{B}}^{\mathscr{B}} = \begin{cases} \begin{array}{c} 1 \\ \vdots \\ k \\ k+1 \\ \vdots \\ n \end{array}\!\!\begin{bmatrix} 0 & & \\ \vdots & \ddots & \\ 0 & \ddots & \ddots \\ 1 & \ddots & \ddots \\ & \ddots & 0 \cdots 0 \end{bmatrix} & \text{if } 1 \le k \le n-1, \\ 0 & \text{if } k \ge n. \end{cases}$$

(the k zeros in the last column are underbraced by k)

□

Exercise 3.2.36. Let $D\colon \mathcal{P}(\mathbf{R})_n \to \mathcal{P}(\mathbf{R})_n$ be the differentiation operator: $D(p) = p'$, and let $\mathscr{B} = (1, x, x^2, \dots, x^n)$ be the standard basis of $\mathcal{P}(\mathbf{R})_n$. Find $[D^k]_{\mathscr{B}}^{\mathscr{B}}$ for $k \in \mathbf{N}_{\ge 1}$

Solution. We have $D(1) = 0$ and $D(x^i) = ix^{i-1}$ for $1 \ge i \ge n$, which gives us the $(n+1, n+1)$-matrix

$$[D]_{\mathscr{B}}^{\mathscr{B}} = \begin{bmatrix} 0 & 1 & 0 & & \\ & 0 & 2 & \ddots & \\ & & 0 & \ddots & 0 \\ & & & \ddots & n \\ & & & & 0 \end{bmatrix}.$$

In general, for $1 \le k \le n$, we have

$$D^k(x^i) = \begin{cases} i(i-1)\cdots(i-k+1)x^{i-k} & \text{if } 1 \le k \le i, \\ 0 & \text{if } k \ge i+1, \end{cases}$$

which gives us the matrix

$$[D^k]_{\mathscr{B}}^{\mathscr{B}} = \begin{cases} \begin{bmatrix} 0 & \cdots & 0 & k! & & 0 & \cdots & 0 \\ & \ddots & & & \ddots & & & \vdots \\ & & & & \frac{(k+1)!}{1} & & & 0 \\ & & & & & \ddots & & \frac{n!}{(n-k)!} \\ & & & & & & \ddots & 0 \\ & & & & & & & \vdots \\ & & & & & & & 0 \end{bmatrix} & \text{if } 1 \leq k \leq n, \\ 0 & \text{if } k \geq n+1. \end{cases}$$

□

3.2.5 Change of basis

Add motivation for the change of basis formula. Why do we do these computations?

So far, bases have played important roles in studying finite dimensional vector spaces and linear maps between them. But bases are not unique! So it is natural to ask what happens when we change the basis.

Question 3.2.37. Let $\mathscr{B}$ and $\mathscr{C}$ be two bases for V. What is the relation between $[v]_{\mathscr{B}}$ and $[v]_{\mathscr{C}}$?

To answer this question, let us first consider the identity map

$$\underset{\mathscr{B}}{V} \xrightarrow{\mathrm{Id}_V} \underset{\mathscr{C}}{V}.$$

That is, we think of $\mathscr{B}$ as a basis of V the domain of Id_V, while we think of $\mathscr{C}$ as a basis of the codomain V of Id_V. Then it follows from Lemma 3.2.25 that for any $v \in V$ we have:

$$[v]_{\mathscr{C}} = [\mathrm{Id}_V]_{\mathscr{B}}^{\mathscr{C}} [v]_{\mathscr{B}}.$$

We say that $[\mathrm{Id}_V]_{\mathscr{B}}^{\mathscr{C}}$ is the **change of basis matrix** from $\mathscr{B}$ to $\mathscr{C}$.

In other words, for $\mathscr{B} = (v_1, \ldots, v_n)$ and $\mathscr{C} = (w_1, \ldots, w_n)$, if

$$\begin{aligned} v_1 &= a_{11} w_1 + \cdots + a_{n1} w_n \\ &\vdots \\ v_n &= a_{1n} w_1 + \cdots + a_{nn} w_n \end{aligned}$$

then we have

$$[\mathrm{Id}_V]_{\mathscr{B}}^{\mathscr{C}} = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{bmatrix} \in \mathbf{F}^{n,n}.$$

Say that this is $v = \alpha A$.

Example 3.2.38. Let $\mathscr{E} = \left(\begin{bmatrix}1\\0\end{bmatrix}, \begin{bmatrix}0\\1\end{bmatrix}\right)$ be the standard basis of $\mathbf{R}^2$ and let $\mathscr{C} = \left(\begin{bmatrix}1\\0\end{bmatrix}, \begin{bmatrix}0\\-2\end{bmatrix}\right)$. Then

$$\begin{aligned}\mathrm{Id}_{\mathbf{R}^2}\begin{bmatrix}1\\0\end{bmatrix} &= 1\begin{bmatrix}1\\0\end{bmatrix} + 0\begin{bmatrix}0\\-2\end{bmatrix},\\ \mathrm{Id}_{\mathbf{R}^2}\begin{bmatrix}0\\1\end{bmatrix} &= 0\begin{bmatrix}1\\0\end{bmatrix} + (-\tfrac{1}{2})\begin{bmatrix}0\\-2\end{bmatrix}.\end{aligned}$$

Therefore,

$$[\mathrm{Id}_V]^{\mathscr{C}}_{\mathscr{E}} = \begin{bmatrix}1 & 0\\ 0 & -\frac{1}{2}\end{bmatrix}.$$

Lemma 3.2.39. *Let $\mathscr{B}$ and $\mathscr{C}$ be two bases of a finite dimensional vector space V. Then $[\mathrm{Id}_V]^{\mathscr{C}}_{\mathscr{B}}$ is invertible and $([\mathrm{Id}_V]^{\mathscr{C}}_{\mathscr{B}})^{-1} = [\mathrm{Id}_V]^{\mathscr{B}}_{\mathscr{C}}$.*

Proof. This is simply Proposition 3.2.30 applied to the invertible map $\mathrm{Id}_V \colon V \to V$. □

Exercise 3.2.40. Suppose $\mathscr{C} = \left(\begin{bmatrix}1\\2\end{bmatrix}, \begin{bmatrix}3\\4\end{bmatrix}\right)$. One easily checks that $\mathscr{C}$ is linearly independent and so is a basis for $\mathbf{R}^2$. Given $v = \begin{bmatrix}a\\b\end{bmatrix} \in \mathbf{R}^2$, compute $[v]_{\mathscr{C}}$.

Solution. First we compute $[\mathrm{Id}_V]^{\mathscr{C}}_{\mathscr{E}}$ where $\mathscr{E}$ is the standard basis of $\mathbf{R}^2$. In order to do that we start by solving $\begin{bmatrix}1\\0\end{bmatrix} = c_1\begin{bmatrix}1\\2\end{bmatrix} + c_2\begin{bmatrix}3\\4\end{bmatrix}$. We find $\begin{bmatrix}c_1\\c_2\end{bmatrix} = \begin{bmatrix}-2\\1\end{bmatrix}$. Then we solve $\begin{bmatrix}0\\1\end{bmatrix} = d_1\begin{bmatrix}1\\2\end{bmatrix} + d_2\begin{bmatrix}3\\4\end{bmatrix}$ and find $\begin{bmatrix}d_1\\d_2\end{bmatrix} = \begin{bmatrix}3/2\\-1/2\end{bmatrix}$. Putting this together, we have

$$[\mathrm{Id}_V]^{\mathscr{C}}_{\mathscr{E}} = \begin{bmatrix}-2 & \frac{3}{2}\\ 1 & -\frac{1}{2}\end{bmatrix}.$$

Finally, we have

$$[v]_{\mathscr{C}} = [\mathrm{Id}_V]^{\mathscr{C}}_{\mathscr{E}}[v]_{\mathscr{E}} = \begin{bmatrix}-2 & \frac{3}{2}\\ 1 & -\frac{1}{2}\end{bmatrix}\begin{bmatrix}a\\b\end{bmatrix} = \begin{bmatrix}-2a + \frac{3}{2}b\\ a - \frac{b}{2}\end{bmatrix}.$$

□

Observe that it was also possible to directly solve the system

$$\begin{bmatrix}a\\b\end{bmatrix} = \begin{bmatrix}1 & 3\\ 2 & 4\end{bmatrix}\begin{bmatrix}x\\y\end{bmatrix}.$$

Exercise 3.2.41. Let V be a vector space of dimension m and let $\mathscr{B} = (v_1, \ldots, v_m)$ be a basis for V. Let $\sigma \colon \{1, \ldots, m\} \to \{1, \ldots, m\}$ be a bijective function. Show that $\mathscr{C} := (v_{\sigma(1)}, \ldots, v_{\sigma(m)})$ is also a basis for V.

Can you describe $[\mathrm{Id}_V]^{\mathscr{C}}_{\mathscr{B}}$? *Hint:* if $[v]_{\mathscr{B}} = [c_1, \ldots, c_m]^{\mathsf{T}}$, then $[v]_{\mathscr{C}} = [c_{\sigma(1)}, \ldots, c_{\sigma(m)}]^{\mathsf{T}}$.

We have seen how coordinate vectors change under change of basis. But how about matrix representations of linear maps? Let us consider the simpler case of operators. So let $T \in \mathcal{L}(V)$ and let $\mathscr{B}$ and $\mathscr{C}$ be two bases for V.

Question 3.2.42. What is the relation between $[T]^{\mathscr{B}}_{\mathscr{B}}$ and $[T]^{\mathscr{C}}_{\mathscr{C}}$?

Answer.

$$\begin{array}{ccc} {}^{\mathscr{B}}V & \xrightarrow{T} & V^{\mathscr{B}} \\ {\scriptstyle \mathrm{Id}_V}\downarrow & & \downarrow{\scriptstyle \mathrm{Id}_V} \\ {}^{\mathscr{C}}V & \xrightarrow[T]{} & V^{\mathscr{C}} \end{array}$$

We have $\mathrm{Id}_V T = T = T\,\mathrm{Id}_V$. Therefore, using the bases as chosen, we have $[\mathrm{Id}_V]^{\mathscr{C}}_{\mathscr{B}}[T]^{\mathscr{B}}_{\mathscr{B}} = [T]^{\mathscr{C}}_{\mathscr{C}}[\mathrm{Id}_V]^{\mathscr{C}}_{\mathscr{B}}$, or

$$[T]^{\mathscr{C}}_{\mathscr{C}} = [\mathrm{Id}_V]^{\mathscr{C}}_{\mathscr{B}}[T]^{\mathscr{B}}_{\mathscr{B}}[\mathrm{Id}_V]^{\mathscr{B}}_{\mathscr{C}} \tag{3.7}$$

where we used the fact that $([\mathrm{Id}_V]^{\mathscr{C}}_{\mathscr{B}})^{-1} = [\mathrm{Id}_V]^{\mathscr{B}}_{\mathscr{C}}$. ■

If you tried to compute some example of change of basis matrices, the result you obtained might have seen familiar to you. Indeed, they look like matrix representations of linear transformations. This ressemblance is not a coincidence.

To take a concrete example, let $\mathscr{E} = \left(e_1 = \begin{bmatrix}1\\0\end{bmatrix}, e_2 = \begin{bmatrix}0\\1\end{bmatrix}\right)$ be the standard basis of $\mathbf{R}^2$ and let R_θ be the rotation of angle θ around the origin. Finally, let $\mathscr{B} := (R_\theta e_1, R_\theta e_2)$. This is a basis of $\mathbf{R}^2$ and

$$[\mathrm{Id}_{\mathbf{R}^2}]^{\mathscr{E}}_{\mathscr{B}} = \begin{bmatrix}\cos(\theta) & -\sin(\theta)\\ \sin(\theta) & \cos(\theta)\end{bmatrix}$$

where you can recognise the matrix $[R_\theta]^{\mathscr{E}}_{\mathscr{E}}$ from Equation (3.5). This phenomenon is more general and we have.

Lemma 3.2.43. *Let V be a vector space with basis $\mathscr{B} = (v_1, \dots, v_m)$ and let $T \in \mathcal{L}(V)$ be an isomorphism. Then $T\mathscr{B} = (Tv_1, \dots, Tv_m)$ is a basis by Proposition 3.1.45 and $[\mathrm{Id}_V]^{\mathscr{B}}_{T\mathscr{B}} = [T]^{\mathscr{B}}_{\mathscr{B}}$.*

Proof. The i^{th} column of $[T]^{\mathscr{B}}_{\mathscr{B}}$ is given by the coefficients of $T(v_i) = a_{1i}v_1 + \cdots + a_{mi}v_m$ while the i^{th} column of $[\mathrm{Id}_V]^{\mathscr{B}}_{T\mathscr{B}}$ is given by the coefficients of $\mathrm{Id}_V(Tv_i) = Tv_i = a_{1i}v_1 + \cdots + a_{mi}v_m$. □

You can think of $[T]^{\mathscr{B}}_{\mathscr{B}}$ as "the space is fixed, vectors are moved by T" and of $[\mathrm{Id}_V]^{\mathscr{B}}_{T\mathscr{B}} = ([\mathrm{Id}_V]^{T\mathscr{B}}_{\mathscr{B}})^{-1}$ as "vectors are fixed, the underlying space is moved by T^{-1}". See Figure 3.8 for an example with $T = R_\theta$ the rotation of angle θ around the origin.

Definition 3.2.44.

Two matrices A and B in $\mathbf{F}^{m,m}$ are **similar** if there exists an invertible matrix P in $\mathbf{F}^{m,m}$ such that $B = PAP^{-1}$.

Lemma 3.2.45. *Similarity is an* equivalence relation*:*

1. *A and A are similar;*

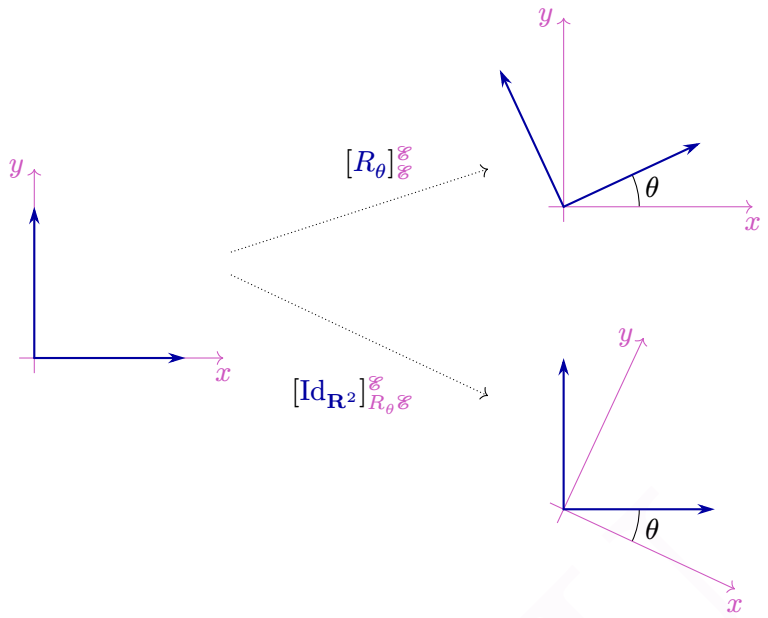


Figure 3.8: Rotation of an angle θ with respect to the standard basis, versus change of basis matrix.

2. *If A and B are similar, then B and A are similar;*

3. *If A is similar to B and B is similar to C, then A is similar to C.*

Proof. 1. $A = \mathrm{Id}_m A \mathrm{Id}_m^{-1}$.
2. If $B = PAP^{-1}$, then $A = QBQ^{-1}$ for $Q = P^{-1}$.
3. If $B = PAP^{-1}$ and $C = QBQ^{-1}$, then $C = RAR^{-1}$ for $R = QP$. □

Proposition 3.2.46. *Let V be a vector space and let $T \in \mathcal{L}(V)$. Let $\mathscr{B}$ and $\mathscr{C}$ be two bases for V. Then $[T]^{\mathscr{B}}_{\mathscr{B}}$ and $[T]^{\mathscr{C}}_{\mathscr{C}}$ are similar.*

Proof. This directly follows from Equation (3.7) on page 89. □

We have seen that any operator on a finite dimensional vector space admits a matrix representation. So a natural question to ask is: does there always exist a nice matrix representation?

Major Question 3.2.47.

Given V and $T \in \mathcal{L}(V)$, find a basis $\mathscr{B}$ such that $[T]^{\mathscr{B}}_{\mathscr{B}}$ is "as simple as possible" (for example: diagonal, upper triangular, with many zeroes, …).

The main idea below this question is that a matrix is "nice" or "simple" if we can do fast computations with it. This is the case as soon as the matrix is sparse enough (has many zeroes).

We will later see (Section 5.3 and in particular Theorem 5.3.8) that each $n \times n$ matrix is equivalent (similar to) to a matrix of the form

$$J = \begin{bmatrix} \boxed{J_1} & & & \\ & \boxed{J_2} & & \\ & & \ddots & \\ & & & \boxed{J_k} \end{bmatrix} \tag{3.8}$$

where each J_i is a "Jordan block". That is, there exists an integer m_i and a complex number λ_i such that J_i is a $m_i \times m_i$ matrix of the form

$$J_i = \begin{bmatrix} \lambda_i & 1 & & \\ & \ddots & \ddots & \\ & & \ddots & 1 \\ & & & \lambda_i \end{bmatrix}.$$

we should have $m_1 + \cdots + m_k = m$. But this is the only restriction on the m_i and λ_i. Such a matrix J is called a Jordan matrix.

In other words, if V is a finite dimensional vector space and $\mathsf{T} \in \mathcal{L}(V)$ a linear operator, there always exists a basis $\mathscr{B}$ of V such that $[T]^{\mathscr{B}}_{\mathscr{B}}$ is given by a Jordan matrix of the form given in Equation (3.8). Such a $[T]^{\mathscr{B}}_{\mathscr{B}}$ is called the "Jordan form" of T

3.3 Projections

Projections are useful tools that allow us to go from one "big" space (infinite dimensional) to "smaller" spaces (finite dimensional) to make approximations. We will first discuss general projections, and will then see how we can apply them to make approximation of functions.

3.3.1 Projections: definition and first properties

We start this subsection by defining some very special operators.

Definition 3.3.1.

Let $V = U \oplus W$ be a direct sum decomposition. We define the **projection onto** U (along direction W) to be the map

$$\begin{aligned} P_U = P_{U,W} : V &\longrightarrow V \\ v = u + w &\longmapsto u. \end{aligned}$$

By direct sum decomposition, for any $v \in V$, there exists a unique $u \in U$ (and a unique $w \in W$) such that $v = u + w$. So the above map P_U is well-defined.

Example 3.3.2. Let $V = \mathbf{R}^2$ and let $U = \{\begin{bmatrix} x \\ 0 \end{bmatrix} \mid x \in \mathbf{R}\}$ be the x-axis and $W = \{\begin{bmatrix} 0 \\ y \end{bmatrix} \mid y \in \mathbf{R}\}$ be the y-axis. Then $V = U \oplus W$ and P_U is the first coordinate projection: $P_U \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} x \\ 0 \end{bmatrix}$.

Remark 3.3.3.

We write P_U, but the projection $P_U : U \oplus W \to V$ depends both on U and on W! Let us demonstrate this dependence by an example. Let $V = \mathbf{R}^2$ and let $U = \{\begin{bmatrix} x \\ 0 \end{bmatrix} \mid x \in \mathbf{R}\}$ be the x-axis. Let $W_1 = \{\begin{bmatrix} 0 \\ y \end{bmatrix} \mid y \in \mathbf{R}\}$ be the y-axis and $W_2 = \{\begin{bmatrix} y \\ y \end{bmatrix} \mid y \in \mathbf{R}\}$ be the line $y = x$. We have $V = U \oplus W_1 = U \oplus W_2$. For $v = \begin{bmatrix} 2 \\ 1 \end{bmatrix}$ we have $\begin{bmatrix} 2 \\ 1 \end{bmatrix} = \begin{bmatrix} 2 \\ 0 \end{bmatrix} + \begin{bmatrix} 0 \\ 1 \end{bmatrix} \in U \oplus W_1$ but also $\begin{bmatrix} 2 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix} + \begin{bmatrix} 1 \\ 1 \end{bmatrix} \in U \oplus W_2$. Therefore, $P_{U,W_1} \begin{bmatrix} 2 \\ 1 \end{bmatrix} = \begin{bmatrix} 2 \\ 0 \end{bmatrix}$ is not the same as $P_{U,W_2} \begin{bmatrix} 2 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$. See Figure 3.9 for a picture.

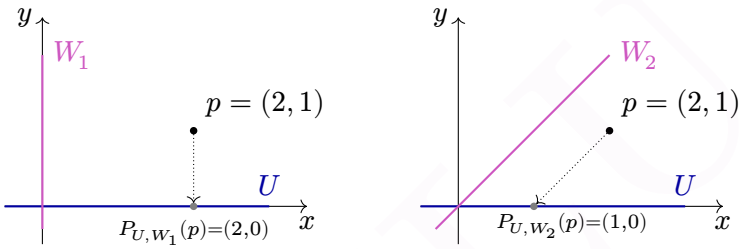


Figure 3.9: Projection of $\begin{bmatrix} 2 \\ 1 \end{bmatrix}$ on the x-axis, along direction W_1 (on the right) and along direction W_2 (on the left). For readability, only the point $p = (2, 1)$ and its images are represented, not the full vector $v = \begin{bmatrix} 2 \\ 1 \end{bmatrix} = \overrightarrow{0p}$ and its images $P_{U,W_*}(v) = \overrightarrow{0P_{U,W_*}(v)}$.

We defined projections merely as functions. But it turns out that they are linear maps satisfying many interesting properties.

Proposition 3.3.4 (Properties of projection onto P_U)**.** *Let $V = U \oplus W$ be a direct sum decomposition. Then the projection P_U satisfies the following properties:*

1. $P_U \in \mathcal{L}(V)$;
2. $P_U(u) = u$ *for all* $u \in U$;
3. $P_U(w) = 0_V$ *for all* $w \in W$;
4. $\mathrm{Im}(P_U) = U$;
5. $\ker(P_U) = W$;
6. $v - P_U(v) \in W$ *for all* $v \in V$;
7. $P_U^2 = P_U$.

Proof. For v in V, let $v = u + w$ be its direct sum decomposition: $u \in U$ and $w \in W$.

1. Let v_1 and v_2 be two vectors in V and let $\lambda \in \mathbf{F}$ be a scalar. There exists a unique way to write $v_1 = u_1 + w_1$ and $v_2 = u_2 + w_2$ with $u_1, u_2 \in U$ and $w_1, w_2 \in W$. But then $\lambda u_1 + u_2$ is in U while $\lambda w_1 + w_2$ is in W. A simple computation gives

$$P_U(\lambda v_1 + v_2) = P_U((\lambda u_1 + u_2) + (\lambda w_1 + w_2)) = \lambda u_1 + u_2 = \lambda P_U(v_1) + P_U(v_2).$$

Hence P_U is a linear map from V to V.

2. Suppose u is in U. We have $u = u + 0_V$ with $0_V \in W$. So $P_U(u) = u$.

3. Suppose w is in w. We have $w = 0_V + w$ with $0_V \in U$. So $P_U(w) = 0_V$.

4. By definition of P_U, its image is included in U. Furthermore, 2 implies that U is included in the image of P_U. Therefore, we have the equality $\mathrm{Im}(P_U) = U$.

5. It follows from 3 that $W \subseteq \ker(P_U)$. For the other inclusion, let $v = u + w$ be in the kernel of P_U. That is $P_U(v) = u = 0$, so $v = w$ is in W.

6. For $v = u + w \in V$, we have $v - P_U(v) = u + w - u = w \in W$.

7. For all $v = u + w$ we have $P_U^2(v) = P_U(u) = u = P_U(v)$, so $P_U^2 = P_U$. □

Projections are an easy way to test if a vector u belongs to a direct summand. Indeed, if $V = U \oplus W$, then by Proposition 3.3.4, $v \in V \iff P(v) = v$.

We have defined projections with respect to a direct sum decomposition. But Properties 4 and 5 in Proposition 3.3.4 say that we can recover the spaces U and W from the linear map P_U. And we can use Properties 1 and 7 to define abstract projections.

Definition 3.3.5.

An operator $P \in \mathcal{L}(V)$ is a **projection** if it satisfies $P^2 = P$.

Projections onto a subspace give us examples of projections.

Lemma 3.3.6. *If $V = U \oplus W$, then P_U is a projection.*

Proof. This is Properties 1 and 7 of Proposition 3.3.4. □

We also have the following two basic examples.

Example 3.3.7. For any vector space V, both the zero map $0 \in \mathcal{L}(V)$ and the identity map Id_V are projections.

The above example should remind you that 0 and 1 are both solution to the real equation $z^2 = z$. But in a vector space of dimension $\dim(V) \geq 2$, the zero map and the identity map are not the only projections as demonstrated by Example 3.3.2. To elaborate a little bit: 0 is a solution of $z^2 = z$ while 1 is the only invertible solution (divide by z on both sides). Since non-zero complex numbers are invertible, these are all the solutions. Similarly, 0 is a solution of $P^2 = P$, while Id_V is the only invertible solution. But if V is a vector space of dimension at least 2, then $\mathcal{L}(V)$ is also a vector space of dimension at least 2 and hence there exists non-zero linear maps that are not invertible. Therefore, the equation $P^2 = P$ might have more than 2 solutions.

The following (easy) result shows that we may determine if a linear map is a projection by studying its matrix representation.

Lemma 3.3.8. *Let V be a finite dimensional vector space and let $T \in \mathcal{L}(V)$ be an operator. Let $\mathscr{B}$ be a basis of V. Then T is a projection if and only if $([T]_{\mathscr{B}}^{\mathscr{B}})^2 = [T]_{\mathscr{B}}^{\mathscr{B}}$.*

Proof. We have $[T^2]_{\mathscr{B}}^{\mathscr{B}} = ([T]_{\mathscr{B}}^{\mathscr{B}})^2$. Therefore, $T = T^2$ if and only if $([T]_{\mathscr{B}}^{\mathscr{B}})^2 = [T]_{\mathscr{B}}^{\mathscr{B}}$. □

One immediately obtain as a corollary that if V has dimension 2, then $\left[\begin{smallmatrix}1 & 0\\ 0 & 0\end{smallmatrix}\right]$ represents a projection P that is not conjugated to the zero map nor to the identity map. We conclude that if the dimension of V is at least 2, the equation $P^2 = P$ has at least 3 solutions (that are pairwise non similar).

Example 3.3.9. Let $T \in \mathcal{L}(\mathbf{F}^2)$ be an operator. Suppose that there exists a basis $\mathscr{B}$ such that $[T]_{\mathscr{B}}^{\mathscr{B}} = A = \left[\begin{smallmatrix}1 & -1\\ 0 & 0\end{smallmatrix}\right]$. Then T is a projection. Indeed, it is easy to check that $\left[\begin{smallmatrix}1 & -1\\ 0 & 0\end{smallmatrix}\right]^2 = \left[\begin{smallmatrix}1 & -1\\ 0 & 0\end{smallmatrix}\right]$.

Similarly, if $[T]_{\mathscr{B}}^{\mathscr{B}} = \left[\begin{smallmatrix}1/2 & 1/2\\ 1/2 & 1/2\end{smallmatrix}\right]$ then T is a projection.

It turns out that *projections* (Definition 3.3.5) and *projections onto* a subspace(Definition 3.3.1) are exactly the same things as demonstrated by the following proposition.

Proposition 3.3.10. *Let V be a vector space and let $P \in \mathcal{L}(V)$ be a projection. Then $V = \operatorname{Im}(P) \oplus \ker(P)$ and $P = P_{\operatorname{Im}(P),\ker(P)}$.*

Proof. It is clear that $\operatorname{Im}(P) + \ker(P) \subseteq V$. So we need to prove that the sum is direct and that it is equal to V. Let $v \in V$. Then one have $v = P(v) + (v - P(v))$ with $P(v) \in \operatorname{Im}(P)$ and $v - P(v)$ is in $\ker(P)$. Indeed, $P(v - P(v)) = P(v) - P^2(v) = P(v) - P(v) = 0$. Now, for the direct sum part. If $v \in \operatorname{Im}(P) \cap \ker(P)$ we have $v = P(w)$ and $0 = P(v) = P^2(w) = P(w) = v$, so $\operatorname{Im}(P) \cap \ker(P) = 0$ which finishes the proof of $\operatorname{Im}(P) \oplus \ker(P) = V$.

Finally, let $v \in V$. Then $v = P(v) + (v - P(v))$ is the unique decomposition $v = u + w$ with $u \in \operatorname{Im}(P)$ and $w \in \ker(P)$. By definition of $P_{\operatorname{Im}(P),\ker(P)}$, we have $P_{\operatorname{Im}(P),\ker(P)}(v) = P(v)$ for all v in V and so these two maps are equal. □

Another way to interpret Proposition 3.3.10 is that there is a one-to-one correspondance between projections $P \in \mathcal{L}(V)$ and direct sums decomposition $V = U \oplus W$ where the order matters. This gives us another proof that if V has dimension at least 2, then the equation $P^2 = P$ has at least three distinct solutions. Indeed, the decomposition $V = \{0\} \oplus V = V \oplus \{0\}$ corresponds to the projections 0 and Id. If U is a subspace with $1 \leq \dim(U) \leq \dim(V)$ and W is any direct complement, the decomposition $V = U \oplus W = W \oplus U$ corresponds to two news projections. By varying the dimension of U, we can even show that the equation $P^2 = P$ has at least $\dim(V) + 1$ solutions.

We can also use Proposition 3.3.10 to show that, for finite dimensional vector spaces, projections always admit an specially nice matrix representation.

Lemma 3.3.11. *Let V be a finite dimensional vector space and let $P \in \mathcal{L}(V)$ be a projection. Then there exists a basis $\mathscr{B}$ of V such that*

$$[T]_{\mathscr{B}}^{\mathscr{B}} = \begin{matrix} \left.\vphantom{\begin{matrix}1\\&\ddots\\&&1\end{matrix}}\right\} \dim \operatorname{Im}(P) \\ \left.\vphantom{\begin{matrix}0\\&\ddots\\&&0\end{matrix}}\right\} \dim \ker(P) \end{matrix} \begin{bmatrix} 1 & & & \\ & \ddots & & \\ & & 1 & \\ & & & 0 \\ & & & & \ddots \\ & & & & & 0 \end{bmatrix}.$$

Proof. Let $\mathscr{A}$ be a basis of $\operatorname{Im}(P)$ and $\mathscr{C}$ be a basis of $\ker(P)$. Then $\mathscr{B} = \mathscr{A} \cup \mathscr{C}$ is a basis of $V = \operatorname{Im}(P) \oplus \ker(P)$. Finally, for every $v \in \mathscr{B}$ we have $Pv = 1 \cdot v$ and for every $w \in \mathscr{C}$ we have $Pw = 0$. The formula follows. □

We can use the above lemma to obtain the following result about matrices.

Corollary 3.3.12. *Let $A \in \mathbf{F}^{m,m}$ be a square matrix. If $A^2 = A$, then is similar to a diagonal matrix with only 1s and 0s on the diagonal.*

Proof. The operator $\mathrm{L}_A \in \mathcal{L}(\mathbf{F}^m)$ defined by $\mathrm{L}_A(v) = Av$ is a projection. Let $\mathscr{B}$ be the basis given by Lemma 3.3.11 and let $\mathscr{E}$ be the standard basis of $\mathbf{F}^m$. Then $[T]_{\mathscr{B}}^{\mathscr{B}}$ has the desired form while $[\mathrm{L}_A]_{\mathscr{E}}^{\mathscr{E}} = A$. So for $B = [\mathrm{Id}]_{\mathscr{B}}^{\mathscr{E}}$ we have $A = B[T]_{\mathscr{B}}^{\mathscr{B}} B^{-1}$ as desired. □

We conclude this subsection by the following result that is a generalisation of Proposition 3.3.10.

Theorem 3.3.13.

Suppose $P_1, \dots, P_k \in \mathcal{L}(V)$ are projections such that $P_1 + \cdots + P_k = \mathrm{Id}_V$ and $P_i P_j = 0_{\mathcal{L}(V)}$ if $i \neq j$. Then $V = \operatorname{Im}(P_1) \oplus \cdots \oplus \operatorname{Im}(P_k)$.

Proof. Let v be any vector in V. Then

$$v = \mathrm{Id}_V\, v = (P_1 + \cdots + P_k)v = P_1 v + \cdots + P_k v \in \operatorname{Im}(P_1) + \cdots + \operatorname{Im}(P_k) \tag{3.9}$$

and thus $V = \operatorname{Im}(P_1) + \cdots + \operatorname{Im}(P_k)$. We now prove that the sum is direct. Suppose $0 = v_1 + \cdots + v_k$ with $v_i \in \operatorname{Im}(P_i)$ for $1 \leq i \leq k$. We want to prove that all the v_i are zero. By definition of the image, there exist w_i such that $P_i w_i = v_i$. Using that P_i is a projection we have $P_i v_i = P_i^2 w_i = P_i w_i = v_i$ while $P_i v_j = P_i P_j w_j = 0 w_j = 0$ if $i \neq j$. Now, if we apply P_i to both sides of (3.9) we obtain $0 = v_i$. By doing this for all $1 \leq i \leq k$ we have that all the v_i are zero as desired, and so the sum is direct. □

Now that we have proven Theorem 3.3.13, let us discuss why it is a generalisation of Proposition 3.3.10. Let $P \in \mathcal{L}(V)$ be a projection, $P_1 := P$ and $P_2 := \mathrm{Id}_V - P$. One easily checks the following properties:

- P_2 is a projection: $P_2^2 = \mathrm{Id}_V^2 - \mathrm{Id}_V P - P \mathrm{Id}_V + P^2 = \mathrm{Id}_V - P - P + P = P_2$;

- $P_1 + P_2 = \mathrm{Id}_V$;
- and $P_1P_2 = P - P^2 = 0 = P_2P_1$.

We can hence can apply Theorem 3.3.13 to P_1 and P_2 to obtain $V = \mathrm{Im}(P) \oplus \mathrm{Im}(\mathrm{Id}_V - P)$. Finally, $\mathrm{Im}(\mathrm{Id}_V - P) = \ker(P)$ and we recover the Proposition. Indeed, if v is in $\ker(P)$, then $v = v - 0 = v - P(v) = (\mathrm{Id}_V - P)(v)$, which proves $\ker(P) \subseteq \mathrm{Im}\,\mathrm{Id}_V - P$. For the other inclusion, if $v \in \mathrm{Im}(\mathrm{Id}_V - P)$, then $v = (\mathrm{Id}_V - P)(w)$ for some w and so $P(v) = P(\mathrm{Id}_V - P)(w) = P(w) - P^2(w) = 0$.

3.3.2 Left/right inverses and projections

An easy way to create projections is to use left and right inverses.

Proposition 3.3.14. *Let V and W be two vector spaces and let $T \in \mathcal{L}(V, W)$ and $S \in \mathcal{L}(W, V)$ such that $TS = \mathrm{Id}_W$. Then $V = \mathrm{Im}(S) \oplus \ker(T)$ and $ST \in \mathcal{L}(V)$ is a projection to $\mathrm{Im}(S)$ along direction $\ker(T)$.*

Proof. We first show that ST is an abstract projection: $(ST)^2 = S(TS)T = S\,\mathrm{Id}_W\,T = ST$. It follows from Proposition 3.3.10 that ST is a projection onto $\mathrm{Im}(ST)$ along direction $\ker(ST)$.

It now remains to show that $\mathrm{Im}(ST) = \mathrm{Im}(S)$ and $\ker(ST) = \ker(T)$. We already know that $\mathrm{Im}(ST) \subseteq \mathrm{Im}(S)$ for every functions. For the other inclusion, let $v \in \mathrm{Im}(S)$. Thus there exists $w \in W$ with $v = S(w) = S\,\mathrm{Id}_W(w) = STS(w) = ST(S(w))$ which shows that $\mathrm{Im}(S) \subseteq \mathrm{Im}(ST)$.

Totorial 4, Question 2

For the kernels we have $\ker(ST) \supseteq \ker(T)$ for every linear maps. For the other inclusion, let v be an element in $\ker(ST)$. We have $0_V = ST(v)$ and by applying T to both sides $0_W = TST(v) = \mathrm{Id}_W\,T(v) = T(v)$, which shows that $\ker(ST) \subseteq \ker(T)$. □

Observe that for a given $T \in \mathcal{L}(V, W)$ there exists a right inverse S such that $TS = \mathrm{Id}_W$ if and only if T is surjective. If such an inverse exists, it is not unique unless T is an isomorphism. This is related to the fact that given a general subspace U $(= \ker(T))$ of V, there exists more than one direct sum complement X $(= \mathrm{Im}(S))$ such that $V = U \oplus X$. Let us exemplify this.

Example 3.3.15. Let $T\colon \mathbf{R}^2 \to \mathbf{R}$ be the map $\begin{bmatrix} x \\ y \end{bmatrix} \mapsto x$. This is a linear map with $\ker(T) = \{\begin{bmatrix} 0 \\ y \end{bmatrix} \mid y \in \mathbf{R}\}$. Define $S_1, S_2\colon \mathbf{R} \to \mathbf{R}^2$ by

$$S_1(x) = \begin{bmatrix} x \\ 0 \end{bmatrix} \qquad \text{and} \qquad S_2(x) = \begin{bmatrix} x \\ x \end{bmatrix}.$$

These two maps are linear and one easily verify that $TS_1 = TS_2 = \mathrm{Id}_{\mathbf{R}}$. By the above proposition, both S_1T and S_2T are projections. On one hand, S_1T is the projection onto $\mathrm{Im}(S_1T) = \mathrm{Im}(S_1) = \{\begin{bmatrix} x \\ 0 \end{bmatrix} \mid x \in \mathbf{R}\}$ and along direction $\ker(T)$. On the other hand, S_2T is the projection onto $\mathrm{Im}(S_2T) = \mathrm{Im}(S_2) = \{\begin{bmatrix} x \\ x \end{bmatrix} \mid x \in \mathbf{R}\}$ and along direction $\ker(T)$. See Figure 3.10.

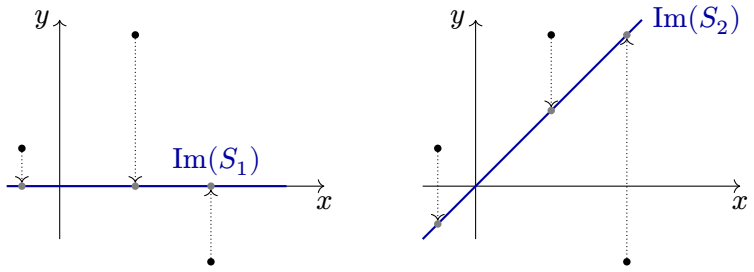


Figure 3.10: Two projections along the y-axis direction. The left one is onto the x-axis, and the right one is onto the diagonal $y = x$.

Many examples of the phenomenon described in Proposition 3.3.14 arise when you want to do approximations. Suppose we have some "complicated" space V (usually a space of functions) where we want to be able to do some approximations. We can consider a linear map $T\colon V \to \mathbf{F}^n$ which we think of as "taking samples/measurements/evaluating". We then construct a right inverse $S\colon \mathbf{F}^n \to V$ which "selects a solution/reconstructs something" using this data. Finally, the map $ST \in \mathcal{L}(V)$ will be a projection onto U a nice subspace of V, for example $U = \mathcal{P}(\mathbf{R})_n$.

Example 3.3.16. Let $V = \mathcal{C}^\infty(\mathbf{R}) = \{f\colon \mathbf{R} \to \mathbf{R} \mid f^{(n)} \text{ exists } \forall n\}$ be the space of smooth real functions. This space is infinite dimensional and quite complicated. To better understand it, we want to approximate it by polynomials. That is, we would like to have projections $P_n\colon \mathcal{C}^\infty(\mathbf{R}) \to \mathcal{P}(\mathbf{R})_n$. If $n = 0$, then we will approximate continuous functions by constant functions, if $n = 1$ the approximation will be by lines, by parabola if $n = 2$ and so on. Bigger n give better approximations. However, bigger n also give more complicated approximations. In order to define the projections, we will use Proposition 3.3.14. We consider the linear surjective maps $T_n\colon \mathcal{C}^\infty(\mathbf{R}) \to \mathbf{R}^{n+1}$ and right inverses maps $S_n\colon \mathbf{R}^{n+1} \to \mathcal{C}^\infty(\mathbf{R})$. Let us define

$$T_n(f) \coloneqq [f(a), f'(a), \dots, f^{(n)}(a)]^\mathsf{T} \in \mathbf{R}^{n+1},$$
$$S_n[x_0, \dots, x_n]^\mathsf{T} \coloneqq x_0 + x_1(x-a) + \frac{x_2}{2!}(x-a)^2 + \cdots + \frac{x_n}{n!}(x-a)^n \in \mathcal{P}(\mathbf{R})_n \subseteq \mathcal{C}^\infty(\mathbf{R}).$$

These maps are linear (exercise) and are left/right inverses. Indeed,

$$\begin{aligned}
(T_nS_n)[1,0,\dots,0]^\mathsf{T} &= T_n(1) = [1,0,\dots,0]^\mathsf{T},\\
(T_nS_n)[0,1,0,\dots,0]^\mathsf{T} &= T_n(x-a) = [0,1,0,\dots,0]^\mathsf{T},\\
(T_nS_n)[0,0,1,0,\dots,0]^\mathsf{T} &= T_n(\tfrac{(x-a)^2}{2}) = [0,0,1,0,\dots,0]^\mathsf{T},\\
&\vdots\\
(T_nS_n)[0,\dots,0,1]^\mathsf{T} &= T_n(\tfrac{(x-a)^n}{n!}) = [0,\dots,0,1]^\mathsf{T}.
\end{aligned}$$

Therefore, $P_n \coloneqq S_nT_n \in \mathcal{L}(\mathcal{C}^\infty(\mathbf{R}))$ is a projection to $\operatorname{Im}(S_n) \subseteq \mathcal{P}(\mathbf{R})_n$. One easily shows that $(a, (x-a), \dots, (x-a)^n$ is linearly independent, and thus a basis of $\mathcal{P}(\mathbf{R})_n$. It

follows that $\mathrm{Im}(S_n) \subseteq \mathcal{P}(\mathbf{R})_n$ has dimension $n+1$. In fact,

$$S_nT_n(f) = f(a) + f'(a)(x-a) + \frac{f''(a)}{2!}(x-a)^2 + \cdots + \frac{f^{(n)}(a)}{n!}(x-a)^n$$

is the n^{th} Taylor polynomial of f at $x = a$. Finally, the $\ker(S_nT_n) = \ker(T_n)$ is the set of all functions g such that $0 = g(a) = g'(a) = \cdots = g^{(n)}(a)$.

The sequence of Taylor polynomials forms a good *local approximation* of f around a. Local approximation means that for x close to a (and big n), the value of $f(x)$ and $((S_nT_n)(f))(x)$ are nearly the same. More formally, since $V = \mathrm{Im}(S_nT_n) \oplus \ker(S_nT_n)$, every function f can be written in a unique way as $p + g$, where p a polynomial of degree at most n and $g \in \ker(T_n)$. In other words, $(f - (S_nT_n)f)^{(i)}(a) = 0$ for all $0 \leq i \leq n$. That is, near a, the function $(f - (S_nT_n)f)$ is close to be the constant function 0.

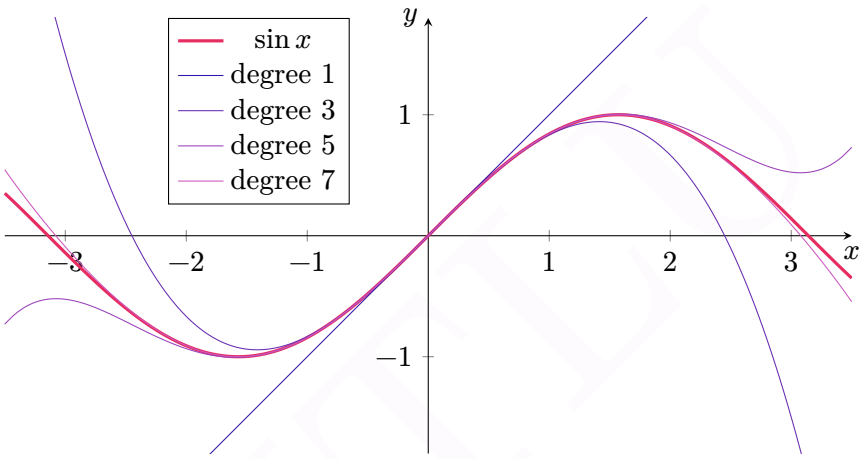


Figure 3.11: Taylor polynomials of degree n of $\sin(x)$ at $x = 0$ for $n \in \{1, 3, 5, 7\}$.

Example 3.3.17. In the previous example, we approximated a function f by a polynomial P such that P and f agree on a (that is $P(a) = f(a)$) and also the the i^{th} derivatives of P and f agree on a ($P^{(i)}(a) = f^{(i)}(a)$ for $1 \leq i \leq n$). This is a local approximation of the function f. Another way to approximate f is to find a polynomial G such that $f(x) = G(x)$ for many values of x. This is what we will do now, using Lagrange polynomials. Let us fix a sequence of pairwise distinct real numbers $(x_0, x_1, x_2, \dots)$ and define

$$\begin{aligned} Q_n : \mathcal{C}^\infty &\longrightarrow \mathbf{R}^{n+1} \\ f &\longmapsto [f(x_0), f(x_1), \dots, f(x_n)]^\mathsf{T}. \end{aligned}$$

For the other direction, we define R_n by its value on the standard basis vectors

$(e_1 = [1, 0 \dots, 0]^\mathsf{T}, \dots, e_{n+1} = [0, \dots, 0, 1]^\mathsf{T})$:

$$\begin{aligned} R_n(e_i) &:= \prod_{\substack{0 \le m \le n \\ m \neq i}} \frac{x - x_m}{x_i - x_m} \\ &= \frac{x - x_0}{x_i - x_0} \cdots \frac{x - x_{i-1}}{x_i - x_{i-1}} \frac{x - x_{i+1}}{x_i - x_{i+1}} \cdots \frac{x - x_n}{x_i - x_n}. \end{aligned}$$

The maps Q_n and R_n are linear and left/right inverses: $Q_n R_n = \mathrm{Id}_{\mathbf{R}^{n+1}}$ (exercise).

The polynomial $R_n(e_i)$ is known as the i^{th} *Lagrange polynomial*. This is the unique polynomial p of degree at most n such that $p(x_j) = 0$ if $j \neq i$ and $p(x_i) = 1$. This property directly implies that $(Q_n R_n)(e_i) = e_i$ and so $Q_n R_n = \mathrm{Id}_{\mathbf{R}^n}$. Therefore, $R_n Q_n \in \mathcal{L}(\mathcal{C}^\infty)$ is a projection to $\mathrm{Im}(R_n) = \mathcal{P}(\mathbf{R})_n$, which has dimension $n + 1$. In fact, $R_n Q_n(f)$ is a polynomial of degree at most n such that for $0 \le i \le n$ we have $(R_n Q_n(f))(x_i) = f(x_i)$. In this sense, the sequence of Lagrange polynomials forms another series of approximations of f.

See also Tutorial 5, Questions 5 and 6

This time, $\ker(R_n Q_n) = \ker(Q_n) = \{g \in \mathcal{C}^\infty \mid 0 = g(x_0) = \cdots = g(x_n)\}$.

4 Inner product spaces

Standing assumption

In this whole chapter, $\mathbf{F}$ will always be either $\mathbf{R}$ the field of real numbers or $\mathbf{C}$ the field of complex numbers. V will always denote a vector space over $\mathbf{F}$.

When going from $\mathbf{R}^2$ to abstract vector spaces, we generalised the notions of vector addition and of scalar multiplication. But they are some other features of $\mathbf{R}^2$ that we didn't capture. For example, in $\mathbf{R}^2$, one can talk about the length of a vector, or about the angle between two vectors. For a general vector space V, we do not have (yet) such notions as "length" or "angle". The aim of this chapter is to generalise the notion of length for real and complex vector spaces, and to generalise the notion of angle for real vector spaces.

4.1 Inner products and norms

Recall (from high school or MTH008) that for $x = \begin{bmatrix} x_1 \\ x_2 \end{bmatrix}$ and $y = \begin{bmatrix} y_1 \\ y_2 \end{bmatrix}$ two vectors in $\mathbf{R}^2$ we have the dot product $x \bullet y := x_1y_1 + x_2y_2 \in \mathbf{R}$. This is useful as the length of x is equal to $\sqrt{x_1^2 + x_2^2} = \sqrt{x \bullet x}$.

4.1.1 Dot product in $\mathbf{R}^m$

We first generalise scalar product to $\mathbf{R}^m$.

Definition 4.1.1.

Let $x = [x_1, \dots, x_m]^\mathsf{T}$ and $y = [y_1, \dots, y_m]^\mathsf{T}$ be two vectors in $\mathbf{R}^m$. We define their **dot product**[a] to be

$$x \bullet y := x_1y_1 + \cdots + x_my_m \in \mathbf{R}.$$

[a] The dot product is sometimes also called scalar product; which is not the same thing as the scalar multiplication!

Definition 4.1.2.

Let $x = [x_1, \dots, x_m]^\mathsf{T}$ be a vector in $\mathbf{R}^m$. We define its **norm** to be

$$\|x\| := \sqrt{x \bullet x} = \sqrt{x_1^2 + \cdots + x_m^2} \in \mathbf{R}.$$

The norm $\|x\|$ of x is a generalisation of the length of x in $\mathbf{R}$, $\mathbf{R}^2$ or $\mathbf{R}^3$. We may think of it as the distance between the point $(0, \dots, 0)$ and the point $(x_1, \dots, x_m)$.

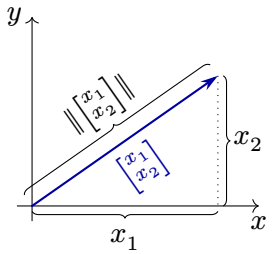


Figure 4.1: The norm of the vector $\begin{bmatrix} x_1 \\ x_2 \end{bmatrix} \in \mathbf{R}^2$ is $\left\| \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} \right\| = \sqrt{x_1^2 + x_2^2}$.

Proposition 4.1.3. *The dot product in $\mathbf{R}^m$ satisfies the following properties.*

1. *For all $x \in \mathbf{R}^m$ we have $x \bullet x \geq 0$;*
2. *For all $x \in \mathbf{R}^m$ we have $x \bullet x = 0 \iff x = 0$;*
3. *For any $y \in \mathbf{R}^m$, the map $\bullet\, y \colon \mathbf{R}^m \to \mathbf{R}$, $x \mapsto x \bullet y$ is linear;*
4. *For all $x, y \in \mathbf{R}^m$, we have $x \bullet y = y \bullet x$.*

Proof. 1. For $x = [x_1, \dots, x_m]^\mathsf{T} \in \mathbf{R}^m$, we have $x \bullet x = x_1^2 + \cdots + x_m^2 \geq 0$.
2. $x \bullet x = 0$ if and only if $x_1^2 + \cdots + x_m^2 = 0$, if and only if all the x_j are 0, if and only if $x = 0$.
3. Using the definition, one can easily check that $(x + x') \bullet y = x \bullet y + x' \bullet y$ and $(\lambda x) \bullet y = \lambda(x \bullet y)$ for $\lambda \in \mathbf{R}$.
4. This directly follows from the definition and the commutativity of addition in $\mathbf{R}$. □

The above proposition suggests how to generalise the dot product to other real vector spaces. Before doing that, we will turn our attention to complex vector spaces.

4.1.2 Dot product in $\mathbf{C}^m$

Can we simply mimic the dot product in $\mathbf{R}^m$ for $\mathbf{C}^m$? No! Indeed, if we use the same definition then we are going to have a problem for the length of i. Indeed, $\sqrt{\mathrm{i}^2} = \sqrt{-1}$ is not a real number, while we would like $\|z\|$ to be the "length of z" and hence a positive real number. In order to solve this problem we will need to use the complex conjugation.

Definition 4.1.4.

The **complex conjugate** of a complex number $a + b\mathrm{i}$ $(a, b \in \mathbf{R})$ is the number $\overline{a + b\mathrm{i}} := a - b\mathrm{i}$.

Complex conjugation satisfies the following properties, which can all be easily checked from the definition.

Lemma 4.1.5. *Let w and z be two complex numbers. Then we have*

1. $\overline{w+z} = \overline{w} + \overline{z}$;
2. $\overline{wz} = \overline{z} \cdot \overline{w}$;
3. $\overline{(\overline{w})} = w$;
4. *If $w \neq 0$, then* $\overline{\left(\frac{z}{w}\right)} = \frac{\overline{z}}{\overline{w}}$,
5. *For $z = a + b\mathrm{i}$ we have $z\overline{z} = a^2 + b^2 = |z|^2$ is the square of the modulus of z.*

Definition 4.1.6.

Let $z = [z_1, \dots, z_m]^\mathsf{T}$ and $w = [w_1, \dots, w_m]^\mathsf{T}$ be two vectors in $\mathbf{C}^m$. We define their **dot product** to be

$$z \bullet w := z_1\overline{w}_1 + \cdots + z_n\overline{w}_n.$$

Using complex conjugation, one can define a dot product on $\mathbf{C}^m$.

Definition 4.1.7.

Let $z = [z_1, \dots, z_m]^\mathsf{T}$ be a vector in $\mathbf{C}^m$. We define its **norm** to be

$$\|z\| := \sqrt{z \bullet z}.$$

If w_j is a real number, then $\overline{w_j} = w_j$, so the above definitions are indeed generalisations of the dot product and norm on $\mathbf{R}^m$.

Before going further, we prove one important property of the complex dot product.

Lemma 4.1.8. *For every $z \in \mathbf{C}^m$ the dot product $z \bullet z$ is a non-negative real number.*

Proof. For $w = a + b\mathrm{i} \in \mathbf{C}$ with a and b in $\mathbf{R}$, we have $\overline{w} = a - b\mathrm{i}$ and so $w\overline{w} = (a+b\mathrm{i})(a-b\mathrm{i}) = a^2+b^2 = |w|^2$ is in $\mathbf{R}_{\geq 0}$. So we have $z \bullet z = |z|_1{}^2 + \cdots + |z|_m{}^2 \in \mathbf{R}_{\geq 0}$. □

Corollary 4.1.9. *For every $z \in \mathbf{C}^m$ we have $\|z\| \in \mathbf{R}_{\geq 0}$.*

Complex dot product enjoys properties similar to the real dot product.

Proposition 4.1.10. *The dot product in $\mathbf{C}^m$ satisfies the following properties.*

1. *For all $z \in \mathbf{C}^m$ we have $z \bullet z \in \mathbf{R}_{\geq 0}$;*
2. *For all $z \in \mathbf{C}^m$ we have $z \bullet z = 0 \iff z = 0$;*
3. *Fix $w \in \mathbf{C}^m$. The map $\bullet w \colon \mathbf{C}^m \to \mathbf{C}$, $z \mapsto z \bullet w$ is linear;*
4. *For all $w, z \in \mathbf{C}^m$, we have $z \bullet w = \overline{w \bullet z}$.*

Proof. The proof is left to the reader as an exercise. Be careful that property 3 is about $\mathbf{C}$-linearity. □

4.1.3 Inner product spaces

We can use the dot products in $\mathbf{R}^m$ and $\mathbf{C}^m$ as inspiration to define a generalisation of "inner product" on abstract real or complex vector spaces.

Definition 4.1.11.

Let $\mathbf{F}$ be either $\mathbf{R}$ or $\mathbf{C}$ and let V be an $\mathbf{F}$-vector space. An **inner product** on V is a function

$$\begin{aligned} \langle \cdot\,, \cdot \rangle \colon V \times V &\longrightarrow \mathbf{F} \\ (u, v) &\longmapsto \langle u, v \rangle \end{aligned}$$

satisfying the following properties:

(1) $\langle v, v \rangle \in \mathbf{R}_{\geq 0}$ for all $v \in V$; (positivity)

(2) $\langle v, v \rangle = 0 \iff v = 0$; (definiteness)

(3) For all $u, v, w \in V$ and all $\lambda \in \mathbf{F}$ we have (linearity in 1st variable)[a]

$$\begin{aligned} \langle u + v, w \rangle &= \langle u, w \rangle + \langle v, w \rangle, \\ \langle \lambda v, w \rangle &= \lambda \langle v, w \rangle; \end{aligned}$$

(4) $\langle v, w \rangle = \overline{\langle w, v \rangle}$ for all $v, w \in V$. (conjugate symmetry)

[a] For us, an inner product is linear in the first variable. Some people prefer to define inner product to be linear in the second variable. Both definitions are fine, but once you have chosen one, you should stick with it.

Remark 4.1.12.

If V is an $\mathbf{R}$-vector space, then condition $\langle v, w \rangle = \overline{\langle w, v \rangle}$ is equivalent to $\langle v, w \rangle = \langle w, v \rangle$. Therefore, if $\langle \cdot\,, \cdot \rangle$ is an inner-product on a real vector space, it is also linear in the second variable. That is, for all $u, v, w \in V$ and all $\lambda \in \mathbf{R}$ we have

$$\begin{aligned} \langle u, v + w \rangle &= \langle u, v \rangle + \langle u, w \rangle, \\ \langle v, \lambda w \rangle &= \lambda \langle v, w \rangle. \end{aligned}$$

Since $\langle \cdot\,, \cdot \rangle$ is linear on both variable, it is says to be **bilinear**. For real vector spaces, we can replace Conditions (3) and (4) in the definition of inner product by the condition that $\langle \cdot\,, \cdot \rangle$ is bilinear.

Remark 4.1.13.

If $\langle \cdot, \cdot \rangle$ is an inner-product on a $\mathbf{C}$ vector space, then it is not linear in the second coordinate, but **semilinear**. That is, for all $u, v, w \in V$ and all $\lambda \in \mathbf{C}$ we have

$$\langle u, v + w \rangle = \langle u, v \rangle + \langle u, w \rangle,$$
$$\langle v, \lambda w \rangle = \overline{\lambda} \langle v, w \rangle.$$

In this case, we say that $\langle \cdot, \cdot \rangle$ is **sesquilinear**, which means 1.5-*linear*. For complex vector spaces, we can replace conditions (3) and (4) in the definition of inner product by the condition that $\langle \cdot, \cdot \rangle$ is sesquilinear.

The following result is an easy consequence of the definition.

Lemma 4.1.14. *Let $\langle \cdot, \cdot \rangle$ be an inner product on a vector space V. Then for every $v \in V$ we have*

$$\langle v, 0 \rangle = 0 = \langle 0, v \rangle.$$

Definition 4.1.15.

Let $\mathbf{F}$ be either $\mathbf{R}$ or $\mathbf{C}$. An **inner product space** over $\mathbf{F}$ is an $\mathbf{F}$ vector space equipped with an inner product $\langle \cdot, \cdot \rangle$.

We will often simply write V instead of $(V, \langle \cdot, \cdot \rangle)$ for an inner product space.

Example 4.1.16. $\mathbf{R}^m$ with the dot product is an inner product space over $\mathbf{R}$, sometimes called an **Euclidean space**. $\mathbf{C}^m$ with the dot product is an inner product space over $\mathbf{C}$.

Example 4.1.17. Let $c_1, \ldots, c_m > 0$ be positive real numbers. Define $\langle \cdot, \cdot \rangle \colon \mathbf{F}^m \times \mathbf{F}^m \to \mathbf{F}$ by

$$\langle (z_1, \ldots, z_m), (w_1, \ldots, w_m) \rangle := c_1 z_1 \overline{w}_1 + \cdots + c_m z_m \overline{w}_m.$$

Then $\langle \cdot, \cdot \rangle$ is an inner product.

Proof. We have $\langle z, z \rangle = c_1 |z_1|^2 + \cdots + c_m |z_m|^2$. This implies both that $\langle z, z \rangle$ is a positive real number and that $\langle z, z \rangle = 0 \iff z = 0$.

The other two defining properties of an inner product are easily checked. For linearity in 1st coordinate:

$$\begin{aligned} \langle \lambda z, w \rangle &= c_1 \lambda z_1 \overline{w}_1 + \cdots + c_m \lambda z_m \overline{w}_m \\ &= \lambda (c_1 z_1 \overline{w}_1 + \cdots + c_m z_m \overline{w}_m) = \lambda \langle z, w \rangle. \end{aligned}$$

For conjugate symmetry:

$$\begin{aligned} \overline{\langle w, z \rangle} &= \overline{c_1 w_1 \overline{z}_1 + \cdots + c_m w_m \overline{z}_m} \\ &= \overline{c}_1 z_1 \overline{w}_1 + \cdots + \overline{c}_m z_m \overline{w}_m \\ &= c_1 z_1 \overline{w}_1 + \cdots + \overline{c}_m z_m \overline{w}_m \\ &= \langle z, w \rangle, \end{aligned}$$

where we used both that $\overline{\overline{z}_j} = z_j$ and that $\overline{c}_j = c_j$ since the c_j are real numbers. □

Remark 4.1.18.

The above example shows that there can be more than one inner product structure on the same vector space.

Example 4.1.19. Let $\mathcal{C}^0([-1,1]) = \{f\colon [-1,1] \to \mathbf{R} \mid f \text{ is continuous}\}$ be the real vector space of continuous functions from $[-1,1]$ to $\mathbf{R}$. Define $\langle \cdot, \cdot \rangle : \mathcal{C}^0([-1,1]) \times \mathcal{C}^0([-1,1]) \to \mathbf{R}$ by

$$\langle f, g \rangle := \int_{-1}^{1} f(x)g(x)\,\mathrm{d}x.$$

Then $\langle \cdot, \cdot \rangle$ is an inner product.

Proof. If both f and g are continuous functions defined on $[-1,1]$, then $f \cdot g$ is also continuous and hence integrable. This implies that $\langle \cdot, \cdot \rangle$ is well-defined. Moreover,

$$\langle f, f \rangle = \int_{-1}^{1} f(x)f(x)\,\mathrm{d}x \geq 0.$$

This proves positivity.

It is clear that $\langle 0, 0 \rangle = 0$. Definiteness is a little more difficult to show and we will do it later.

Linearity of $\langle \cdot, \cdot \rangle$ is the well-known linearity of definite integral.

The definition is symmetric in 1st and 2nd variable: $\langle f, g \rangle = \langle g, f \rangle$ and we have conjugate symmetry since $\langle f, g \rangle$ is a real number.

In order to prove definiteness, we need to show that if $\int_{-1}^{1} (f(x))^2\,\mathrm{d}x = 0$, then $f = 0$. The proof of this claim requires analysis. We will actually show the converse, namely:

> *If $g\colon [-1,1]$ is a non-negative continuous function such that $g(x_0) \neq 0$ for some $x_0 \in [-1,1]$, then $\int_{-1}^{1} g(x)\,\mathrm{d}x \neq 0$.*

Let $\varepsilon := 1/2 \cdot g(x_0) > 0$. By continuity, there exists $\delta > 0$ such that if $|x - x_0| < \delta$, then $|g(x) - g(x_0)| < \varepsilon$. In particular, if x is in $[x_0 - \delta, x_0 + \delta]$, then $g(x) > \varepsilon$.

We conclude that

$$\begin{aligned}\int_{-1}^{1} g(x)\,\mathrm{d}x &= \int_{-1}^{x_0-\delta} g(x)\,\mathrm{d}x + \int_{x_0-\delta}^{x_0+\delta} g(x)\,\mathrm{d} + \int_{x_0+\delta}^{1} g(x)\,\mathrm{d}x \\ &\geq \int_{-1}^{x_0-\delta} g(x)\,\mathrm{d}x + 2\delta\varepsilon + \int_{x_0+\delta}^{1} g(x)\,\mathrm{d}x \geq 0 + 2\delta\varepsilon + 0 > 0.\end{aligned}$$

This proves the claim, and finishes the proof of definiteness. □

Exercise 4.1.20. Show that $\langle p, q \rangle := \int_0^\infty p(x)q(x)\mathrm{e}^{-x}\,\mathrm{d}x$ defines an inner product on $\mathcal{P}(\mathbf{R})$.

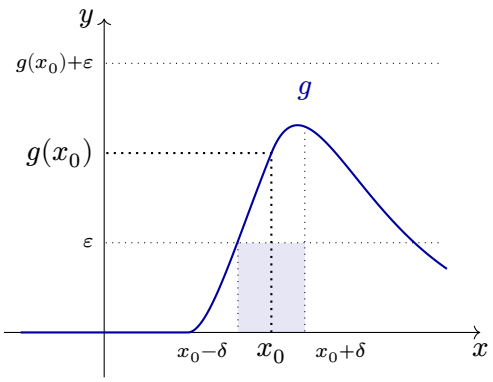


Figure 4.2: A non-zero positive continuous function. Its integral is at least the area of the blue rectangle: $\int_{x_0-\delta}^{x_0+\delta} g(x)\,\mathrm{d}x \geq 2\delta\varepsilon$.

Solution. The bilinearity of $\langle\,\cdot\,,\cdot\,\rangle$ directly follows from the linearity of the integral. We also have $\langle 0,0\rangle = 0$ and $\langle p,p\rangle = \int_0^\infty p(x)^2 \mathrm{e}^{-x}\,\mathrm{d}x \geq 0$ for every polynomial p.

It remains to prove that if $\langle p,p\rangle = 0$, then p is the zero polynomial. This follows from the fact that $g(x) = p(x)^2\mathrm{e}^{-x}$ is a non-negative continuous function, see Example 4.1.19. □

Definition 4.1.21.

Let $(V, \langle\,\cdot\,,\cdot\,\rangle)$ be an inner product space over $\mathbf{F}$. For a vector $v \in V$, we define its **norm** to be $\|v\| := \sqrt{\langle v,v\rangle}$.

If V is an inner product space, we can regard the norm as a function

$$\begin{aligned} \|v\| \colon V &\longrightarrow \mathbf{R}_{\geq 0} \\ v &\longmapsto \sqrt{\langle v,v\rangle}. \end{aligned}$$

Remark 4.1.22.

The norm depends on the choice of an inner product. Different inner products will give different norms.

Example 4.1.23. For the dot product on $\mathbf{F}^m$, the corresponding norm is the standard norm: $\|(z_1,\ldots,z_m)\| = \sqrt{z_1^2+\cdots+z_m^2}$.

Example 4.1.24. For $\mathcal{C}^0([-1,1])$ with inner product $\langle f,g\rangle = \int_{-1}^1 f(x)g(x)\,\mathrm{d}x$, the norm is $\|f\| = \sqrt{\int_{-1}^1 f^2(x)\,\mathrm{d}x}$.

The norm is not linear, but behaves well with respect to scalar multiplication.

Proposition 4.1.25. *Let V be an inner product space over $\mathbf{F}$ with norm $\|\,\cdot\,\|$. Then*

1. *For all $v \in V$, we have $\|v\| = 0$ if and only if $v = 0$;*
2. *For all $v \in V$ and all $\lambda \in \mathbf{F}$ we have $\|\lambda v\| = |\lambda| \cdot \|v\|$, where $|\lambda| \in \mathbf{R}_{\geq 0}$ is the modulus (absolute value if $\mathbf{F} = \mathbf{R}$) of λ.*

Proof. For the first statement, $\|v\| = 0 \iff \langle v, v\rangle = 0 \iff v = 0$.

For the second statement,

$$\begin{aligned}\|\lambda v\| &= \sqrt{\langle \lambda v, \lambda v\rangle} = \sqrt{\lambda\overline{\lambda}\langle v, v\rangle} \\ &= \sqrt{|\lambda|^2\langle v, v\rangle} = |\lambda| \cdot \|v\|.\end{aligned}$$

□

In practice, it is often easier to compute $\|v\|^2 = \langle v, v\rangle$. If you do that, don't forget to take the square-root after computing $\|v\|^2$.

4.2 Orthogonality and its consequences

Now that we have generalised the notion of length, we would like to generalise the notion of angle. In general, this is not possible, but one can at least generalise the notion of perpendicularity. Recall that in $\mathbf{R}^2$ if θ is the angle between two vectors u and v we have

$$u \bullet v = \|u\|\|v\| \cos(\theta). \tag{4.1}$$

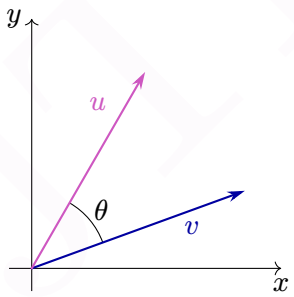


Figure 4.3: An angle between two vectors in $\mathbf{R}^2$. The angle satisfies the relation $u \bullet v = \|u\|\|v\| \cos(\theta)$.

We conclude that u and v are perpendicular if and only if $\langle u, v\rangle = 0$. One will use this notion to generalise perpendicularity. In fact, we will see later that Equation (4.1) can also be used to generalise the notion of angles for real inner product spaces.

4.2.1 Orthogonality

The following fundamental definition is inspired by Equation (4.1).

Definition 4.2.1.

Let $(V, \langle \cdot, \cdot \rangle)$ be an inner product space. Two vectors u and v in V are **orthogonal**, written $u \perp v$, if $\langle u, v \rangle = 0$.

Observe that $u \perp v$ if and only if $v \perp u$.

Remark 4.2.2.

The notion of orthogonality depends on the inner product we have chosen!

Example 4.2.3. Let $V = \mathbf{R}^2$ and let $u = \begin{bmatrix} 1 \\ 1 \end{bmatrix}$ and $v = \begin{bmatrix} 1 \\ -1 \end{bmatrix}$. We have $u \bullet v = 0$ so u and v are orthogonal for the dot product. However, $\left\langle \begin{bmatrix} x_1 \\ x_2 \end{bmatrix}, \begin{bmatrix} y_1 \\ y_2 \end{bmatrix} \right\rangle := 4x_1x_2 + y_1y_2$ is also an inner product on V. For this inner product, we have $\langle u, v \rangle = 4 - 1 = 3 \neq 0$ so u and v are not orthogonal for $\langle \cdot, \cdot \rangle$.

Orthogonality possesses interesting properties, notably in relation to the 0 vector.

Lemma 4.2.4 (Orthogonality and 0_V)**.** *Let V be an inner product space. Then*

1. *0_V is orthogonal to every vector $v \in V$;*
2. *A vector $v \in V$ is orthogonal to itself if and only if $v = 0_V$.*

Proof. 1 This follows from $\langle 0_V, v \rangle = 0_v$.
2 If v is orthogonal to itself, then $0_V = \langle v, v \rangle$ which implies $v = 0_V$. □

If a vector v is orthogonal to some vectors u_j, then it is orthogonal to all linear combinations of the u_j.

Lemma 4.2.5. *Let V be an inner product space. Suppose that we have vectors v and $(u_1, \ldots, u_k)$ such that $v \perp u_j$ for all $j \int \{1, \ldots, k\}$. Then $v \perp u$ for any $u \in \operatorname{span}(u_1, \ldots, u_k)$.*

Proof. We have $u = \lambda_1 u_1 + \cdots + \lambda_k u_k$ for some k. By linearity, we obtain $\langle u, v \rangle = \sum_{j=1}^{k} \lambda_j \langle u_j, v \rangle = 0$. □

We now recover a classical theorem from Euclidean geometry that holds in any inner product space.

Theorem 4.2.6 (Pythagorean[1] Theorem)**.**

Suppose u and v are two orthogonal vectors in an inner product space. Then

$$\|u + v\|^2 = \|u\|^2 + \|v\|^2.$$

[1] Pythagoras of Samos (Πυθαγόρας) (c. 570–c. 495 BC).

Proof. We have

$$\begin{aligned}\|u+v\|^2 &= \langle u+v, u+v\rangle = \langle u,u\rangle + \langle u,v\rangle + \langle v,u\rangle + \langle v,v\rangle \\ &= \|u\|^2 + 0 + 0 + \|v\|^2 = \|u\|^2 + \|v\|^2.\end{aligned}$$

□

Corollary 4.2.7. *Let $k \geq 1$. Suppose $u_1, \dots, u_k$ are pairwise orthogonal vectors in an inner product space: $u_i \perp u_j$ for all $i \neq j \in \{1, \dots, k\}$. Then*

$$\|u_1 + \cdots + u_k\|^2 = \|u_1\|^2 + \cdots + \|u_k\|^2.$$

Proof. If $k = 1$ this is trivial. The case $k = 2$ is the Pythagorean Theorem. Now suppose $k \geq 3$ and that the statement is true for $k-1$. Then u_k is orthogonal to $u_1 + \cdots + u_{k-1}$. The pythagorean Theorem applied to $u = u_1 + \cdots + u_{k-1}$ and $v = u_k$ gives

$$\|u_1 + \cdots + u_k\|^2 = \|u_1 + \cdots + u_{k-1}\|^2 + \|u_k\|^2 = \|u_1\|^2 + \cdots + \|u_k\|^2.$$

□

If $\mathbf{F} = \mathbf{R}$, then the converse of the Pythagorean Theorem also holds:

Proposition 4.2.8. *Let V be an inner product space over $\mathbf{R}$ and let u and v be two vectors. Then u and v are orthogonal if and only if $\|u+v\|^2 = \|u\|^2 + \|v\|^2$.*

Proof. The proof is left as an exercise. □

Tutorial 8, Question 3

Remark 4.2.9.

Observe that the proof of Proposition 4.2.8 does not work for inner product spaces over $\mathbf{C}$. Indeed, in this case we have $\|u+v\|^2 = \|u\|^2 + \langle u,v\rangle + \overline{\langle u,v\rangle} + \|v\|^2$. But in general, $\langle u,v\rangle + \overline{\langle u,v\rangle} \neq 2\langle u,v\rangle$.

Actually, Proposition 4.2.8 is false for all complex inner product spaces.

Lemma 4.2.10. *Let $V \neq \{0\}$ be a complex inner product space. Then for any $v \neq 0$ and $u = \mathrm{i}v$ we have $\|u+v\|^2 = \|u\|^2 + \|v\|^2$ but $\langle u,v\rangle \neq 0$.*

Proof. The proof is left as an exercise. □

Tutorial 8, Question 3

We have defined orthogonality for vectors. We can also define it for subspaces, and even for subsets.

Definition 4.2.11.

Let V be an inner product space and let X and Y be two subsets of V. We say that X and Y are **orthogonal**, written $X \perp Y$, if for all $x \in X$ and $y \in Y$ we have $\langle x,y\rangle = 0$.

We know that in general, direct sum complements are not unique. However, in an inner product space any subspace U admits a unique "nice complement". Let us first define what it means to be a nice complement and then show its unicity when U is of dimension 1.

Definition 4.2.12.

Let V be an inner product space. For a subset $U \subseteq V$ we define its **orthogonal complement** to be

$$U^{\perp} := \{v \in V \mid \forall u \in U, \langle u, v\rangle = 0\}.$$

That is, $U^{\perp}$ is the set of vectors that are orthogonal to all vectors of U.

One can easily show that $U^{\perp}$ is always subspace (see the forthecoming Proposition 4.3.15 for a proof).

Lemma 4.2.13. *Let V be an inner product space and u be any non-zero vector. Then, for any $v \in V$ there exists a unique decomposition $v = \lambda u + w$ with $\lambda \in \mathbf{F}$ and such w orthogonal to u. In fact, we have*

$$v = \frac{\langle v, u\rangle}{\|u\|^2} u + w.$$

Proof. The idea is to first find the *orthogonal projection* of v onto $\operatorname{span}(u)$. This will both give λ and $w = v - \lambda u$. See Figure 4.4.

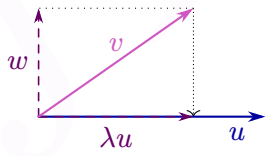


Figure 4.4: An orthogonal decomposition of v with respect to u.

Let $w := v - \lambda u$ for some $\lambda \in \mathbf{F}$ to be determined. We want w to be orthogonal to u, that is $\langle w, u\rangle = 0$. So let us compute:

$$0 = \langle w, u\rangle = \langle v - \lambda u, u\rangle = \langle v, u\rangle - \lambda\langle u, u\rangle.$$

So w and u are orthogonal if and only if $\lambda = \frac{\langle v,u\rangle}{\|u\|^2}$. This proves both the existence and the unicity. □

Here is a rewriting of the previous lemma in terms of direct sum complements.

Proposition 4.2.14. *Let V be an inner product space and U be a one dimensional subspace. Then $V = U \oplus U^\perp$.*

Moreover, $U^\perp$ is the unique orthogonal complement. That is, if $V = U \oplus W$ with $U \perp W$, then $W = U^\perp$.

Proof. Since U is one dimensional, we have $U = \operatorname{span}(u)$ for every non-zero vector $u \in U$. Let us fix such a vector u. By Lemma 4.2.13, any vector $v \in V$ admits a unique decomposition of the form $v = \lambda u + w$ for $\lambda \in \mathbf{F}$ and $w \in U^\perp$. Since $U = \operatorname{span}(u)$, this is equivalent to the uniqueness of the decomposition $v = u' + w$ for $u' \in U$ and $w \in W$. The unicity of this last decomposition is exactly the fact that $V = U \oplus U^\perp$.

Finally, let W be another orthogonal complement of U. By definition of $U^\perp$, we must have $W \subseteq U^\perp$. For the other inclusion, let v be any element of U. Then we have at the same time $v = 0 + x \in V = U \oplus U^\perp$ and $v = u + w \in V = U \oplus W$. Since w is in $W \subseteq U^\perp$ we conclude that $x - w = u$ is in $U \cap U^\perp$ and thus $v = 0 + x = w$ is in W as desired. □

4.2.2 Cauchy–Schwarz inequality

Cauchy–Schwarz[2] inequalities exist for sums, series, integrals, ... They are really useful both in algebra and in analysis. All these inequalities follow from a general inequality for inner product spaces, which we now prove.

Theorem 4.2.15 (Cauchy–Schwarz inequality)**.**

Let V be an inner product space. Then for all u and v in V we have

$$|\langle u, v\rangle| \leq \|u\| \cdot \|v\|. \tag{4.2}$$

Moreover, we have $|\langle u, v\rangle| = \|u\| \cdot \|v\|$ if and only if u and v are linearly dependent.

Proof. If $u = 0_V$, then u and v are linearly dependent and Equation (4.2) is $0 = 0 \cdot \|v\|$.

Let us now suppose that $u \neq 0_V$ and consider the decomposition $v = \frac{\langle v,u\rangle}{\|u\|^2} u + w$ where w is given by Lemma 4.2.13 and orthogonal to u. By the Pythagorean Theorem (Theorem 4.2.6)

$$\|v\|^2 = \left\| \frac{\langle v, u\rangle}{\|u\|^2} u \right\|^2 + \|w\|^2 = \left| \frac{\langle v, u\rangle}{\|u\|^2} \right|^2 \|u\|^2 + \|w\|^2 \geq \frac{|\langle v, u\rangle^2|}{\|u\|^2}.$$

That is $|\langle u, v\rangle|^2 = |\langle v, u\rangle^2| \leq \|v\|^2 \|u\|^2$.

Finally, we have equality in (4.2) if and only if $\|w\|^2 = 0$, if and only if $w = 0$. But w is zero if and only if u and v are linearly dependent. □

Some special cases of the Cauchy–Schwarz inequality may be familiar to you. Observe that in application, we usually use the squared version of the inequality: $|\langle u, v\rangle|^2 \leq \|u\|^2 \|v\|^2$.

[2] Augustin-Louis Cauchy (1789–1857) and Karl Hermann Amandus Schwarz (1843–1921).

Example 4.2.16. Let $V = \mathbf{R}^m$ be the Euclidean space with standard dot product. The Cauchy–Schwarz inequality applied to $(x_1, \dots, x_m)$ and $(y_1, \dots, y_m)$ gives

$$\Big|\sum_{j=1}^{m} x_j y_j\Big|^2 \leq \Big(\sum_{j=1}^{m} x_j^2\Big)\Big(\sum_{j=1}^{m} y_j^2\Big).$$

Example 4.2.17. Let $V = \mathcal{C}^0([-1,1])$ be the space of continuous functions from $[-1,1]$ to $\mathbf{R}$ with inner product $\langle f, g\rangle = \int_{-1}^{1} f(x)g(x)\,\mathrm{d}x$. Then for f and g in $V = \mathcal{C}^0([-1,1])$ the Cauchy–Schwarz inequality is

$$\Big(\int_{-1}^{1} f(x)g(x)\,\mathrm{d}x\Big)^2 \leq \Big(\int_{-1}^{1} f(x)^2\,\mathrm{d}x\Big)\Big(\int_{-1}^{1} g(x)^2\,\mathrm{d}x\Big).$$

It is an interesting exercise to try to give an analytic proof of this inequality.

4.2.3 Angles in inner product spaces over $\mathbf{R}$

When $\mathbf{F} = \mathbf{R}$ we can define angles using the Cauchy–Schwarz inequality and Equation (4.1). Let V be an inner product space over $\mathbf{R}$. By the Cauchy–Schwarz inequality, for non-zero u and v in V we have

$$-1 \leq \frac{\langle u, v\rangle}{\|u\|\|v\|} \leq 1.$$

Definition 4.2.18.

Let V be an inner product space over $\mathbf{R}$ and let u and v be two non-zero vectors. We define the **angle between u and v** by

$$\angle(u, v) := \arccos \frac{\langle u, v\rangle}{\|u\|\|v\|} \in [0, \pi].$$

If one of u or v is 0_V, we say that the angle between u and v is arbitrary.

Using this definition of angles, we have that u and v are orthogonal if and only if $\langle u, v\rangle = 0$, if and only if $\angle(u, v) = \frac{\pi}{2}$.

Remark 4.2.19.

If $\mathbf{F} = \mathbf{C}$, the above definition does not make sense! Indeed, in this case $\langle u, v\rangle$ can be a non-real complex number.

4.2.4 Classical geometry results in inner product spaces

Using the notion of norm and orthogonality, it is possible to recover some of the classical geometry results in a more general context.

Theorem 4.2.20 (Triangle inequality)**.**

Let V be an inner product space. Then for any u and v in V we have

$$\big|\|u\| - \|v\|\big| \leq \|u+v\| \leq \|u\| + \|v\|.$$

Moreover, we have

- $\|u+v\| = \|u\| + \|v\|$ *if and only if there exists* $\lambda \in \mathbf{R}_{\geq 0}$ *such that* $u = \lambda v$ *or* $v = \lambda u$*;*
- $|\|u\| - \|v\|| = \|u+v\|$ *if and only if there exists* $\mu \in \mathbf{R}_{\leq 0}$ *such that* $u = \mu v$ *or* $v = \mu u$*.*

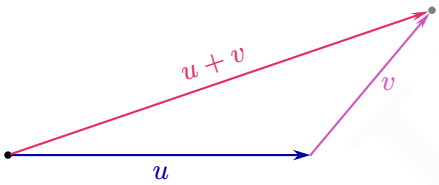


Figure 4.5: The shortest path between the black dot and the graydot is given by the vector $u+v$.

Proof. We have

$$\begin{aligned}\|u+v\|^2 &= \langle u+v, u+v\rangle \\ &= \langle u,u\rangle + \langle v,v\rangle + \langle u,v\rangle + \overline{\langle u,v\rangle} \\ &= \|u\|^2 + \|v\|^2 + 2\,\mathrm{Re}\langle u,v\rangle.\end{aligned}$$

Recall that for any complex number z we have $-|z| \leq \mathrm{Re}\, z \leq |z|$. Applying this to $z = \langle u,v\rangle$ and plugging it in the above equality, we obtain

$$\|u\|^2 + \|v\|^2 - 2|\langle u,v\rangle| \leq \|u+v\|^2 \leq \|u\|^2 + \|v\|^2 + 2|\langle u,v\rangle|.$$

Using the Cauchy–Schwarz inequality $|\langle u,v\rangle| \leq \|u\| \cdot \|v\|$, we obtain

$$\|u\|^2 + \|v\|^2 - 2\|u\| \cdot \|v\| \leq \|u+v\|^2 \leq \|u\|^2 + \|v\|^2 + 2\|u\| \cdot \|v\|.$$

This is equivalent to

$$(\|u\| - \|v\|)^2 \leq \|u+v\|^2 \leq (\|u\| + \|v\|)^2,$$

or in other words

$$\big|\|u\| - \|v\|\big| \leq \|u+v\| \leq \|u\| + \|v\|.$$

Now, the right inequality is an equality if and only if $\mathrm{Re}\langle u,v\rangle = |\langle u,v\rangle| = \|u\|\|v\|$, if and only if $\langle u,v\rangle = \|u\|\|v\|$. Indeed, $\mathrm{Re}\langle u,v\rangle = |\langle u,v\rangle|$ is equivalent to $|\langle u,v\rangle| = \langle u,v\rangle$

(that is: $\langle u, v\rangle$ being a non-negative real number). Finally, $\langle u, v\rangle = \|u\|\|v\|$ if and only if there exists $\lambda \in \mathbf{R}_{\geq 0}$ such that $u = \lambda v$ or $v = \lambda u$.

The proof for the left equality is similar. □

Figure 4.5 explains the name *triangle inequality*. This inequality is really important as it shows that $\|u - v\|$ is a **distance**.[3] Meaning that:

1. $\forall u, v : \|u - v\| \in \mathbf{R}_{\geq 0}$ (the distance is always a positive number);
2. $\forall u : \|u - u\| = 0$ (if you don't move, the distance is 0);
3. If $u \neq v$, then $\|u - v\| > 0$ (if you move, the distance is positive);
4. $\forall u, v : \|u - v\| = \|v - u\|$ (the distance from u to v is the same as the distance from v to u);
5. $\forall u, v, w : \|u - v\| \leq \|u - w\| + \|w - u\|$ (if on the way between u to v we go through w, this cannot shorten the distance).

We now recover another result from classical geometry.

Theorem 4.2.21 (Parallelogram equality)**.**

Let V be an inner product space. Then for any u and v in V we have

$$\|u + v\|^2 + \|u - v\|^2 = 2(\|u\|^2 + \|v\|^2).$$

Proof. The proof is just direct computations.

$$\begin{aligned}\|u + v\|^2 + \|u - v\|^2 &= \langle u + v, u + v\rangle + \langle u - v, u - v\rangle \\ &= \langle u, u\rangle + \langle u, v\rangle + \langle v, u\rangle + \langle v, v\rangle \\ &\quad + \langle u, u\rangle - \langle u, v\rangle - \langle v, u\rangle + \langle v, v\rangle \\ &= 2\langle u, u\rangle + 2\langle v, v\rangle \\ &= 2(\|u\|^2 + \|v\|^2).\end{aligned}$$

□

Figure 4.6 is here to explain the name of the above theorem. Observe that the equality $\|u + v\|^2 + \|u - v\|^2 = 2(\|u\|^2 + \|v\|^2)$ means that in a parallelogram the sum of the square of the diagonal lengths is equal to the sum of the square of the side lengths.

Corollary 4.2.22 (Appolonius's identity)**.** *Let ABC be a triangle in $\mathbf{F}^m$, and let D be the midpoint of AB. Then*

$$\|BC\|^2 + \|AC\|^2 = \frac{1}{2}\|AB\|^2 + 2\|CD\|^2.$$

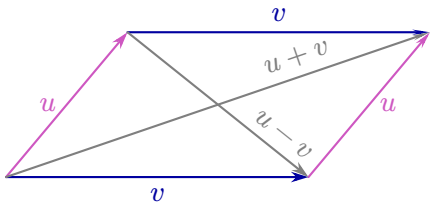


Figure 4.6: A parallelogram and its two diagonals.

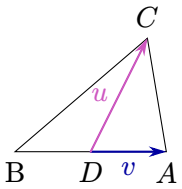


Figure 4.7: A triangle ABC, where D is the midpoint of AB.

Proof. Let $u := \overrightarrow{DC}$ and $v := \overrightarrow{DA}$. Then $\overrightarrow{AC} = u - v$, $\overrightarrow{DB} = -v$ and $\overrightarrow{BC} = v + u$. See Figure 4.7.

By the parallelogram equality

$$\|\overrightarrow{BC}\|^2 + \|\overrightarrow{AC}\|^2 = 2\left(\left\|\frac{1}{2}\overrightarrow{AB}\right\|^2 + \|\overrightarrow{CD}\|^2\right) = \frac{1}{2}\|\overrightarrow{AB}\|^2 + 2\|\overrightarrow{CD}\|^2.$$

□

4.3 Orthonormal bases

In this section we will use inner product and orthogonality to define nice bases with specifically good properties.

4.3.1 Orthonormality

We start with a definition.

Definition 4.3.1.

Let V be an inner product space over $\mathbf{F}$. A list of vectors $(v_1, \dots, v_m)$ is **orthogonal** if its elements are pairwise orthogonal. That is, if for all $j, k \in \{1, \dots, m\}$ with $j \neq k$ the vectors v_j and v_k orthogonal.
The list $(v_1, \dots, v_m)$ is **orthonormal** if it is orthogonal and all the vectors have norm 1.

[3]You will learn more about distances in MTH224 - Metric spaces.

Infinite dimensional vector spaces

It is possible to define orthogonality and orthonormality in a similar way for an infinite family $(v_\alpha)_{\alpha\in I}$.

Observe that a list of vectors $(v_1, \dots, v_m)$ is orthonormal if and only if[4]

$$\langle v_j, v_k\rangle = \delta_{j,k} := \begin{cases} 1 & \text{if } j = k, \\ 0 & \text{if } j \neq k. \end{cases}$$

Observe that the notion of orthogonal and orthonormal list depends on the choice of an inner product!

We already have encountered examples of orthonormal lists.

Example 4.3.2. The standard basis of $\mathbf{F}^m$ is orthonormal for the dot product.

But other examples exist as well.

Example 4.3.3. The list $\left(u = \begin{bmatrix} 1/\sqrt{3} \\ 1/\sqrt{3} \\ 1/\sqrt{3} \end{bmatrix}, v = \begin{bmatrix} -1/\sqrt{2} \\ 1/\sqrt{2} \\ 0 \end{bmatrix}\right)$ in $\mathbf{F}^3$ is orthonormal for the dot product.

Indeed, we have

$$u \bullet u = \tfrac{1}{3} + \tfrac{1}{3} + \tfrac{1}{3} = 1, \qquad v \bullet v = \tfrac{1}{2} + \tfrac{1}{2} + 0 = 1, \qquad u \bullet v = \tfrac{-1}{\sqrt{6}} + \tfrac{1}{\sqrt{6}} + 0 = 0.$$

Proposition 4.3.4. *Let V be an inner product space and let $(v_1, \dots, v_k)$ be an orthonormal list of vectors. Then for every $\lambda_1, \dots, \lambda_k \in \mathbf{F}$ we have*

$$\|\lambda_1 v_1 + \cdots + \lambda_k v_k\|^2 = |\lambda_1|^2 + \cdots + |\lambda_k|^2.$$

Proof. This is a direct application of the Pythagorean Theorem (Theorem 4.2.6):

$$\begin{aligned} \|\lambda_1 v_1 + \cdots + \lambda_k v_k\|^2 &= \|\lambda_1 v_1\|^2 + \cdots + \|\lambda_k v_k\|^2 \\ &= |\lambda_1|^2\|v_1\|^2 + \cdots + |\lambda_k|^2\|v_k\|^2 \\ &= |\lambda_1|^2 + \cdots + |\lambda_k|^2. \end{aligned}$$

□

Corollary 4.3.5. *An orthonormal list $(v_1, \dots, v_k)$ is linearly independent.*

Proof. Let $(v_1, \dots, v_k)$ be an orthonormal list. Then , if $\lambda_1 v_1 + \cdots + \lambda_k v_k = 0$, the previous proposition tells us that $0 = |\lambda_1|^2 + \cdots + |\lambda_k|^2$ and therefore all the λ_j are 0. □

[4] $\delta_{j,k}$ is called the **Kronecker delta** from Leopold Kronecker (1823–1891).

Infinite dimensional vector spaces

Corollary 4.3.5 is true even for infinite families. In fact, we have that any *orthogonal* family (finite or infinite) of non-zero vectors is linearly independent! Can you prove it for finite lists?

It is natural to ask which orthonormal lists are also spanning. Since an orthonormal lists is linearly independent, it is spanning if and only if it is a basis.

Definition 4.3.6.

Let V be an inner product space over $\mathbf{F}$. A list of vectors $(e_1, \dots, e_m)$ is an **orthonormal basis** if it is both an orthonormal list and a basis.

Infinite dimensional vector spaces

Similarly, one say that an infinite family $(e_\alpha)_{\alpha \in I}$ is an orthonormal basis if it is both an orthonormal family and a basis.

It follows from Example 4.3.2 that the standard basis of $\mathbf{F}^m$ is an orthonormal basis, but it is not the only one.

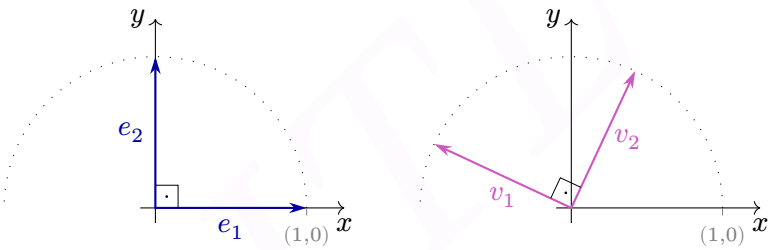


Figure 4.8: Two orthonormal bases of $\mathbf{R}^2$.

Proposition 4.3.7. *If V is finite dimensional, then any orthonormal list with of length $\dim(V)$ is an orthonormal basis.*

Proof. Any orthonormal list is linearly independent. But any linearly independent list of length $\dim(V)$ is a basis by Corollary 2.4.44. □

Example 4.3.8. The vectors $u_1 = [1/2, 1/2, 1/2, 1/2]^\mathsf{T}$, $u_2 = [1/2, 1/2, -1/2, -1/2]^\mathsf{T}$, $u_3 = [1/2, -1/2, -1/2, 1/2]^\mathsf{T}$ and $u_4 = [-1/2, 1/2, -1/2, 1/2]^\mathsf{T}$ form an orthonormal basis of $\mathbf{F}^4$.

Since $\dim(\mathbf{F}^4) = 4$, it is enough to check that the family is orthonormal. It is easy to show that $\|u_j\| = 4 \cdot 1/4 = 1$ for $1 \leq j \leq 4$. The fact that $u_j \bullet u_k = 0$ if $j \neq k$ is left as an exercice.

The main advantage of orthonormal bases is the following result.

Theorem 4.3.9 (Orthonormal decomposition)**.**

Let V be a finite dimensional inner product space and let $(e_1, \dots, e_m)$ be an orthonormal basis. Then for any vector $v \in V$ we have

1. $v = \langle v, e_1\rangle e_1 + \cdots + \langle v, e_m\rangle e_m$;
2. $\|v\|^2 = |\langle v, e_1\rangle|^2 + \cdots + |\langle v, e_m\rangle|^2$;
3. $\langle u, v\rangle = \langle u, e_1\rangle\overline{\langle v, e_1\rangle} + \cdots + \langle u, e_m\rangle\overline{\langle v, e_m\rangle}$ *for every* $u \in V$.

Proof. 1. Since $(e_1, \dots, e_m)$ is a basis, there exists $\lambda_j \in \mathbf{F}$ such that $v = \lambda_1 e_1 + \cdots + \lambda_m e_m$. Then for $1 \leq j \leq m$ we have

$$\begin{aligned}\langle v, e_j\rangle &= \langle \lambda_1 e_1 + \cdots + \lambda_m e_m, e_j\rangle \\ &= \lambda_1\langle e_1, e_j\rangle + \cdots + \lambda_m\langle e_m, e_j\rangle \\ &= \lambda_m 1 = \lambda_m.\end{aligned}$$

2. The formula for $\|v\|^2$ follows by using the Pythagorean Theorem (Theorem 4.2.6) on 1 and the fact that $\|\langle v, e_j\rangle e_j\| = |\langle v, e_j\rangle|\|e_j\| = |\langle v, e_j\rangle|$.

3. This follows from taking the inner product $\langle u, \cdot\,\rangle$ on both sides of 1 and using the conjugate symmetry $\langle e_j, v\rangle = \overline{\langle v, e_j\rangle}$. □

Observe that $\langle v, e_1\rangle e_1$ is nothing else than the projection of v onto $\operatorname{span}(e_1)$ along direction $\operatorname{span}(e_1)^\perp = \{w \in V \mid \langle w, e_1\rangle = 0\}$. We will make this explicit in the next subsection.

Infinite dimensional vector spaces

Theorem 4.3.9 is also true for infinite dimensional spaces. The trick is that if $(e_\alpha)_{\alpha\in I}$ is an infinite orthonormal basis, then for a given v the inner product $\langle v, e_\alpha\rangle$ is non-zero only for finitely many α.

Theorem 4.3.9.1 is particularly useful for the matrix representation of a vector.

Corollary 4.3.10. *Let V be a finite dimensional inner product space and let $\mathscr{E} = (e_1, \dots, e_m)$ be an orthonormal basis. Then for any vector $v \in V$ we have*

$$[v]_{\mathscr{E}} = \begin{bmatrix}\langle v, e_1\rangle \\ \vdots \\ \langle v, e_m\rangle\end{bmatrix}.$$

Let us end this subsection with the following announcement.

Theorem 4.3.11.

Let V be a finite dimensional inner product space. Then V admits an orthonormal basis.

We will prove this result later in Subsection 4.3.3 (it follows from Theorem 4.3.30), but we still state it as it is a good motivation for what is coming next.

Remark 4.3.12.

Theorem 4.3.11 is not true in general for infinite dimensional inner product spaces. That is, infinite dimensional inner product spaces might not have orthonormal basis. See Example 4.3.19 for a counter-example.

4.3.2 Orthogonal projections

In Proposition 4.2.14 we saw that if U is a 1 dimensional subspace of V, then it has a unique *orthogonal complement*. Our aim is now to generalise Proposition 4.2.14 to subspaces of dimension bigger than 1.

Recall that for a subset $U \subseteq V$ its orthogonal complement is the subset $U^\perp = \{v \in V \mid \forall u \in U, \langle u, v\rangle = 0\}$ of vectors of V that are orthogonal to all vectors of U.

Example 4.3.13. Let $V = \mathbf{R}^2$ and $U_1 = \left\{\begin{bmatrix}1\\2\end{bmatrix}\right\}$. Then $U_1^\perp = \left\{\begin{bmatrix}x\\y\end{bmatrix} \in \mathbf{R}^2 \mid x + 2y = 0\right\}$; see Figure 4.9.

For $U_2 = \left\{\begin{bmatrix}t\\t\end{bmatrix} \,\middle|\, t \in \mathbf{R}\right\}$ we have

$$U_2^\perp = \left\{\begin{bmatrix}x\\y\end{bmatrix} \in \mathbf{R}^2 \,\middle|\, \forall t \in \mathbf{R}, tx + ty = 0\right\} = \left\{\begin{bmatrix}-x\\x\end{bmatrix} \in \mathbf{R}^2 \,\middle|\, x \in \mathbf{R}\right\}.$$

For $U_3 = \left\{\begin{bmatrix}t\\1\end{bmatrix} \in \mathbf{R}^2 \,\middle|\, t \in \mathbf{R}\right\}$ we have $U_3 = \left\{\begin{bmatrix}x\\y\end{bmatrix} \in \mathbf{R}^2 \mid \forall t \in \mathbf{R}, tx + y = 0\right\} = \left\{\begin{bmatrix}0\\0\end{bmatrix}\right\}$.

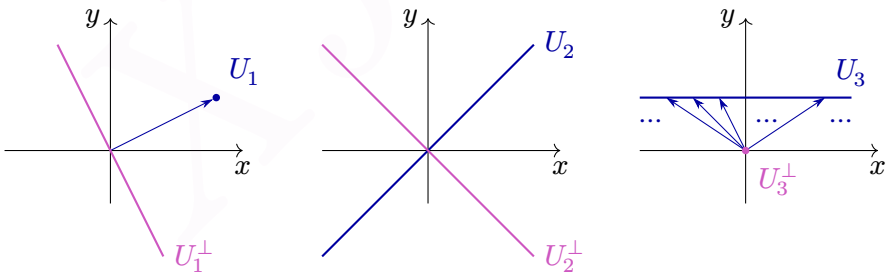


Figure 4.9: Orthogonal complements in $\mathbf{R}^2$.

Example 4.3.14. Let $V = \mathbf{R}^3$ and $U_4 = \{[x, y, 0]^\mathsf{T} \mid x, y \in \mathbf{R}\}$. Then $U_4^\perp = \{[0, 0, z]^\mathsf{T} \mid z \in \mathbf{R}\}$; see Figure 4.10.

For $U_5 = \{[0, y, 0]^\mathsf{T} \mid y \in \mathbf{R}\}$ we have $U_5^\perp = \{[x, 0, z]^\mathsf{T} \mid x, z \in \mathbf{R}\}$.

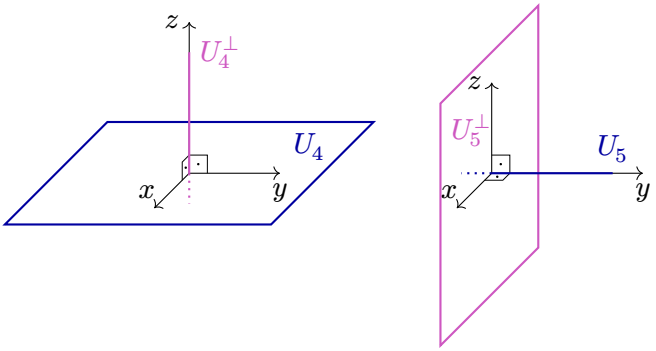


Figure 4.10: Orthogonal complements in $\mathbf{R}^3$.

One of the advantage of orthogonal complements is that they automatically are subspaces. In fact, we have

Proposition 4.3.15. *Let V be an inner product space. Then for any* subsets *U and W of V the following hold*

1. *$U^\perp$ is a subspace of V;*
2. *$\{0\}^\perp = V$ and $V^\perp = \{0\}$;*
3. *$U \cap U^\perp \subseteq \{0\}$, with equality if and only if U contains 0;*
4. *$U \subseteq (U^\perp)^\perp$;*
5. *If $U \subseteq W$, then $W^\perp \subseteq U^\perp$.*

Proof. "1" Firstly, since 0 is orthogonal to every vector in V, it belongs to $U^\perp$. Now, let v_1 and v_2 be two vectors in $U^\perp$ and let $\lambda \in \mathbf{F}$ be a scalar. For all $u \in U$ we have $\langle \lambda v_1 + v_2, u\rangle = \lambda\langle v_1, u\rangle + \langle v_2, u\rangle = \lambda 0 + 0 = 0$ and therefore $\lambda v_1 + v_2$ belongs to $U^\perp$.

"2" On one hand, the vector 0 is orthogonal to every vector, which implies $\{0\}^\perp = V$. On the other hand, if v is in $V^\perp$ then it is orthogonal to itself and therefore equal to 0. This shows that $V^\perp \subseteq \{0\}$ and we have equality since $V^\perp$ is a subspace.

"3" Suppose that $U \cap U^\perp$ is not empty and let v be any element inside the intersection. Then, as above, we have $\langle v, v\rangle = 0$ and so $v = 0$. This shows that $U \cap U^\perp \subseteq \{0\}$. We have equality if and only if both U and $U^\perp$ contains 0, but $U^\perp$ is a subspace and hence always contains 0.

"4" Let $u \in U$. Then for any $v \in U^\perp$, $\langle u, v\rangle = 0$ which show that u is in $(U^\perp)^\perp$.

"5" Let v be in $W^\perp$. Then $\langle v, w\rangle = 0$ for every $w \in W$ and therefore in particular for every $w \in U$. So v is in $U^\perp$ and $W^\perp \subseteq U^\perp$. □

If U is a subspace of V, in order to describe $U^\perp$, it is enough to check orthogonality with respect to a spanning family, as demonstrated by the following result.

Lemma 4.3.16. *Let V be an inner product space and let U be a subspace with a spanning family $(u_\alpha)_{\alpha\in I}$. We have*

$$U^\perp = \{v \in V \mid \forall \alpha \in I, \langle v, u_\alpha\rangle = 0\}.$$

Proof. We will give the proof for a finite dimensional subspace with spanning family $(u_1, \dots, u_l)$. The general case is similar.

The left-to-right inclusion is obvious, so we only need to check the right to left inclusion. Let V be vector such that $\langle v, u\rangle_j = 0$ for all $j \in \{1, \dots, l\}$. For every $u \in U$, we have $u = \lambda_1 u_1 + \cdots + \lambda_l u_l$ for some $\lambda_j \in \mathbf{F}$ (not necessarily unique). By linearity, $\langle v, u\rangle = \lambda_1\langle v, u_1\rangle + \cdots + \lambda_l\langle v, u_l\rangle = 0$ and therefore v is in $U^\perp$. □

Another nice property of orthogonal complements is that they can be use for direct sum decompositions.

Theorem 4.3.17.

Let V be an inner product space and let U be a finite dimensional subspace. Suppose that there exists an orthonormal basis $(u_1, \dots, u_l)$ of U. Finally, let $(e_1, \dots, e_l)$ be the standard basis of $\mathbf{F}^l$. Consider the linear maps $T\colon V \to \mathbf{F}^l$ and $S\colon \mathbf{F}^l \to V$ given by

$$T(v) := \begin{bmatrix}\langle v, u_1\rangle \\ \vdots \\ \langle v, u_l\rangle\end{bmatrix},$$
$$S(e_j) := u_j,$$

where S is extended linearly to $\mathbf{F}^l$. Then we have $TS = \mathrm{Id}_{\mathbf{F}^l}$, $V = U \oplus U^\perp$, and $ST \in \mathcal{L}(V)$ is the projection onto U along the direction $U^\perp$.

Proof.

$$\begin{aligned} TS(e_j) = T(u_j) &= [\langle u_j, u_1\rangle, \dots, \langle u_j, u_l\rangle]^\mathsf{T} \\ &= [0, \dots, 0, 1, 0, \dots, 0]^\mathsf{T} = e_j. \end{aligned}$$

Therefore, $TS(e_j) = \mathrm{Id}_{\mathbf{F}^l}(e_j)$ for all basis vectors e_j, and since both TS and $\mathrm{Id}_{\mathbf{F}^l}$ are linear we have $TS = \mathrm{Id}_{\mathbf{F}^l}$.

By Proposition 3.3.14, the map ST is a projection onto $\mathrm{Im}(S)$ along the direction $\ker(T)$ and $V = \mathrm{Im}(S) \oplus \ker(T)$.

Since $S(e_j)$ belongs to U for basis vectors, we have $\mathrm{Im}(S) \subseteq U$. Moreover, all the $u_j = Se_j$ belongs to $\mathrm{Im}(S)$, which implies $U = \mathrm{span}(e_1, \dots, u_l) \subseteq \mathrm{Im}(S)$. This shows that $\mathrm{Im}(S) = U$. Finally, a vector $v \in V$ is in $\ker(T)$ if and only if $\langle v, u_j\rangle = 0$ for all j, if and only if v is in $U^\perp$. So $\ker(T) = U^\perp$. □

We will later prove Theorem 4.3.32 that asserts that any finite dimensional subspace admits an orthonormal basis. As a direct consequence we obtain

Corollary 4.3.18. *Let V be an inner product space and let U be a finite dimensional subspace. Then $V = U \oplus U^\perp$.*

Infinite dimensional vector spaces

Theorem 4.3.17 remains true for infinite dimensional subspace. Namely, if U is a subspace that admits an orthonormal basis $(u_\alpha)_{\alpha \in I}$, then one can define linear maps $T \in \mathcal{L}(V, \mathbf{F}^{(I)})$ and $S \in \mathcal{L}(\mathbf{F}^{(I)}, V)$ such that $TS = \mathrm{Id}_{\mathbf{F}^{(I)}}$. So $ST \in \mathcal{L}(V)$ is the orthogonal projection onto U and we have $V = U \oplus U^\perp$.
However, a subspace U of uncountable dimension does not necessarily admit an orthonormal basis and so Corollary 4.3.18 might fails for such subspaces. This is demonstrated in the next example.

Example 4.3.19. Let $V = \mathcal{C}^0([-1,1])$ be the space of continuous functions from $[-1,1]$ to $\mathbf{R}$ equipped with the inner product $\langle f, g \rangle = \int_{-1}^{1} f(x)g(x)\,\mathrm{d}x$. Let $U := \{f \in V \mid f(0) = 0\}$. This is an infinite dimensional proper subspace of V (the constant function $f = 1$ is in $V \setminus U$). Using analysis, one can show that $U^\perp = \{0\}$ (exercise). Therefore, we have $U + U^\perp = U + \{0\} = U \subsetneq V$. As a consequence, we conclude that U does not admit an orthonormal basis (and not even an orthogonal basis) as this would contradict Theorem 4.3.17 (see also the "Infinite dimensional vector spaces" just above).

As a direct corollary of Corollary 4.3.18, we can compute the dimension of $U^\perp$.

Corollary 4.3.20. *Let V be an inner product space and let U be a finite dimensional subspace. Then* $\dim(U^\perp) + \dim(U) = \dim(V)$.

Another important consequence of Corollary 4.3.18 is that taking orthogonal complement twice is the same as doing nothing.

Corollary 4.3.21. *Let V be an inner product space and let U be a finite dimensional subspace. Then $(U^\perp)^\perp = U$.*

Proof. "$\subseteq$" This is true for any subset of V, see Proposition 4.3.15.
"$\supseteq$" Let $v \in (U^\perp)^\perp \subseteq V = U \oplus U^\perp$ since U is finite dimensional. So there exists a unique decomposition $v = u + w$ with $u \in U$ and $w \in U^\perp$. We want to show that v is in U, or equivalently that $w = 0$. We have $u \in U \subseteq (U^\perp)^\perp$. So $w = v - u$ belongs both to $(U^\perp)^\perp$ and to $U^\perp$. But then $w \in (U^\perp)^\perp \cap U^\perp = \{0\}$ which is what we wanted to prove. □

Using Corollary 4.3.21 and Proposition 4.3.15 we can prove the following result.

Lemma 4.3.22. *Let V be an inner product space and let U be a finite dimensional subspace of V. Then $U^\perp = \{0\} \iff U = V$.*

Proof. If $U = V$, then $U^\perp = V^\perp = \{0\}$.
If U is finite dimensional and $U^\perp = \{0\}$, then $U = (U^\perp)^\perp = \{0\}^\perp = V$. □

We can use Corollary 4.3.18 to define specific projections.

Definition 4.3.23.

Let V be an inner product space and let U be a subspace such that $V = U \oplus U^\perp$ (for example, U finite dimensional). The **orthogonal projection** of V onto U is the projection $P_U = P_{U,U^\perp}$ onto U along direction $U^\perp$. That is, this is the map

$$P_U \colon V = U \oplus U^\perp \to U$$
$$v = u + w \longmapsto u.$$

Remark 4.3.24.

To be defined an orthogonal projection need V to be an inner product space and U such that $V = U \oplus U^\perp$. While this is automatically true if U is finite dimensional, it might fail for infinite dimensional subspaces, see Example 4.3.19.

Example 4.3.25. Let V be an inner product space. For u a non-zero vector of V, define $U := \operatorname{span} u$. Then for any $v \in V$, by Lemma 4.2.13 we have $v = \frac{\langle v,u\rangle}{\langle u,u\rangle}u + w$ with $w \in U^\perp$. So $P_U(v) = \frac{\langle v,u\rangle}{\langle u,u\rangle}u$.

Example 4.3.26. Let V be an inner product space and let U be a finite dimensional subspace. Then the map ST from Theorem 4.3.17 is an orthogonal projection. Observe that while we used an orthonormal basis $\mathscr{B}$ of U to construct T and S, the map ST does not depend on $\mathscr{B}$, but only on U! Indeed, ST only depends on $\operatorname{Im}(S) = U$ and $\ker(T) = U^\perp$, and none of this subspaces depend on the choice of an orthonormal basis for U.

To check that a projection PU, W is orthogonal, it is enough to check that W is contained in $U^\perp$.

Lemma 4.3.27. *Let V be an inner product space and let $P \in \mathcal{L}(V)$ be a projection. Suppose that $\operatorname{Im}(P)$ and $\ker(P)$ are orthogonal. Then P is the orthogonal projection onto $\operatorname{Im}(P)$.*

Proof. By Proposition 3.3.10, P is the projection onto $U = \operatorname{Im}(P)$ along direction $W = \ker(P)$ and thus $V = U \oplus W$. So we only need to prove that $W = U^\perp$. By hypothesis, $W \subseteq U^\perp$. Now, let v be an element of $U^\perp$. We have the decomposition $v = u + w$ with $u \in U$ and $w \in W$. Since both v and w are in $U^\perp$ we have $0 = \langle v, u\rangle = \langle u, u\rangle + \langle w, u\rangle = \langle u, u\rangle$. But this implies $u = 0$ and thus $v = w \in W$, showing $W = U^\perp$. □

Orthogonal projections are projections. They hence satisfies all properties of projections of Proposition 3.3.4. They also satisfy two additional properties.

Proposition 4.3.28. *Let V be an inner product space and let U be a finite dimensional subspace. Then the orthogonal projection onto U satisfies*

8. *$\|P_U v\| \leq \|v\|$ for every $v \in V$;*

9. *For every orthonormal basis* $(e_1, \dots, e_l)$ *of* U *we have* $P_U v = \langle v, e_1\rangle e_1 + \cdots + \langle v, e_l\rangle e_l$.

Proof. "8" The proof is left as an exercise. Tutorial 9, Question 3

"9" This is (the proof of) Theorem 4.3.17. □

Corollary 4.3.29. *Let* V *be an inner product space and suppose that* $P \in \mathcal{L}(V)$ *is a projection onto a subspace* U*. Prove that* P *is an orthogonal projection if and only if* $\|Pv\| \leq \|v\|$ *for all* $v \in V$*.*

Proof. One direction is simply Proposition 4.3.28.

For the other direction, one claims that if $\|Pv\| \leq \|v\|$ for every $v \in V$, then $\mathrm{Im}(P)$ and $\ker(P)$ are orthogonal. The result then follows from Corollary 4.3.29. □ Tutorial 9, Question 3

Infinite dimensional vector spaces

Most of the results of this subsection are corollaries of Corollary 4.3.18. That means that they remain true for any infinite dimensional subspace U satisfying $V = U \oplus U^\perp$, in particular for U of countable dimension. For such subspaces U, Corollary 4.3.21 and Lemma 4.3.22 are still true. However, Corollary 4.3.21 and Lemma 4.3.22 fail for general U, as demonstrated by Example 4.3.19.
It is also possible to define orthogonal projections onto U (in the sense of Definition 4.3.23) as soon as $V = U \oplus U^\perp$. Proposition 4.3.28 remains true in this context.

4.3.3 The Gram–Schmidt procedure

In the last subsection, we defined orthogonal complements. We then assumed Theorem 4.3.11 (every finite dimensional vector space admits an orthonormal basis) to prove many results about orthogonal complements and orthogonal projections. We now finally prove this theorem.

First of all, observe that if $\dim(V) = 0$, then the empty set is an orthonormal basis! If $\dim(V) = 1$, for any non-zero vector $v \in V$, the vector $\frac{v}{\|v\|}$ is an orthonormal basis of V.

If $\dim V = 2$, let $v_1 \in V$ be any non-zero vector and define $U := \mathrm{span}(v_1)$, so $\frac{v_1}{\|v_1\|}$ is an orthonormal basis of U. Using Proposition 4.2.14, $V = U \oplus U^\perp$. Moreover, the same proposition tells us that the orthogonal projection P_U onto U exists. Now, let $v_2 \in V \setminus U$ and consider

$$u_2 := v_2 - P_U v_2 = \frac{\langle v_2, v_1\rangle}{\langle v_1, v_1\rangle} v_1.$$

By Lemma 4.2.13, u_2 is orthogonal to v_1. Moreover, $u_2 \neq 0$ as this would implies $v_2 \in U$. Hence, $\left(\frac{v_1}{\|v_1\|}, \frac{u_2}{\|u_2\|}\right)$ is an orthonormal basis for V.

Let us have a closer look at the construction of our orthonormal basis for an inner product space of dimension 2. We can start with any basis (v_1, v_2). Then we obtain and orthogonal basis (u_1, u_2) where $u_1 = v_1$ and $u_2 = v_2 - P_U v_2$ is v_2 minus its "v_1-component". Finally, we obtain an orthonormal basis (e_1, e_2) by dividing each of the vector u_i by its norm.

The above procedure can be extended to any finite dimensional inner product space.

Theorem 4.3.30 (Gram–Schmidt[5] procedure)**.**

Let V be an inner product space and let $(v_1, \dots, v_l)$ be a linearly independent list. Define inductively

$$\begin{aligned}
u_1 &:= v_1, \\
u_2 &:= v_2 - \frac{\langle v_2, u_1\rangle}{\|u_1\|^2} u_1 = v_2 - P_{\operatorname{span}(u_1)}(v_2), \\
u_3 &:= v_3 - \frac{\langle v_3, u_1\rangle}{\|u_1\|^2} u_1 - \frac{\langle v_3, u_2\rangle}{\|u_2\|^2} u_2 = v_3 - P_{\operatorname{span}(u_1,u_2)}(v_3), \\
&\vdots \\
u_l &:= v_l - \frac{\langle v_l, u_1\rangle}{\|u_1\|^2} u_1 - \dots - \frac{\langle v_l, u_{l-1}\rangle}{\|u_{l-1}\|^2} u_{l-1} \\
&= v_l - P_{\operatorname{span}(u_1,\dots,u_{l-1})}(v_l).
\end{aligned}$$

Finally, for $j \in \{1, \dots, l\}$ define $e_j := \frac{u_j}{\|u_j\|}$.
Then $(u_1, \dots, u_l)$ is an orthogonal list and $(e_1, \dots, e_l)$ is an orthonormal list. Moreover, for $j \in \{1, \dots, l\}$ we have

$$\operatorname{span}(e_1, \dots, e_j) = \operatorname{span}(u_1, \dots, u_j) = \operatorname{span}(v_1, \dots, v_j).$$

Proof. The proof is done by induction on l. If $l = 1$, then $u_1 = v_1$ is orthogonal and $\operatorname{span}(u_1) = \operatorname{span}(v_1)$. Moreover, by linear independence, $v_1 \neq 0$, so $\|u_1\| \neq 0$ which implies that e_1 is well-defined and is a non-zero multiple of u_1. This directly gives $\operatorname{span}(e_1) = \operatorname{span}(u_1)$. Finally, $\|e_1\| = \left\| \frac{u_1}{\|u_1\|} \right\| = 1$.

Suppose that the conclusion holds for $\leq l - 1 \geq 0$, so for every $1 \leq j \leq l - 1$, the list $(e_1, \dots, e_j)$ is an orthonormal basis for $U_j := \operatorname{span}(e_1, \dots, e_j) = \operatorname{span}(u_1, \dots, u_j) = \operatorname{span}(v_1, \dots, v_j)$. Since U_{l-1} has an orthonormal basis, we can apply Theorem 4.3.17 to it to obtain $V = U_{l-1} \oplus U_{l-1}^{\perp}$. Moreover, v_l does not belong to U_{l-1} as the list $(v_1, \dots, v_l)$ is linearly independent. Considering $P_{U_{l-1}} \in \mathcal{L}(V)$ the orthogonal projection onto U_{l-1}, by Proposition 4.3.28.9 we have

$$\begin{aligned}
P_{U_{l-1}}(v_l) &= \langle v_l, e_1\rangle e_1 + \dots + \langle v_l, e_{l-1}\rangle e_{l-1} \\
&= \frac{\langle v_l, u_1\rangle}{\|u_1\|^2} u_1 + \dots + \frac{\langle v_l, u_{l-1}\rangle}{\|u_{l-1}\|^2} u_{l-1}.
\end{aligned}$$

Hence $u_l := v_l - P_{U_{l-1}}(v_l)$ belongs to $U_{l-1}^{\perp}$ and $(u_1, \dots, u_l)$ is an orthogonal list of non-zero vectors and therefore $(e_1, \dots, e_l)$ is an orthonormal list. From $\operatorname{span}(u_1, \dots, u_{l-1}) = \operatorname{span}(v_1, \dots, v_{l-1})$ and the fact that $v_l = u_l + P_{U_{l-1}}(l_j)$ belongs to $\operatorname{span}(u_1, \dots, u_l)$ we

[5] Jørgen Pedersen Gram (1850–1916) and Erhard Schmidt (1876–1959).

conclude that $\operatorname{span}(v_1, \dots, v_l) \subseteq \operatorname{span}(u_1, \dots, u_l)$. The other inclusion follows from the fact that $u_l = v_l - P_{U_{l-1}}(v_l)$ belongs to $\operatorname{span}(v_1, \dots, v_l)$. Finally, since $u_l \neq 0$ the vector e_l is well-defined and it is clear that $\operatorname{span}(u_1, \dots, u_l) = \operatorname{span}(e_1, \dots, e_l)$.

We have just proved that if the conclusion holds for $l-1$ it also holds for l. Since the conclusion holds for $l = 1$, we conclude that it holds for all l as desired. □

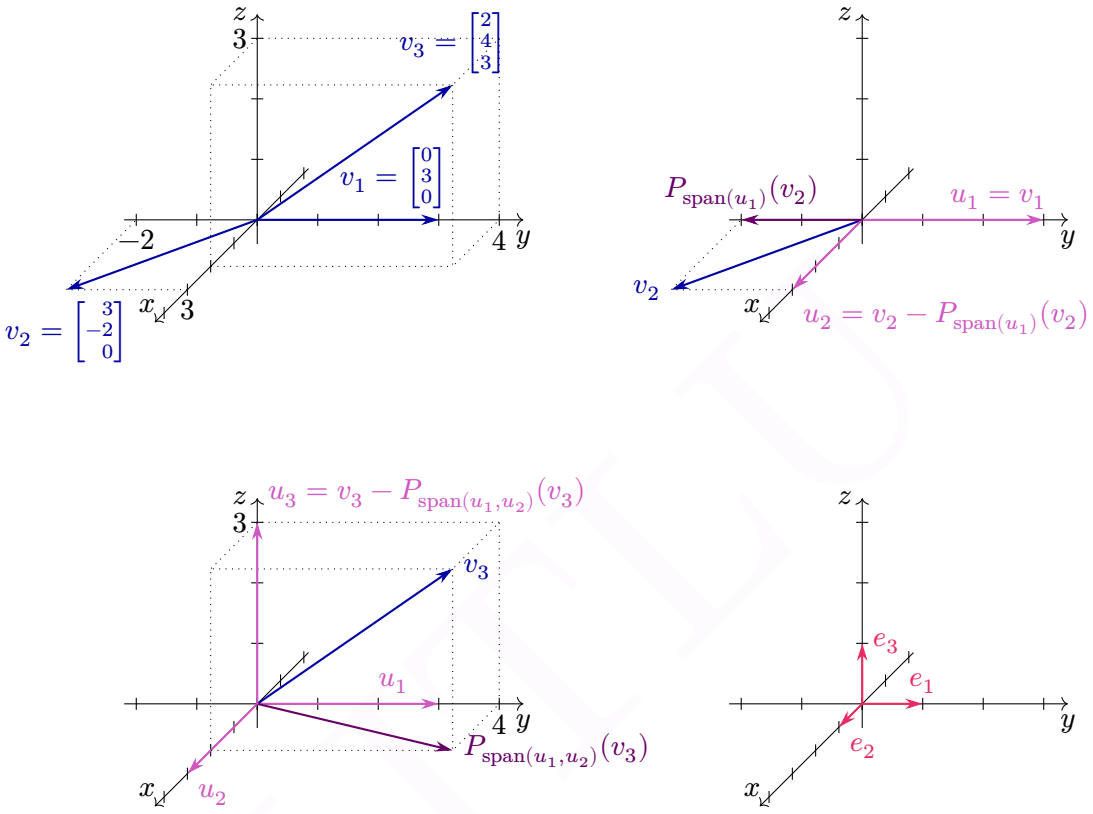


Figure 4.11: The Gram–Schmidt procedure applied to the linearly independent list $\left(v_1 = \begin{bmatrix} 0 \\ 3 \\ 0 \end{bmatrix}, v_2 = \begin{bmatrix} 3 \\ -2 \\ 0 \end{bmatrix}, v_3 = \begin{bmatrix} 2 \\ 4 \\ 3 \end{bmatrix}\right)$ (top left). We first put $u_1 = v_1$ and compute $u_2 = v_2 - P_{\operatorname{span}(u_1)}(v_2)$ (top right). We then compute $u_3 = v_3 - P_{\operatorname{span}(u_1,u_2)}(v_3)$ (bottom left). Finally we normalise the vectors to obtain the orthonormal list $\left(\begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix}\right)$ (bottom right).

Exercise 4.3.31. Find an orthonormal basis for $\mathcal{P}(\mathbf{R})_2$, where the inner product is given by $\langle p, q \rangle := \int_{-1}^{1} p(x)q(x)\,\mathrm{d}x$.

Solution. Start with the standard basis $(v_1 = 1, v_2 = x, v_3 = x^2)$ and apply Gram–

Schmidt to it. We have

$$\begin{aligned} u_1 &= v_1 = 1, \\ u_2 &= v_2 - \frac{\langle v_2, u_1\rangle}{\langle u_1, u_1\rangle} u_1, \\ u_3 &= v_3 - \frac{\langle v_3, u_1\rangle}{\langle u_1, u_1\rangle} u_1 - \frac{\langle v_3, u_2\rangle}{\langle u_2, u_2\rangle} u_2. \end{aligned}$$

Let us compute $\langle u_1, u_1\rangle = \int_{-1}^{1} 1\,\mathrm{d}x = 2$ and $\langle v_2, u_1\rangle = \int_{-1}^{1} x\,\mathrm{d}x = 0$. We also have $\langle v_3, u_1\rangle = \int_{-1}^{1} x^2 \cdot 1\,\mathrm{d}x = 2/3$, $\langle u_2, u_2\rangle = \int_{-1}^{1} x \cdot x\,\mathrm{d}x = 2/3$, and $\langle v_3, u_2\rangle = \int_{-1}^{1} x^2 \cdot x\,\mathrm{d}x = 0$. So

$$u_1 = v_1 = 1, \qquad u_2 = x - \frac{0}{2}1 = x, \qquad u_3 = x^2 - \frac{2/3}{2}1 - \frac{0}{2/3}x = x^2 - \frac{1}{3}.$$

Finally, we compute $\langle u_3, u_3\rangle = \int_{-1}^{1} (x^2 - 1/3)^2\,\mathrm{d}x = 8/45$ and we normalise the u_i to obtain an orthonormal basis for $\mathcal{P}(\mathbf{R})_2$:

$$\begin{aligned} e_1 &= \frac{u_1}{\|u_1\|} = \frac{1}{\sqrt{2}}, \\ e_2 &= \frac{u_2}{\|u_2\|} = \sqrt{\frac{3}{2}}x, \\ e_3 &= \frac{u_3}{\|u_3\|} = \sqrt{\frac{45}{8}}\left(x^2 - \frac{1}{3}\right). \end{aligned}$$

□

As a corollary of the Gram–Schmidt procedure, we obtain Theorem 4.3.11.

Theorem 4.3.32.

Every finite dimensional inner product space has an orthonormal basis.

Proof. Since V is finite dimensional, it has a basis $(v_1, \dots, v_m)$. Applying the Gram–Schmidt procedure to this basis gives an orthonormal spanning list, that is an orthonormal basis. □

Infinite dimensional vector spaces

The same idea gives us that every inner product space of countable dimension (as for example $\mathcal{P}(\mathbf{F})$) has an orthonormal basis. However, this does not work for inner product spaces of uncountable dimension, as for example $\mathcal{C}^0([-1, 1])$.
Even if the Gram–Schmidt procedure does not work for spaces of uncountable dimension, they might still have an orthonormal basis. Indeed, let V be a real or complex vector space and let $\mathscr{B} = (v_\alpha)_{\alpha \in I}$ be a given basis. Then $\langle v_\alpha, v_\beta\rangle = 1$ if $\alpha = \beta$ and 0 otherwise can be extended to a unique inner product on V. This

inner product turns $\mathscr{B}$ into an orthonormal basis.
However, in application we are interested in V with a fixed inner product $\langle \cdot, \cdot \rangle$ and a given subspace U of V. As Example 4.3.19 demonstrates, it might be impossible to find an orthonormal basis for U in this context.

4.4 Orthogonality, matrices and minimisations problems

In finite dimensional spaces, orthogonal projections can conveniently be described using matrices. This can in turn be used to solve minimisation problems, to approximate functions or to find best-fit curves.

4.4.1 Conjugate transpose matrices

Let $\mathscr{E}$ be the standard basis of $\mathbf{F}^m$ and let $T \in \mathcal{L}(\mathbf{F}^m)$ be a linear map. One can associate to T a matrix $[T]_{\mathscr{E}}^{\mathscr{E}} \in \mathbf{F}^{m,m}$. We have seen that T is a projection if and only if $\left([T]_{\mathscr{E}}^{\mathscr{E}}\right)^2 = [T]_{\mathscr{E}}^{\mathscr{E}}$. At this point, it is natural to ask: can we detect on $[T]_{\mathscr{E}}^{\mathscr{E}}$ if T is an orthogonal projection? The answer is yes!

Before going further, let us recall a classical definition from high school.

Definition 4.4.1.

Let $A \in \mathbf{R}^{m,n}$ be a matrix. The **transpose matrix** of A is the matrix A^{T} given by taking the symmetric of A along the diagonal:

$$A = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{bmatrix} \longmapsto A^{\mathsf{T}} := \begin{bmatrix} a_{11} & a_{21} & \cdots & a_{m1} \\ a_{12} & a_{22} & \cdots & a_{n} \\ \vdots & \vdots & & \vdots \\ a_{1n} & a_{2n} & \cdots & a_{mn} \end{bmatrix}.$$

When we generalised the dot product from real vector spaces to complex vector spaces (Subsection 4.1.2), we had to introduce complex conjugation in the definition in order to keep the nice properties of the real dot products. A similar phenomenon happens for matrices.

Definition 4.4.2.

Let $A \in \mathbf{F}^{m,n}$ be a matrix. The **conjugate transpose matrix** (also called **adjoint matrix**) of A is the matrix $A^* := \overline{A^{\mathsf{T}}} = \overline{A}^{\mathsf{T}} \in \mathbf{F}^{n,m}$.

Remark 4.4.3.

You might have seen the formula $A^{-1} = \text{adj}(A)\det(A)$ for an invertible matrix A. The matrix $\text{adj}(A)$ is the transpose of the cofactor matrix of A and is called the **adjugate** or **classical adjoint** of A. Despite similar names, the matrices A^* and $\text{adj}(A)$ are not related.

For example, if $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ is a 2×2 complex matrix, then $A^* = \begin{bmatrix} \overline{a} & \overline{c} \\ \overline{b} & \overline{d} \end{bmatrix}$ while $\text{adj}(A) = \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$.

Observe that if $\mathbf{F} = \mathbf{R}$, then $A^* = A^\mathsf{T}$ is simply the transpose matrix. Here are some properties of the conjugate transpose of a matrix. For real matrices, they translate to properties of the transpose matrix.

Proposition 4.4.4. *The conjugate transpose of a matrix satisfies the following properties.*

1. *For all vectors u, v in $\mathbf{F}^m$ we have $u \bullet v = v^* u$;*
2. *For all $A \in \mathbf{F}^{m,n}$ we have $(A^*)^* = A$;*
3. *For all $A, B \in \mathbf{F}^{m,n}$ we have $(A + B)^* = A^* + B^*$;*
4. *For all $A \in \mathbf{F}^{m,n}$ and $B \in \mathbf{F}^{n,k}$, we have $(AB)^* = B^* A^*$;*
5. *For all $A \in \mathbf{F}^{m,n}$ we have $\text{null}(A^*) = \text{col}(A)^\perp$ (with respect to the standard dot product).*

Proof. Properties 1 to 3 directly follow from the definitions and their proof is an easy exercise.

4. We have $(AB)^* = \overline{(AB)^\mathsf{T}} = \overline{B^\mathsf{T} A^\mathsf{T}} = \overline{B^\mathsf{T}} \cdot \overline{A^\mathsf{T}} = B^* A^*$.
5. This is left as an exercise to the reader. □

Tutorial 9, Question 2

The above proposition implies the following fundamental properties of adjoint matrices.

Lemma 4.4.5. *Let $A \in \mathbf{F}^{m,n}$ be matrix. Then for every vectors $v \in \mathbf{F}^n$ and $w \in \mathbf{F}^m$ we have*

$$Av \bullet w = v \bullet A^* w.$$

Proof. We have

$$\begin{aligned} Av \bullet w &= w^* Av \\ &= (A^* w)^* v \\ &= v \bullet A^* w, \end{aligned}$$

where we used Property 1 from Proposition 4.4.4 for the first and last equality, and properties 2 and 4 for the second equality. □

Infinite dimensional vector spaces

Lemma 4.4.5 can be used to define the adjoint of an operator in the following way. Let V and W be possibly infinite dimensional inner product spaces, and let $T\colon V \to W$ be a linear map. We say that $S\colon W \to V$ is an **adjoint** of T and write $S = T^*$ if for all $v \in V$ and $w \in W$ we have $\langle Tv, w\rangle_W = \langle v, Sw\rangle_V$. If V and W are finite dimensional, then the adjoint always exists and is unique. Moreover, for $T \in \mathcal{L}(\mathbf{F}^n, \mathbf{F}^m)$ we have $[T^*]_{\mathscr{E}_n}^{\mathscr{E}_m} = ([T]_{\mathscr{E}_m}^{\mathscr{E}_n})^*$.
If V and W are infinite dimensional but "nice enough" (that is, are *Hilbert spaces*) and if T is continuous, then the adjoint of T always exists, is unique and enjoys properties similar to ones enjoyed by adjoints in the finite dimensional case.

An important consequence of Proposition 4.4.4 is that we can detect on $[T]_{\mathscr{B}}^{\mathscr{B}}$ if an operator is an orthogonal projection.

Theorem 4.4.6.

A $m \times m$ matrix A represents an orthogonal projection (with respect to the standard dot product) if and only if $A^2 = A = A^*$.

Proof. The proof is left as an exercise to the reader. □

Tutorial 9, Question 4

The adjoint is also related to linear independence of the columns of the matrix, in the following way.

Lemma 4.4.7. *Let $A \in \mathbf{F}^{m,n}$ be a matrix. Then the columns of A are linearly independent if and only if the matrix $A^*A \in \mathbf{F}^{n,n}$ is invertible.*

Proof. We will prove the equivalence: the columns of A are linearly dependent if and only if A^*A is not invertible. Before doing that, we recall that the columns of a matrix $B \in \mathbf{F}^{m,n}$ are linearly dependent if and only if the linear map represented by B is non-injective. That is, if and only if there exists a non-zero $u \in \mathbf{F}^n$ such that $Bu = 0$. Moreover, if B is a square matrix, this is also equivalent to the non-invertibility of B. Indeed, in this case the linear map represented by B is injective if and only if it is bijective, if and only if it is invertible.

"⇒" If the columns of A are linearly dependent, then there exists a non-zero $u \in \mathbf{F}^n$ such that $Au = 0$. But for this non-zero vector we have $(A^*A)u = A^*(Au) = A^*0 = 0$, which implies that A^*A is not invertible.

"⇐" The matrix A^*A is a square matrix. Therefore, if is not invertible the linear map it represents is not injective and then there exists a non-zero vector $v \in \mathbf{F}^n$ with $A^*Av = 0$. But then we have $0 = v^*A^*Av = (Av)^*(Av) = \langle Av, Av\rangle = \|Av\|^2$, which implies $Av = 0$. Since $v \neq 0$, the columns of A are linearly dependent. □

By the above lemma, if the columns of A are linearly independent, then the matrix $A(A^*A)^{-1}A^*$ is well-defined. This is not any matrix, but a matrix representing an orthogonal projection.

Theorem 4.4.8.

Let $A \in \mathbf{F}^{m,n}$ be a matrix with linearly independent columns. Let $U := \mathrm{col}(A)$ be the subspace of $\mathbf{F}^m$ spanned by the columns of A. Then $P := A(A^*A)^{-1}A^* \in \mathbf{F}^{m,m}$ represents the orthogonal projection onto U (with respect to the standard dot product).

Proof. We will use left/right inverses. Let $S := A(A^*A)^{-1}$ and $T := A^*$. It is immediate that $TS = \mathrm{Id}_n$, and therefore by Proposition 3.3.14, $ST = A(A^*A)^{-1}A$ represents a projection onto $\mathrm{col}(S)$ along direction $\ker(T)$.

On one hand, since $(A^*A)^{-1}$ is invertible, we have $\mathrm{col}(S) = \mathrm{col}(A(A^*A)^{-1}) = \mathrm{col}(A) = U$, where the second equality follows from Lemma 3.1.47. On the other hand, $\ker(T) = \mathrm{null}(A^*) = \mathrm{col}(A)^\perp$ by Proposition 4.4.4. □

We will see later (in Example 4.4.15) that for applications it is enough to compute $(A^*A)^{-1}A^*$.

4.4.2 QR decomposition

One can use the Gram–Schmidt procedure to find nice decomposition of invertible matrices. Let V be a finite dimensional inner product space over $\mathbf{F}$ and let $\mathscr{B} = (v_1, \dots, v_m)$ be a basis for V. By applying Gram–Schmidt to $\mathscr{B}$ we obtain an orthogonal basis $\mathscr{C} = (u_1, \dots, u_m)$ and an orthonormal basis $\mathscr{E} = (e_1, \dots, e_m)$ of V.

Question 4.4.9. What do the change of basis matrices $[\mathrm{Id}]_{\mathscr{E}}^{\mathscr{B}}$ and $[\mathrm{Id}]_{\mathscr{B}}^{\mathscr{E}}$ look like?

Answer. We have $[\mathrm{Id}]_{\mathscr{E}}^{\mathscr{B}} = [\mathrm{Id}]_{\mathscr{C}}^{\mathscr{B}}[\mathrm{Id}]_{\mathscr{E}}^{\mathscr{C}}$. From the Gram–Schmidt procedure, we have (the missing coefficients are all 0)

$$[\mathrm{Id}]_{\mathscr{E}}^{\mathscr{B}} = \begin{bmatrix} 1 & * & \cdots & * \\ 0 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & * \\ 0 & \cdots & 0 & 1 \end{bmatrix}, \qquad [\mathrm{Id}]_{\mathscr{E}}^{\mathscr{C}} = \begin{bmatrix} \frac{1}{\|u_1\|} & & & \\ & \ddots & & \\ & & \ddots & \\ & & & \frac{1}{\|u_n\|} \end{bmatrix}$$

for some coefficients $*$ in $\mathbf{F}$. So we have just proven that

$$[\mathrm{Id}]_{\mathscr{E}}^{\mathscr{B}} = \begin{bmatrix} \frac{1}{\|u_1\|} & * & \cdots & * \\ & \ddots & \ddots & \vdots \\ & & \ddots & * \\ & & & \frac{1}{\|u_n\|} \end{bmatrix}$$

is an invertible upper triangular matrix, and so is

$$[\mathrm{Id}]_{\mathscr{B}}^{\mathscr{E}} = \begin{bmatrix} \|u_1\| & * & \cdots & * \\ & \ddots & \ddots & \vdots \\ & & \ddots & * \\ & & & \|u_n\| \end{bmatrix}.$$

■

Example 4.4.10. Let $V = \mathbf{R}^m$ be the Euclidean space with standard dot product. And let $A = [v_1 \ \cdots \ v_m]$ be an invertible $m \times m$ matrix (v_j is the j^{th} column of A). Then $\mathscr{B} = (v_1, \dots, v_m)$ is a basis for $\mathbf{R}^m$ and applying Gram–Schmidt to $\mathscr{B}$ one obtain an orthonormal basis $\mathscr{E} = (e_1, \dots, e_m)$ of $\mathbf{R}^m$. Now, write $Q := [e_1 \ \cdots \ e_m]$ and $R := [\mathrm{Id}]^{\mathscr{E}}_{\mathscr{B}}$. By the above, R is an invertible upper triangular matrix, while Q is an *orthogonal matrix*[6] ($QQ^{\mathsf{T}} = \mathrm{Id}_n = Q^{\mathsf{T}}Q$) and we have the equality

$$A = QR,$$

which can be checked by direct computations. This is called the QR **decomposition** of A.

If $V = \mathbf{C}^m$, then we similarly obtain an UR **decomposition** of $A = UR$, where R is an invertible triangular matrix and U is an *unitary matrix* ($UU^* = \mathrm{Id}_m = U^*U$).

4.4.3 Minimisation problems

In this subsection we will see how to use linear algebra to solve minimisation problems of the following form.

Problem 4.4.11. Let V be an inner product space and let U be a subspace. Given a vector $v \in V$, we would like to find $u \in U$ such that $\|v - u\|$ is as small as possible.

A typical situation where we want to solve this problem is when V is a complicated inner product space, U is a nicer subspace and given $v \in V$ we are looking at an approximation $u \in U$ of v. The approximation is good if the "error" $\|v - u\|$ is as small as possible. A typical example of a pair $U \subseteq V$ is $V = \mathcal{C}^\infty(\mathbf{R})$ the space of smooth functions and $U = \mathcal{P}(\mathbf{R})$ the subspace of polynomials.

The following result shows that Problem 4.4.11 admits a unique solution.

Theorem 4.4.12.

Let V be an inner product space and let U be a finite dimensional subspace of V. Write $P_U = P_{U,U^\perp}$ for the orthogonal projection onto U. Then for any $v \in V$ we have

$$\forall u \in U : \|v - P_U v\| \leq \|v - u\|.$$

Moreover, $\|v - P_U v\| = \|v - u\|$ if and only if $u = P_U v$.
That is, $P_U v$ is the unique $u \in U$ minimising the distance between u and v.

Proof. We have

$$\begin{aligned} \|v - P_U v\|^2 &\leq \|v - P_U v\|^2 + \|P_U v - u\|^2 \\ &= \|v - u\|^2, \end{aligned}$$

[6] Be careful: despite a similar name, an orthogonal matrix is not the matrix of an orthogonal projections! Indeed, by Theorem 4.4.6, if a real matrix M represents a projection then $M^2 = M$. If the matrix M is also orthogonal in the above sense, then it is invertible an hence $M = \mathrm{Id}_m$.

where the last equality is by the Pythagorean Theorem (Theorem 4.2.6) since $P_U v - u \in U$ and $v - P_U v \in U^\perp$ are orthogonal.

We have equality if and only if $\|P_U v - u\| = 0$, that is if and only if $P_U v - u = 0$. □

See Figure 4.12 for an example of the inequality from the theorem.

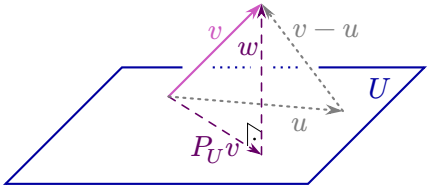


Figure 4.12: The orthogonal projection of v onto U, with "error" $\|w\| = \|v - P_U(v)\|$ and a worst approximation u with error $\|v - u\| > \|v - P_U(v)\|$.

Observe that in Theorem 4.4.12, U has to be finite dimensional[7], but V can be infinite dimensional, which will be the case in many applications.

Theorem 4.4.12 is often combined with Proposition 4.3.28.9 to compute explicit solutions to minimisation problems.

Now, let us see some application of Theorem 4.4.12, starting with an easy example.

Example 4.4.13. Let $V = \mathbf{R}^4$ with the standard dot product. Le $v := [1, 2, 3, 4]^\mathsf{T}$, $v_1 := [1, 1, 0, 0]^\mathsf{T}$ and $v_2 := [1, 1, 1, 2]^\mathsf{T}$ be three vectors in V. Find $u \in U := \operatorname{span}(v_1, v_2)$ minimising $\|v - u\|$.

Solution. By the theorem, we know that $u = P_U v$. To find $P_U v$ we need an orthonormal basis for U. To obtain such a basis, we can apply Gram–Schmidt to (v_1, v_2). So we have $u_1 = v_1 = [1, 1, 0, 0]^\mathsf{T}$ and $\|u_1\|^2 = \langle u_1, u_1 \rangle = 2$. Therefore

$$u_2 = v_2 - \frac{\langle v_2, u_1 \rangle}{\langle u_1, u_1 \rangle} u_1 = \begin{bmatrix} 1 \\ 1 \\ 1 \\ 2 \end{bmatrix} - \frac{2}{2} \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 1 \\ 2 \end{bmatrix}$$

and $\|u_2\|^2 = 1 + 2^2 = 5$. Normalising the u_i by their norm we obtain an orthonormal basis $(e_1 = \frac{1}{\sqrt{2}}[1, 1, 0, 0]^\mathsf{T}, e_2 = \frac{1}{\sqrt{5}}[0, 0, 1, 2]^\mathsf{T})$ for U. Finally we compute the projection

$$\begin{aligned} u = P_U v &= \langle v, e_1 \rangle e_1 + \langle v, e_2 \rangle e_2 \\ &= \frac{3}{\sqrt{2}} \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \end{bmatrix} + \frac{11}{\sqrt{5}} \frac{1}{\sqrt{5}} \begin{bmatrix} 0 \\ 0 \\ 1 \\ 2 \end{bmatrix} = \begin{bmatrix} 1.5 \\ 1.5 \\ 2.2 \\ 4.4 \end{bmatrix}. \end{aligned}$$

□

We will now do a more realistic example and use linear algebra to compute an approximation of the sine function.

Example 4.4.14. Suppose we want to find a polynomial u of degree at most 5 that gives the best possible approximation of the sine function on the interval $[-\pi, \pi]$.

[7] To be more precise, we only need $U \oplus U^\perp = V$, which is true for subspaces of countable dimension.

Solution. The sine function is continuous and hence belongs to $V = \mathcal{C}^0[-\pi, \pi]$. The space V has a natural inner product:

$$\langle f, g \rangle = \int_{-\pi}^{\pi} f(x)g(x)\,\mathrm{d}x.$$

Polynomials of degree at most 5 form a subspace $\mathcal{P}(\mathbf{R})_5 \subseteq \mathcal{C}^0[-\pi, \pi]$ of finite dimension. So we are looking at $u \in \mathcal{P}(\mathbf{R})_5$ minimising $\int_{-\pi}^{\pi} |\sin(x) - u(x)|^2\,\mathrm{d}x = \|\sin(x) - u(x)\|^2$. To find such a polynomial, we start from the standards basis $1, x, x^2, x^3, x^4, x^5$ of $\mathcal{P}(\mathbf{R})_5$ and apply Gram–Schmidt to it to obtain an orthornormal basis $(e_1, \dots, e_6)$. We can then use Proposition 4.3.28.9 to compute $P_U \sin(x)$. Using a computer, one can find

$$P_U \sin(x) \approx 0.987\,862x - 0.155\,271x^3 + 0.005\,643\,12x^5,$$

where π has been replaced by a decimal approximation.

As one can see on Figure 4.13, the polynomial approximation given by the projection of $\sin x$ onto $\mathcal{P}(\mathbf{R})_5$ is much better than the Taylor approximation of the same degree. In fact, $P_{\mathcal{P}(\mathbf{R})_5} \sin(x)$ is even a better approximation that the degree 7 Taylor polynomial of $\sin x$.

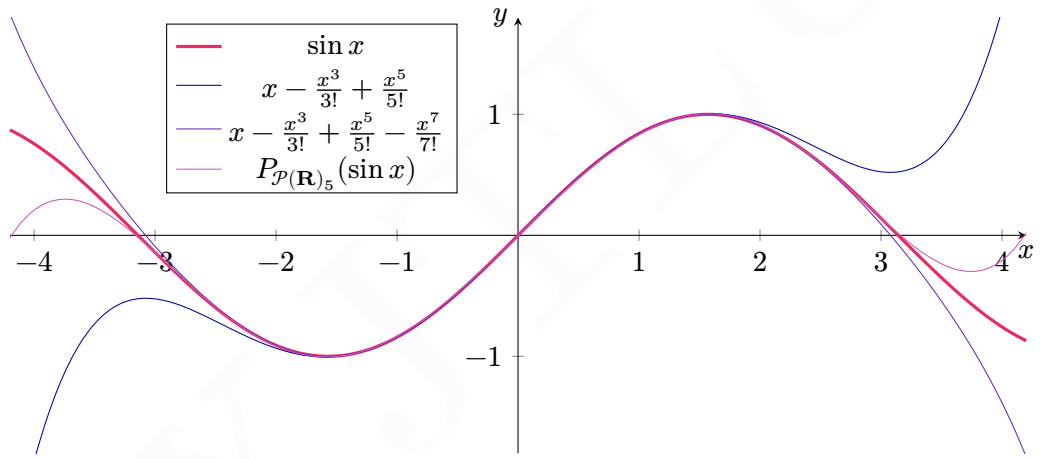


Figure 4.13: Three polynomial approximations of the sine function. By the Taylor polynomials of degree 5 and 7, and a better one by the projection on $\mathcal{P}(\mathbf{R})_5$.

□

In many real world experiments, we obtain a cloud of points $\{(x_j, y_j) \mid 1 \leq j \leq m\}$ in $\mathbf{R}^2$ that we would like to approximate by an easy function like a line or a parabola. One can use orthogonal projections to find such an approximation. First we need to explicit what we mean by "an approximation". One usual approximation is the *least square regression* where we want to find a function minimising $(y_1 - f(x_1))^2 + \cdots + (y_m - f(x_m))^2$. This corresponds to look at the standard dot product on $\mathbf{R}^m$ and try to minimise $\|y - f(x)\|$, where $y = [y_1, \dots, y_m]^\mathsf{T}$ and $f(x) = [f(x_1), \dots, f(x_m)]^\mathsf{T}$ is the value of the approximating

function at the points x_j. Now that we have fixed an inner product on $\mathbf{R}^m$, we need to decide on which subspace we project.

For example, if we want to approximate our data by a line, we will project on $U := \{[f(x_1), \dots, f(x_m)]^\mathsf{T} \mid f \in \mathcal{P}(\mathbf{R})_1\}$ which is a subspace of dimension 2 of $\mathbf{R}^m$. A basis of this subspace is given by $([x_1, \dots, x_m]^\mathsf{T}, [1, \dots, 1]^\mathsf{T},)$ (the first vector correspond to the polynomial x, and the second to the constant polynomial 1). In more concrete words, we are looking for two real numbers a and b minimising

$$\left\| \begin{bmatrix} y_1 \\ \vdots \\ y_m \end{bmatrix} - \left(a \begin{bmatrix} x_1 \\ \vdots \\ x_m \end{bmatrix} + b \begin{bmatrix} 1 \\ \vdots \\ 1 \end{bmatrix} \right) \right\|.$$

One can try to minimise the above system by hand, but this is a priori not an easy task. It is easier to use Theorem 4.4.12. So we need to find the orthogonal projection P_U. To do so, we can use Gram–Schmidt. But a more efficient method is to use Theorem 4.4.8 to obtain $\begin{bmatrix} a \\ b \end{bmatrix} = (A^*A)^{-1}A^*y$, where A is the $m \times 2$ matrix:

$$A = \begin{bmatrix} x_1 & 1 \\ \vdots & \vdots \\ x_m & 1 \end{bmatrix}.$$

Let us demonstrate that on a concrete example.

Example 4.4.15. Imagine we measured the following values in an experiment: $(0, 6)$, $(1, 0)$ and $(2, 0)$. It is obvious that no line in $\mathbf{R}^2$ go through these 3 points. However, our model/intuition for this experiment says that these points should lie on line. Maybe our measurements were not precise enough? So we try to find the best-fit line. In order to do that, we need to minimise

$$\left\| \begin{bmatrix} 6 \\ 0 \\ 0 \end{bmatrix} - \left(a \begin{bmatrix} 0 \\ 1 \\ 2 \end{bmatrix} + b \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix} \right) \right\|.$$

To solve this minimisation problem, we will use Theorem 4.4.8 for

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

So the projection of $[6,0,0]^\mathsf{T}$ onto U is given by

$$\begin{aligned} A \cdot (A^*A)^{-1}A^* \begin{bmatrix} 6 \\ 0 \\ 0 \end{bmatrix} &= A \left(\begin{bmatrix} 0 & 1 & 2 \\ 1 & 1 & 1 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 1 \\ 2 & 1 \end{bmatrix} \right)^{-1} \begin{bmatrix} 0 & 1 & 2 \\ 1 & 1 & 1 \end{bmatrix} \begin{bmatrix} 6 \\ 0 \\ 0 \end{bmatrix} \\ &= A \begin{bmatrix} 5 & 3 \\ 3 & 3 \end{bmatrix}^{-1} \begin{bmatrix} 0 \\ 6 \end{bmatrix} \\ &= A \frac{1}{6} \begin{bmatrix} 3 & -3 \\ -3 & 5 \end{bmatrix} \begin{bmatrix} 0 \\ 6 \end{bmatrix} \\ &= A \begin{bmatrix} -3 \\ 5 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & 1 \\ 2 & 1 \end{bmatrix} \begin{bmatrix} -3 \\ 5 \end{bmatrix} = \begin{bmatrix} 5 \\ 2 \\ -1 \end{bmatrix}. \end{aligned}$$

As we can see above, the best-fit line is given by the equation $y = -3x + 5$, while the projection of of $[6,0,0]^\mathsf{T}$ onto U is $[5,2,-1]^\mathsf{T} = -3[x_1,x_2,x_3]^\mathsf{T} + 5[1,1,1]^\mathsf{T}$. We can also compute the error:

$$\left\| \begin{bmatrix} 6 \\ 0 \\ 0 \end{bmatrix} - \begin{bmatrix} 5 \\ 2 \\ -1 \end{bmatrix} \right\| = \sqrt{1^2 + (-2)^2 + (-1)^2} = \sqrt{6}.$$

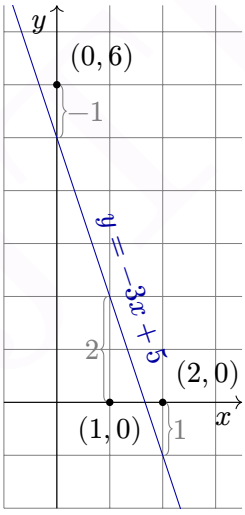


Figure 4.14: Best-fit line for the three black dots. The error is $\sqrt{6}$.

The above example can be adapted to any kind of best-fit curve. For example, if we are looking for a best-fit parabola for our 3 points, our matrix A will be:

$$A = \begin{bmatrix} (x_1)^2 & x_1 & 1 \\ (x_2)^2 & x_2 & 1 \\ (x_3)^2 & x_3 & 1 \end{bmatrix}.$$

because $(1, x, x^2)$ is a basis of $\mathcal{P}(\mathbf{R})_3$. Then we should compute

$$(A^*A)^{-1}A^* \begin{bmatrix} y_1 \\ y_2 \\ y_3 \end{bmatrix} =: \begin{bmatrix} a \\ b \\ c \end{bmatrix}.$$

This gives us that the best fit parabola for $((x_1, y_1), (x_2, y_2), (x_2, y_2))$ is given by the equation $y = ax^2 + bx + c$. Observe that for this specific easy example, our approximation will actually passes through all three points.

5 Eigenvalues and eigenvectors

In this chapter we will try to better understand operators $T \in \mathcal{L}(V)$. The main idea is to decompose V into smaller subspaces on which T acts, and use this to describe T. This will ultimately (see Section 5.3 and in particular Theorem 5.3.8) allows us to answer

Major Question 3.2.47.

Given V and $T \in \mathcal{L}(V)$, find a basis $\mathscr{B}$ such that $[T]_{\mathscr{B}}^{\mathscr{B}}$ is "as simple as possible" (for example: diagonal, upper triangular, with many zeroes, …).

Before going further into the details, let us recall an easy example we already saw.

Tutorial 6, Question 2.

Example 5.0.1. Let $V = \mathbf{R}^2$, and let S_θ be the orthogonal reflection across the line L that makes an angle θ with the x-axis, see Figure 5.1. We would like to find a basis $\mathscr{B}$ for which $[T]_{\mathscr{B}}^{\mathscr{B}}$ is "nice", meaning that it has many zeroes. First, we observe that for any v in L, we have $S_\theta v = v$. So it might be a good idea to take $v_1 = \begin{bmatrix} \cos\theta \\ \sin\theta \end{bmatrix} \in \mathbf{R}^2$ as our first basis vector. Indeed, this vector is of norm 1 and $L = \operatorname{span}(v_1)$.

We can also observe that for any u in $L^\perp$ we have $S_\theta u = -u$, which is also an easy formula. So one take $v_2 = \begin{bmatrix} -\sin\theta \\ \cos\theta \end{bmatrix}$ as our second basis vector. One easily verify that $\operatorname{span}(v_2) = L^\perp$, $v_1 \bullet v_2 = 0$ and $\|v_1\| = \|v_2\| = 1$, so our basis $\mathscr{B} = (v_1, v_2)$ is an orthonormal basis and $\mathbf{R}^2 = L \oplus L^\perp$. Altogether, we have

$$[S_\theta]_{\mathscr{B}}^{\mathscr{B}} = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}.$$

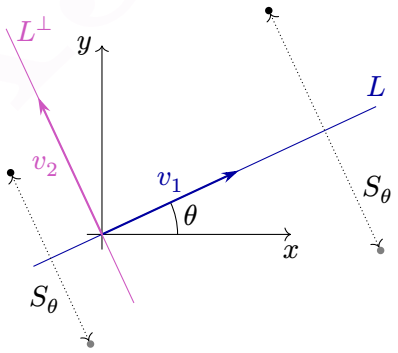


Figure 5.1: Orthogonal reflection S_θ across the line $L = \operatorname{span}\left(\begin{bmatrix} \cos\theta \\ \sin\theta \end{bmatrix}\right)$.

We can see many interesting things happening in this example. First of all, the existence of an orthonormal basis $\mathscr{B}$ for which $[S_\theta]_{\mathscr{B}}^{\mathscr{B}}$ is diagonal. Secondly, for any $u \in L$ we have $S_\theta u = u \in L$. Therefore, if we restrict S_θ to L we have an operator $S_\theta|_L \in \mathcal{L}(L)$. Similarly, for $w \in L^\perp$ we have $S_\theta w = -w \in L^\perp$ and we hence have an operator $S_\theta|_{L^\perp} \in \mathcal{L}(L^\perp)$. Altogether, we obtain the following description of S_θ:

$$\begin{aligned} S_\theta \colon \mathbf{R}^2 = L \oplus L^\perp &\to L \oplus L^\perp \\ v = u + w &\longmapsto u - w. \end{aligned}$$

For a general $T \in \mathcal{L}(V)$, we will not obtain a decomposition of V as nice as the decomposition of Example 5.0.1. However, we will still be able to decompose V onto smaller subspaces (Theorem 5.1.49) on which the action of T will not be too complicated (Theorem 5.3.8).

5.1 Eigen-theory

We start by generalising the idea of "nice vectors for T" from Example 5.0.1. This will give us a first answer to Question 3.2.47: if $T \in \mathcal{L}(V)$ is an operator on a finite dimensional complex vector space, then there exists a basis for which T is a diagonal by blocks matrix, see Proposition 5.1.56. We will then develop further tool in order to show that such a T admits a Jordan normal form, see Section 5.3 and in particular Theorem 5.3.8.

5.1.1 Invariant subspaces

One of the important feature of Example 5.0.1 was the existence of subspaces (L and $L^\perp$) for which the restriction $S_\theta|_L$ was still an operator. Let us generalise this notion.

Definition 5.1.1.

Let V be a vector space over $\mathbf{F}$, let $T \in \mathcal{L}(V)$ be an operator and let $U \subseteq V$ be a subspace. We say that U is **invariant under** T or **T-invariant** if for every $u \in U$ we have $Tu \in U$.

If we denote $TU := \{Tu \mid u \in U\}$, then U is T-invariant if and only if $TU \subseteq U$, if and only if $T|_U \in \mathcal{L}(U)$.

Below are some examples of T-invariant subspaces for various operators T.

Example 5.1.2. For any $T \in \mathcal{L}(V)$ the following four (not necessarily distinct) subspaces of V are all T-invariant: $\{0\}$, V, $\ker(T)$ and $\mathrm{Im}(T)$.

Indeed, $T0 = 0$ and $TV \subseteq V$. Moreover, for every $u \in \ker(T)$, $Tu = 0$ is still in $\ker(T)$ while for $v \in \mathrm{Im}(T)$, Tv is in $\mathrm{Im}(T)$.

Since $\{0\}$ and V are always T-invariant subspaces, we are interested to find the other invariant subspaces of T. However these do not always exist when $\mathbf{F} = \mathbf{R}$.

Example 5.1.3. Let S_θ be the orthogonal reflection across line L from Example 5.0.1. Then both L and $L^\perp$ are S_θ-invariant. In fact, one can easily show that: L and $L^\perp$ are the only invariant subspaces of S_θ — beside the trivial ones $\ker(S_\theta) = \{0\}$, $\mathrm{Im}(S_\theta) = \mathbf{R}^2$.

Example 5.1.4. Let $V = \mathcal{P}(\mathbf{R})$ and let $D \in \mathcal{L}(\mathcal{P}(\mathbf{R}))$ be the differentiation operator $D(p) = p'$. Then for every m, the subspace $\mathcal{P}(\mathbf{R})_m$ is D-invariant.

Example 5.1.5. Let $V = \mathbf{R}^2$ and let $\theta \in [0, 2\pi)$. Let R_θ be the rotation of angle θ around the origin. Then if $\theta \notin \{0, \pi\}$, the only invariant subspaces under R_θ are $\{0\}$ and V. Indeed, suppose that $U \neq \{0\}$ is a R_θ-invariant subspace and take $0 \neq u \in U$. Since $\theta \neq \{0, \pi\}$, $R_\theta u$ is not in $\mathrm{span}(u)$. Therefore $U \supsetneq \mathrm{span}(u, R_\theta u) = V$.

On the opposite, every subspace U is an invariant subspace of $R_0 = \mathrm{Id}$ and of R_π as $R_\pi u = -u$ for every u.

Example 5.1.6. Let V be any vector space, let Id_V be the identity operator and let $\lambda \in \mathbf{F}$ be any scalar number. Then any subspace U of V is $\lambda \mathrm{Id}_V$-invariant. Indeed, for every $u \in U$ we have $\lambda \mathrm{Id}_V u = \lambda u \in U$.

As the above examples shows, when we say that U is an invariant subspace, it is important to precise for which T it is invariant.

5.1.2 Eigenvalues and eigenvectors

In Example 5.0.1, not only do we have L and $L^\perp$ as non-trivial invariant subspaces, but the action of S_θ on them is particularly easy to describe. Indeed, for $v \in L$ we have $S_\theta v = v$, while for or $u \in L^\perp$ we have $S_\theta u = -u$. In both cases, the linear operator S_θ acts as the scalar multiplication by some λ.

Definition 5.1.7.

Let V be a vector space and let $T \in \mathcal{L}(V)$ be an operator. We say that $\lambda \in F$ is an **eigenvalue** of T if there exists a non-zero vector $v \in V$ such that $Tv = \lambda v$.
Such a non-zero vector v satisfying $Tv = \lambda v$ is called an **eigenvector** of T, corresponding to the eigenvalue λ.
The **eigenspace** of T corresponding to $\lambda \in \mathbf{F}$ is the set

$$\mathrm{E}(\lambda, T) := \{v \in V \mid Tv = \lambda v\}.$$

Observe that while by definition 0_V is never an eigenvector, 0 might be an eigenvalue. In fact, one always have $\mathrm{E}(0, T) = \ker(T)$. So 0 is an eigenvalue of T if and only if T is not injective. We do not allow 0 to be an eigenvector as $T0 = \lambda 0$ is true for all λ (and all T), so this would give a rather uninteresting notion of eigenvalue.

Be careful that the eigenspace of T corresponding to λ always contain 0_V. In fact,

$$\mathrm{E}(\lambda, T) = \{0_V\} \sqcup \{v \in V \mid v \text{ is an eigenvector corresponding to } \lambda\}.$$

We add 0 to the set of eigenvectors because we want $\mathrm{E}(\lambda, T)$ to be a subspace, as suggested by its name.

Lemma 5.1.8. *Let V be a vector space and let $T \in \mathcal{L}(V)$ be an operator. Then for any $\lambda \in \mathbf{F}$ we have*

$$\mathrm{E}(\lambda, T) = \ker(T - \lambda \mathrm{Id}_V),$$

and this is a T-invariant subspace.

Proof. A vector v is in $\ker(T - \lambda \mathrm{Id}_V)$ if and only if $(T - \lambda \mathrm{Id}_V)v = 0$, if and only if $Tv = \lambda v$, if and only if $v = 0$ or v is an eigenvector of eigenvalue λ.

This implies that $\mathrm{E}(\lambda, T)$ and it remains to show invariance. If v is an eigenvector of eigenvalue λ, then $T(Tv) = T(\lambda v) = \lambda Tv$ by linearity, and therefore Tv is also an eigenvector of eigenvalue λ. Since $T0 = 0 \in \mathrm{E}(\lambda, T)$, this shows that $\mathrm{E}(\lambda, T)$ is T-invariant. □

Example 5.1.9. Let S_θ be the orthogonal reflection across the line L, as in Example 5.0.1. Then as discuted above, both 1 and -1 are eigenvalue of S_θ. Moreover, for every u in L, we have $S_\theta v = v$, so $\mathrm{E}(1, S_\theta) \supseteq \mathrm{span}(v_1)$. But if u is not in L, then $S_\theta u \neq u$ and thus $\mathrm{E}(1, S_\theta) = L$. Similarly, one can show that $\mathrm{E}(-1, S_\theta) = L^\perp$.

So we have proved that $\mathbf{R}^2 = \mathrm{E}(1, S_\theta) \oplus \mathrm{E}(-1, S_\theta)$. This is not a coincidence, and we will come back to this later.

One useful property of eigenspaces is that they contain the 1-dimensional T-invariant subspaces.

Lemma 5.1.10. *Let V be a vector space and let $T \in \mathcal{L}(V)$ be an operator. Then if U is an 1-dimensional T-invariant subspace, there exists an eigenvalue λ such that $U \subseteq \mathrm{E}(\lambda, T)$.*

Proof. Since U is 1-dimensional, for all $0 \neq v \in U$ we have $U = \mathrm{span}(v)$. Fix such a $v \in U$. Then by T-invariance, $Tv \in U$ and so $Tv = \lambda v$ for some $\lambda \in \mathbf{F}$. Now, for every $w \in U$ there exists μ with $w = \mu v$, and hence $Tw = \mu Tv = \mu\lambda v = \lambda w$. This proves that U is contained in $\mathrm{E}(\lambda, T)$. □

Observe that the definition of $\mathrm{E}(\lambda, T)$ makes sense even if λ is not an eigenvalue, and that Lemma 5.1.8 is true for all $\lambda \in \mathbf{F}$, not only for eigenvalues of T. Actually, we can use $\mathrm{E}(\lambda, T)$ to characterise eigenvalues.

Proposition 5.1.11. *Let V be a vector space and let $T \in \mathcal{L}(V)$ be an operator. Then for $\lambda \in \mathbf{F}$ the following are equivalent.*

I. *λ is an eigenvalue of T;*

II. *$(T - \lambda \mathrm{Id}_V)$ is not injective;*

III. $\dim(\mathrm{E}(\lambda, T)) \geq 1$.[1]

If V is finite dimensional, then the above conditions are also equivalent to

[1] By $\dim(U) \geq 1$ we mean that either U is finite dimensional with $\dim(U) \geq 1$, or U is infinite dimensional.

IV. $(T - \lambda \operatorname{Id}_V)$ *is not surjective;*

V. $(T - \lambda \operatorname{Id}_V)$ *is not invertible.*

Proof. Let $\lambda \in \mathbf{F}$. Then

$$\begin{aligned} \lambda \text{ is an eigenvalue of } T &\iff \exists v \neq 0, Tv = \lambda v \\ &\iff \exists v \neq 0, (T - \lambda \operatorname{Id}_V)v = 0 \\ &\iff \ker(T - \lambda \operatorname{Id}_V) \neq \{0\}. \end{aligned}$$

The last condition is equivalent both to the non-injectivity of $T - \lambda \operatorname{Id}_V$ and to the fact that $\{0\} \neq \ker(T - \lambda \operatorname{Id}_V) = \mathrm{E}(\lambda, T)$. But $\mathrm{E}(\lambda, T) \neq \{0\}$ if and only if $\dim(\mathrm{E}(\lambda, T)) \geq 1$.

If V is finite dimensional, then Conditions II, IV and V are all equivalent by the fundamental theorem of linear algebra (Theorem 3.1.33). □

Exercise 5.1.12. Let $T \in \mathcal{L}(\mathbf{F}^2)$ be the linear map $T\begin{bmatrix} w \\ z \end{bmatrix} = \begin{bmatrix} z \\ -w \end{bmatrix}$. Find the eigenvalues and eigenvectors of T for $\mathbf{F} = \mathbf{R}$ and for $\mathbf{F} = \mathbf{C}$.

Solution. We are looking at $\lambda \in \mathbf{F}$ such that the equation $\lambda\begin{bmatrix} w \\ z \end{bmatrix} = T\begin{bmatrix} w \\ z \end{bmatrix} = \begin{bmatrix} z \\ -w \end{bmatrix}$) admits a non-zero solution. But this equation is equivalent to the system

$$\begin{cases} \lambda w = z, \\ \lambda z = -w. \end{cases}$$

This system implies that $(1 + \lambda^2)w = 0$.

If $\mathbf{F} = \mathbf{R}$ the only possibility to solve $(1 + \lambda^2)w = 0$ is to have $w = 0$ and hence $z = 0$. That is, if $\mathbf{F} = \mathbf{R}$, then T has no eigenvalues (and no eigenvectors).

Now, if $\mathbf{F} = \mathbf{C}$, both $\lambda = \mathrm{i}$ and $\lambda = -\mathrm{i}$ are eigenvalues of T and we have $\mathrm{E}(\mathrm{i}, T) = \left\{ \begin{bmatrix} w \\ \mathrm{i}w \end{bmatrix} \mid w \in \mathbf{C} \right\}$ while $\mathrm{E}(-\mathrm{i}, T) = \left\{ \begin{bmatrix} w \\ -\mathrm{i}w \end{bmatrix} \mid w \in \mathbf{C} \right\}$. □

As we have just seen, operators on real vector spaces do not necessarily have eigenvalues. It turns out that operators on complex vector spaces do always have eigenvalues (and eigenvectors). This makes complex linear algebra easier than real linear algebra.

Theorem 5.1.13.

Let $V \neq \{0\}$ be a non-trivial finite dimensional vector space over $\mathbf{C}$ and let $T \in \mathcal{L}(V)$ be an operator. Then T has at least one eigenvalue.

Before proving this theorem, recall that if $T \in \mathcal{L}(V)$ is an operator and $p(t) = a_0 + a_1 t + \cdots + a_n t^n \in \mathcal{P}\mathbf{F}$, then $p(T)$ is the operator $p(T) = a_0 \operatorname{Id}_V + a_1 T + \cdots + a_n T^n \in \mathcal{L}(V)$.

Proof. Let $m > 0$ be the dimension of V and choose any non-zero vector v. Then the list

$$v, Tv, T^2 v, \ldots, T^m v$$

has $m+1$ elements and hence is not linearly independent. Therefore, some linear combination (with not all coefficients equal to 0) of the above vectors equals 0:

$$\lambda_0 v + \lambda_1 Tv + \cdots + \lambda_m T^m v = 0$$

with the λ_j in $\mathbf{C}$ not all zeros.

Equivalently, there exists a non-zero polynomial $p(t) = \lambda_0 + \lambda_1 t + \cdots + \lambda_m t^m$ such that $p(T)v = 0$. Take such a polynomial $p(t)$ of minimal degree. Observe that since $v \neq 0$, the polynomial $p(t)$ is non-constant.

By the fundamental theorem of algebra, $p(t)$ has at least one complex root $\lambda \in \mathbf{C}$. In other words, there exists a polynomial $q \in \mathcal{P}(\mathbf{C})$ (non-zero, but possibly constant) such that $p(t) = (t-\lambda)q(t)$. This implies that $0 = p(T)v = (T - \lambda \mathrm{Id}_V)(q(T)v)$. We have $\deg(q) = \deg(p) - 1$, which by minimality implies that $q(T)v \neq 0$. We have just proved that $T(q(T)v) = \lambda(q(T)v)$ with $q(T)v \neq 0$. So λ is an eigenvalue of T with eigenvector $q(T)v$. □

Remark 5.1.14.

Theorem 5.1.13 is not true for infinite dimensional vector spaces over $\mathbf{C}$. For example, let $V = \mathcal{P}(\mathbf{C})$ and let $T(p) = xp(x)$ be the multiplication by x. Then T has no eigenvalues. Indeed, suppose by contradiction that λ is an eigenvalue with eigenvector $p \neq 0$ of degree d. Then $\lambda p(x) = Tp(x) = xp(x)$. But the left hand side has degree d while the right hand side has degree $d+1$ which is absurd.

Corollary 5.1.15. *Let V be a finite dimensional vector space over $\mathbf{C}$ and let $T \in \mathcal{L}(V)$ be an operator. If $\dim(V) \geq 2$, then T has an invariant subspace which is neither $\{0\}$ nor V.*

Proof. Let λ be an eigenvalue and let v be any eigenvector. Then $\mathrm{span}(v)$ is a T-invariant subspace of dimension 1. □

Remark 5.1.16.

The above corollary is not true if we replace $\mathbf{C}$ by $\mathbf{R}$. Indeed, a rotation of angle $\pi/2$ in $\mathbf{R}^2$ has only $\{0\}$ and $\mathbf{R}^2$ has invariant subspaces.

Lemma 5.1.17. *Let $T \in \mathcal{L}(V)$ be an operator. Suppose that v_1 and v_2 are two eigenvectors, corresponding to the eigenvalues λ_1 and λ_2 respectively. If $\lambda_1 \neq \lambda_2$ the vectors v_1 and v_2 are linearly independent.*

Proof. Suppose that

$$0 = \mu_1 v_1 + \mu_2 v_2 \tag{5.1}$$

for some $\mu_1, \mu_2 \in \mathbf{F}$. On one hand, if we multiply both sides of Equation (5.1) by λ_1 we have

$$0 = \mu_1 \lambda_1 v_1 + \mu_2 \lambda_1 v_2. \tag{5.2}$$

On the other hand, applying T to both sides of Equation (5.1) gives us

$$\begin{aligned} 0 = T0 &= T(\mu_1 v_1 + \mu_2 v_2) \\ &= \mu_1 \lambda_1 v_1 + \mu_2 \lambda_2 v_2. \end{aligned}$$

Substracting this to Equation (5.2) we obtain

$$\mu_2(\lambda_1 - \lambda_2)v_2 = 0.$$

Since $v_2 \neq 0$ and $\lambda_1 - \lambda_2 \neq 0$ we conclude that $\mu_2 = 0$. A similar argument shows that $\mu_1 = 0$. We conclude that v_1 and v_2 are linearly independent. □

As an easy but important consequence of the above lemma we obtain the following generalisation.

Theorem 5.1.18.

Let $T \in \mathcal{L}(V)$ be an operator. Suppose that $v_1, \dots, v_l$ are k eigenvectors, corresponding to the eigenvalues $\lambda_1, \dots, \lambda_k$ respectively. If the λ_j are pairwise distinct, then $v_1, \dots, v_k$ is a linearly independent list.

Proof. The proof is by induction. If $k = 1$, then any eigenvector v is a non-zero vector and therefore (v) is a linearly independent list. If $k = 2$, this is the lemma.

Now suppose that $k \geq 3$ and that the statement is proven for all lists of $m < k$ eigenvectors corresponding to distinct eigenvalues. Suppose by contradiction that $v_1, \dots, v_k$ is not linearly independent. Therefore, by Lemma 2.4.36 there exists $j \in \{1, \dots, k\}$ such that $v_j \in \operatorname{span}(v_1, \dots, v_{j-1})$. By induction hypothesis, j cannot be smaller than k and therefore we have

$$v_k = \mu_1 v_1 + \cdots + \mu_{k-1} v_{k-1} \tag{5.3}$$

for some $\mu_1, \dots, \mu_{k-1} \in \mathbf{F}$. By applying T to both sides of Equation (5.3) and comparing with Equation (5.3) multiplied by λ_k we obtain

$$\begin{aligned} \mu_1 \lambda_1 v_1 + \cdots + \mu_{k-1} \lambda_{k-1} v_{k-1} &= Tv_k = \lambda_k v_k \\ &= \mu_1 \lambda_k v_1 + \cdots + \mu_{k-1} \lambda_k v_{k-1}. \end{aligned}$$

Therefore,

$$0 = \mu_1(\lambda_1 - \lambda_k)v_1 + \cdots + \mu_{k-1}(\lambda_{k-1} - \lambda_k)v_{k-1}$$

and we conclude that all the μ_j are 0 and hence that $v_k = 0$ which is absurd. □

We can use Theorem 5.1.18 to better understand the sum of the eigenspaces.

Corollary 5.1.19. *Let $T \in \mathcal{L}(V)$ be an operator and let $\lambda_1, \dots, \lambda_k$ be pairwise distinct eigenvalues of T. Then the sum $\mathrm{E}(\lambda_1, T) + \cdots + \mathrm{E}(\lambda_k, T)$ is a direct sum and*

$$\dim(\mathrm{E}(\lambda_1, T)) + \cdots + \dim(\mathrm{E}(\lambda_k, T)) \leq \dim(V).$$

Moreover, if V is finite dimensional, the equality $\dim(\mathrm{E}(\lambda_1, T)) + \cdots + \dim(\mathrm{E}(\lambda_k, T)) = \dim(V)$ holds if and only if V is the direct sum of the $\mathrm{E}(\lambda_j, T)$.

Proof. We will write the proof for V finite dimensional. The general case is similar.

Let $0 = u_1 + \cdots + u_k$ with $u_j \in \mathrm{E}(\lambda_i, T)$. By linear independence, (Theorem 5.1.18), all the u_j are 0. We hence conclude that the sum of the $\mathrm{E}(\lambda_j, T)$ is direct.

Since the $\mathrm{E}(\lambda_j, T)$ are in direct sum we have

$$\dim\left(\sum_{j=1}^{k} \dim(\mathrm{E}(\lambda_j, T))\right) = \dim\left(\bigoplus_{j=1}^{k} \mathrm{E}(\lambda_j, T)\right) \leq \dim(V).$$

Since V is finite dimensional, we have equality in the above inequation if and only if $\bigoplus_{j=1}^{k} \mathrm{E}(\lambda_j, T) = V$. □

Corollary 5.1.20. *Let $T \in \mathcal{L}(V)$ be an operator. Then T has at most $\dim(V)$ distinct eigenvalues.*

Proof. We will write the proof for V finite dimensional. The general case is similar.

Let $\lambda_1, \ldots, \lambda_k$ be a complete list of eigenvalues for T. Then for all $j \in \{1, \ldots, k\}$ we have $\dim \mathrm{E}(\lambda_j, T) \geq 1$. Therefore,

$$k \leq \sum_{j=1}^{k} \dim \mathrm{E}(\lambda_j, T) \leq \dim(V).$$ □

Example 5.1.21. Let S_θ be the reflection across the line L from Example 5.0.1. Then v_1 is an eigenvector of eigenvalue 1, while v_2 is an eigenvector with eigenvalue $-1 \neq 1$. They are linearly independent as announced by Lemma 5.1.17. Moreover, we have $\dim(\mathbf{R}^2) = 2 = 1 + 1 = \dim(\mathrm{E}(1, S_\theta)) + \dim(\mathrm{E}(-1, S_\theta))$ and $\mathbf{R}^2 = \mathrm{E}(1, S_\theta) \oplus \mathrm{E}(-1, S_\theta)$ as predicted by Corollary 5.1.19. Finally, 1 and -1 are the only eigenvalues of S_θ by Corollary 5.1.20, but this can also be directly checked by hand.

5.1.3 Diagonalizability

Standing assumption

In this subsection, V will always be a *finite dimensional* vector space.

One of the very nice feature of Example 5.0.1 is the existence of a basis $\mathscr{B} = (v_1, v_2)$ such that $[S_\theta]_{\mathscr{B}}^{\mathscr{B}}$ is diagonal. If we write $\mathscr{E}$ for the standard basis and compare

$$[S_\theta]_{\mathscr{B}}^{\mathscr{B}} = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \qquad [S_\theta]_{\mathscr{E}}^{\mathscr{E}} = \begin{bmatrix} \cos 2\theta & \sin 2\theta \\ \sin 2\theta & -\cos 2\theta \end{bmatrix},$$

it is clear that the left expression is easier to use for computations than the right one.

Definition 5.1.22.

Let V be a finite dimensional vector space, of dimension m. An operator T is

diagonalisable if there exists a basis $\mathscr{B} = (v_1, \dots, v_m)$ of V such that

$$[T]_{\mathscr{B}}^{\mathscr{B}} = \underbrace{\begin{bmatrix} \lambda_1 & & \\ & \ddots & \\ & & \lambda_m \end{bmatrix}}_{\text{diagonal matrix}}$$

for some $\lambda_1, \dots, \lambda_m \in \mathbf{F}$.

Remark 5.1.23.

It follows from the definition of $[T]_{\mathscr{B}}^{\mathscr{B}}$ that the operator $T \in \mathcal{L}(V)$ is diagonalisable if and only if there exists a basis $\mathscr{B} = (v_1, \dots, v_m)$ and scalars $\lambda_1, \dots, \lambda_m \in \mathbf{F}$ with $Tv_j = \lambda_j v_j$. That is, T is diagonalisable if and only if there exists a basis $\mathscr{B} = (v_1, \dots, v_m)$ of eigenvectors (with eigenvalues $\lambda_1, \dots, \lambda_m \in \mathbf{F}$).

As we just discussed, the diagonalisability of an operator is linked to its eigenvalues. But it can also be characterised by its eigenspaces.

Theorem 5.1.24.

Let V be an m-dimensional vector space and let $T \in \mathcal{L}(V)$ be an operator. Let $\lambda_1, \dots, \lambda_k$ be the distinct eigenvalues of T (so $k \leq m$ by Corollary 5.1.20). Then the following are equivalent.

I. T is diagonalisable;

II. There exists a basis of V consisting of eigenvectors of T;

III. There exists 1-dimensional T-invariant subspaces $U_1, \dots, U_m$ such that $V = U_1 \oplus \cdots \oplus U_m$;

IV. $V = \mathrm{E}(\lambda_1, T) \oplus \cdots \oplus \mathrm{E}(\lambda_k, T)$;

V. $\dim(V) = \sum_{j=1}^{k} \dim(\mathrm{E}(\lambda_i, T))$.

Proof. "I $\iff$ II and IV $\iff$ V" These are Remark 5.1.23 and Corollary 5.1.19.

"II$\Rightarrow$III" Suppose $\mathscr{B} = (v_1, \dots, v_m)$ is a basis of eigenvectors and let $U_j := \mathrm{span}(v_j)$ for $j \in \{1, \dots, m\}$. Each of the U_j is a T-invariant subspace of dimension 1. Since $\mathscr{B}$ is a basis, it is also a linearly independent list. Therefore, the sum $U_1 + \cdots + U_m \subseteq V$ is direct. Finally, $m \leq \dim(U_1 \oplus \cdots \oplus U_m) \leq \dim(V) = m$, which implies $V = U_1 \oplus \cdots \oplus U_m$.

"III$\Rightarrow$IV" Each U_j is a T-invariant subspace of dimension 1, and hence is contained in a eigenspace. Up to reordering, we can suppose that $U_1 \oplus \cdots \oplus U_{r_1} \subseteq \mathrm{E}(\lambda_1, T)$, $U_{r_1+1} \oplus \cdots \oplus U_{r_2} \subseteq \mathrm{E}(\lambda_2, T)$ etc. for some $1 \leq r_1 < r_2 < \cdots < r_k = m$. We conclude that

$$V = U_1 \oplus \cdots \oplus U_m \subseteq \mathrm{E}(\lambda_1, T) + \cdots + \mathrm{E}(\lambda_k, T) \subseteq V,$$

and thus V is the sum of the $\mathrm{E}(\lambda_j, T)$. This sum is direct by Corollary 5.1.19.

"IV⇒II" For each $j \in \{1, \dots, k\}$, choose a basis $\mathscr{B}_j$ for $\mathrm{E}(\lambda_j, T)$. On one hand, the family $\mathscr{B} := \mathscr{B}_1 \cup \cdots \cup \mathscr{B}_k$ is spanning since V is the sum of the $\mathrm{E}(\lambda_j, T) = \mathrm{span}(\mathscr{B}_j)$. On the other hand, the $\mathscr{B}_j$ being linearly independent families and the sum $\mathrm{E}(\lambda_1, T) \oplus \cdots \oplus \mathrm{E}(\lambda_k, T)$ being direct imply that $\mathscr{B}$ is a linearly independent family. Altogether, $\mathscr{B}$ is a basis of V consisting of eigenvectors of T. □

Let us work through some of these equivalences on a concrete case.

Example 5.1.25. Let $V = \mathbf{R}^3$ and let $\mathscr{E} = (e_1, e_2, e_3)$ be the standard basis. Let T the operator represented in the standard basis by

$$[T]_{\mathscr{E}}^{\mathscr{E}} = \begin{bmatrix} 4 & & \\ & 5 & \\ & & 4 \end{bmatrix}.$$

Then T is diagonalisable (I), with eigenvalues 4 and 5. Moreover, e_1, e_2 and e_3 are all eigenvectors (II), corresponding respectively to the eigenvalues 4, 5 and 4.

If we put $U_j := \mathrm{span}(e_j)$, then $U_1 = \{[x, 0, 0]^T \mid x \in \mathbf{R}\}$ is the x-axis, U_2 is the y-axis and U_3 is the z-axis. All the U_j are 1 dimensional invariant subspaces and we indeed have $\mathbf{R}^3 = U_1 \oplus U_2 \oplus U_3$ (III).

Now, since both e_1 and e_3 have the same eigenvalue 4, we write (IV)

$$\mathbf{R}^3 = (U_1 \oplus U_3) \oplus U_2 = \mathrm{E}(4, T) \oplus \mathrm{E}(5, T).$$

Finally, $\mathrm{E}(4, T) = U_1 \oplus U_3 = \{[x, 0, z]^T \mid x, z \in \mathbf{R}\}$ is of dimension 2 while $\mathrm{E}(5, T) = U_3$ is of dimension 1. So we indeed have $\dim(\mathbf{R}^3) = 3 = 2 + 1 = \dim(\mathrm{E}(4, T)) + \dim(\mathrm{E}(5, T))$ (V).

Using Theorem 5.1.24, one can exhibit operators that are not diagonalisable, even for $\mathbf{F} = \mathbf{C}$.

Exercise 5.1.26. Let $T \in \mathcal{L}(\mathbf{C}^2)$ be defined by $T\begin{bmatrix} w \\ z \end{bmatrix} := \begin{bmatrix} z \\ 0 \end{bmatrix}$. Is T diagonalisable?

Solution. First, we find all eigenvalues of T. Let $\lambda\begin{bmatrix} w \\ z \end{bmatrix} = T\begin{bmatrix} w \\ z \end{bmatrix} = \begin{bmatrix} z \\ 0 \end{bmatrix}$. Then we have

$$\begin{cases} \lambda w = z, \\ \lambda z = 0. \end{cases}$$

This implies that $\lambda^2 w = 0$ and therefore that $\lambda = 0$, as otherwise $w = z = 0$. Therefore, 0 is the only eigenvalue of T. Moreover, $\mathrm{E}(0, T) = \ker(T - 0\,\mathrm{Id}) = \ker(T) = \{\begin{bmatrix} w \\ 0 \end{bmatrix} \mid w \in \mathbf{C}\}$. We hence have $\dim(\mathbf{C}^2) = 2 > 1 = \dim(\mathrm{E}(0, T))$. We conclude by Theorem 5.1.24 that T is not diagonalisable. □

Theorem 5.1.24 says that T is diagonalisable if, and only if, it has enough linearly independent eigenvectors. Using this, one can show that having enough distinct eigenvalues is a sufficient condition for T being diagonalisable.

Corollary 5.1.27. *Let V be a finite dimensional vector space and let $T \in \mathcal{L}(V)$ be an operator. If T has $\dim(V)$ distinct eigenvalues, then it is diagonalisable.*

Proof. Let $m := \dim(V)$ and let $\lambda_1, \dots, \lambda_m$ be the eigenvalues of T. Then all the $\mathrm{E}(\lambda_j, T)$ have dimension at leat 1 by Proposition 5.1.11 and therefore V is the direct sum of the $\mathrm{E}(\lambda_j, T)$ by Corollary 5.1.19. We conclude by Theorem 5.1.24. □

The converse of the above proposition is false, as demonstrated by $T = \mathrm{Id}_V$ which has only one eigenvalue (1) despite being diagonalisable.

Until now, we have seen conditions that imply (or are equivalent to) diagonalisability. One important consequence of diagonalisability is the following more precise version of the fundamental theorem of linear maps (Theorem 3.1.33).

Lemma 5.1.28. *Let V be a finite dimensional vector space and let $T \in \mathcal{L}(V)$ be an operator. If T is diagonalisable, then $V = \mathrm{Im}(T) \oplus \ker(T)$.*

Proof. Let $\mathscr{B} = (v_1, \dots, v_m)$ be a basis for which

$$[T]^{\mathscr{B}}_{\mathscr{B}} = \begin{bmatrix} \lambda_1 & & \\ & \ddots & \\ & & \lambda_m \end{bmatrix}.$$

Up to reordering the v_j, one can suppose that $\lambda_1 = \cdots = \lambda_k = 0$ while $\lambda_{k+1}, \dots, \lambda_n$ are non-zero for $k \in \{0, m, \dots,\}$. Then $\ker(T) = \mathrm{span}(v_1, \dots, v_k)$ and $\mathrm{Im}(T) = \mathrm{span}(v_{k+1}, \dots, v_m)$.

Observe that if no λ_j are 0, then $k = 0$ and we indeed have $V = \mathrm{Im}(T) \oplus \{0\}$ since $\ker(T) = \mathrm{span}(\varnothing) = \{0\}$. Similarly, if all λ_j are 0, then $V = \{0\} \oplus \ker(T)$. □

Question 5.1.29. Can you find an operator T such that $\mathrm{Im}(T) \oplus \ker(T) \subsetneq V$?
Hint: T cannot be diagonalisable.

Infinite dimensional vector spaces

If T is an operator on an infinite dimensional vector space V, then the equivalences II $\iff$ III $\iff$ IV of Theorem 5.1.24 are still true. Some people use them to define the diagonalisability of T. That is, $T \in \mathcal{L}(V)$ is said to be **diagonalisable** if there exists a basis of V consisting of eigenvectors of T. While the infinite dimensional situation is much more complex than the finite dimensional one, some results remain true, as for example Lemma 5.1.28.

5.1.4 Nilpotent operators

In this subsection, we introduce a new kind of operators that have a special relationship with the eigenvalue 0. This definition will be useful to show some of the forthcoming results.

Definition 5.1.30.

An operator $T \in \mathcal{L}(V)$ is **nilpotent** if there exists $k \in \mathbf{N}$ such that $T^k = 0_{\mathcal{L}(V)}$.

The 0 operator is of course nilpotent, but it is easy to find other examples.

Example 5.1.31. The differentiation operator $D \in \mathcal{L}(\mathcal{P}(\mathbf{R})_m)$ defined by $Dp := p'$ is nilpotent. Indeed, $D^m p = p^{(m)} = 0$ for every polynomial of degree at most m.

However, the differentiation operator $D \in \mathcal{L}(\mathcal{P}(\mathbf{R}))$ is *not* nilpotent. Indeed, for every k we have $D^k(x^{k+1}) = k! \neq 0$.

Example 5.1.32. For $\lambda \in \mathbf{F}$, define an operator $T \in \mathcal{L}(\mathbf{F}^2)$ by

$$Tv = \begin{bmatrix} 0 & \lambda \\ 0 & 0 \end{bmatrix} v.$$

If $\lambda = 1$, this is the operator from Exercise 5.1.26. Using the matrix, one can check that $T^2 = 0$, and hence that T is nilpotent.

More generally, if $T \in \mathcal{L}(\mathbf{F}^m)$ is represented by a matrix with zeros on and below the diagonal, it is nilpotent. In fact, we will soon show that all nilpotent operators on finite dimensional vector spaces appear in this form. In order to do that, we will need a few technical lemmas about kernels.

Lemma 5.1.33. *Let V be a vector space and let $T \in \mathcal{L}(V)$ be an operator.*

1. $\{0\} = \ker(T^0) \subseteq \ker(T^1) \subseteq \cdots \subseteq \ker(T^j) \subseteq \ker(T^{j+1}) \subseteq \cdots$;
2. *If there exists k with $\ker(T^{k+1}) = \ker(T^k)$, then $\ker(T^n) = \ker(T^k)$ for all $n \geq k$.*

Proof. For the first assertion, suppose that $v \in \ker(T^j)$ for some non-negative integer j. Then $T^{j+1}v = T(T^j v) = T0 = 0$ and therefore $v \in \ker(T^{j+1})$ as desired.

For the second assertion, we want to prove that $\ker(T^{k+j}) = \ker(T^{k+j+1})$ for every non-negative integer j. We already know that the left to right inclusion is true. To prove the other inclusion, let v be in $\ker(T^{k+j+1})$. Then $T^{k+1}(T^j v) = T^{k+j+1}v = 0$ and thus $T^j v$ is in $\ker(T^{k+1}) = \ker(T^k)$. Therefore, $T^{k+j}v = T^k(T^j v) = 0$, which shows that $v \in \ker(T^{k+j})$. □

The above result is particularly useful for finite dimensional spaces. Indeed, in this case we have the following.

Lemma 5.1.34. *Let V be a finite dimensional vector space. Then* $\ker(T^{\dim(V)}) = \ker(T^{\dim(V)+1}) = \ker(T^{\dim(V)+2}) = \cdots$.

Proof. By the first assertion of the last lemma, we have

$$0 \leq \dim\big(\ker(T)\big) \leq \cdots \leq \dim\big(\ker(T^{\dim(V)})\big) \leq \dim\big(\ker(T^{\dim(V)+1})\big) \leq \dim(V).$$

By the pigeonhole principle,[2] at least one of these inequalities is an equality. Therefore, there exists $k \leq \dim(V)$ with $\dim(\ker(T^k)) = \dim(\ker(T^{k+1}))$. We conclude using the second assertion of Lemma 5.1.33. □

To go further

Results similar to Lemmas 5.1.33 and 5.1.34 hold for $\mathrm{Im}(T^j)$, but with the inclusions reversed. More precisely, for any vector space T and any operator, one always have

$$V = \mathrm{Im}(T^0) \supseteq \mathrm{Im}(T) \supseteq \mathrm{Im}(T^2) \supseteq \cdots \supseteq \mathrm{Im}(T^j) \subseteq \mathrm{Im}(T^{j+1}) \supseteq \cdots$$

Moreover, if there exists k with $\mathrm{Im}(T^k) = \mathrm{Im}(T^{k+1})$, then $\mathrm{Im}(T^k) = \mathrm{Im}(T^n)$ for all $n \geq k$. Finally, if V is finite dimensional, then $\mathrm{Im}(T^{\dim(V)}) = \mathrm{Im}(T^n)$ for all $n \geq \dim(V)$. The proofs of these statements are similar to the proofs of Lemmas 5.1.33 and 5.1.34.

Using Lemma 5.1.34, one obtain a variations of Lemma 5.1.28.

Proposition 5.1.35. *Let V be a finite dimensional vector space and let T be an operator on V. Then*

$$V = \ker(T^{\dim(V)}) \oplus \mathrm{Im}(T^{\dim(V)}).$$

Proof. Let $m \coloneqq \dim(V)$. We first prove that the sum is direct, that is:

$$\ker(T^m) \cap \mathrm{Im}(T^m) = \{0\}. \tag{5.4}$$

Suppose v is in the intersection $\ker(T^m) \cap \mathrm{Im}(T^m)$. Then $T^m v = 0$ and there exists $u \in V$ with $T^m u = v$. If we apply T^m to both sides of the last equation, we obtain $T^{2m}u = T^m v = 0$. Therefore u is in $\ker(T^{2m}) = \ker(T^m)$ by Lemma 5.1.34 and $v = T^m u = 0$.

Equation (5.4) implies that $\ker(T^m) + \mathrm{Im}(T^m)$ is a direct sum. By Theorem 3.1.33 we have

$$\dim(\ker(T^m) \oplus \mathrm{Im}(T^m)) = \dim(\ker(T^m)) + \dim(\mathrm{Im}(T^m)) = \dim(V)$$

and we hence conclude that $V = \ker(T^{\dim(V)}) \oplus \mathrm{Im}(T^{\dim(V)})$ as desired. □

Proposition 5.1.36. *Let V be a finite dimensional vector space and let $T \in \mathcal{L}(V)$ be a nilpotent operator. Then $T^{\dim(V)} = 0$.*

Proof. Since T is nilpotent, there exists $k \in \mathbf{N}$ with $T^k = 0$, and thus $\ker(T^k) = V$. If $k \leq \dim(V)$, then $\ker(T^{\dim(V)}) = \ker(T^k) = V$ by Lemma 5.1.33, while if $k \geq \dim(V)$, then $\ker(T^{\dim(V)}) = \ker(T^k) = V$, but this time by Lemma 5.1.34. In both cases, we have $T^{\dim(V)} = 0$. □

[2] Recall that the piegeonhole principle asserts that if we need to distribute l elements among k sets, for some $l > k$, then there is a set containing at least two elements.

As announced after Example 5.1.32, nilpotent operators have a special matrix representation.

Proposition 5.1.37. *Let V be a finite dimensional vector space and let $T \in \mathcal{L}(V)$ be an operator. Then T is nilpotent if and only if there exists a basis $\mathscr{B}$ of V such that*

$$[T]_{\mathscr{B}}^{\mathscr{B}} = \begin{bmatrix} 0 & * & \cdots & * \\ \vdots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & * \\ 0 & \cdots & \cdots & 0 \end{bmatrix}.$$

Proof. "⇒" We have $\ker(T) \subseteq \ker(T^2) \subseteq \cdots \subseteq \ker(T^m) = V$ where $m = \dim(V)$. Moreover, since T is nilpotent it is not injective. In particular, $\ker(T) \neq \{0\}$. So we can start with a basis $\mathscr{B}_1$ of $\ker(T)$ and extend it to a basis $\mathscr{B}_2$ of $\ker(T^2)$ and continue step by step to obtain a basis $\mathscr{B} = (v_1, \ldots, v_m)$ of V. By the above, v_1 is in $\ker(T)$. Therefore, $Tv_1 = 0$ and hence the first column of $[T]_{\mathscr{B}}^{\mathscr{B}}$ contains only 0. More generally, v_j is in $\ker(T^j)$. Therefore, Tv_j is in $\ker(T^{j-1}) \subseteq \operatorname{span}(v_1, \ldots, v_{j-1})$. In other words, $Tv_j = a_{1,j}v_1 + \cdots + a_{j,j-1}v_{j-1}$ for some $a_{l,j} \in \mathbf{F}$. That is, the j^{th} column of $[T]_{\mathscr{B}}^{\mathscr{B}}$ has zeroes on the diagonal and below.

"⇐" Suppose that $A = [T]_{\mathscr{B}}^{\mathscr{B}}$ is an upper triangular $m \times m$ matrix with 0 on the diagonal. Then A^m is the zero matrix, and therefore T^m is the zero operator. □

When $\mathbf{F} = \mathbf{C}$, nilpotent operators can be characterised by their eigenvalues.

Proposition 5.1.38. *Let $\mathbf{F}$ be a field, let $V \neq \{0\}$ be an $\mathbf{F}$-vector space and let $T \in \mathcal{L}(V)$ be an operator.*

1. *If T is nilpotent, then 0 is an eigenvalue of T, and T has no other eigenvalues;*
2. *If $\mathbf{F} = \mathbf{C}$, V is finite dimensional and 0 is the only eigenvalue of T, then T is nilpotent.*

Proof. 1. If T is nilpotent, then $T^k = 0$ for some $k \in \mathbf{N}$, so T is not injective and hence 0 is an eigenvalue. Now, suppose that λ is an eigenvalue of T with eigenvector $v \neq 0$. Then $0 = T^k v = \lambda^k v$. We conclude that $\lambda^k = 0$ and hence that $\lambda = 0$.

2. The proof is postponed to Proposition 5.1.51. □

5.1.5 Generalised eigenvectors

At the end of the chapter on linear maps, we asked

Major Question 3.2.47.

Given V and $T \in \mathcal{L}(V)$, find a basis $\mathscr{B}$ such that $[T]_{\mathscr{B}}^{\mathscr{B}}$ is "as simple as possible" (for example: diagonal, upper triangular, with many zeroes, …).

A first answer to this question was given by Theorem 5.1.24 which asserts that T is diagonalisable if and only if there exists a basis $\mathscr{B}$ of V consisting of eigenvectors of T, if and only if $\dim(V) = \sum_{j=1}^{k} \dim(\mathrm{E}(\lambda_j, T))$, where the sum is taken over all the eigenvalues of T. If T does not have enough eigenvectors, then it is not diagonalisable. But there is still hope we can find a basis $\mathscr{B}$ consisting "almost eigenvectors" such that $[T]_{\mathscr{B}}^{\mathscr{B}}$ is "almost diagonal". See Proposition 5.1.56 for an intermediate result in this direction.

Definition 5.1.39.

Let V be a vector space, let $T \in \mathcal{L}(V)$ be an operator and let $\lambda \in \mathbf{F}$ be a scalar. A non-zero vector v is a **generalised eigenvector** of T corresponding to λ if there exists a positive integer j such that $(T - \lambda \mathrm{Id}_V)^j v = 0$.
For $\lambda \in \mathbf{F}$, its **generalised eigenspace** is the set

$$\mathrm{G}(\lambda, T) := \{v \in V \mid \exists j, (T - \lambda \mathrm{Id}_V)^j v = 0\}.$$

Given a generalised eigenvector v, one can always obtain an eigenvector w by applying $T - \lambda \mathrm{Id}_V$ to v enough time, as demonstrated by the next result.

Lemma 5.1.40. *Let V be a vector space and let $T \in \mathcal{L}(V)$ be an operator. Let v be a generalised eigenvector corresponding to $\lambda \in \mathbf{F}$. Then there exists $j \in \mathbf{N}$ such that $w := (T - \lambda \mathrm{Id}_V)^j v$ is an eigenvector of T corresponding to λ. In particular, λ is an eigenvalue of T.*

Proof. Let k be the smallest non-negative integer such that $(T - \lambda \mathrm{Id}_V)^k v \neq 0$. Since $v \neq 0$, such a k always exists. Then $w := (T - \lambda \mathrm{Id}_V)^k v$ is non-zero and $(T - \lambda \mathrm{Id}_V) w = 0$ by minimality of k. □

The following result directly follows from the definition.

Lemma 5.1.41. *For V a vector space, $T \in \mathcal{L}(V)$ and operator and $\lambda \in \mathbf{F}$ (not necessarily an eigenvalue), we have*

$$\mathrm{G}(\lambda, T) = \{0\} \sqcup \{v \in V \mid v \text{ is a generalised eigenvector of } T \text{ corresponding to } \lambda\}.$$

In the last section, we proved some results about kernels. As an interesting consequence of Lemma 5.1.34, we show that generalised eigenspaces are indeed subspaces of V.

Proposition 5.1.42. *Let V be a finite dimensional vector space and let $T \in \mathcal{L}(V)$ be an operator. Then for all $\lambda \in \mathbf{F}$*

$$\mathrm{G}(\lambda, T) = \ker(T - \lambda \mathrm{Id}_V)^{\dim(V)}.$$

In particular, $\mathrm{G}(\lambda, T)$ is a subspace of V.

Proof. It follows from the definition that we have $\mathrm{G}(\lambda, T) = \bigcup_{j \geq 1} \ker(T - \lambda \mathrm{Id}_V)^j$. Using Lemmas 5.1.33 and 5.1.34 we have $\bigcup_{j \geq 1} \ker(T - \lambda \mathrm{Id}_V)^j = \ker(T - \lambda \mathrm{Id}_V)^{\dim(V)}$ which concludes the proof. □

As we just saw, $\mathrm{G}(\lambda, T)$ is a subspace of V and we have $\mathrm{E}(\lambda, T) \subseteq \mathrm{G}(\lambda, T) \subseteq V$. This explains the name of generalised eigenspace. If v is an eigenvector, then the corresponding eigenvalue λ is uniquely determined by the equation $Tv = \lambda v$. For generalised eigenvectors, it is a priori not obvious that the corresponding eigenvalue is unique. Fortunately, this is the case if V is finite dimensional.

Lemma 5.1.43. *Let V be a finite dimensional vector space and let $T \in \mathcal{L}(V)$ be an operator. Then each generalised eigenvector corresponds to a unique eigenvalue.*

Proof. Suppose that v is a generalised eigenvector of T corresponding to the eigenvalues λ and μ. We need to show that $\lambda = \mu$. Let k be the smallest positive integer such that $(T - \mu \operatorname{Id}_V)^k v = 0$, and let $m := \dim(V)$. One can suppose $m \geq 1$, as otherwise there is no generalised eigenvector. Then

$$\begin{aligned} 0 &= (T - \lambda \operatorname{Id}_V)^m v \\ &= \left((T - \mu \operatorname{Id}_V) + (\mu - \lambda) \operatorname{Id}_V\right)^m v \\ &= \sum_{j=0}^{m} b_j (\mu - \lambda)^{m-j} (T - \mu \operatorname{Id}_V)^j v, \end{aligned}$$

where $b_0 = 1$ and the values of the other binomial coefficients b_j do not matter. If we apply the operator $(T - \mu \operatorname{Id}_V)^{k-1}$ to both sides of the above equation we obtain

$$0 = (\mu - \lambda)^m (T - \mu \operatorname{Id}_V)^{k-1} v.$$

By minimality of k, $(T - \mu \operatorname{Id}_V)^{k-1} v \neq 0$ and hence $\mu = \lambda$. □

Exercise 5.1.44. Let $T \in \mathcal{L}(\mathbf{C}^3)$ be the operator defined by $T \begin{bmatrix} z_1 \\ z_2 \\ z_3 \end{bmatrix} := \begin{bmatrix} 4z_2 \\ 0 \\ 5z_3 \end{bmatrix}$. Compute the eigenspaces and generalised eigenspaces for T.

Solution. Let $\mathscr{E} = (e_1, e_2, e_3)$ be the standard basis of $\mathbf{C}^3$. Then

$$A := [T]^{\mathscr{E}}_{\mathscr{E}} = \begin{bmatrix} 0 & 4 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 5 \end{bmatrix}.$$

Then the eigenvalues of T are 0 and 5 (see Subsection 5.2.1 and specifically Lemma 5.2.6 for how to easily compute them). Let us compute the eigenspaces and the generalised eigenspaces of the eigenvalues.

Eigenspace and generalised eigenspace for $\lambda = 0$. We have

$$A - 0 \operatorname{Id} = A, \qquad (A - 0 \operatorname{Id})^3 = A^3 = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 5^3 \end{bmatrix}.$$

Therefore,

$$\mathrm{E}(0,T) = \ker T = \left\{ \begin{bmatrix} z_1 \\ 0 \\ 0 \end{bmatrix} \,\middle|\, z_1 \in \mathbf{C} \right\}, \quad \mathrm{G}(0,T) = \ker T^3 = \left\{ \begin{bmatrix} z_1 \\ z_2 \\ 0 \end{bmatrix} \,\middle|\, z_1, z_2 \in \mathbf{C} \right\}.$$

So $\mathrm{E}(0,T)$ is of dimension 1 and hence a strict subspace of $\mathrm{G}(0,T)$ which is of dimension 2.

Eigenspace and generalised eigenspace for $\lambda = 5$. We have

$$A - 5\,\mathrm{Id} = \begin{bmatrix} -5 & 4 & 0 \\ 0 & -5 & 0 \\ 0 & 0 & 0 \end{bmatrix}, \qquad (A - 5\,\mathrm{Id})^3 = A^3 = \begin{bmatrix} -5^3 & 300 & 0 \\ 0 & -5^3 & 0 \\ 0 & 0 & 0 \end{bmatrix}.$$

Therefore,

$$\mathrm{E}(5,T) = \ker(T - 5\,\mathrm{Id}) = \left\{ \begin{bmatrix} 0 \\ 0 \\ z_3 \end{bmatrix} \,\middle|\, z_3 \in \mathbf{C} \right\},$$
$$\mathrm{G}(5,T) = \ker(T - 5\,\mathrm{Id})^3 = \left\{ \begin{bmatrix} 0 \\ 0 \\ z_3 \end{bmatrix} \,\middle|\, z_3 \in \mathbf{C} \right\}.$$

So $\mathrm{E}(5,T) = \mathrm{G}(5,T)$ is of dimension 1.

Altogether, we have

$$\mathrm{E}(0,T) \oplus \mathrm{E}(5,T) \subsetneq \mathrm{G}(0,T) \oplus \mathrm{G}(5,T) = \mathbf{C}^3.$$

□

Some of the results of Subsection 5.1.2 for eigenvectors still hold for generalised eigenvectors.

Lemma 5.1.45. *Let V be a finite dimensional vector space and let $T \in \mathcal{L}(V)$ be an operator. Suppose that v_1 and v_2 are two generalised eigenvectors, corresponding to the eigenvalues λ_1 and λ_2 respectively. If $\lambda_1 \neq \lambda_2$ the vectors v_1 and v_2 are linearly independent.*

Proof. Let μ_1 and μ_2 be two scalars such that

$$0 = \mu_1 v_1 + \mu_2 v_2. \tag{5.5}$$

We want to show that $\mu_1 = \mu_2 = 0$. Let $m := \dim(V)$, let $k := \max\{l \mid v_1 \notin \ker(T - \lambda_1 \mathrm{Id}_V)^l\} \geq 0$ and let $w := (T - \lambda_1 \mathrm{Id}_V)^k v_1 \neq 0$. By maximality of k we have $(T - \lambda_1 \mathrm{Id}_V)w = 0$. That is, $w \neq 0$ is an eigenvector of T, with eigenvalue λ_1. Let $f(t) =$

$(t-\lambda_1)^k$ and let $g(t) = (t-\lambda_2)^m$. Both are polynomials in $\mathcal{P}(\mathbf{F})$. Now, we apply $f(T)g(T) = g(T)f(T)$ to Equation (5.5) and obtain

$$\begin{aligned} 0 &= \mu_1(T-\lambda_2 \operatorname{Id}_V)^m(T-\lambda_1 \operatorname{Id}_V)^k v_1 + \mu_2(T-\lambda_1 \operatorname{Id}_V)^k(T-\lambda_2 \operatorname{Id}_V)^m v_2 \\ &= \mu_1(T-\lambda_2 \operatorname{Id}_V)^m w + 0. \end{aligned}$$

Since $w \neq 0$ is an eigenvector corresponding to λ_1, and since $\lambda_1 \neq \lambda_2$, w is not a generalised eigenvector corresponding to λ_2. We conclude that $(T-\lambda_2 \operatorname{Id}_V)^m w \neq 0$ and hence that $\mu_1 = 0$. A similar argument shows that $\mu_2 = 0$ and therefore that v_1 and v_2 are linearly independent. □

The above Lemma can easily be generalised to the case of finite families of vectors. The proof is left to the reader.

Theorem 5.1.46.

Let V be a finite dimensional vector space and let $T \in \mathcal{L}(V)$ be an operator. Suppose that $v_1, \dots, v_k$ are k eigenvectors, corresponding to the eigenvalues $\lambda_1, \dots, \lambda_k$ respectively. If the λ_j are pairwise distincts, then $(v_1, \dots, v_k)$ is a linearly independent list.

We have seen that if T is an operator on V, then both $\operatorname{Im}(T)$ and $\ker(T)$ are T-invariant. We can generalise this.

Lemma 5.1.47. *Let V be a vector space and let $T \in \mathcal{L}(V)$ be an operator. Let $p(t) \in \mathcal{P}(\mathbf{F})$ be any polynomial. Then both $\operatorname{Im}(p(T))$ and $\ker(p(T))$ are T-invariant.*

Proof. Suppose u belongs to $\ker(p(T))$. Then $p(T)u = 0$. Thus

$$(p(T))(Tu) = (p(T)T)u = (Tp(T))u = T(p(T)u) = T0 = 0,$$

where we used the fact that for polynomials $p(t)$ and $q(t)$ we always have $p(t)q(t) = q(t)p(t)$. Hence Tu is in $\ker(p(T))$. So we have just proved that $\ker(p(T))$ is invariant under T as desired.

Suppose u belongs to $\operatorname{Im}(p(T))$. Then there exists $v \in V$ such that $u = p(T)v$. Thus

$$Tu = T(p(T)v) = p(T)(Tv).$$

By the above equation, Tu is still in $\operatorname{Im}(p(T))$, which shows that $\operatorname{Im}(p(T))$ is T-invariant. □

In Corollary 5.1.19, we showed that $\sum_{j=1}^{k} \mathrm{E}(\lambda_j, T)$ is always a direct sum, and a subspace of V. In Theorem 5.1.24, we then showed that $\bigoplus_{j=1}^{k} \mathrm{E}(\lambda_j, T) = V$ if and only T is diagonalisable, if and only if there exists a basis consisting of eigevectors. Theorems 5.1.48 and 5.1.49 will show that even if T is not diagonalisable a similar formula holds for generalised eigenspaces.

Theorem 5.1.48.

Let V be a finite dimensional vector space over $\mathbf{C}$ and let $T \in \mathcal{L}(V)$ be an operator. Then there exists a basis of V consisting of generalised eigenvectors of T.

Proof. We will do an induction on $m := \dim(V)$. Observe that the desired result holds if $m = 0$ as in this (degenerated) case we have no generalised eigenvectors but the empty list is a basis. If $m = 1$, then any non-zero vector is both a basis of V and an eigenvector for T.

Now, suppose that $m \geq 2$ and that the desired result holds for all complex vector spaces of dimension strictly less than m. Let λ be an eigenvalue of T, whose existence is guarantee by Theorem 5.1.13. Applying Proposition 5.1.35 to $T - \lambda \operatorname{Id}_V$ we obtain

$$V = \ker(T - \lambda \operatorname{Id}_V)^m \oplus \operatorname{Im}(T - \lambda \operatorname{Id}_V)^m.$$

On one hand, every non-zero vector in $\ker(T - \lambda \operatorname{Id}_V)^m \neq \{0\}$ is a generalised eigenvector of T. Hence, any basis $\mathscr{B}$ of $\ker(T - \lambda \operatorname{Id}_V)^m \neq \{0\}$ consists of generalised eigenvectors of T. On the other hand, $\ker(T - \lambda \operatorname{Id}_V)^m \neq \{0\}$ as λ is an eigenvalue of T. Therefore, $\operatorname{Im}(T - \lambda \operatorname{Id}_V)^m \neq V$ is of dimension strictly less than m, and is invariant under T (by Lemma 5.1.47 for the polynomial $p(t) = (t - \lambda)^m$). Let $S \in \mathcal{L}(\operatorname{Im}(T - \lambda \operatorname{Id}_V)^m)$ be the restriction of T to $\operatorname{Im}(T - \lambda \operatorname{Id}_V)^m$. By the induction hypothesis applied to the operator S, there exists a basis $\mathscr{C}$ of $\operatorname{Im}(T - \lambda \operatorname{Id}_V)^m$ consisting of generalised eigenvectors of S. Since S is the restriction of T, every generalised eigenvectors of S is also a generalised eigenvector of T. Altogether, $\mathscr{B} \cup \mathscr{C}$ is a basis of V consisting of generalised eigenvectors of T. □

The following theorem makes the link between nilpotent operators and generalised eigenspaces. It also shows why generalised eigenspaces are the right enlargement of eigenspaces.

Theorem 5.1.49.

Let V be a finite dimensional vector space over $\mathbf{C}$, and let $T \in \mathcal{L}(V)$ be an operator. Let $\lambda_1, \dots, \lambda_k$ be the distinct eigenvalues of T. Then

1. *Each of the $\mathrm{G}(\lambda_j, T)$ is a T-invariant subspace;*
2. *$V = \mathrm{G}(\lambda_1, T) \oplus \cdots \oplus \mathrm{G}(\lambda_k, T)$;*
3. *The operator $T_j := (T - \lambda_j \operatorname{Id}_V)\big|_{\mathrm{G}(\lambda_j, T)}$ is a nilpotent operator on $\mathrm{G}(\lambda_j, T)$.*

Proof. 1. We have $\mathrm{G}(\lambda_j, T) = \ker(T - \lambda_j \operatorname{Id}_V)^m$. We conclude by Lemma 5.1.47.

2. Firstly, the sum $\sum_{j=1}^{k} \mathrm{G}(\lambda_j, T)$ is a direct sum since generalised eigenvectors corresponding to distinct eigenvalues are linearly independent the sum. See the proof of Corollary 5.1.19 for more details. Secondly, the existence of a basis of generalised eigenvectors (Theorem 5.1.48) implies that $V = \mathrm{G}(\lambda_1, T) + \cdots + \mathrm{G}(\lambda_k, T)$.

3. By 1, $T_j := T - \lambda_j \operatorname{Id}$ is an operator on $\mathrm{G}(\lambda_j, T)$. It then follows from Proposition 5.1.42 that $T_j^{\dim(\mathrm{G}(\lambda_j,T))}$ is the zero operator on $\mathrm{G}(\lambda_j, T)$, and hence that T_j is nilpotent. □

Remark 5.1.50.

As an easy corollary, one can finally shows that an operator whose eigenvalues are all 0 is nilpotent. This finishes the proof of Proposition 5.1.38.

Proposition 5.1.51. *Let V be a finite dimensional vector space over $\mathbf{C}$ and let $T \in \mathcal{L}(V)$ be an operator. Suppose that 0 is the only eigenvalue of T. Then T is nilpotent.*

Proof. Since 0 is the only eigenvalue, $T = T - 0\operatorname{Id}_v$ is nilpotent on $V = \mathrm{G}(0, T)$. □

Proposition 5.1.51 is not true for real vector spaces. The reason is that an operator T might have only 0 has a real eigenvalues, but other complex eigenvalues.

Example 5.1.52. Let $V = \mathbf{R}^3$ and let

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

Then the characteristic polynomial of A is $\chi_A(t) = t(t^2 + 1)$ and the complex eigenvalues of A are 0, i and $-$i. So the only real eigenvalue of A is 0. However, we have $A \neq 0$,

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

and $A^j = \mathrm{Id}_3 \neq 0$ for all $j \geq 3$. So A is not nilpotent, despite having all its real eigenvalues equal to 0.

As another corollary of Theorem 5.1.49 we have the following, which finishes the proof of Proposition 5.1.38.

Proposition 5.1.53. *Let V be a finite dimensional vector space over $\mathbf{C}$, and let $T \in \mathcal{L}(V)$ be an operator. Then T is diagonalisable if and only if $\mathrm{E}(\lambda, T) = \mathrm{G}(\lambda, T)$ for all $\lambda \in \mathbf{C}$.*

Using (generalised) eigenspaces, one can defined to quantities associated to an eigenvalue λ of an operator T.

Definition 5.1.54.

Let V be a vector space, let $T \in \mathcal{L}(V)$ be an operator and let $\lambda \in \mathbf{F}$ be an eigenvalue of T. The **algebraic multiplicity** of λ in T is defined as

$$\mathrm{m}_{\mathrm{alg}}(\lambda) = \mathrm{m}_{\mathrm{alg}}(\lambda, T) := \dim(\mathrm{G}(\lambda, T)).$$

The **geometric multiplicity** of λ in T is defined as

$$\mathrm{m}_{\mathrm{geo}}(\lambda) = \mathrm{m}_{\mathrm{geo}}(\lambda, T) \coloneqq \dim(\mathrm{E}(\lambda, T)).$$

Clearly, we always have $\mathrm{m}_{\mathrm{geo}}(\lambda) \leq \mathrm{m}_{\mathrm{alg}}(\lambda)$. The following characterisation of diagonalisability for operators on complex vector spaces directly follows from Proposition 5.1.53.

Lemma 5.1.55. *Let V be a finite dimensional complex vector space and let $T \in \mathcal{L}(V)$. Then T is diagonalisable if and only if $\mathrm{m}_{\mathrm{geo}}(\lambda, T) = \mathrm{m}_{\mathrm{alg}}(\lambda, T)$ for all $\lambda \in \mathbf{C}$.*

The name "geometric multiplicity" is because it is related to $\mathrm{E}(\lambda, T)$, which we think of as some geometric invariant of T. The name "algebraic multiplicity" is because we can compute it directly from a polynomial associated to T. We will talk more about this polynomial in the next section.

Before ending this section, let us mention one more use of Theorem 5.1.49. Namely the fact that for operators on complex vector spaces, one can always find a basis $\mathscr{B}$ for which $[T]^{\mathscr{B}}_{\mathscr{B}}$ is particularly nice.

Proposition 5.1.56. *Let $V \neq \{0\}$ be a finite dimensional vector space over $\mathbf{C}$, and let $T \in \mathcal{L}(V)$ be an operator. Then there exists a basis $\mathscr{B}$ for which $[T]^{\mathscr{B}}_{\mathscr{B}}$ is* diagonal by [triangular blocks]. *More precisely, $[T]^{\mathscr{B}}_{\mathscr{B}}$ is of the form (all matrix entries not shown are zero)*

$$[T]^{\mathscr{B}}_{\mathscr{B}} = \begin{bmatrix} \boxed{\begin{matrix} \lambda_1 & & * \\ & \ddots & \\ * & & \lambda_1 \end{matrix}} & & & \\ & \boxed{\begin{matrix} \lambda_2 & & * \\ & \ddots & \\ * & & \lambda_2 \end{matrix}} & & \\ & & \ddots & \\ & & & \boxed{\begin{matrix} \lambda_k & & * \\ & \ddots & \\ * & & \lambda_k \end{matrix}} \end{bmatrix},$$

where the j^{th} diagonal block is an $\mathrm{m}_{\mathrm{alg}}(\lambda_j) \times \mathrm{m}_{\mathrm{alg}}(\lambda_j)$ triangular matrix with λ_j on the diagonal and 0 below the diagonal.

Proof. Let $\lambda_1, \ldots, \lambda_k$ be the distinct eigenvalues of T and let us write $U_j \coloneqq \mathrm{G}(\lambda_j, T)$. For each $j \in \{1, \ldots, k\}$, the restriction $T_j \coloneqq (T - \lambda_j \mathrm{Id}_V)\big|_{U_j}$ is a nilpotent operator on U_j. So by Proposition 5.1.37 there exists a basis $\mathscr{B}_j$ of U_j such that $[T_j]^{\mathscr{B}_j}_{\mathscr{B}_j}$ is a $m_{\lambda_j} \times m_{\lambda_j}$ matrix with zeros on the diagonal and below the diagonal. This implies that $[T|_{U_j}]^{\mathscr{B}_j}_{\mathscr{B}_j}$ is

a $\mathrm{m}_{\mathrm{alg}}(\lambda_j) \times \mathrm{m}_{\mathrm{alg}}(\lambda_j)$ matrix with λ_j on the diagonals and 0 below the diagonal.

$$\left[(T-\lambda_j \operatorname{Id}_V)\big|_{\mathrm{G}(\lambda_j,T)}\right]_{\mathscr{B}_j}^{\mathscr{B}_j} = \begin{bmatrix} 0 & * & \cdots & * \\ & \ddots & \ddots & \vdots \\ & & \ddots & * \\ & & & 0 \end{bmatrix}, \quad \left[T\big|_{\mathrm{G}(\lambda_j,T)}\right]_{\mathscr{B}_j}^{\mathscr{B}_j} = \begin{bmatrix} \lambda_j & * & \cdots & * \\ & \ddots & \ddots & \vdots \\ & & \ddots & * \\ & & & \lambda_j \end{bmatrix}.$$

Let $\mathscr{B} := \mathscr{B}_1 \cup \cdots \cup \mathscr{B}_k$. Since V is a direct sum of the generalised eigenspaces, $\mathscr{B}$ is a basis of V. It then follows from the T-invariance of the U_j that $[T]_{\mathscr{B}}^{\mathscr{B}}$ is diagonal by block, with the j^{th} diagonal block being equal to $[T|_{U_j}]_{\mathscr{B}_j}^{\mathscr{B}_j}$. □

In this subsection, we defined generalised eigenvectors and we have seen that V is a direct sum of generalised eigenspaces. Moreover, we also proved that for operator on complex vector spaces, there exists a basis $\mathscr{B}$ for which $[T]_{\mathscr{B}}^{\mathscr{B}}$ is diagonal by [triangular blocks]. But it is possible to find an even "nicer" (with more zeroes) matrix representation of T. In order to do that, we need to introduce some new tools. The first of them, the characteristic polynomial, will help us to compute eigenvalues.

5.2 Characteristic and minimal polynomials

Standing assumption

In this Section, V will always be a finite dimensional non-zero vector space.

The aim of this section is to define powerful tools, called the characteristic polynomial and the minimal polynomials, that will help us to compute the eigenvalues of an operator. In order to define the characteristic polynomial of T will we use the determinant, and hence the matrix representation of T. We hence start by developing an eigen-theory for matrices similar to the one for operator.

5.2.1 Characteristic polynomial for matrices

The eigen-theory for matrices mirrors to the one for operators studied in Subsection 5.1.2. Let us make that explicit.

Definition 5.2.1.

Let $A \in \mathbf{F}^{m,m}$ be a matrix. We say that $\lambda \in F$ is an **eigenvalue** of A if there exists a non-zero $v \in \mathbf{F}^m$ such that $Av = \lambda v$.
A non-zero vector v satisfying $Av = \lambda v$ is called an **eigenvector** of A, corresponding to the eigenvalue λ.
The **eigenspace** of T corresponding to $\lambda \in \mathbf{F}$ is the set

$$\mathrm{E}(\lambda, A) := \{v \in \mathbf{F}^m \mid Av = \lambda v\}.$$

Recall that given a matrix $A \in \mathbf{F}^{m,m}$ we have an operator $\mathrm{L}_A \in \mathcal{L}(\mathbf{F}^m)$

$$\begin{aligned} \mathrm{L}_A \colon \mathbf{F}^m &\longrightarrow \mathbf{F}^m \\ x &\longmapsto Ax. \end{aligned}$$

It directly follows from the definitions that λ is an eigenvalue for A if and only if it is an eigenvalue for L_A. Similar statements hold for eigenvectors and eigenspaces. This implies that results similar to the ones in Subsection 5.1.2 hold for matrices.

As for operators, it is important to clarify the base field $\mathbf{F}$. The following example is simply Exercise 5.1.12 rewritten in term of matrices.

Example 5.2.2. Let $A = \left[\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right]$. Then L_A is the operator T from Exercise 5.1.12, so we know that A has no eigenvalues if $\mathbf{F} = \mathbf{R}$, and has eigenvalues i and $-\mathrm{i}$ if $\mathbf{F} = \mathbf{C}$. One can also observe that whenever $\mathbf{F} = \mathbf{R}$, L_A is the rotation by angle $\pi/2$, which explains why it has no eigenvalues.

Using matrices instead of operators allows us to use the determinant. We can hence define

Definition 5.2.3.

Let $A \in \mathbf{F}^{m,m}$ be a square matrix. The **characteristic polynomial** of A is

$$\chi_A(t) := \det(t\,\mathrm{Id}_m - A).$$

Remark 5.2.4.

Some authors define the characteristic polynomial as $\det(A - t\,\mathrm{Id}_m)$ instead of as $\det(t\,\mathrm{Id}_m - A)$. The only difference between the two definitions is a $(-1)^m$ multiplicative factor. In practice this does not change anything. Indeed, the two things that interest us about $\chi_A(t)$ are its roots and its divisors. Both notions are unchanged by the multiplicative factor $(-1)^m$.

If A is a $m \times m$ matrix, then its characteristic polynomial is a polynomial in t of degree m with coefficients in $\mathbf{F}$. Moreover, the leading coefficient of $\chi_A(t)$ (that is the coefficient of t^m) is 1.

The characteristic polynomial is a powerful tool that allows to easily compute the eigenvalues.

Theorem 5.2.5.

Let $A \in \mathbf{F}^{m,m}$ be a square matrix and let $\lambda \in \mathbf{F}$. Then λ is an eigenvalue for A if and only if it is a root of χ_A (that is, if and only if $\chi_A(\lambda) = 0$).

Proof. Analogously to Proposition 5.1.11, λ is an eigenvalue of A if and only if $\lambda\,\mathrm{Id}_m - A$ is not an invertible matrix, that is if and only if $\det(\lambda\,\mathrm{Id}_m - A) = 0$. □

The following important result directly follows from the definition.

Lemma 5.2.6. *Let $A \in \mathbf{F}^{m,m}$ be a square matrix. If A is a diagonal matrix or a triangular matrix (upper triangular, or lower triangular), then the eigenvalues of A are exactly its diagonal coefficients.*

We can now easily compute the eigenvalues from Exercise 5.1.44.

Example 5.2.7. Let

$$A := \begin{bmatrix} 0 & 4 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 5 \end{bmatrix}.$$

Then $\chi_A(t) = (t-5)(t-0)^2$ and the eigenvalues of A are 5 and 0.

Let us revisite Exercise 5.1.12 and Example 5.2.2.

Example 5.2.8. Let $A = \left[\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right]$. Then

$$\chi_A(t) = \det \begin{bmatrix} -t & 1 \\ -1 & -t \end{bmatrix} = t^2 + 1.$$

Therefore, it is clear that A has no eigenvalues if $\mathbf{F} = \mathbf{R}$, and has eigenvalues i and $-$i if $\mathbf{F} = \mathbf{C}$.

The characteristic polynomial is of great help to prove fundamental properties of eigenvalues.

Proposition 5.2.9. *Let $A \in \mathbf{R}^{m,m}$ be a matrix with real entries. If $\lambda \in \mathbf{C}$ is a complex eigenvalue of A, then its conjugate $\overline{\lambda}$ is also an eigenvalue of A.*

Proof. In general, λ is an eigenvalue of A if and only if $\chi_A(\lambda) = 0$, if and only if $\overline{\chi_A(\lambda)} = 0$. But since A has real entries, its characteristic polynomial $\chi_A(t) = a_0 + a_1 t + \cdots + a_m t^m$ has real coefficients. Therefore, $\overline{\chi_A(t)} = a_0 + a_1 \overline{t} + \cdots + a_m \overline{t}^m$. We conclude that $\overline{\chi_A(\lambda)} = 0$ if and only if $\chi_A(\overline{\lambda}) = 0$, if and only if $\overline{\lambda}$ is an eigenvalue of A. □

Theorem 5.2.10.

Let $A \in \mathbf{C}^{m,m}$. Then

1. *$\chi_A(t) = (-1)^m \det(A) + a_1 t + a_2 t^2 + \cdots + a_{m-1} t^{m-1} + t^m$, with $a_1, \ldots, a_{m-1} \in \mathbf{C}$;*
2. *$\chi_A(t) = (t-\lambda_1)(t-\lambda_2)\cdots(t-\lambda_m)$, where $\lambda_1, \ldots, \lambda_m \in \mathbf{C}$ are the $\mathbf{C}$-eigenvalues of A, possibly with repetition.*

Proof. The first assertion comes from the product formula for the determinant. The second assertion, is the fundamental theorem of algebra: an m-degree polynomial with complex coefficients has m roots when counted with multiplicity. □

The characteristic polynomial also helps us to show that two similar matrices have the same eigenvalues. Recall that two matrices $A, B \in \mathbf{F}^{m,m}$ and B are similar if there exists an invertible matrix $P \in \mathbf{F}^{m,m}$ with $A = P^{-1}BP$.

Proposition 5.2.11. *If $A, B \in \mathbf{F}^{m,m}$ are similar matrices, then*

1. $\det(A) = \det(B)$;
2. $\chi_A(t) = \chi_B(t)$.

Proof. Let P be an invertible matrix such that $A = P^{-1}BP$. Then we have $\det(A) = \det(P^{-1}BP) = \det(P^{-1})\det(B)\det(P) = \det(B)$.

For the second assertion,

$$\begin{aligned}\chi_A(t) &= \det(t\,\mathrm{Id}_m - A) = \det(t\,\mathrm{Id}_m - P^{-1}BP)\\ &= \det(P^{-1}(t\,\mathrm{Id}_m - B)P)\\ &= \det(t\,\mathrm{Id}_m - B) = \chi_B(t).\end{aligned}$$

□

5.2.2 Characteristic polynomial for operators

We now have everything that we need to define the characteristic polynomial of an operator. Indeed, if $T \in \mathcal{L}(V)$ is an operator on a finite dimensional vector space of dimension m, and $\mathscr{B}$ and $\mathscr{C}$ are two bases of V, it follows from Proposition 3.2.46 that the matrices $[T]_{\mathscr{B}}^{\mathscr{B}}$ and $[T]_{\mathscr{C}}^{\mathscr{C}}$ are similar. Therefore, by Proposition 5.2.11, $\det(t\,\mathrm{Id}_m - [T]_{\mathscr{B}}^{\mathscr{B}}) = \det(t\,\mathrm{Id}_m - [T]_{\mathscr{C}}^{\mathscr{C}})$.

Definition 5.2.12.

Let V be a finite dimensional vector space and let $T \in \mathcal{L}(V)$ be an operator. The **characteristic polynomial** of T is

$$\chi_T(t) := \det([T]_{\mathscr{B}}^{\mathscr{B}} - t\,\mathrm{Id}_{\dim(V)}),$$

where $\mathscr{B}$ is any basis of V.

Similarly, if $T \in \mathcal{L}(V)$ is an operator on a finite dimensional vector space, using Proposition 5.2.11 one can define its **determinant** by $\det(T) := \det([T]_{\mathscr{B}}^{\mathscr{B}})$ for any basis $\mathscr{B}$ of V.

Using our work on matrices, one can show the analogous of Theorem 5.2.5.

Theorem 5.2.13.

Let V be a finite dimensional space, let $T \in \mathcal{L}(V)$ be an operator and let $\lambda \in \mathbf{F}$. Then λ is an eigenvalue for T if and only if it is a root of χ_T (that is, if and only if $\chi_T(\lambda) = 0$).

Proof. Let B be a basis for V. Then λ is an eigenvalue of T if and only if $T - \lambda \operatorname{Id}_V$ is not an invertible map, if and only if

$$[T_\lambda - \operatorname{Id}_V]_{\mathscr{B}}^{\mathscr{B}} = [T]_{\mathscr{B}}^{\mathscr{B}} - \lambda \operatorname{Id}_{\dim(V)}$$

is not an invertible matrix, if and only if λ is an eigenvalue of $[T]_{\mathscr{B}}^{\mathscr{B}}$. We conclude by Theorem 5.2.5. □

Corollary 5.2.14. *Let V be a finite dimensional vector space over $\mathbf{C}$ and let $T \in \mathcal{L}(V)$ be an operator. Then T is nilpotent if and only if $\chi_T(t) = t^{\dim(V)}$.*

Proof. By the previous theorem, $\chi_T(t) = t^{\dim(V)}$ if and only if 0 is the only eigenvalue of T. By Proposition 5.1.38 this is equivalent to T being nilpotent. □

So the eigenvalues of T are exactly the eigenvalues of $[T]_{\mathscr{B}}^{\mathscr{B}}$, where $\mathscr{B}$ is any basis of V. How about the eigenvectors of T ? Recall that given a basis $\mathscr{B}$ of an m dimensional vector space V, we have an isomorphism

$$\begin{aligned} [\,\cdot\,]_{\mathscr{B}} \colon V &\longrightarrow \mathbf{F}^m \\ v &\longmapsto [v]_{\mathscr{B}}. \end{aligned}$$

Theorem 5.2.15.

Let V be a m dimensional vector space, let $T \in \mathcal{L}(V)$ and let $\mathscr{B}$ be a basis of V. Then for any $v \in V$, the vector $v \in V$ is an eigenvector of $T \in \mathcal{L}(V)$ (corresponding to the eigenvalue λ) if and only if $[v]_{\mathscr{B}} \in \mathbf{F}^m$ is an eigenvector of $[T]_{\mathscr{B}}^{\mathscr{B}} \in \mathbf{F}^{m,m}$ (corresponding to the eigenvalue λ).

Proof. Recall we have a commutative diagram

$$\begin{array}{ccc} V & \xrightarrow{T} & V \\ {\scriptstyle [\,\cdot\,]_{\mathscr{B}}}\downarrow & & \downarrow{\scriptstyle [\,\cdot\,]_{\mathscr{B}}} \\ \mathbf{F}^m & \xrightarrow[[T]_{\mathscr{B}}^{\mathscr{B}}]{} & \mathbf{F}^m \end{array}$$

where $[\,\cdot\,]_{\mathscr{B}} \colon V \to \mathbf{F}^m$ is an isomorphism. For every $v \in V$ we have $[Tv]_{\mathscr{B}} = [T]_{\mathscr{B}}^{\mathscr{B}}[v]_{\mathscr{B}}$. Therefore, $Tv = \lambda v$ if and only if $[Tv]_{\mathscr{B}} = [\lambda v]_{\mathscr{B}}$ if and only if $[T]_{\mathscr{B}}^{\mathscr{B}}[v]_{\mathscr{B}} = \lambda[v]_{\mathscr{B}}$, which finishes the proof. □

Exercise 5.2.16. Let $T \in \mathcal{L}(\mathcal{P}(\mathbf{R})_2)$ be defined by $T(f(x)) := f(x) + (x+1)f'(x)$. Find the eigenvalues and eigenvectors of T.

Solution. Let $\mathscr{B} = (1, x, x^2)$ be the standard basis of $\mathcal{P}(\mathbf{R})_2$. We compute:

$$\begin{aligned} T(1) &= 1, \\ T(x) &= x + (x+1) \cdot 1 = 1 + 2x, \\ T(x^2) &= x^2 + (x+1) \cdot 2x = 2x + 3x^2. \end{aligned}$$

We hence have

$$A := [T]_{\mathscr{B}}^{\mathscr{B}} = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 2 & 2 \\ 0 & 0 & 3 \end{bmatrix}.$$

The characteristic polynomial of T (and hence of A) is given by the following easy computation

$$\chi_T(t) = \det(A - t\,\mathrm{Id}_3) = \det \begin{bmatrix} t-1 & -1 & 0 \\ 0 & t-2 & -2 \\ 0 & 0 & t-3 \end{bmatrix} = (t-1)(t-2)(t-3).$$

We conclude that the eigenvalues of T (and of A) are 1, 2 and 3. Finally, the eigenvectors of T are given the eigenvectors of A. Therefore, to find it we need to solve system of linear equations.

Eigenspace for $\lambda = 1$. We have $\mathrm{E}(1, [T]_{\mathscr{B}}^{\mathscr{B}}) = \mathrm{E}(1, A) = \mathrm{null}(\mathrm{Id}_3 - A)$ and hence

$$\begin{aligned} \mathrm{E}(1, T) &= \{z \in \mathbf{R}^3 \mid (A - \mathrm{Id}_3)z = 0\} \\ &= \left\{ \begin{bmatrix} z_1 \\ z_2 \\ z_3 \end{bmatrix} \;\middle|\; \begin{bmatrix} 0 & -1 & 0 \\ 0 & -1 & -2 \\ 0 & 0 & -2 \end{bmatrix} \begin{bmatrix} z_1 \\ z_2 \\ z_3 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix} \right\} \\ &= \left\{ \begin{bmatrix} a \\ 0 \\ 0 \end{bmatrix} \;\middle|\; a \in \mathbf{R} \right\}. \end{aligned}$$

Therefore, $\mathrm{E}(1, T) = \{a \mid a \in \mathbf{R}\}$. In other words, the eigenvectors of T corresponding to the eigenvalue 1 are exactly the non-zero constant polynomials.

Eigenspace for $\lambda = 2$. This time we solve

$$\begin{aligned} \mathrm{E}(2, T) &= \{z \in \mathbf{R}^3 \mid (A - 2\,\mathrm{Id}_3)z = 0\} \\ &= \left\{ \begin{bmatrix} z_1 \\ z_2 \\ z_3 \end{bmatrix} \;\middle|\; \begin{bmatrix} 1 & -1 & 0 \\ 0 & 0 & -2 \\ 0 & 0 & -1 \end{bmatrix} \begin{bmatrix} z_1 \\ z_2 \\ z_3 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix} \right\} \\ &= \left\{ \begin{bmatrix} a \\ a \\ 0 \end{bmatrix} \;\middle|\; a \in \mathbf{R} \right\}. \end{aligned}$$

Therefore, $\mathrm{E}(2, T) = \{a + ax \mid a \in \mathbf{R}\}$ and the eigenvectors of T corresponding to the eigenvalue 2 are $\{a + ax \mid a \in \mathbf{R}, a \neq 0\}$.

Eigenspace for $\lambda = 3$. Finally we solve

$$\begin{aligned}\mathrm{E}(3,T) &= \{z \in \mathbf{R}^3 \mid (A - 3\,\mathrm{Id}_3)z = 0\} \\ &= \left\{ \begin{bmatrix} z_1 \\ z_2 \\ z_3 \end{bmatrix} \;\middle|\; \begin{bmatrix} 2 & -1 & 0 \\ 0 & 1 & -2 \\ 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} z_1 \\ z_2 \\ z_3 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix} \right\} \\ &= \left\{ \begin{bmatrix} a \\ 2a \\ a \end{bmatrix} \;\middle|\; a \in \mathbf{R} \right\}.\end{aligned}$$

Therefore, $\mathrm{E}(2,T) = \{a + 2ax + ax^2 \mid a \in \mathbf{R}\}$ and the eigenvectors of T corresponding to the eigenvalue 3 are $\{a + 2ax + ax^2 \mid a \in \mathbf{R}, a \neq 0\}$. □

The next result shows that the characteristic polynomial behaves well with respect to restriction to invariant subspaces.

Lemma 5.2.17. *Let V be a finite dimensional vector space and let $T \in \mathcal{L}(V)$ be an operator. If $U \subseteq V$ is a T-invariant subspace, then $\chi_{T|_U}(t)$ divides $\chi_T(t)$.*

Proof. Let $\mathscr{A} = (u_1, \dots, u_l)$ be a basis of U. Extend it to $\mathscr{B} = (u_1, \dots, u_l, v_1, \dots, v_{m-l})$ a basis of V, where $l = \dim(U)$ and $m = \dim(V) \geq l$. Write $B = [T]^{\mathscr{B}}_{\mathscr{B}}$ and $A = [T|_U]^{\mathscr{A}}_{\mathscr{A}}$. Then it follows from the definition of matrix representations that

$$B = \left[\begin{array}{c|c} A & C \\ \hline 0 & D \end{array}\right]$$

for some $C \in \mathbf{F}^{l,m-l}$ and $D \in \mathbf{F}^{m-l,m-l}$. Then $\chi_B(t) = \det(t\,\mathrm{Id}_m - B) = \det(t\,\mathrm{Id}_l - A) \cdot \det(t\,\mathrm{Id}_{m-l} - D) = \chi_A(t)\chi_D(t)$. □

While we were able to define the characteristic polynomial for a finite dimensional space over $\mathbf{F}$, for the following result we will need that $\mathbf{F} = \mathbf{C}$. This result explains the name "algebraic mutliplicity" for $\mathrm{m}_{\mathrm{alg}}(\lambda, T)$.

Proposition 5.2.18. *Let V be a finite dimensional vector space over $\mathbf{C}$ and let $T \in \mathcal{L}(V)$ be an operator. Let $\lambda_1, \dots, \lambda_k$ be all the distinct eigenvalues of T. Then $\chi_T(t) = (\lambda_1 - t)^{\mathrm{m}_{\mathrm{alg}}(\lambda_1,T)} \cdots (\lambda_k - t)^{\mathrm{m}_{\mathrm{alg}}(\lambda_k,T)}$.*

Proof. This directly follows from the matrix representation of T given in Proposition 5.1.56. □

We can finally prove one of the fundamental results of eigen-theory.

Theorem 5.2.19 (Cayley–Hamilton theorem[3]).

Let V be a finite dimensional vector space and let $T \in \mathcal{L}(V)$. Then $\chi_T(T) = 0_{\mathcal{L}(V)}$.

Proof. We will only prove the theorem for $\mathbf{C}$ and $\mathbf{R}$. For a general field $\mathbf{F}$, see Appendix 5.

Let us first suppose that $\mathbf{F} = \mathbf{C}$. Let $\lambda_1, \dots, \lambda_k$ be the eigenvalue of T. Then $V = \bigoplus_{j=1}^{k} \mathrm{G}(\lambda_j, T)$ by Theorem 5.1.49. Let v be any vector in V. Then $v = v_1 + \cdots + v_k$ for some $v_j \in \mathrm{G}(\lambda_j, T)$. Using that $(T - \lambda_j \operatorname{Id}_V)\big|_{\mathrm{G}(\lambda_j,T)}$ is nilpotent on $\mathrm{G}(\lambda_j, T)$ we have $(T - \lambda_j \operatorname{Id}_V)^{\mathrm{m_{alg}}(\lambda_j,T)} v_j = 0$ for all $j \in \{1, \dots, k\}$. It follows that

$$\begin{aligned}\chi_T(T)v_1 &= ((T - \lambda_2 \operatorname{Id}_V)^{\mathrm{m_{alg}}(\lambda_2)} \cdots (T - \lambda_k \operatorname{Id}_V)^{\mathrm{m_{alg}}(\lambda_k)})(T - \lambda_1 \operatorname{Id}_V)^{\mathrm{m_{alg}}(\lambda_1)} v_1 \\ &= ((T - \lambda_2 \operatorname{Id}_V)^{\mathrm{m_{alg}}(\lambda_2)} \cdots (T - \lambda_k \operatorname{Id}_V)^{\mathrm{m_{alg}}(\lambda_k)})0 = 0.\end{aligned}$$

And similarly, $\chi_T(T)v_j = 0$ for all $j \in \{1, \dots, k\}$. Therefore,

$$\chi_T(T)v = (\chi_T(T))(v_1 + \cdots + v_k) = 0 + \cdots + 0 = 0.$$

We now prove the case $\mathbf{F} = \mathbf{R}$. Let T be an operator on a real vector space V of dimension m. Fix a basis $\mathscr{B}$ of V and let $A = [T]_{\mathscr{B}}^{\mathscr{B}} \in \mathbf{R}^{m,m}$. The trick is that an $m \times m$ matrix with real coefficients is also an $m \times m$ matrix with complex coefficients, so we can apply the Cayley–Hamilton theorem to the complex matrix A. Here are the details. One can define an operator S on $\mathbf{C}^m$ such that the matrix representation of S, with respect to the standard basis $\mathscr{E}$ of $\mathbf{C}$, is also A. That is, $S = \mathrm{L}_A \colon \mathbf{C}^m \to \mathbf{C}^m$, $v \mapsto Av$. Then $\chi_T(t) = \det(t \operatorname{Id}_m - A) = \chi_S(t)$ and $[\chi_T(T)]_{\mathscr{B}}^{\mathscr{B}} = \chi_T(A) = \chi_S(A) = [\chi_S(S)]_{\mathscr{E}}^{\mathscr{E}} = 0$ is the 0 matrix. □

5.2.3 Minimal polynomial

Standing assumption

In this subsection, $V \neq \{0\}$ will always be a *non zero finite dimensional* vector space.

The characteristic polynomial is a powerful tool that encode informations about eigenvalues. But it is sometimes not precise enough. For example, the following two matrices have the same characteristic polynomial $(t-1)^2$ despite being quite different:

$$\operatorname{Id}_2 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \qquad A = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}.$$

While these two matrices have the same characteristic polynomial, they are very different from the point of view of eigen-theory. Indeed, we have $\mathbf{C}^2 = \mathrm{E}(1, \operatorname{Id}) \supsetneq \mathrm{E}(1, A) = \left\{ \begin{bmatrix} z \\ 0 \end{bmatrix} \mid z \in \mathbf{C} \right\}$.

[3] Named after Arthur Cayley (1821–1895) and William Rowan Hamilton (1805–1865), but the first general proof was published by Ferdinand Georg Frobenius (1849–1917).

In this subsection, we will introduce another polynomial naturally associated to an operator, which will be able to distinguish between Id_2 and A.

Definition 5.2.20.

A non-zero polynomial $p(t) = a_n t^n + \cdots + a_1 t + a_0$ ($a_n \neq 0$) is **monic** if the leading coefficient is 1, that is if $a_n = 1$.

Example 5.2.21. If $T \in \mathcal{L}(V)$ is an operator on a finite dimensional vector space $V \neq \{0\}$, then $\chi_T(t)$ is monic.[4]

Proposition 5.2.22. *Let $V \neq \{0\}$ be a finite dimensional non-zero vector space and let $T \in \mathcal{L}(V)$ be an operator. Then there exists a unique monic polynomial $\mathrm{M}_T(t)$ such that:*

1. $\mathrm{M}_T(T) = 0_{\mathcal{L}(V)}$;
2. $\mathrm{M}_T(t)$ *has the smallest degree among non-zero polynomials satisfying 1.*

Moreover, $\mathrm{M}_T(t)$ has degree at most $\dim(V)$.

Proof. Let $m := \dim(V)$. Then $\dim(\mathcal{L}(V)) = m^2$ and hence the family $\mathrm{Id}_V, T \dots, T^{m^2}$ is linearly dependent in $\mathcal{L}(V)$. Let $l := \min\{k \mid T^k \in \mathrm{span}(\mathrm{Id}_V, T, \dots, T^{k-1})\}$, so $l \leq m^2$ by the linear dependence lemma (Lemma 2.4.36). Since $T^0 = \mathrm{Id}_V$ is not in $\mathrm{span}(\varnothing) = \{0\}$ we have $l \geq 1$.

By definition of l, there exists $\lambda_0, \lambda_1, \dots, \lambda_{l-1}$ in $\mathbf{F}$ such that $0 = \lambda_0 \mathrm{Id}_V + \lambda_1 T + \cdots + \lambda_{l-1} T^{l-1} + T^l$. Define $\mathrm{M}_T(t) := t^l + \lambda_{l-1} t^{l-1} + \cdots + \lambda_1 t + \lambda_0$. Then $\mathrm{M}_T(t)$ satisfies 1, but also 2 by minimality of l.

Suppose now that $q(t)$ is also a monic polynomial satisfying 1 and 2. In particular, $q(t)$ is a monic polynomial with $\deg q = \deg \mathrm{M}_T$. Then, $(\mathrm{M}_T - q)(T) = 0 - 0 = 0$ and $\deg(\mathrm{M}_T - q) \leq l - 1$. We conclude that $\mathrm{M}_T - q$ is the zero polynomial and thus $\mathrm{M}_T = q$ is unique.

Finally, the characteristic polynomial χ_T satisfies 1 by the Cayley–Hamilton Theorem (Theorem 5.2.19) and has degree $m = \dim(V)$. By minimality of the degree, M_T has degree at most m. □

Definition 5.2.23.

Let $V \neq \{0\}$ be a finite dimensional non-zero vector space and let $T \in \mathcal{L}(V)$ be an operator. The **minimal polynomial** of T is the unique monic polynomial $\mathrm{M}_T(t) \in \mathcal{P}(\mathbf{F})$ given by Proposition 5.2.22.

Lemma 5.2.24. *Let $V \neq \{0\}$ be a finite dimensional vector space and let $T \in \mathcal{L}(V)$ be an operator. Then $\deg(\mathrm{M}_T(t)) \geq 1$. Moreover, $\deg(\mathrm{M}_T(t)) = 1$ if and only if there exists $\lambda \in \mathbf{F}$ such that $T = \lambda \mathrm{Id}_V$.*

[4] This is why we choose to define $\chi_A(t)$ by $\det(t \mathrm{Id} - A)$ instead of by $\det(A - t \mathrm{Id})$.

Proof. Since $\mathrm{M}_T(t)$ is monic, it is not the zero polynomial. But since $\mathrm{M}_T(T) = 0$, $\mathrm{M}_T(t)$ cannot be a non-zero constant polynomial. We conclude that $\mathrm{M}_T(t)$ has degree at least 1.

Since the minimal polynomial has degree at least one, we have $\mathrm{M}_T(t) = t - \lambda$ if and only if $T - \lambda \mathrm{Id}_V = 0$, if and only if $T = \lambda \mathrm{Id}_V$. □

The above lemma implies that the minimal polynomial distinguishes the matrices from the introduction of this subsection.

Example 5.2.25. Let $\mathscr{E}$ be the standard basis of $\mathbf{C}^2$ and let T be the operator represented by $[T]_{\mathscr{E}}^{\mathscr{E}} = \left[\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right]$. Then $\chi_T(t) = (t-1)^2 = \chi_{\mathrm{Id}_{\mathbf{C}^2}}(t)$. However, $\mathrm{M}_T(t)$ has degree at least 2 (and hence exactly 2 by Proposition 5.2.22), while $\mathrm{M}_{\mathrm{Id}_{\mathbf{C}^2}}(t) = t - 1$.

Not only the minimal polynomial is the unique polynomial of smallest degree annulling T, it is also the smallest one for divisibility.

Proposition 5.2.26. *Let $V \neq \{0\}$ be a finite dimensional non-zero vector space and let $T \in \mathcal{L}(V)$ be an operator. Then for any $q(t) \in \mathcal{P}(\mathbf{F})$, $q(T) = 0$ if and only if $\mathrm{M}_T(t)$ divides $q(t)$.*

Proof. "⇐" Suppose $\mathrm{M}_T(t)$ divides $q(t)$. Then there exists a polynomial $p(t) \in \mathcal{P}(\mathbf{F})$ such that $q(t) = \mathrm{M}_T(t)p(t)$. Therefore, $q(T) = p(T)\,\mathrm{M}_T(T) = 0$.

"⇒" By the Euclidean division of polynomials, there exists $r(t), s(t) \in \mathcal{P}(\mathbf{F})$ such that $q(t) = s(t)\,\mathrm{M}_T(t) + r(t)$ and $\deg r(t) < \deg \mathrm{M}_T(t)$. Now, if $q(T) = 0$ we also have $r(T) = 0$, which by minimality of $\mathrm{M}_T(t)$ implies that $r(t)$ is the zero polynomial. That is, $q(t) = s(t)\,\mathrm{M}_T(t)$. □

Corollary 5.2.27. *Let $V \neq \{0\}$ be a finite dimensional vector space and let $T \in \mathcal{L}(V)$ be an operator. Then the minimal polynomial $\mathrm{M}_T(t)$ divides the characteristic polynomial $\chi_T(t)$.*

Proof. This directly follows from the proposition and the Cayley–Hamilton theorem (Theorem 5.2.19). □

Theorem 5.2.28.

Let $V \neq \{0\}$ be a finite dimensional vector space, let $T \in \mathcal{L}(V)$ be an operator and let $\lambda \in \mathbf{F}$. Then λ is an eigenvalue of T if and only if it is a root of the minimal polynomial.

Proof. "⇐" If $\mathrm{M}_T(\lambda) = 0$, then $\chi_T(\lambda) = 0$ and thus λ is an eigenvalue of T by Theorem 5.2.13.

"⇒" We have $\mathrm{M}_T(t) = t^l + a_{l-1}t^{l-1} + \cdots + a_1 t + a_0$ for some $l \leq \dim(V)$ and some coefficients $a_j \in \mathbf{F}$. Suppose that λ is an eigenvalue of T. Then there exists a non-zero vector v with $Tv = \lambda v$. Therefore, for all positive integer j we have $T^j v = \lambda^j v$. Then $\mathrm{M}_T(\lambda)v = (\lambda^l + a_{l-1}\lambda^{l-1} + \cdots + a_1\lambda + a_0)v = \mathrm{M}_T(T)v = 0$. Since $v \neq 0$, we conclude that $\mathrm{M}_T(\lambda) = 0$. □

Corollary 5.2.29. *Let $V \neq \{0\}$ be a finite dimensional vector space over $\mathbf{C}$ and let $T \in \mathcal{L}(V)$ be an operator. Let $\lambda_1, \dots, \lambda_l$ be the distinct eigenvalues of T. Then there exists integers $k_1, \dots, k_l$ with $1 \leq k_j \leq \mathrm{m}_{\mathrm{alg}}(\lambda_j, T)$ such that $\mathrm{M}_T(t) = (t-\lambda_1)^{k_1} \cdots (t-\lambda_l)^{k_l}$.*

Example 5.2.30. Let $\mathscr{E}$ be the standard basis of $\mathbf{C}^3$ and let $T \in \mathcal{L}(\mathbf{C}^3)$ be the operator given by

$$[T]_{\mathscr{E}}^{\mathscr{E}} = \begin{bmatrix} 6 & 3 & 4 \\ 0 & 6 & 2 \\ 0 & 0 & 7 \end{bmatrix} =: A.$$

Then $\chi_T(t) = (t-6)^2(t-7)$ and the eigenvalues of T are 6 (with algebraic multiplicity 2) and 7 (with algebraic multiplicity 1). Then we have two possibilities for the minimal polynomial: either $\mathrm{M}_T(t) = (t-6)^2(t-7)$, or $\mathrm{M}_T(t) = (t-6)(t-7)$. The second possibility occurs if and only if $(A - 6\,\mathrm{Id}_3)(A - 7\,\mathrm{Id}_3) = 0$. But

$$(A - 6\,\mathrm{Id}_3)(A - 7\,\mathrm{Id}_3) = \begin{bmatrix} 0 & 3 & 4 \\ 0 & 0 & 2 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} -1 & 3 & 4 \\ 0 & -1 & 2 \\ 0 & 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & -3 & * \\ * & * & * \\ * & * & * \end{bmatrix} \neq 0,$$

where the $*$ are entries that might or might not be 0. We conclude that $\mathrm{M}_T(t) = (t-6)^2(t-7)$. Therefore, for all eigenvalues, the geometric and the algebraic multiplicities are the same.

The minimal polynomial has the advantage to be able to distinguish operators that the characteristic polynomial cannot. However, the minimal polynomial has the disadvantage to be more complicated to compute in general. Hopefully, for nilpotent operators, one can easily compute it.

Proposition 5.2.31. *Let $V \neq \{0\}$ be a finite dimensional vector space and let $T \in \mathcal{L}(V)$ be an operator such that $T - \lambda\,\mathrm{Id}_V$ is nilpotent for some $\lambda \in \mathbf{F}$. Let k be the smallest integer such that $(T - \lambda\,\mathrm{Id}_V)^k = 0$. Then λ is the only eigenvalue of T and $\mathrm{M}_T(t) = (t-\lambda)^k$.*

Proof. Let $S := T - \lambda\,\mathrm{Id}_V$. The minimal polynomial $\mathrm{M}_S(t)$ is a monic polynomial that divides (by Corollary 5.2.27) $\chi_S(t) = t^{\dim V}$. Therefore, $\mathrm{M}_S(t) = t^k$ for some $1 \leq k \leq \dim(V)$. By minimality, k is the smallest integer such that $S^k = 0$. We conclude that $\mathrm{M}_T(t) = (t-\lambda)^k$. □

Observe that if T is nilpotent, it satisfies the hypothesis of Proposition 5.2.31 for $\lambda = 0$.

5.2.4 A word about matrices

All the work we did on nilpotent operators, the characteristic polynomial and the minimal polynomial naturally translates to the realm of matrices. For example, we say that a square matrix $A \in \mathbf{F}^{m,m}$ is **nilpotent** if there exists an integer k such that $A^k = 0$ is the zero matrix. One easily shows that an operator $T \in \mathcal{L}(V)$ on a finite dimensional vector space is nilpotent if and only if the matrix $[T]_{\mathscr{B}}^{\mathscr{B}}$ is nilpotent for any basis $\mathscr{B}$ of V. One can

also define the generalised eigenspace of A as $\mathrm{G}(\lambda, A) := \mathrm{G}(\lambda, \mathrm{L}_A) = \mathrm{null}(A - \lambda \mathrm{Id}_m)^m$, where L_A is the operator defined by $\mathrm{L}_A(x) = Ax$. Finally, the minimal polynomial of A is defined in a natural way, and one have $\mathrm{M}_T(t) = \mathrm{M}_{[T]_{\mathscr{B}}^{\mathscr{B}}}(t)$.

The Cayley–Hamilton theorem Theorem 5.2.19 remains true for matrices. More precisely, it says that for any square matrix A we have $\chi_A(A) = 0 \in \mathbf{F}^{m,m}$.

Remark 5.2.32.

When seeing the Cayley–Hamilton theorem for the first time, some people would like to write the following incorrect "proof" of the matrix version of the theorem: "*We have* $\chi_A(A) = \det(A\,\mathrm{Id} - A) = \det(0) = 0$". While this seems appealing, this does not work. First of all, the matrix version of the theorem says that $\chi_A(A) = 0_{\mathbf{F}^{n,n}}$ is the zero matrix, not the scalar $0_{\mathbf{F}} = \det(0_{\mathbf{F}^{n,n}})$. Secondly, in the expression $\det(t\,\mathrm{Id} - A)$, the variable t appears as the diagonal entries of the matrix $t\,\mathrm{Id}_n$. To illustrate this, let us consider the simple example $A = \left[\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}\right]$ (this is the orthogonal projection onto the x-axis). This matrix has eigenvalues 0 and 1, and hence characteristic polynomial $t(t-1)$. We can easily verify that the matrix A indeed satisfy $A(A - \mathrm{Id}_2) = 0$. However, we have $t\,\mathrm{Id}_2 - A = \left[\begin{smallmatrix} t-1 & 0 \\ 0 & t \end{smallmatrix}\right]$. If we substitute the matrix A for t in this expression, we obtain

$$\begin{bmatrix} \left[\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}\right] - 1 & 0 \\ 0 & \left[\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}\right] \end{bmatrix},$$

which is not even a valid matrix expression.

Finally, here is an example showing that the above incorrect proof cannot be made correct. Let $q_A(t) := t\,\mathrm{Id} - A$ be the trace (sum of the diagonals entries) of $t\,\mathrm{Id} - A$. Then $q_A(A - A) = q(0) = 0$, but $q_A(A) \neq 0$ in general. If we take $A = \left[\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}\right]$ as above then $q_A(t) = t - 1 + t = 2t - 1$ and we easily verify that $q_A(A) = 2A - \mathrm{Id}_2 = \left[\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right] \neq 0$.

When solving concrete problems about $T \in \mathcal{L}(V)$, it is often easier to take a basis $\mathscr{B}$ of V, translate the problem into a problem for $[T]_{\mathscr{B}}^{\mathscr{B}}$, solve the matrix version and then translate the solution back to T. Let us exemplify that by computing the minimal polynomial of an operator.

Example 5.2.33. Let $T \in \mathcal{L}(V)$ be an operator on a finite dimensional vector space.

Suppose we have a basis $\mathscr{B}$ such that

$$[T]_{\mathscr{B}}^{\mathscr{B}} = \begin{bmatrix} \boxed{\begin{matrix} \lambda_1 & & * \\ & \ddots & \\ * & & \lambda_1 \end{matrix}} & & & \\ & \boxed{\begin{matrix} \lambda_2 & & * \\ & \ddots & \\ * & & \lambda_2 \end{matrix}} & & \\ & & \ddots & \\ & & & \boxed{\begin{matrix} \lambda_l & & * \\ & \ddots & \\ * & & \lambda_l \end{matrix}} \end{bmatrix}.$$

(If V is a complex vector space, such a basis always exists by Proposition 5.1.56.) The minimal polynomial of T is hence of the form $\mathrm{M}_T(t) = (t-\lambda_1)^{k_1} \cdots (t-\lambda_l)^{k_l}$ for some $k_j \in \{1, \dots, \mathrm{m}_{\mathrm{alg}}(\lambda_j, T)\}$. Write $A_1, \dots, A_l$ for the diagonal blocs occurring in $[T]_{\mathscr{B}}^{\mathscr{B}}$. To compute k_1, observe that $N_1 := \lambda_1 \mathrm{Id}_{\mathrm{m}_{\mathrm{alg}}(\lambda_1, T)} - A_1$ is a triangular matrix with 0s on the diagonal, and hence nilpotent. Therefore, $\mathrm{M}_{N_1}(t) = t^{k_1}$, where k_1 is the smallest integer such that $(N_1)^{k_1} = 0$. In other words, to find k_1 it is enough to compute $N_1, N_1^2, \dots, N_1^{\mathrm{m}_{\mathrm{alg}}(\lambda_1, T)}$ and to stop as soon one of those matrix is the 0 matrix. Finally, $\mathrm{M}_{A_1}(t) = \mathrm{M}_{N_1}(t - \lambda_1) = (t-\lambda_1)^{k_1}$. The other exponents $k_2, \dots, k_l$ are computed in a similar way.

Let us apply this procedure on a concrete example. Suppose that

$$[T]_{\mathscr{B}}^{\mathscr{B}} = A = \begin{bmatrix} 1 & 2 & & \\ & 1 & & \\ & & 3 & \\ & & & 3 \end{bmatrix}.$$

Then $\chi_T(t) = (t-1)^2(t-3)^2$ and $\mathrm{M}_T(t) = (t-1)^{k_1}(t-3)^{k_2}$ with $1 \leq k_1, k_2 \leq 2$. Using the above notation we have $A_1 = \left[\begin{smallmatrix} 1 & 2 \\ 0 & 1 \end{smallmatrix}\right]$ and $N_1 = \left[\begin{smallmatrix} 0 & 2 \\ 0 & 0 \end{smallmatrix}\right]$. So $N_1 \neq 0$ but $N_1^2 = 0$ and we conclude that $k_1 = 2$. For the eigenvalue 3 we have $A_2 = \left[\begin{smallmatrix} 3 & 0 \\ 0 & 3 \end{smallmatrix}\right]$ and $N_2 = 0$, so $k_2 = 1$. Altogether, $\mathrm{M}_T(t) = (t-1)^2(t-3)$.

5.3 Jordan normal form

In this section, we will finally give the definitive answer to our main question.

Major Question 3.2.47.

Given V and $T \in \mathcal{L}(V)$, find a basis $\mathscr{B}$ such that $[T]_{\mathscr{B}}^{\mathscr{B}}$ is "as simple as possible" (for example: diagonal, upper triangular, with many zeroes, …).

5.3.1 Existence of the Jordan normal form

We already saw in Proposition 5.1.56 that if T is an operator on a complex finite dimensional vector space, there always exists a basis such that $[T]_{\mathscr{B}}^{\mathscr{B}}$ is a diagonal by blocks matrix. Moreover, if $\lambda_1, \dots, \lambda_l$ are the eigenvalues of T, then $[T]_{\mathscr{B}}^{\mathscr{B}}$ has l diagonal block $A_1, \dots, A_l$, and each A_j is an $\mathrm{m}_{\mathrm{alg}}(\lambda_j, T) \times \mathrm{m}_{\mathrm{alg}}(\lambda_j, T)$ upper triangular matrix with λ_j on the diagonal. In this section, we will see that one can always choose a basis such that the A_j itself are made of particularly nice blocks.

Definition 5.3.1.

A square matrix $J \in \mathbf{F}^{k,k}$ is called a **Jordan block** of eigenvalue $\lambda \in \mathbf{F}$ if it is of the form

$$J = \begin{bmatrix} \lambda & 1 & & \\ & \lambda & \ddots & \\ & & \ddots & 1 \\ & & & \lambda \end{bmatrix}.$$

In particular, if $k = 1$, then a Jordan block of eigenvalue λ is simply the following 1×1 matrix $\begin{bmatrix} \lambda \end{bmatrix}$.

It directly follows from the definition that the eigenvalues of a $k \times k$ "Jordan block of eigenvalue λ" J is indeed λ, with algebraic multiplicity k. We have $\chi_J(t) = (t-\lambda)^k$ and the matrix $\lambda \operatorname{Id}_k - J$ is nilpotent. Moreover, by direct matrix computations we have

$$(\lambda \operatorname{Id}_k - J)^{k-1} = \begin{bmatrix} 0 & \cdots & 0 & -1 \\ & \ddots & & 0 \\ & & \ddots & \vdots \\ & & & 0 \end{bmatrix}.$$

Therefore, $(\lambda \operatorname{Id}_k - J)^k = 0$ and $\mathrm{M}_J(t) = (t-\lambda)^k$ by Proposition 5.2.31.

Proposition 5.3.2. *Let*

$$J = \begin{bmatrix} J_1 & & & \\ & J_2 & & \\ & & \ddots & \\ & & & J_n \end{bmatrix} \in \mathbf{F}^{m,m}$$

be a matrix where each $J_j \in \mathbf{F}^{k_j,k_j}$ is a Jordan block of eigenvalue λ and size k_j. (So $m = \sum_{j=1}^{n} k_j$.) Then $\chi_J(t) = (t-\lambda)^m$ and $\mathrm{M}_J(t) = (t-\lambda)^k$ where $k = \max\{k_1, \dots, k_n\}$.

Proof. This is basically Example 5.2.33. But here is a detailed proof. The matrix J is upper triangular, of size n with λ on the diagonal. This directly implies the formula for the characteristic polynomial. For the minimal polynomial, since J is diagonal by block,

we have

$$(\lambda \operatorname{Id}_m - J)^l = \begin{bmatrix} (\lambda \operatorname{Id}_{k_1} - J_1)^l & & & \\ & (\lambda \operatorname{Id}_{k_2} - J_2)^l & & \\ & & \ddots & \\ & & & (\lambda \operatorname{Id}_{k_n} - J_n)^l \end{bmatrix}$$

for all $l \in \mathbf{N}$. Therefore, $\mathrm{M}_J(t) = (t-\lambda)^k$ for

$$k = \min\{l \mid \forall j \in \{1, \dots, n\}, (J_j - \lambda \operatorname{Id}_{k_j})^l = 0\} = \max\{k_1, \dots, k_n\}. \qquad \square$$

Example 5.3.3. Let $m = 4$ and $\lambda = 2$. Up to permutation of the blocks, there are 5 matrices that are diagonal by [Jordan blocks]:

$$J = \begin{bmatrix} 2 & 1 & & \\ & 2 & 1 & \\ & & 2 & 1 \\ & & & 2 \end{bmatrix}, \qquad K = \begin{bmatrix} 2 & 1 & & \\ & 2 & 1 & \\ & & 2 & \\ & & & 2 \end{bmatrix}, \qquad L = \begin{bmatrix} 2 & 1 & & \\ & 2 & & \\ & & 2 & 1 \\ & & & 2 \end{bmatrix},$$

$$M = \begin{bmatrix} 2 & 1 & & \\ & 2 & & \\ & & 2 & \\ & & & 2 \end{bmatrix}, \qquad N = \begin{bmatrix} 2 & & & \\ & 2 & & \\ & & 2 & \\ & & & 2 \end{bmatrix}.$$

All of these matrices have characteristic polynomial $\chi_*(t) = (t-2)^4$. For the minimal polynomials, we have $\mathrm{M}_J(t) = (t-2)^4$, $\mathrm{M}_K(t) = (t-2)^3$, $\mathrm{M}_L(t) = \mathrm{M}_M(t) = (t-2)^2$ and $\mathrm{M}_N(t) = t-2$.

The case of Jordan blocks of distinct eigenvalues is similar to what happens in Proposition 5.3.2. Simply treat together all the block sharing one common eigenvalue.

Example 5.3.4. Let

$$A = \begin{bmatrix} 4 & 1 & & \\ & 4 & & \\ & & 4 & \\ & & & 5 \end{bmatrix}.$$

Then we have $\mathrm{M}_A(t) = (t-4)^2(t-5)$, where the exponent 2 in $(t-4)^2$ is the size of the largest Jordan block of eigenvalue 4, while the exponent 1 in $(t-5)^1$ is the size of the largest Jordan block of eigenvalue 5.

In Question 3.2.47 we asked if it was always possible to have a "nice" matrix representation of an operator. By nice, we mean: a diagonal by Jordan blocks matrix.

Definition 5.3.5.

Let $V \neq \{0\}$ be a finite dimensional vector space and let $T \in \mathcal{L}(V)$ be an operator. A **Jordan normal form** (also called a **Jordan normal form**) for T is a matrix

representation of the form

$$[T]_{\mathscr{B}}^{\mathscr{B}} = \begin{bmatrix} J_1 & & & \\ & J_2 & & \\ & & \ddots & \\ & & & J_l \end{bmatrix}, \tag{5.6}$$

where J_j is a Jordan block of an eigenvalue of T (different blocks might have the same eigenvalue).
A basis $\mathscr{B}$ for which $[T]_{\mathscr{B}}^{\mathscr{B}}$ is a Jordan normal form is called a **Jordan basis** for T.
A square matrix is a **Jordan matrix** if it is diagonal by block, with each block a Jordan block. That is, if it is as the matrix appearing in the right-hand side of Equation (5.6).
Let $A \in \mathbf{F}^{m,m}$ be a square matrix. The **Jordan normal form** of A is the Jordan normal form the operator $\mathrm{L}_A \in \mathcal{L}(\mathbf{F}^m)$, $\mathrm{L}_A : v \mapsto Av$.

As a direct corollary of Proposition 5.3.2 we obtain.

Corollary 5.3.6. *Let $V \neq \{0\}$ be a finite dimensional vector space and let $T \in \mathcal{L}(V)$ be an operator. Suppose that T admits a Jordan normal form J and let $\lambda_1, \dots, \lambda_l$ be the distinct eigenvalues of T. Then $\mathrm{M}_T(t) = (t-\lambda_1)^{k_{\lambda_1}} \cdots (t-\lambda_l)^{k_{\lambda_l}}$ where k_{λ_j} is the maximal size of a Jordan block of eigenvalue λ_j occurring in J.*

Every nilpotent operator admits a Jordan normal form (here we don't need that $\mathbf{F} = \mathbf{C}$).

Lemma 5.3.7. *Let $V \neq \{0\}$ be a finite dimensional vector space and let $T \in \mathcal{L}(V)$ be a nilpotent operator. Then there exists a Jordan basis $\mathscr{B}$ for T. Moreover, the Jordan normal form for T is unique up to a permutation of the Jordan blocks.*

Proof. If $T = 0$ is the zero operator, then in any basis the matrix representing T is the 0 matrix and hence a Jordan matrix. We can hence suppose that $T \neq 0$. Let k be the smallest integer such that $T^k = 0$. By the above, $k \geq 2$.

$$\{0\} = \ker(T^0) \subsetneq \ker(T) \subsetneq \cdots \subsetneq \ker(T^{k-1}) \subsetneq \ker(T^k) = V.$$

In Proposition 5.1.37, we started with a basis of $\ker(T)$ an extended it step by step to obtain a basis $\mathscr{C}$ of $\ker(T^k) = V$ such that $[T]_{\mathscr{C}}^{\mathscr{C}}$ is upper triangular (with 0 on the diagonal). Here we will go in the opposite direction: start with a maximal independent family of $\ker(T^k) \setminus \ker(T^{k-1})$ and extend it carefully to a basis $\mathscr{B}$ of V such that $[T]_{\mathscr{B}}^{\mathscr{B}}$ is a Jordan matrix.

For $j \in \{1, \dots, k\}$, let us write $d_j := \dim \ker(T^j)$. So $1 \leq d_1 < d_2 < \cdots < d_k$ and $d_1 = \dim(\mathrm{E}(0,T))$ is the geometric multiplicity of 0 while $d_k = \dim(\mathrm{G}(0,T)) = \dim(V)$ is the algebraic multiplicity of 0. Write $c_k := d_k - d_{k-1} \geq 1$. We will show that J has c_k blocks of size k.

In order to ease the understanding of the proof, we will illustrate it (in blue) for $k = 4$ and $d_1 = 4, d_2 = 7, d_3 = 9, d_4 = 11$.

We have $d_k = d_{k-1} + c_k$. Therefore, it is possible to find c_k vectors $v_{k,1}, v_{k,2}, \dots, v_{k,c_k}$ in $\ker(T^k)$ such that $\operatorname{span}(\ker(T^{k-1}), v_{k,1}, v_{k,2}, \dots, v_{k,c_k}) = \ker(T^k)$. (For example, take any basis of $\ker(T^{k-1})$ and extend it to a basis of $\ker(T^k)$.) This implies in particular that the $v_{k,1}, v_{k,2}, \dots, v_{k,c_k}$ are linearly independent and moreover that a non-trivial linear combination of the $v_{k,1}, v_{k,2}, \dots, v_{k,c_k}$ never belongs to $\ker(T^{k-1})$. For $l \in \{1, \dots, c_k\}$ and $j \in \{1, \dots, k-1\}$, let $v_{j,l} := T^{k-j} v_{k,l}$. So for example, $v_{k-2,3} = T^2 v_{k,3}$. In our example, we have $c_4 = 2$, which gives us the following 8 vectors.

$$\underset{\substack{v_{1,1}\\v_{1,2}}}{\ker(T)} \subsetneq \underset{\substack{v_{2,1}\\v_{2,2}}}{\ker(T^2)} \subsetneq \underset{\substack{v_{3,1}\\v_{3,2}}}{\ker(T^3)} \subsetneq \underset{\substack{v_{4,1}\\v_{4,2}}}{\ker(T^4)} = V. \tag{5.7}$$

Since the $v_{k,l}$ are in in $\ker(T^k)$ but not in $\ker(T^{k-1})$, the $v_{j,l}$ are in in $\ker(T^j)$ but not in $\ker(T^{j-1})$. Moreover, it follows from the fact that non-trivial linear combination of the $v_{k,1}, v_{k,2}, \dots, v_{k,c_k}$ never belongs to $\ker(T^{k-1})$ that the list

$$\mathscr{B}_k := (v_{1,1}, v_{2,1}, \dots, v_{k,1}, \dots, v_{1,c_k}, \dots, v_{k,c_k})$$

is linearly independent.

Observe that $T(v_{j,l}) = v_{j-1,l}$ if $j \geq 2$ by definition, and $T(v_{1,l}) = 0$ as $v_{1,l}$ is in $\ker(T)$. Before going further, let us look a little more at $\mathscr{B}_k$. As we have just seen, $U_k := \operatorname{span}(\mathscr{B}_k)$ is T-invariant and $[T|_{U_k}]^{\mathscr{B}_k}_{\mathscr{B}_k}$ is a diagonal by block matrix, with c_k Jordan blocks of size k.

$$[T|_{U_k}]^{\mathscr{B}_k}_{\mathscr{B}_k} = \begin{bmatrix} J_1 & & & \\ & J_2 & & \\ & & \ddots & \\ & & & J_{c_k} \end{bmatrix}, \qquad J_j = \begin{array}{c} \begin{matrix} 1 & 2 & \cdots & \cdots & k \end{matrix} \\ \begin{matrix} 1 \\ 2 \\ \vdots \\ \vdots \\ k \end{matrix} \begin{bmatrix} 0 & 1 & & & \\ & \ddots & \ddots & & \\ & & \ddots & \ddots & \\ & & & \ddots & 1 \\ & & & & 0 \end{bmatrix} \end{array}.$$

We will now take care of the Jordan blocks of size $k-1$ (if any). Let $c_{k-1} := d_{k-1} - d_{k-2} - c_k$. By the above, $c_{k-1} \geq 0$. If $c_{k-1} = 0$, then there will be no Jordan blocks of size $k-1$ and we can directly go to the next step. This is the case in our example, so we do not add vectors to the list in Equation (5.7). If $c_{k-1} \geq 1$, take any basis $\mathscr{C}_{k-2}$ of $\ker(T^{k-2})$. It is possible to complete $\mathscr{C}_{k-2}, v_{k-1,1}, \dots, v_{k-1,c_k}$ to a basis $\mathscr{C}_{k-2}, v_{k-1,1}, \dots, v_{k-1,c_k}, v_{k-1,c_k+1}, \dots, v_{k-1,c_k+c_{k-1}}$ of $\ker(T^{k-1})$. For $l \in \{c_k + 1, \dots, c_k + c_{k-1}\}$ and $j \in \{1, \dots, k-2\}$, let $v_{j,l} := T^{k-j} v_{k,l}$. Then both the list

$$\mathscr{B}_{k-1} := (v_{1,c_k+1}, \dots, v_{k-1,c_k+1}, \dots, v_{1,c_k+c_{k-1}}, \dots, v_{k-1,c_k+c_{k-1}})$$

and $\mathscr{B}_k \cup \mathscr{B}_{k-1}$ are linearly independent. Moreover, for any $v_{j,l} \in \mathscr{B}_k \cup \mathscr{B}_{k-1}$, $T(v_{j,l}) = v_{j-1,l}$ if $j \geq 2$ while $T(v_{1,l}) = 0$. Finally, $U_{k-1} := \operatorname{span}(\mathscr{B}_{k-1})$ is T-invariant and $[T|_{U_{k-1}}]^{\mathscr{B}_{k-1}}_{\mathscr{B}_{k-1}}$ is a diagonal by block matrix, with c_{k-1} Jordan blocks of size $k-1$.

We conclude that $U_k + U_{k-1}$ is a direct sum, that $U_k \oplus U_{k-1}$ is T-invariant and that $[T|_{U_k \oplus U_{k-1}}]^{\mathscr{B}_k \cup \mathscr{B}_{k-1}}_{\mathscr{B}_k \cup \mathscr{B}_{k-1}}$ is a diagonal by block matrix, with c_k Jordan blocks of size k followed by c_{k-1} Jordan blocks of size $k-1$.

$$[T|_{U_k \oplus U_{k-1}}]^{\mathscr{B}_k \cup \mathscr{B}_{k-1}}_{\mathscr{B}_k \cup \mathscr{B}_{k-1}} = \begin{bmatrix} J_1 & & & & \\ & \ddots & & & \\ & & J_{c_k} & & \\ & & & J_{c_k+1} & \\ & & & & \ddots \\ & & & & & J_{c_k+c_{k-1}} \end{bmatrix},$$

$$J_j = \begin{cases} \begin{array}{c} \\ 1 \\ 2 \\ \vdots \\ k-1 \\ k \end{array} \begin{array}{c} \begin{array}{cccc} 1 & 2 & \cdots & k \end{array} \\ \begin{bmatrix} 0 & 1 & & \\ & \ddots & \ddots & \\ & & \ddots & 1 \\ & & & 0 \end{bmatrix} \end{array} & \text{if } j \in \{1, \dots, c_k\}, \\ \begin{array}{c} \\ 1 \\ 2 \\ \vdots \\ k-1 \end{array} \begin{array}{c} \begin{array}{ccc} 1 & 2 \cdots & k-1 \end{array} \\ \begin{bmatrix} 0 & 1 & \\ & \ddots & \ddots \\ & & 1 \\ & & 0 \end{bmatrix} \end{array} & \text{if } j \in \{c_k + 1, \dots, c_m + c_{k-1}\}. \end{cases}$$

Iterating this procedure, we obtain integers $c_{k-2} = d_{k-2} - d_{k-3} - c_k - c_{k-1}$ up to $c_1 = d_1 - 0 - c_k - \cdots - c_2$ and $\mathscr{B} := \mathscr{B}_k \cup \mathscr{B}_{k-1} \cup \cdots \cup \mathscr{B}_1$ is a basis for V such that $[T]^{\mathscr{B}}_{\mathscr{B}}$ is a diagonal by block matrix, with c_k Jordan blocks of size k, c_{k-1} Jordan blocks of size $k-1$, ..., and c_1 Jordan blocks of size 1. In our example, we have $c_3 = 0$, $c_2 = 1$ and $c_2 = 0$, which gives 11 vectors forming a Jordan basis

$$\begin{array}{ccccccccc} \ker(T) & \subsetneq & \ker(T^2) & \subsetneq & \ker(T^3) & \subsetneq & \ker(T^4) & = & V. \\ v_{1,1} & \mapsto & v_{2,1} & \mapsto & v_{3,1} & \mapsto & v_{4,1} & & \\ v_{1,2} & \mapsto & v_{2,2} & \mapsto & v_{3,2} & \mapsto & v_{4,2} & & \\ v_{1,3} & \mapsto & v_{2,3} & & & & & & \\ v_{1,4} & & & & & & & & \end{array}$$

For our particular example, we conclude that the normal Jordan normal form has 2

Jordan blocks of size 4, 0 of size 3, one of size 2 and one of size 1.

$$J = \begin{bmatrix} \boxed{\begin{matrix} 0 & 1 & & \\ & 0 & 1 & \\ & & 0 & 1 \\ & & & 0 \end{matrix}} & & & & \\ & \boxed{\begin{matrix} 0 & 1 & & \\ & 0 & 1 & \\ & & 0 & 1 \\ & & & 0 \end{matrix}} & & & \\ & & \boxed{\begin{matrix} 0 & 1 \\ & 0 \end{matrix}} & & \\ & & & \boxed{\begin{matrix} 0 \end{matrix}} & \\ & & & & \boxed{\begin{matrix} 0 \end{matrix}} \end{bmatrix}.$$

In order to finish the proof, we still need to show the unicity of the Jordan from. But in any Jordan normal form, a Jordan block of size k in a Jordan normal form of T correspond to a vector in $\ker(T^k) \setminus \ker(T^{k-1})$. Therefore, the number of Jordan blocks of size k is equal to $c_k = \dim(\ker(T^k)) - \dim(\ker(T^{m-1}))$, which depends only on T. Similarly, one can show that for every $j \in \{1, \dots, k\}$, the number of Jordan blocks of size j is exactly c_j and hence depends only on T. This proves that the Jordan normal form is unique, up to permutation of the Jordan blocks. □

We finally answer Question 3.2.47: every operator on a complex vector space admits a nice matrix representation.

Theorem 5.3.8.

Let $V \neq \{0\}$ be a finite dimensional vector space over $\mathbf{C}$ and let $T \in \mathcal{L}(V)$ be an operator. Then there exists a basis $\mathscr{B}$ of V such that $[T]^{\mathscr{B}}_{\mathscr{B}}$ is a Jordan normal form for T. Moreover, the Jordan normal form for T is unique up to a permutation of the Jordan blocks.

Proof. Let $\lambda_1, \dots, \lambda_l$ be the eigenvalues of T. Then, by Theorem 5.1.49, $V = \mathrm{G}(\lambda_1, T) \oplus \cdots \oplus \mathrm{G}(\lambda_l, T)$, each of the $U_j := \mathrm{G}(\lambda_j, T)$ is invariant by $T - \lambda_j \operatorname{Id}_V$ and $S_j := T - \lambda_j \operatorname{Id}_V|_{U_j}$ is a nilpotent operator on U_j. Therefore, by Lemma 5.3.7 there exists a basis $\mathscr{B}_j$ be a basis of U_j for which $[S_j]^{\mathscr{B}_j}_{\mathscr{B}_j}$ is diagonal by [Jordan blocks of eigenvalue 0]. We conclude that $[T|_{U_j}]^{\mathscr{B}_j}_{\mathscr{B}_j}$ is diagonal by [Jordan blocks of eigenvalues λ_j]. Finally, $\mathscr{B} = \mathscr{B}_1 \cup \cdots \cup \mathscr{B}_l$ is a basis for V (by direct sum) and $[T]^{\mathscr{B}}_{\mathscr{B}}$ is diagonal by block, with blocks $[T|_{U_1}]^{\mathscr{B}_1}_{\mathscr{B}_1}, \dots, [T|_{U_m}]^{\mathscr{B}_l}_{\mathscr{B}_l}$ (by invariance of the U_j and construction of $\mathscr{B}$):

$$[T]^{\mathscr{B}}_{\mathscr{B}} = \begin{bmatrix} [T_1]^{\mathscr{B}_1}_{\mathscr{B}_1} & & & \\ & [T_2]^{\mathscr{B}_2}_{\mathscr{B}_2} & & \\ & & \ddots & \\ & & & [T_2]^{\mathscr{B}_l}_{\mathscr{B}_l} \end{bmatrix}. \qquad \square$$

By looking carefully at the proofs of Lemma 5.3.7 and Theorem 5.3.8 one obtain the following important relation between the Jordan form and the geometric multiplicity.

Proposition 5.3.9. *Let $V \neq \{0\}$ be a finite dimensional vector space over $\mathbf{C}$ and let $T \in \mathcal{L}(V)$ be an operator. Let λ be an eigenvalue for T. Then $\mathrm{m}_{\mathrm{geo}}\,\lambda T$ is the number of blocks of eigenvalue λ in any Jordan form of T.*

Proof. In the proof of Lemma 5.3.7, each sequence $v_{1,j}, \dots, v_{r_j,j}$ gives rise to one Jordan block. The number of such sequences is equal to the dimension of $\ker(T)$.

Therefore, for a general (not necessarily nilpotent) operator, the number of Jordan blocks of eigenvalues λ in a Jordan form is equal to $\dim(\ker(T - \lambda\,\mathrm{Id})) = \mathrm{m}_{\mathrm{geo}}\,\lambda T$. □

Theorem 5.3.8 relies on Theorems 5.1.48 and 5.1.49. A careful look at the proofs of these results shows that the key point is that the operator T has "enough eigenvalues", which is equivalent to $\chi_T(t) = (t-\lambda_1)^{\mathrm{m_{alg}}(\lambda_1,T)} \cdots (t-\lambda_l)^{\mathrm{m_{alg}}(\lambda_l,T)}$ splits as a product of monomial. So we have

Theorem 5.3.10.

Let $\mathbf{F}$ be a field, $V \neq \{0\}$ be a finite dimensional $\mathbf{F}$-vector space and $T \in \mathcal{L}(V)$ be an operator. Suppose that $\chi_T(t) = (t-\lambda_1)^{a_1} \cdots (t-\lambda_l)^{a_l}$ for some $\lambda_j \in \mathbf{F}$ and $a_j \in \mathbf{N}$. Then

1. *The λ_j are the distinct eigenvalues of T and $a_j = \mathrm{m_{alg}}(\lambda_j, T)$;*
2. *Each of the $\mathrm{G}(\lambda_j, T)$ is a T-invariant subspace;*
3. *$V = \mathrm{G}(\lambda_1, T) \oplus \cdots \oplus \mathrm{G}(\lambda_k, T)$;*
4. *The operator $T_j := (T - \lambda_j \mathrm{Id}_V)\big|_{\mathrm{G}(\lambda_j,T)}$ is a nilpotent operator on $\mathrm{G}(\lambda_j, T)$.*
5. *There exists a basis $\mathscr{B}$ of V such that $[T]^{\mathscr{B}}_{\mathscr{B}}$ is a Jordan normal form for T. Moreover, the Jordan normal form for T is unique up to a permutation of the Jordan blocks.*

Below is a small example that follows the algorithm of Lemma 5.3.7 to find a Jordan basis.

Example 5.3.11. Let $A = \begin{bmatrix} 2 & & \\ 1 & 2 & \\ 0 & 0 & 2 \end{bmatrix}$. Since A is triangular, its only eigenvalue is 2, with algebraic multiplicity 3.

We compute

$$2\,\mathrm{Id} - A = \begin{bmatrix} 0 & & \\ -1 & 0 & \\ 0 & 0 & 0 \end{bmatrix}, \qquad (2\,\mathrm{Id} - A)^2 = 0.$$

So we have $\{0\} \subsetneq \ker(2\,\mathrm{Id} - A) \subsetneq \ker(2\,\mathrm{Id} - A)^2 = V$ and $\mathrm{M}_A(t) = (t-2)^2$. In other words, in the Jordan normal form for A the size of the biggest Jordan block is 2. Since A is a 3×3 matrix, it means we have two Jordan blocks, the second one being of size 1. That is, the Jordan normal form of A is $J = \begin{bmatrix} \boxed{\begin{matrix} 2 & 1 \\ & 2 \end{matrix}} & & \\ & & \\ & & \boxed{2} \end{bmatrix}$.

To find a Jordan basis, we solve $\begin{bmatrix} 0 & & \\ -1 & 0 & \\ 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} x \\ y \\ z \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}$ and find $\ker(2\,\mathrm{Id} - A) = \mathrm{E}(2, A) = \left\{ \begin{bmatrix} 0 \\ y \\ z \end{bmatrix} \,\middle|\, y, z \in \mathbf{R} \right\}$. This means that $\dim(\ker(2\,\mathrm{Id} - A)) = 2$ while $\dim(\ker(2\,\mathrm{Id} - A)^2) = \dim V = 3$. Since $3 - 2 = 1$, we need to find one vector $v_{2,1}$ in $\ker(2\,\mathrm{Id} - A)^2 = V$ but not in $\ker(2\,\mathrm{Id} - A)$. One can for example take $v_{2,1} = \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}$.

Now, we compute

$$v_{1,1} = (2\,\mathrm{Id} - A)v_{2,1} = \begin{bmatrix} 0 & & \\ -1 & 0 & \\ 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ -1 \\ 0 \end{bmatrix}.$$

Finally, we complete $v_{1,1}$ into a basis $(v_{1,1}, v_{1,2})$ of $\ker(2\,\mathrm{Id} - A)$. One can for example take $v_{1,2} = \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix}$.

Altogether, $v_{2,1}, v_{1,1}, v_{1,2}$ is the desired Jordan basis.

Remark 5.3.12.

A careful analysis of the proof of Theorem 5.3.8 shows that even if $\mathbf{F} \neq \mathbf{C}$, the proof still works for all T with "enough" eigenvalues. For $\mathbf{F} = \mathbf{R}$ this means that all complex eigenvalues are real numbers. In general, this mean that the characteristic polynomial can be written as a product of degree 1 polynomials: $\chi_T(t) = (t - \lambda_1)^{\mathrm{m_{alg}}(\lambda_1)} \cdots (t - \lambda_l)^{\mathrm{m_{alg}}(\lambda_l)}$.
While we will no check the details of the above assertion, we will use it to prove the next corollary.

Corollary 5.3.13. *Let $V \neq \{0\}$ be a finite dimensional vector space and let $T \in \mathcal{L}(V)$ be an operator. Let $\lambda_1, \ldots, \lambda_l$ be the distinct eigenvalues of T. Then T is diagonalisable if and only if $\mathrm{M}_T(t) = (t - \lambda_1) \cdots (t - \lambda_l)$.*

Proof. Suppose that T is diagonalisable in some basis $\mathscr{B}$. Then $[T]^{\mathscr{B}}_{\mathscr{B}}$ is a Jordan normal form for T, in which all blocks have size 1. We conclude that $\mathrm{M}_T(t) = (t - \lambda_1) \cdots (t - \lambda_l)$ by Corollary 5.3.6.

Now suppose that $\mathrm{M}_T(t) = (t - \lambda_1) \cdots (t - \lambda_l)$. Then T admits a Jordan normal form J by Theorem 5.3.10. The maximal size of a Jordan block with eigenvalue λ_j in J is 1 (the exponent of $(t - \lambda_j)$ in $\mathrm{M}_T(t)$. So all Jordan blocks have size 1 and J is a diagonal matrix. □

In term of matrices, we obtain the following results.

Lemma 5.3.14. *For every $A \in \mathbf{C}^{m,m}$ there exists an invertible matrix $P \in \mathbf{C}^{m,m}$ such that $P^{-1}AP$ is the Jordan normal form of A.*

If $(v_1, \ldots, v_m)$ is a Jordan basis for A, then one can take $P = [v_1\ v_2\ \ldots\ v_m]$ (v_j is the j^{th} column of P).

Proof. Let us write $\mathrm{L}_A \in \mathcal{L}(\mathbf{C}^m)$ for the operator $\mathrm{L}_A(v) = Av$. Then we have $[\mathrm{L}_A]^{\mathscr{E}}_{\mathscr{E}} = A$ for the standard basis $\mathscr{E}$, while by Theorem 5.3.8 there exists a Jordan basis $\mathscr{B}$ such that $[\mathrm{L}_A]^{\mathscr{B}}_{\mathscr{B}} =: J$ is a Jordan matrix. But then the matrices A and J are similar.

If $\mathscr{B} = (v_1, \dots, v_m)$ is a Jordan basis, with corresponding Jordan matrix J, then $AP = [Av_1 \ Av_2 \ \dots \ Av_m] = [v_1 \ v_2 \ \dots \ v_m]J = PJ$, so $P^{-1}AP = J$ as desired. □

Corollary 5.3.15. *Two complex square matrices $A, B \in \mathbf{C}^{m,m}$ are similar if and only if they have the same Jordan normal form.*

Proof. "⇒" If the matrices A and B are similar, they represent the same operator T and hence have the same Jordan normal form (up to permutation of the Jordan block).

"⇐" Let J be the Jordan normal form of A and B. Since the Jordan normal form is unique (up to permutation of the Jordan block), $J = P^{-1}AP = Q^{-1}BQ$ for some invertible matrices $P, Q \in \mathbf{C}^{m,m}$. This gives $A = (QP^{-1})^{-1}B(QP^{-1})$. (Observe that the "⇐" implication is true for any field $\mathbf{F}$, not only for $\mathbf{C}$.) □

The following summarises the important relations between eigen-theory and the Jordan normal form.

Summary 5.3.16.

Let $V \neq \{0\}$ be a m dimensional vector space over $\mathbf{C}$ and let $T \in \mathcal{L}(V)$ be an operator. To such a T, one can associate:

- *Its distinct eigenvalues $\lambda_1, \dots, \lambda_l$ (we necessarily have $1 \leq l \leq \dim(V)$);*
- *For each eigenvalue, its algebraic multiplicity $\mathrm{m}_{\mathrm{alg}}(\lambda_j, T) = \dim(\mathrm{G}(\lambda_j, T))$;*
- *For each eigenvalue, its geometric multiplicity $\mathrm{m}_{\mathrm{geo}}(\lambda_j, T) = \dim(\mathrm{E}(\lambda_j, T))$;*
- *The characteristic polynomial $\chi_T(t) = (t - \lambda_1)^{\mathrm{m}_{\mathrm{alg}}(\lambda_1)} \cdots (t - \lambda_l)^{\mathrm{m}_{\mathrm{alg}}(\lambda_l)}$;*
- *The minimal polynomial $\mathrm{M}_T(t) = (t - \lambda_1)^{k_{\lambda_1}} \cdots (t - \lambda_l)^{k_{\lambda_l}}$, where the k_j are positive integers;*
- *The Jordan normal form J of T.*

Then we have the following:

- $\mathrm{m}_{\mathrm{alg}}(\lambda_j) \in \{1, \dots, \dim(V)\}$ *and* $\sum_{j=1}^{l} \mathrm{m}_{\mathrm{alg}}(\lambda_j) = \dim(V)$ *(Theorem 5.1.49);*
- $J = \begin{bmatrix} J_{\lambda_1} & & & \\ & J_2 & & \\ & & \ddots & \\ & & & J_{\lambda_l} \end{bmatrix}$, *where J_{λ_j} is the Jordan normal form of $T|_{\mathrm{G}(\lambda_j, T)}$ (Theorem 5.3.8);*

- $\mathrm{m}_{\mathrm{geo}}(\lambda_j) \in \{1, \dots, \mathrm{m}_{\mathrm{alg}}(\lambda_j)\}$ *is the number of Jordan blocks of eigenvalue* λ_j *in* J_{λ_j}. *In particular* J_{λ_j} *is diagonal if and only if and only if* $\mathrm{m}_{\mathrm{geo}}(\lambda_j) = \mathrm{m}_{\mathrm{alg}}(\lambda_j)$ *(proof of Lemma 5.3.7);*
- $k_{\lambda_j} \in \{1, \dots, \mathrm{m}_{\mathrm{alg}}(\lambda_j)\}$ *is the size of the biggest Jordan block of eigenvalue* λ_j *in* J_{λ_j}. *In particular* J_{λ_j} *is diagonal if and only if and only if all* $k_{\lambda_j} = 1$ *(Corollary 5.3.6);*
- *The sum of the size of all Jordan blocks of eigenvalue* λ_j *is equal to* $\mathrm{m}_{\mathrm{alg}}(\lambda_j)$ *(follows from the definition of* $\mathrm{m}_{\mathrm{alg}}(\lambda_j)$*).*

5.3.2 Computation of the Jordan normal form

Knowing that the Jordan normal form exists is good. Being able to compute it is better. This is the subject of this subsection. As we have seen in the last subsection, in order to find a Jordan basis for a matrix A or for an operator T, it is enough to be able to find a Jordan basis $\mathscr{B}_j$ it for each generalised eigenspace $\mathrm{G}(\lambda_j, A)$, which is done by looking at $\mathrm{null}(\lambda_j \mathrm{Id} - A) \subsetneq \cdots \subsetneq \mathrm{null}(\lambda_j \mathrm{Id} - A)^{k_j} = \mathrm{G}(\lambda_j, A)$, where $1 \leq k_j \leq \mathrm{m}_{\mathrm{alg}}(\lambda_j, A)$ is the smallest integer such that $(\lambda_j \mathrm{Id} - A)^{k_j} = 0$. Alternatively, k_j is the size of the biggest Jordan block of eigenvalue λ_j in the Jordan normal form of A.

Let us work on a concrete example.

Replace by a 3x3 example

Example 5.3.17. Let A be the complex square matrix

$$A = \begin{bmatrix} 2 & -4 & 2 & 2 \\ -2 & 0 & 1 & 3 \\ -2 & -2 & 3 & 3 \\ -2 & -6 & 3 & 7 \end{bmatrix}, \qquad \text{so } t\,\mathrm{Id}_4 - A = \begin{bmatrix} t-2 & 4 & -2 & -2 \\ 2 & t & -1 & -3 \\ 2 & 2 & t-3 & -3 \\ 2 & 6 & -3 & t-7 \end{bmatrix}.$$

We start by computing the characteristic polynomial of A. We will prove that $\chi_A(t) = (t-2)^2(t-4)^2$. It is of course possible and easier to ask a computer to do it. We will do it by hand to show how it can be done. First do rows operations (that do not change the determinant) on $t\,\mathrm{Id}_4 - A$: $r_1 \mapsto r_1 + (1 - t/2)r_2$, $r_3 \mapsto r_3 - r_2$ and $r_4 \mapsto r_4 - r_2$ to obtain

$$\begin{aligned} \det(A - t\,\mathrm{Id}_4) &= \det \begin{bmatrix} 0 & -\frac{t^2}{2} + t + 4 & \frac{t}{2} - 3 & \frac{3t}{2} - 5 \\ 2 & t & -1 & -3 \\ 0 & -t+2 & t-2 & 0 \\ 0 & -t+6 & -2 & t-4 \end{bmatrix} \\ &= -2 \det \begin{bmatrix} -\frac{t^2}{2} + t + 4 & \frac{t}{2} - 3 & \frac{3t}{2} - 5 \\ -t+2 & t-2 & 0 \\ -t+6 & -2 & t-4 \end{bmatrix}, \end{aligned}$$

which we can develop along the third column to obtain

$$\begin{aligned}\det(A - t\,\mathrm{Id}_4) &= (10-3t)\det\begin{bmatrix}-t+2 & t-2\\ -t+6 & -2\end{bmatrix} + (8-2t)\det\begin{bmatrix}-\frac{t^2}{2}+t+4 & \frac{t}{2}-3\\ t+2 & t-2\end{bmatrix}\\ &= (10-3t)(-4+2t-(-12+8t-t^2))\\ &\quad + (8-2t)(-8+2t+2t^2-\tfrac{t^3}{2}-(-6+4t-\tfrac{t^2}{2}))\\ &= (10-3t)(8-6t+t^2) + (4-t)(-4-4t+5t^2-t^3)\\ &= (80-84t+28t^2-3t^3) + (-16-12t+24t^2-9t^3+t^4)\\ &= t^4-12t^3+52t^2-96t+64.\end{aligned}$$

So we have $\chi_A(t) = t^4 - 12t^3 + 52t^2 - 96t + 64$ and we still need to find the roots. Since all the coefficients are integers, if a rational root exists it is of the form p/q, where p is a divisor of 64 (constant coefficient) and q a divisor of 1 (leading coefficient).[5] So the possible rational roots are in $\{\pm1, \pm2, \pm4, \pm8, \pm16, \pm32, \pm64\}$. By testing, we find that both 2 and 4 are roots. Therefore, $(t-2)(t-4) = t^2 - 6t + 8$ divides $\chi_A(t)$. A polynomial division (similar to a long division) gives us $t^4 - 12t^3 + 52t^2 - 96t + 64 / t^2 - 6t + 8 = t^2 - 6t + 8 = (t-2)(t-4)$. We have just showed $\chi_A(t) = (t-2)^2(t-4)^2$. Therefore, the eigenvalues of A are $\lambda_1 = 2$ and $\lambda_2 = 4$, both with algebraic multiplicity 2. We will now give two methods to compute the Jordan normal form. The first one will always work and gives a Jordan basis, but might be computation intensive. The second one might not work for big matrices, but is easier for small matrices.

Method 1: follow the proof of Lemma 5.3.7. For every eigenvalue, we will compute the nullspaces of $(\lambda\,\mathrm{Id} - A)^j$ for $1 \le j \le \mathrm{m}_{\mathrm{alg}}(\lambda, A)$ to determine the number and sizes of Jordan blocks corresponding to eigenvalue λ.

For $\lambda_1 = 2$. We have $\mathrm{m}_{\mathrm{alg}}(2, A) = 2$ hence $\{0\} \subsetneq \mathrm{null}(2\,\mathrm{Id}_4 - A) \subseteq \mathrm{null}(2\,\mathrm{Id}_4 - A)^2 = \mathrm{G}(2, A)$. So we will have 1 Jordan block of size 2 and eigenvalue 2 if $\mathrm{null}(2\,\mathrm{Id}_4 - A) \neq \mathrm{null}(2\,\mathrm{Id}_4 - A)^2$, but 2 blocks of size 1 if $\mathrm{null}(2\,\mathrm{Id}_4 - A) = \mathrm{null}(2\,\mathrm{Id}_4 - A)^2$. We have

$$2\,\mathrm{Id}_4 - A = \begin{bmatrix}0 & 4 & -2 & -2\\ 2 & 2 & -1 & -3\\ 2 & 2 & -1 & -3\\ 2 & 6 & -3 & -5\end{bmatrix}.$$

To compute $\mathrm{null}(2\,\mathrm{Id}_4 - A)$, we solve the system

$$\begin{bmatrix}0 & 4 & -2 & -2\\ 2 & 2 & -1 & -3\\ 2 & 2 & -1 & -3\\ 2 & 6 & -3 & -5\end{bmatrix} \cdot \begin{bmatrix}x\\ y\\ z\\ w\end{bmatrix} = \begin{bmatrix}0\\ 0\\ 0\\ 0\end{bmatrix}$$

[5] This is the "rational root theorem", which is not a trivial result.

Since the second and third rows are equal and $r_4 = r_1 + r_2$, this system is equivalent to

$$\begin{bmatrix} 0 & 4 & -2 & -2 \\ 2 & 2 & -1 & -3 \end{bmatrix} \cdot \begin{bmatrix} x \\ y \\ z \\ w \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix}.$$

So we have $\operatorname{null}(2\operatorname{Id}_4 - A) = \left\{ \begin{bmatrix} 2y-z \\ y \\ z \\ 2y-z \end{bmatrix} \;\middle|\; y, z \in \mathbf{R} \right\}$. This is a dimension 2 subspace and hence equal to $\mathrm{G}(2, A)$. Therefore, we can choose any basis of $\operatorname{null}(2\operatorname{Id}_4 - A)$ as a basis of $\mathrm{G}(2, A)$. For example, one can take $v_1 = [2, 1, 0, 2]^\mathsf{T}$ and $v_2 = [0, 1, 2, 0]^\mathsf{T}$.

We now take care of $\lambda_2 = 4$. Once again $\mathrm{m}_{\mathrm{alg}}(4, A) = 2$ and we thus have 1 Jordan block of size 2 if $\operatorname{null}(4\operatorname{Id}_4 - A) \neq \operatorname{null}(4\operatorname{Id}_4 - A)$, but 2 blocks of size 1 if $\operatorname{null}(4\operatorname{Id}_4 - A) = \operatorname{null}(4\operatorname{Id}_4 - A)$. We have

$$4\operatorname{Id}_4 - A = \begin{bmatrix} 2 & 4 & -2 & -2 \\ 2 & 4 & -1 & -3 \\ 2 & 2 & 1 & -3 \\ 2 & 6 & -3 & -3 \end{bmatrix}.$$

To compute $\operatorname{null}(A - 4\operatorname{Id}_4)$, we solve the system (where we do $r_2 \mapsto r_2 - r_1$, $r_3 \mapsto r_3 - r_1$)

$$\begin{bmatrix} 0 & 4 & -2 & -2 \\ 2 & 2 & -1 & -3 \\ 2 & 2 & -1 & -3 \\ 2 & 6 & -3 & -5 \end{bmatrix} \cdot \begin{bmatrix} x \\ y \\ z \\ w \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \end{bmatrix} \implies \begin{bmatrix} 2 & 4 & -2 & -2 \\ 0 & 0 & 1 & -1 \\ 0 & -2 & 3 & -1 \\ 2 & 6 & -3 & -3 \end{bmatrix} \cdot \begin{bmatrix} x \\ y \\ z \\ w \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}.$$

We hence have $y = z = w$ and $x = 0$. Since $\operatorname{null}(4\operatorname{Id}_4 - A)$ is of dimension at least 1, we conclude $\{0\} \subsetneq \operatorname{null}(4\operatorname{Id}_4 - A) = \{[0, y, y, y]^\mathsf{T} \mid y \in \mathbf{C}\} \subsetneq \operatorname{null}(4\operatorname{Id}_4 - A)^2 = \mathrm{G}(4, A)$. We have

$$(4\operatorname{Id}_4 - A)^2 = 4\begin{bmatrix} 1 & 2 & -1 & -1 \\ 1 & 1 & 0 & -1 \\ 1 & 0 & 1 & -1 \\ 1 & 2 & -1 & -1 \end{bmatrix}.$$

It is not necessary to have a full description of $\operatorname{null}(4\operatorname{Id}_4 - A)^2$, only to find a vector v_4 that is inside $\operatorname{null}(4\operatorname{Id}_4 - A)^2$, but not inside $\operatorname{null}(4\operatorname{Id}_4 - A)$. One can solve a system to find v_4 or simply guess $v_4 = [1, -1, -1, 0]^\mathsf{T}$. Finally, taking $v_3 = (4\operatorname{Id}_4 - A)v_4 = [0, 1, 1, 1]^\mathsf{T}$ gives us a basis v_3, v_4 of $\operatorname{null}(4\operatorname{Id}_4 - A)^2 = \mathrm{G}(4, A)$ with $v_3 \in \operatorname{null}(4\operatorname{Id}_4 - A)$.

Let us take $\mathscr{B} = (v_1, v_2, v_3, v_4)$ for a basis. We have $Av_1 = 2v_1$, $Av_2 = 2v_2$, $Av_3 = 4v_3$ and $Av_4 = v_3 + 4v_4$. So, for $P := [v_1\ v_2\ v_3\ v_4]$ we have

$$AP = [Av_1\ Av_2\ Av_3\ Av_4] = [v_1\ v_2\ v_3\ v_4] \begin{bmatrix} 2 & & & \\ & 2 & & \\ & & 4 & 1 \\ & & & 4 \end{bmatrix}.$$

That is:

$$P^{-1}AP = \begin{bmatrix} 2 & & & \\ & 2 & & \\ & & 4 & 1 \\ & & & 4 \end{bmatrix} =: J$$

is the Jordan normal form of A.

Method 2: compute the minimal polynomial. The characteristic polynomial of A is $\chi_A(t) = (t-2)^2(t-4)^2$, and thus the minimal polynomial is $\mathrm{M}_A(t) = (t-2)_2^k(t-4)_4^k$ for some $1 \leq k_2 \leq 2$ and $1 \leq k_4 \leq 2$. We hence have 4 candidates: $(t-2)(t-4)$, $(t-2)^2(t-4)$, $(t-2)(t-4)^2$ and $(t-2)(t-4)$. Among these four polynomial, we need to find the minimal one satisfying $p(A) = 0$. This means we need to test at most 3 polynomials. We have

$$(A - 2\,\mathrm{Id}_4)(A - 4\,\mathrm{Id}_4) = \begin{bmatrix} 0 & -4 & 2 & 2 \\ -2 & -2 & 1 & 3 \\ -2 & -2 & 1 & 3 \\ -2 & -6 & 3 & 5 \end{bmatrix} \begin{bmatrix} -2 & -4 & 2 & 2 \\ -2 & -4 & 1 & 3 \\ -2 & -2 & -1 & 3 \\ -2 & -6 & 3 & 3 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & -4 & * & * \\ * & * & * & * \\ * & * & * & * \end{bmatrix}$$

Exercise 5.3.18. For the following four matrices, decide which ones are similar. (They all have characteristic polynomial t^4 and are hence nilpotent.)

$$A = \begin{bmatrix} \boxed{\begin{matrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{matrix}} & \begin{matrix} 0 \\ 0 \\ 0 \end{matrix} \\ \begin{matrix} 0 & 0 & 0 \end{matrix} & \boxed{0} \end{bmatrix}, \qquad B = \begin{bmatrix} \boxed{\begin{matrix} 0 & 1 \\ 0 & 0 \end{matrix}} & \begin{matrix} 0 & 0 \\ 0 & 0 \end{matrix} \\ \begin{matrix} 0 & 0 \\ 0 & 0 \end{matrix} & \boxed{\begin{matrix} 0 & 1 \\ 0 & 0 \end{matrix}} \end{bmatrix},$$

$$C = \begin{bmatrix} \boxed{\begin{matrix} 0 & 1 \\ 0 & 0 \end{matrix}} & \begin{matrix} 0 & 0 \\ 0 & 0 \end{matrix} \\ \begin{matrix} 0 & 0 \\ 0 & 0 \end{matrix} & \boxed{\begin{matrix} 0 & 0 \\ 0 & 0 \end{matrix}} \end{bmatrix}, \qquad D = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}.$$

Solution. The matrices A, B and C are already in Jordan normal form. These Jordan normal form are distinct (even up to permutation of the blocks), which implies that these matrices are mutually non-similar. For D, we have $\operatorname{rank}(D) = \dim(\operatorname{col}(D)) = 2$ so $\dim(\operatorname{null}(D)) = 4 - 2 = 2$. But $D^2 = 0$ and thus $\dim(\operatorname{null}(D^2)) = 4$. So we choose $2 = \dim(\operatorname{null}(D^2)) - \dim(\operatorname{null}(D))$ vectors u_2 and v_2 in $\operatorname{null}(D^2)$ but not in $\operatorname{null}(D)$. Then we write $u_1 := Du_2$ and $v_1 := Dv_2$ to obtain a basis (u_1, u_2, v_1, v_2) of $\mathbf{C}^4$. Since we have two sequences u_1, u_2 and v_1, v_2 of length 2 we have two Jordan blocks of size 2×2. In other words, the Jordan normal form of D is

$$\begin{bmatrix} \boxed{\begin{matrix} 0 & 1 \\ 0 & 0 \end{matrix}} & \begin{matrix} 0 & 0 \\ 0 & 0 \end{matrix} \\ \begin{matrix} 0 & 0 \\ 0 & 0 \end{matrix} & \boxed{\begin{matrix} 0 & 1 \\ 0 & 0 \end{matrix}} \end{bmatrix} = B.$$

Therefore, D and B are similar. □

While the minimal polynomial and the characteristic polynomial are useful tools to compute the Jordan normal form, they are not always sufficient to recover the Jordan normal form as demonstrated by the following example.

Example 5.3.19. The following two matrices have the same characteristic polynomial $(t-2)^4$ and the same minimal polynomial $(t-2)^2$, but not the same Jordan normal form.

$$A = \begin{bmatrix} \boxed{\begin{matrix} 2 & 1 \\ & 2 \end{matrix}} & & \\ & \boxed{\begin{matrix} 2 & 1 \\ & 2 \end{matrix}} & \\ & & \end{bmatrix}, \qquad B = \begin{bmatrix} \boxed{\begin{matrix} 2 & 1 \\ & 2 \end{matrix}} & & \\ & \boxed{2} & \\ & & \boxed{2} \end{bmatrix}.$$

Observe that the geometric multiplicity of 2 in A is 2, while it is 3 in B, so we can still distinguish A and B using eigen-theory. (In both cases, the algebraic multiplicity of 2 is 4.)

For following two matrices, the only eigenvalue 2 has geometric multiplicity 2 and algebraic multiplicity 4 in both cases, but the Jordan normal form are not the same.

$$C = \begin{bmatrix} \boxed{\begin{matrix} 2 & 1 & \\ & 2 & 1 \\ & & 2 \end{matrix}} & \\ & \boxed{2} \end{bmatrix}, \qquad D = \begin{bmatrix} \boxed{\begin{matrix} 2 & 1 \\ & 2 \end{matrix}} & \\ & \boxed{\begin{matrix} 2 & 1 \\ & 2 \end{matrix}} \end{bmatrix}.$$

Observe that the above two matrices do not have the same minimal polynomial and so can still be distinguished by eigen-theory. Indeed $\mathrm{M}_C(t) = (t-2)^3$ while $\mathrm{M}_D(t) = (t-2)^2$.

It is possible to construct bigger matrices such that eigen-theory is not able to distinguish between them. The following two matrices have the same characteristic polynomial $(t-2)^7$ and the same minimal polynomial $(t-2)^3$. Moreover, they have the same eigenvalues 2, with the same algebraic multiplicity 7 and the same geometric multiplicity 3. Nevertheless, they do not have the same Jordan normal form.

$$E = \begin{bmatrix} \boxed{\begin{matrix} 2 & 1 & \\ & 2 & 1 \\ & & 2 \end{matrix}} & & \\ & \boxed{\begin{matrix} 2 & 1 \\ & 2 & 1 \\ & & 2 \end{matrix}} & \\ & & \boxed{2} \end{bmatrix}, \qquad F = \begin{bmatrix} \boxed{\begin{matrix} 2 & 1 & \\ & 2 & 1 \\ & & 2 \end{matrix}} & & \\ & \boxed{\begin{matrix} 2 & 1 \\ & 2 \end{matrix}} & \\ & & \boxed{\begin{matrix} 2 & 1 \\ & 2 \end{matrix}} \end{bmatrix}.$$

The matrices from Example 5.3.19 were not randomly chosen. Indeed, one can prove:

Lemma 5.3.20. *Let V be a finite dimensional vector space over $\mathbf{C}$ and let T be an operator with only one eigenvalue, so $\chi_T(t) = (t-\lambda)^{\mathrm{m}_{\mathrm{alg}}(\lambda)}$ and $\mathrm{M}_T(t) = (t-\lambda)^{k_\lambda}$. Then (recall that $\mathrm{m}_{\mathrm{geo}}(\lambda_j) = \dim(\mathrm{E}(\lambda_j, T))$ is the geometric multiplicity)*

1. *If $\mathrm{m}_{\mathrm{alg}}(\lambda) \leq 3$, then $(\mathrm{m}_{\mathrm{alg}}(\lambda), k_\lambda)$ determines the Jordan normal form J of T;*

2. *If* $\mathrm{m}_{\mathrm{alg}}(\lambda) \leq 3$*, then* $(\mathrm{m}_{\mathrm{alg}}(\lambda), \mathrm{m}_{\mathrm{geo}}(\lambda))$ *determines the Jordan normal form* J *of* T*;*

3. *If* $\mathrm{m}_{\mathrm{alg}}(\lambda) \leq 6$*, then* $(\mathrm{m}_{\mathrm{alg}}(\lambda), k_\lambda, \mathrm{m}_{\mathrm{geo}}(\lambda))$ *determines the Jordan normal form* J *of* T*.*

Proof. By Theorem 5.3.16, J is a matrix of size $\mathrm{m}_{\mathrm{alg}}(\lambda)$ with $\mathrm{m}_{\mathrm{geo}}(\lambda)$ blocks of maximal size k_λ. To determine J, it is enough to know the number b_n of blocks of size n for each $1 \leq n \leq \mathrm{m}_{\mathrm{alg}}(\lambda)$. But the total size of J is the sum of the size of the blocks:

$$\mathrm{m}_{\mathrm{alg}}(\lambda) = \underbrace{1 + \cdots + 1}_{b_1} + \underbrace{2 + \cdots + 2}_{b_2} + \cdots + \underbrace{k_\lambda + \cdots + k_\lambda}_{b_{k_\lambda}}, \tag{5.8}$$

where $b_n \geq 0$ for $n \in \{1, \dots, k_\lambda - 1\}$, $b_{k_\lambda} \geq 1$ and $b_1 + b_2 + \cdots + b_{k_\lambda} = \mathrm{m}_{\mathrm{geo}}(\lambda)$ is the number of blocks.

For a given $\mathrm{m}_{\mathrm{alg}}(\lambda) \leq 6$, one can list all the decompositions according to Equation (5.8) and check that no two such decompositions share the same triple $(\mathrm{m}_{\mathrm{alg}}(\lambda), k_\lambda, \mathrm{m}_{\mathrm{geo}}(\lambda))$. Alternatively, one can try to find the smallest counterexample possible. This will both prove the statement and explain how to obtain the matrices Example 5.3.19.

First of all, in order to find two distinct decompositions of a given $\mathrm{m}_{\mathrm{alg}}(\lambda)$, one should have $k_\lambda \geq 2$, as there exists a unique decomposition of $\mathrm{m}_{\mathrm{alg}}(\lambda)$ using only 1s. It is also trivial that such a counterexample need to use at least two summands, that is $\mathrm{m}_{\mathrm{geo}}(\lambda) \geq 2$ and so $\mathrm{m}_{\mathrm{alg}}(\lambda) \geq k_\lambda + 1$.

If $k_\lambda \geq 3$, then $\mathrm{m}_{\mathrm{alg}}(\lambda) \geq 4$. If $k_\lambda = 2$, then the only possibility tow have two different decomposition of $\mathrm{m}_{\mathrm{alg}}(\lambda)$ is to have a 2 in such a decomposition that splits into two 1s in the other decomposition. But in $2 = 1 + 1$, the left hand side has $k_\lambda = 2$ while the right hand side has $c_\lambda = 1$. Therefore, the smallest counterexample to 1 is $2 + 2 = 2 + 1 + 1$, which is matrices A and B from Example 5.3.19.

If one uses only 1s and 2s, one cannot write $\mathrm{m}_{\mathrm{alg}}(\lambda)$ in two different ways using the same number of summands. In other words, a counterexample to 2 necessarily has $k_\lambda \geq 3$. Which, using $\mathrm{m}_{\mathrm{geo}}(\lambda) \geq 2$, gives us $\mathrm{m}_{\mathrm{alg}}(\lambda) \geq 4$. For an explicit counterexample, one can hence take $3 + 1 = 2 + 2$, which is matrices C and D from Example 5.3.19.

For 3, one already knows that a counterexample has $k_\lambda \geq 3$. Moreover, since both decomposition have the same c_λ the smallest counterexample possible is $3+3+1 = 3+2+2$, which is matrices E and F from Example 5.3.19. □

Index

G

H

I

J

K

L

M

N

O

To go further

To go further

The content of this appendix can be skipped without harm and will **NOT** be in the exam. As its name suggests, it is meant for readers interested in delving deeper into the theory of vector spaces.

1 More about set theory

The formalisation of set theory and the use of infinite sets[1] were two major achievements of the 20^{th} century mathematics. They were the tools that allowed to ground mathematics in logic and they still are the foundations of most modern mathematics.

In what follow, we will only take a glimpse at set theory. We will neither be fully formal nor go into the details. Good references to learn set theory are:

- Herbert B. Enderton, *The Elements of Set Theory* (Academic Press, 1997);
- Derek Goldrei, *Classic Set Theory* (Chapman & Hall/CRC 1996);
- The Open Logic Project, *Set Theory, An Open Introduction* (https://builds.openlogicproject.org/courses/set-theory/)

1.1 A glimpse at set theory

In Section 1.1, we only saw a naive version of set theory where sets were "collection of elements" and were not properly defined. We will present here a less naive version, even if not totally formal. The version of set theory we present is known as (ZF) set theory:[2]

The main idea of (ZF) is that we have:

1. The standard symbols of logic: $=$ (equality), $\neg$ (negation), $\vee$ (disjunction, "or"), $\wedge$ (conjunction, "and"), $\implies$ (logical implication), $\forall$ ("for all" quantifier), $\exists$ ("there exists" quantifier), (and) (parentheses);
2. Variables X_1, X_2, ..., all of them representing "sets";

[1] Notably by George Cantor (1845– 1918).

[2] (ZF) is named after Ernst Zermelo (1871–1953) and Abraham Fraenkel (1891–1965). There exist other axiomatisations of set theory, as (NBG), named after John Von Neumann, Paul Isaac Bernays (1888–1977) and Kurt Friedrich Gödel (1906–1978)). (ZF) is probably the most commonly used axiomatisation of set theory.

3. A special new symbol $\in$ we need to make sense of.

Using the logic symbols and the newly added $\in$ symbol, it is possible to write down "formulas", as for example $\exists X \forall Y : \neg(Y \in X)$. Not every sequence of symbol is a formula, as for example the parentheses need to be balanced. We will not here give an explicit definition of what is a formula. The symbol of logic satisfies the standard axioms of logic. For example:

$$\neg(\varphi(x) \wedge \psi(x)) \iff (\neg\varphi(x)) \vee (\neg\psi(x)),$$

which means that if ($\varphi(x)$ and $\psi(x)$) is false, then either $\varphi(x)$ is false or $\psi(x)$ is false (or both), and vice-versa.

To make sense of the symbol $\in$ we need to introduce new axioms, which are formulas containing $\in$ that we decide should be always true.

(1) Axiom of extensionality. If two sets have the same elements, they are equal.

(2) Axiom of the empty set. There exists a set with no elements, written $\varnothing$ (this is equivalent to the existence of at least one set).

Some other axioms are straightforward and easily understood.

(3) Axiom of pairing. If X and Y are sets, then there exists a set Z containing both X and Y as elements and no other elements ($Z = \{X, Y\}$). In particular, given X one can construct a new set $\{X\}$, simply by taking $Y = X$ in the above construction.

(4) Axiom of union. Given a set C (think of C as a collection of sets), there is a set U whose members are exactly the elements that belong to some set X in this collection C. We denote this set U by $\bigcup C$ and call it the union of the sets in Z. For example, if $C = \{X, Y, Z\}$, then $\bigcup C = X \cup Y \cup Z$.

Before writing down the next axiom, we introduce the notation $Y \subseteq Z$, meaning $\forall X : X \in Y \implies X \in Z$. When this happens, we say that Y is a subset of Z.

(5) Axiom of power set. given a set X, there exists a set $\mathscr{P}(X)$ whose elements are exactly the subsets of X. $\mathscr{P}(X)$ is called the power set of X.

Using the above axioms, it is possible to encode integers using sets: $\mathbf{0} := \varnothing$ (the set with 0 elements), $\mathbf{1} := \{\mathbf{0}\} = \{\varnothing\}$ (the set with exactly one element: $\mathbf{0}$), $\mathbf{2} := \mathbf{1} \cup \{\mathbf{1}\} = \{\varnothing, \{\varnothing\}\}$, $\mathbf{3} := \mathbf{2} \cup \{\mathbf{2}\}$, ... That is, we start with $\varnothing$, we apply to it the operation $Y \cup \{Y\}$ to create a new set, and we repeat this indifinetely.

(6) Axiom of infinity. There exists an infinite set X. Formally, there exists a set X containing $\varnothing$ and such that if $Y \in X$, then $Y \cup \{Y\} \in X$. So X contains $\mathbf{0}$, $\mathbf{1}$, $\mathbf{2}$, ...

The final few axioms are more complex. Before writing them down, observe that it is easy to define $X \cap Y = \varnothing$ as $\forall Z : \neg(Z \in X \wedge Z \in Y)$ or equivalently as $\neg\exists Z : Z \in X \wedge Z \in Y$.

(7) Axiom of regularity (or of foundation). It basically says that no set can contain itself. Formally, if X is non-empty, then there exists $Y \in X$ such that $X \cap Y = \varnothing$.

(8) Axiom schema of replacement. This essentially says that if Z is a set and f a "function" with domain Z and such that $f(X)$ is a set for every $X \in Z$, then the "image" of f is a set. (Function and image can be defined in term of logical formula.)

We also have the following, which is in fact a consequence of the axiom schema of replacement and of the existence of the empty set.

(9) Axiom schema of specification (or separation, or restricted comprehension). If X is a set and φ is a logic formula then $\{Y \in X \mid \varphi(Y) \text{ is true}\}$ (the collection of all elements of X satisfying φ) is a set.

Using this axiom, one can finally define $X \cap Y := \{Z \in X \mid Z \in Y\}$. This is $\{Z \in X \mid \varphi(Z) \text{ is true}\}$ for the formula $\varphi(x) := x \in Y$.

Using the above, one can define an ordered pair (X, Y) for example as $\{X, \{X, Y\}\}$, and then use this to define functions, products and so on.

To go further

Below are the formulas for the axioms of (ZF), using the same numbering as above. We use $Y \subseteq X$ as a shorthand for $\forall z : z \in Y \implies z \in S$. In the following formulas, we will use lower case letters as x when we think of x as an element of some bigger set X. But you need to remember that in (ZF), everything is a set. In particular, an element $x \in X$ is itself a set.

(1) $\forall X \forall Y : \forall z (z \in X \iff z \in Y) \implies (X = Y)$.

(2) $\exists X \forall y : \neg(y \in X)$, such an X will be written $\varnothing$ and is unique by (1).

(3) $\forall X \forall Y \exists Z \forall z : z \in Z \iff (z = X \vee z = Y)$, such a Z is written $\{X, Y\}$ and is unique by (1). If $X = Y$, then $Z = \{X\}$.

(4) $\forall X \exists U \forall z : z \in U \iff (\exists Y : Y \in X \wedge z \in Y)$, such U is written $\bigcup X$;

(5) $\forall X \exists P \forall y : y \in P \iff y \subseteq X$, such P is written $\mathscr{P}(X)$;

(6) $\exists X : \varnothing \in X \wedge (\forall y : y \in X \implies (y \cup \{y\}) \in X)$;

(7) $\forall X : X \neq \varnothing \implies \exists y (y \in X \wedge (X \cap y = \varnothing))$, where $X \cap y = \varnothing$ is a shorthand for $\neg \exists z : z \in X \wedge z \in y$.

(8) Let φ be any formula in the language of (ZF) with free variables Z, y, X, but R not free (think of φ as $\varphi = \varphi(Z, y, X)$ not depending on R). Then: $\forall X : (\forall y : y \in X \implies \exists! Z \, \varphi(Z, y, X)) \implies \exists R \forall y (y \in X \iff \exists Z (Z \in R \wedge \varphi(Z, y, X)))$.

The part $\forall y : y \in X \implies \exists! Z \, \varphi(X, y, Z)$ means that for every $y \in X$ there exists a unique Z such that φ is true. That is, we can think as φ as a functional whose domain is X and whose codomain is the collection of all

sets. Given $y \in X$ it uniquely determines a set Z. Under this interpretation, the set R is the "range" of φ. In simpler words, this axiom means that if φ is a "functional" with domain X, then its "range" is a set.

A similar formula holds for the general case where φ has free variables among $Z, y, X, w_1, \dots, w_n$, but R is not free.

(9) Let φ be any formula in the language of (ZF) with free variables y, X, but Z not free. Then: $\forall X \exists Z \forall y : y \in Z \iff ((y \in X) \wedge \varphi(y, X))$. Such a Z is denoted $\{y \in X \mid \varphi(y)\}$.

A similar formula holds for the general case where φ has free variables among $y, X, w_1, \dots, w_n$, but Z is not free.

To go further

For the sake of completeness, here is a definition of **formulas**, or more precisely of well-formed formulas.

- If X and Y are variables, then $X = Y$ and $X \in Y$ are formulas (called atomic formulas);
- If φ and ψ are formulas and X is a variable, then the following are formulas: $\neg\varphi$, $(\varphi \wedge \psi)$, $(\varphi \vee \psi)$, $(\varphi \implies \psi)$, $\exists X \varphi$, and $\forall X \varphi$;
- All formulas are obtained by repeated applications of the above rules.

In the constructions $\exists X \varphi$ and $\forall X \varphi$, any instance of X in φ is said to be bound (we sometimes says that it is a dummy variable).
We say that Y in ψ is free if it appears in ψ and is not bound. Finally, Y is not free in ψ if either it is bound or it does not appear at all in ψ. Intuitively, non-free variables are variables we can use without harm. Non-free variables are the one we can "reuse" without creating problems. For example, in $\exists r : r^2 = x$, the variable r is bound (and not free), x is free and y is not free. So the formula $\exists y : (\exists r : r^2 = x) \wedge y = 0$ (or even $\exists r : (\exists r : r^2 = x) \wedge y = 0$, but this is not recommended) still depends on x, while $\exists x : (\exists r : r^2 = x) \wedge x = 0$ does not depend on x anymore.

1.2 Infinite sets: cardinality and arithmetic

First of all, what is an infinite set? By definition, a set X is finite if there exists a bijection between X and one of the "integer" $\mathbf{m}$ constructed in the previous subsection. Equivalently, a set is finite if it has m elements for some integer m. A set is infinite if it is not finite.

A main difference between finite and infinite sets is the possibility to pick up element inside them. More precisely, if X is a non-empty set, then there exists x in X. This is

trivial. More generally, if Y is a finite set, whose elements are non-empty sets X_1, X_2, …, X_n, then in each X_i one can pick an element x_i. Sadly, the similar statement for a general set Y cannot be proven using only the axioms of set theory from the previous subsection. If we want to be able to simultaneously choose an element x in each element X of a possibly infinite set Y we need to take it as an axiom. This is called the axiom of choice.

(AC) If Y is a set whose elements are non-empty sets, there exists a function $f : Y \to \mathscr{P}(Y)$ such that for each $X \in Y$ we have $f(X) \in X$.

(AC) has a lot of important consequences, but also some strange ones. Most (but not all!) mathematicians accept it as an axiom and so will we do. The main motivation for us to accept it has an axiom, is that it is equivalent to *every vector space has a basis*, see Subsection 2.4.4. If we add (AC) to the other axiom of (ZF), we obtain a theory known as (ZFC).

Another nice consequence of (AC) is that a set X is finite if and only if every injective function $f : X \to X$ is bijective, if and only if every surjective function $f : X \to X$ is bijective. That is, we have a converse to Lemma 1.2.17. This is not necessarily true without (AC)!

We can use injections and bijections to define the cardinality of infinite sets. Indeed, if X and Y are finite sets, then there exists a bijection $X \twoheadrightarrow Y$ if and only if $\#X = \#Y$. Moreover, there exists an injection $X \hookrightarrow Y$ if and only if $\#X \leq \#Y$. We can use this as a definition and say that for two sets X and Y (possibly infinite) we have $\#X \leq \#Y$ if there exists an injection $X \hookrightarrow Y$. One can show that if both $X \hookrightarrow Y$ and $Y \hookrightarrow X$, then there exists a bijection $X \twoheadrightarrow Y$.[3] Therefore, two sets X and Y have the same cardinality if and only if there exists a bijection between them.

One can use the above to show that $\#\mathbf{N} = \#\mathbf{Z} = \#\mathbf{Q}$, but $\#\mathbf{N} \lneq \#\mathbf{R}$.

It is possible to do arithmetic with infinite cardinals. For example, one can define $\#X + \#Y := \#(X \sqcup Y)$, $\#X \cdot \#Y := \#(X \times Y)$ and $(\#X)^{\#Y} := \#(X^Y)$ which works as usual addition, multiplication and exponentation for finite sets. If we assume (AC) arithmetic with infinite sets is very easy. Indeed, let X and Y be two sets with at least one of them infinite, then:

$$\begin{aligned} \#X + \#Y &= \max\{\#X, \#Y\} \\ \#X \cdot \#Y &= \max\{\#X, \#Y\} \\ \#X^{\#Y} &> \#Y \text{ if } \#X \geq 2. \end{aligned}$$

2 Vector spaces beyond $\mathbf{R}$ and $\mathbf{C}$

As said at the beginning of Subsection 2.2.1, the theory of vector spaces can be carried over any field $\mathbf{F}$, where heuristically a field is a set with addition, multiplication, subtraction and division (except by 0).

[3] This is called the Schröder-Bernstein Theorem, from Felix Bernstein (1878–1956) and Friedrich Wilhelm Karl Ernst Schröder (1841–1902). Its proof does not require (AC).

In this section, we will give a formal definition of fields and see some of their elementary properties. In a second time, we will have a glimpse at generalisation of fields and of vector spaces.

2.1 Fields

As stated in Subsection 2.2.1, it is possible to define vector spaces over any field $\mathbf{F}$. But what is exactly a field?

Definition 2.1.

A **field** is a set $\mathbf{F}$ endowed with two internal operations:

$$+_{\mathbf{F}} : \mathbf{F} \times \mathbf{F} \longrightarrow \mathbf{F} \qquad \cdot_{\mathbf{F}} : \mathbf{F} \times \mathbf{F} \longrightarrow \mathbf{F}$$
$$(x, y) \longmapsto x +_{\mathbf{F}} y \qquad (x, y) \longmapsto x \cdot_{\mathbf{F}} y,$$

satisfying the following properties (where we write $+$ for $+_{\mathbf{F}}$ and $\cdot$ for $\cdot_{\mathbf{F}}$)

(1) $\forall x, y, z \in \mathbf{F} : (x + y) + z = x + (y + z)$; (associativity of $+$)

(2) $\exists 0 = 0_{\mathbf{F}} \in \mathbf{F}, \forall x \in \mathbf{F} : 0 + x = x = x + 0$; (neutral element for $+$)

(3) $\forall x \in \mathbf{F}, \exists x' \in \mathbf{F} : x + x' = 0 = x' + x$; (inverse for $+$)

(4) $\forall x, y \in \mathbf{F} : x + y = y + x$; (commutativity of $+$)

(5) $\forall x, y, z \in \mathbf{F} : (x \cdot y) \cdot z = x \cdot (y \cdot z)$; (associativity of $\cdot$)

(6) $\exists 1 = 1_{\mathbf{F}} \in \mathbf{F}, \forall x \in \mathbf{F} : 1 \cdot x = x = x \cdot 1$; (neutral element for $\cdot$)

(7) $\forall x \neq 0 \in \mathbf{F}, \exists \tilde{x} \in \mathbf{F} : x \cdot \tilde{x} = 1 = \tilde{x} \cdot x$; (inverse for $\cdot$)

(8) $\forall x, y \in \mathbf{F} : x \cdot y = y \cdot x$; (commutativity of $\cdot$)

(9) $\forall x, y, z \in \mathbf{F} : x \cdot (y + z) = x \cdot y + x \cdot z$. (left distributivity)

We usually write $-x$ for the additive inverse (x' from (4)) and x^{-1} for the multiplicative inverse ($\tilde{x}$ from (7)).

As seen in Subsection 2.2.1, $\mathbf{Q}$, $\mathbf{R}$ and $\mathbf{C}$ are examples of fields. But they are not the only ones. For example, $\mathbf{Q}[i] := \{a + bi \mid a, b \in \mathbf{Q}\} \subseteq \mathbf{C}$ is also a field. There even exist finite fields!

For every prime number p, there exists a unique field $\mathbf{F}_p$ with p elements. This field, also written $\mathbf{Z}/p\mathbf{Z}$, is the field of integers modulo p. That is, we take $\mathbf{Z}$ and identify m and n if they have the same rest for the Euclidean division by p. For example, if $p = 3$, then 7 and 31 are identified because $7 = 2 \cdot 3 + 1$ and $31 = 10 \cdot 3 + 1$. In particular, any integer can uniquely be identified to an element of $\{0, \dots, p - 1\}$. Addition and multiplication are defined in a natural way. For example, for a, b in $\{0, \dots, p-1\}$, $a +_{\mathbf{F}_p} b$

is the unique integer $c \in \{0, \dots, p-1\}$ with $a + b = mp + c$ for some $m \in \mathbf{Z}$.

Example 2.2. The field $\mathbf{F}_2$ with 2 elements (useful in computer science) is defined by $(\{0,1\}, +, \cdot)$, where the addition and multiplication table are given by

$+$	0	1
0	0	1
1	1	0

$\cdot$	0	1
0	0	0
1	0	1

So, $1 + 1 = 0$ and hence $-1 = 1$.

More generally, for every prime number p and positive integer r, there exists a unique field $\mathbf{F}_{p^r}$ with p^r elements. Moreover, any finite field is of this form. However, if $r \geq 2$, then $\mathbf{F}_{p^r}$ is *not* of the form $\mathbf{Z}/p^r\mathbf{Z}$!

2.2 Vector spaces beyond fields

A careful exam of what we have seen in Chapter 2 shows that we never used the assumption that the multiplication in $\mathbf{F}$ is commutative. Therefore, all the results we have seen remain true for vector spaces over "non-commutative fields". Such non-commutative fields are called **division rings**. Formally, a division ring is a set D with two internal operations $+$ and $\cdot$ satisfying axioms (1) to (7) of Definition 2.1, as well as axiom (9) (left distributivity) and

(10) $\forall x, y, z \in \mathbf{F} : (x +_{\mathbf{F}} y) \cdot_{\mathbf{F}} z = x \cdot_{\mathbf{F}} z +_{\mathbf{F}} y \cdot_{\mathbf{F}} z.$ (right distributivity)

One important result in the theory of division rings is that any finite division ring is necessarily commutative and therefore a field. Another important result, is the Frobenius theorem, see the To go further box on page 16. The full statement of Frobenius Theorem says that it is possible to define a multiplication on $\mathbf{R}^n$ that extends scalar multiplication and turns $(\mathbf{R}^n, +, \cdot)$ into a division algebra if and only if $n \in \{1, 2, 4\}$. In each case, there exists a unique such multiplication. The case $n = 1$ is the usual real numbers. For $n = 2$ we simply recover the complex numbers. Finally, for $n = 4$ we obtain the **quaternions** $\mathbf{H}$.[4] Quaternions are defined similarly to $\mathbf{C}$, by $\mathbf{H} := \{a + bi + cj + dk \mid a, b, c, d \in \mathbf{R}\}$ where i, j, k are symbols not in $\mathbf{R}$ satisfying: $i^2 = j^2 = k^2 = -1$ and $ij = k$, $jk = i$, $ki = j$, $ji = -k$, $kj = -i$ and $ik = -j$.

To go further

If we replace $\mathbf{R}$ by $\mathbf{C}$, we obtain the Gelfand–Mazur Theorem:[a] it is possible to define a multiplication on $\mathbf{C}^n$ that extends scalar multiplication and turns $(\mathbf{C}^n, +, \cdot)$ into a division algebra if and only if $n = 1$.

[a] Israel Moiseevich Gelfand (1913–2009) and Stanisław Mieczysław Mazur (1905–1981).

[4] $\mathbf{H}$ is in honour of William Rowan Hamilton (1805–1865).

All results of Chapter 2 are true for vector spaces over general division rings. Most results of Chapter 3 on linear maps are also true, but extra care needs to be taken for the matrix representation of linear maps developed in Subsection 3.2.2. However, neither the eigentheory from Chapter 5 nor the determinant map can be extended to the generality of division rings.

For more on vector spaces on division rings, see

- Gertrude Ehrlich, *Fundamental Concepts of Abstract Algebra* (Dover Publications, 2013);
- Nathan Jacobson, *Lectures in Abstract Algebra, II. Linear Algebra* (Springer, 1953).

Finally, if you take an advanced course in abstract algebra, you might learn about rings and modules. Rings are "division rings without division". Formally, a ring is a set A with two operations $+$ and $\cdot$ satisfying axioms (1) to (6) of Definition 2.1, as well as the left and right distributivity of $\cdot$ over $+$ (axioms (9) and (10)). For example, $(\mathbf{Z}, +, \cdot)$ is a ring. If in the definition of a vector space (Definition 2.2.2) we replace the field $\mathbf{F}$ by a ring A, we obtain what is called a **module** over A. The theory of modules is far more complex than the theory of vector spaces and most results we have seen are not true anymore in this generality. For example, not every module has a basis.

3 Infinite matrices

We have seen in Section 3.2 that if V and W are vector spaces of dimension m and n we have $\mathcal{L}(V, W) \cong \mathbf{F}^{n,m}$. Can we have a similar statement for infinite dimensional vector spaces? While we can do it to some extent, this approach has serious limits as we will see.

3.1 Countably infinite matrices

Let us first try to understand countably infinite matrices. It is possible to naturally define countably infinite vectors $\mathbf{F}^{\aleph_0,1} \cong \mathbf{F}^{\mathbf{N}}$, where $\aleph_0 = |\mathbf{N}|$ is the cardinality of the set of natural numbers However, we have seen that if V is a vector space with $\dim(V) = |\mathbf{N}|$ we have $V \cong \mathbf{F}^{(\mathbf{N})}$, where $\mathbf{F}^{(\mathbf{N})}$ is the subspace of $\mathbf{F}^{\mathbf{N}}$ consisting of vectors with only finitely many non-zero coordinates. We will see that something similar happens for matrices.

For any integer n, one naturally defines $\mathbf{F}^{\aleph_0,n}$ as the set of $\aleph_0 \times n$ matrices. That is, an element of $\mathbf{F}^{\aleph_0,n}$ is of the form $[a_{i,j}]_{\substack{1\leq i,\\ 1\leq j\leq n}}$ with all the $a_{i,j}$ in $\mathbf{F}$. One similarly define $\mathbf{F}^{m,\aleph_0}$ and $\mathbf{F}^{\aleph_0,\aleph_0}$. All these sets are vector spaces, where addition and scalar multiplication are done coordinate-wise.

In $\mathbf{F}^{\aleph_0,\aleph_0}$ we have a special matrix; the identity matrix $\mathrm{Id}_{\aleph_0}$ which has 1s on the diagonal and 0s everywhere else.

We will see in a moment that $\mathbf{F}^{\aleph_0,\aleph_0}$ is too big for what we want to do. It is therefore tempting to look at the subspace $\mathbf{F}^{(\aleph_0,\aleph_0)}$ of matrices with only finitely many non-zero coordinates. However this subspace is too small for our purpose. Indeed, it does not contain $\mathrm{Id}_{\aleph_0}$.

As we have seen, it is possible to define arbitrary matrices $A = [a_{i,j}]$ in $\mathbf{F}^{\aleph_0,n}$. However, we would like them to satisfy some interesting properties. We will see that this will force us to restrict our attention to a subspace of $\mathbf{F}^{\aleph_0,n}$. Ideally, multiplying on the left by it should be a linear map from $\mathbf{F}^n$ to $\mathbf{F}^{(\mathbf{N})}$. One easily checks that multiplication on the left by A induces a linear map in $\mathcal{L}(\mathbf{F}^n, \mathbf{F}^{\mathbf{N}})$. Now, let $e_1, \dots, e_n$ be the standard basis of $\mathbf{F}^n$. Then for a fixed $1 \leq k \leq n$, the image $Ae_k = [a_{i,k}]_{1\leq i}$ is in $\mathbf{F}^{(\mathbf{N})}$ if and only if all but finitely many of the $a_{i,k}$ are 0. So left multiplication by A is in $\mathcal{L}(\mathbf{F}^n, \mathbf{F}^{(\mathbf{N})})$ if and only if each column of A has only finitely many non-zero elements. (This is equivalent to all but finitely many rows of A are 0.)

Observe that for any matrix A in $\mathbf{F}^{m,\aleph_0}$, left multiplication by it on the left is a linear map from $\mathbf{F}^{(\mathbf{N})}$ to $\mathbf{F}^n$.

Finally, for A in $\mathbf{F}^{\aleph_0,\aleph_0}$, multiplying on the left by it is a linear map from $\mathbf{F}^{(\mathbf{N})}$ to $\mathbf{F}^{\mathbf{N}}$. Its image is inside $\mathbf{F}^{(\mathbf{N})}$ if and only if each column of A has only finitely many non-zero elements.

In view of the above, for $m, n \in \mathbf{N} \cup \{\aleph_0\}$ define $\mathrm{Mat}^{\mathrm{cfin}}_{m,n}(\mathbf{F})$ to be the subset of $\mathbf{F}^{m,n}$ of all matrices such that each column has finitely many non-zero elements. This is a subspace of $\mathbf{F}^{m,n}$. Moreover, we have $(F^{m,n})_0 \subseteq \mathrm{Mat}^{\mathrm{cfin}}_{m,n}(\mathbf{F}) \subseteq \mathbf{F}^{m,n}$, where $(F^{m,n})_0$ is the subspace of matrices with finitely many non-zero entries. The first inclusion is an equality if and only if n is finite, while the second inclusion is an equality if and only if m is finite. One can check that for $m, n, l \in \mathbf{N} \cup \{\aleph_0\}$, if A is in $\mathrm{Mat}^{\mathrm{cfin}}_{m,n}(\mathbf{F})$ and B in $\mathrm{Mat}^{\mathrm{cfin}}_{n,l}(\mathbf{F})$, then AB is well-defined (because columns of B have finitely many non-zero elements) and in $\mathrm{Mat}^{\mathrm{cfin}}_{m,n}(\mathbf{F})$ (because columns of A and B have finitely many non-zero elements).

Given two vector spaces V and W of respective dimension m and n in $\mathbf{N} \cup \{\aleph_0\}$ and respective basis $\mathscr{B}$ and $\mathbf{C}$ one can define a function $[\,\cdot\,]^{\mathbf{C}}_{\mathscr{B}} \colon \mathcal{L}(V, W) \to \mathrm{Mat}^{\mathrm{cfin}}_{m,n}(\mathbf{F})$ similarly to what was done for the finite dimensional case. That is, the j^{th} column of $[T]^{\mathbf{C}}_{\mathscr{B}}$ is given by the coefficients in $T(v_j) = a_{1,j}w_1 + \cdots + a_{k,j}w_k$. The trick here is that any vector $w \in W$ can be expressed as a *finite* combination of elements of $\mathbf{C}$. This ensures that columns of $[T]^{\mathbf{C}}_{\mathscr{B}}$ have finitely many non-zero elements. One then verifies that $[\,\cdot\,]^{\mathbf{C}}_{\mathscr{B}}$ is an isomorphism of vector spaces.

The verification of the rest of the statements of Section 3.2 is left to the curious reader.

Remark 3.1.

In view of the above, one can think that linear maps between vector spaces of countably infinite dimension behave as well as linear maps between finite dimensional vector spaces. Indeed, in both cases the matrix representation map $[\,\cdot\,]^{\mathbf{C}}_{\mathscr{B}} \colon \mathcal{L}(V, W) \to \mathrm{Mat}^{\mathrm{cfin}}_{m,n}(\mathbf{F})$ is an isomorphism.
One of the main advantage of the matrix representation in the finite dimensional case is that $\mathrm{Mat}^{\mathrm{cfin}}_{m,n}(\mathbf{F}) = \mathbf{F}^{m,n}$ is a particularly nice space and that we have many tools to study it. For example one can compute the determinant and the trace of a finite matrix. Such tools are not anymore available (at least not straightforwardly) for infinite matrices. This makes the matrix-representation less useful.

Finally, if at most one of m or n is infinite, the space $\mathrm{Mat}^{\mathrm{cfin}}_{m,n}(\mathbf{F})$ is infinite dimensional. This implies that one cannot hope for "easy" computations on a computer.

3.2 Uncountably infinite matrices

We have seen how to extend the matrix representation to vector space whose dimension is countably infinite. Is it possible to generalise this more and treat the case of arbitrary vector space? We will see that, in some sense, this can indeed be done.

Let κ_1 and κ_2 be cardinals. If at least one of them is uncountable, then it is not anymore possible to define matrices as we did for countable cardinals. So we need to do something similar to what we did to define $\mathbf{F}^S$ for an uncountable S.

For $m, n \in \mathbf{N}$ we defined a $m \times n$ matrix $A = [a_{i,j}]$ as a two dimensional table. One can alternatively see A as a function $A\colon \{1, \dots, m\} \times \{1, \dots, n\} \to \mathbf{F}$ where $A(i,j) = a_{i,j}$. It is therefore possible to define $\mathbf{F}^{\kappa_1,\kappa_2} := \mathbf{F}^{\kappa_1 \times \kappa_2}$ for arbitrary cardinals. This is a space of functions, and hence a vector space. If $\kappa_1 = \kappa_2$, the "identity matrix" is the Kronecker delta function:

$$\delta(\alpha,\beta) = \begin{cases} 1 & \text{if } \alpha = \beta \\ 0 & \text{otherwise} \end{cases}$$

with domain $\kappa_1 \times \kappa_2$ and codomain $\mathbf{F}$.

We then define $\mathrm{Mat}^{\mathrm{cfin}}_{\kappa_1,\kappa_2}(\mathbf{F})$ as the subset of $\mathbf{F}^{\kappa_1,\kappa_2}$ of all functions A such that for any $\beta \in \kappa_2$, only finitely many of the $A(\alpha,\beta)$ are non-zero. It then remains to check that $\mathrm{Mat}^{\mathrm{cfin}}_{\kappa_1,\kappa_2}$ is a subspace of $\mathbf{F}^{\kappa_1,\kappa_2}$.

For $A \in \mathrm{Mat}^{\mathrm{cfin}}_{\kappa_1,\kappa_2}(\mathbf{F})$ and $B \in \mathrm{Mat}^{\mathrm{cfin}}_{\kappa_2,\kappa_3}(\mathbf{F})$, we define their product AB as the function $C \in \mathbf{F}^{\kappa_1,\kappa_3}$ defined by $C(\alpha,\beta) = \sum_{\gamma \in \kappa_2} A(\alpha,\gamma)B(\gamma,\beta)$. While this is an infinite sum, only finitely many of the terms are non-zero since B is in $\mathrm{Mat}^{\mathrm{cfin}}_{\kappa_2,\kappa_3}(\mathbf{F})$, so the product AB is well-defined. One can also check that AB belongs to $\mathrm{Mat}^{\mathrm{cfin}}_{\kappa_1,\kappa_3}(\mathbf{F})$ and that this is the standard matrix product if κ_1, κ_2 and κ_3 are finite.

Finally, for any V and W with given bases $\mathscr{B}$ and $\mathscr{C}$ one can define $[\,\cdot\,]^{\mathscr{C}}_{\mathscr{B}}\colon \mathcal{L}(V,W) \to \mathrm{Mat}^{\mathrm{cfin}}_{\dim(W),\dim(V)}(\mathbf{F})$ and verify that it satisfies the desired properties.

Remark 3.2.

Once again, in this general situation it is not easy to do computations in the space $\mathrm{Mat}^{\mathrm{cfin}}_{\kappa_1,\kappa_2}(\mathbf{F})$. Many of the standard tools for matrix are not anymore available. It is therefore more indicated to see $\mathrm{Mat}^{\mathrm{cfin}}_{\kappa_1,\kappa_2}(\mathbf{F})$ as a curiosity than as a fundamental tool.

4 Inner product spaces beyond $\mathbf{R}$ and $\mathbf{C}$

The theory of inner product spaces can be generalised to some fields, but not to all. We will first explain how to generalise the real case and then explain how to generalise the

complex case.

4.1 Ordered fields

A key point in the definition of inner product is that we ask it to have value in $\mathbf{R}_{\geq 0}$. In order to generalise inner products to a field $\mathbf{F}$ we need to have a meaningful notion of $\lambda \geq 0$ in $\mathbf{F}$.

Definition 4.1.

An **ordered field** is a 4-tuple $(\mathbf{F}, +, \cdot, \leq)$ such that:

(1) $(\mathbf{F}, +, \cdot)$ is a field;

(2) $\leq$ is a total order on $\mathbf{F}$: for every x, y and z in $\mathbf{F}$
   (i) $x \leq x$,
   (ii) If both $x \leq y$ and $y \leq z$, then $x \leq z$,
   (iii) If both $x \leq y$ and $y \leq x$, then $x = y$,
   (iv) $x \leq y$ or $y \leq y$;

(3) The order $\leq$ is compatible with the fields operations: for every x, y and z in $\mathbf{F}$
   (i) If $x \leq y$ then $x + z \leq y + z$,
   (ii) If both $0 \leq x$ and $0 \leq y$, then $0 \leq x \cdot y$.

For example, both $\mathbf{R}$ and $\mathbf{Q}$ are ordered fields (with the standard order). It is possible to show that $\mathbf{C}$ cannot be turned in an ordered field (that is, for any total order $\leq$ we put on it, $(\mathbf{C}, \leq)$ is not an ordered field). Similarly, finite fields are never ordered fields.

If $\mathbf{F}, \leq$ is an ordered field and V is an $\mathbf{F}$-vector space, then one can mimic Definition 4.1.11 to define inner products on V. Every statement about real inner products that do not use the norm generalise to this context, with the exception of Subsection 4.2.3. In particular, any statement that use only the square of the norm $\|v\|^2 = \langle v, v\rangle$ is still true.

To be able to define a norm on V, we need $\mathbf{F}$ to contain all $\sqrt{\langle v, v\rangle}$, so $\mathbf{F} = \mathbf{Q}$ won't work. But if V is an inner product space over $(\mathbf{F}, \leq)$ and $\mathbf{F}$ contains $\{\sqrt{x} \mid x \in \mathbf{F}_{\geq 0}\}$, then it is possible to define the norm by $\|v\| = \sqrt{\langle v, v\rangle}$. In this case, all statements of this chapter about real inner product spaces, with the exception of Subsection 4.2.3, remain true for $\mathbf{F}$-inner product spaces.

As an example, we can look at the field $\mathbf{A} \subseteq \mathbf{R}$ of algebraic numbers: a real number r is in $\mathbf{A}$ if and only if there exists a polynomial p with integer coefficients such that $p(r) = 0$. Then $\mathbf{A}$ is an ordered field (wit the usual order), $\mathbf{A} \neq \mathbf{R}$ (it does not contains π) and for every $a \geq 0$ in $\mathbf{A}$, its square-root $\sqrt{a}$ is still in $\mathbf{A}$. It is therefore possible to define inner product spaces over $\mathbf{A}$ and also to define the norm of vectors in such spaces.

4.2 *-Fields

As we have seen, $\mathbf{C}$ cannot be turned into an ordered field. We were however able to define complex inner product spaces using the complex conjugation. It is possible to generalise this to $\mathbf{Q}[\mathrm{i}] := \{p + q\mathrm{i} \mid p, q \in \mathbf{Q}\}$ but also to a broader context.

Definition 4.2.

A ***-field** is a field $\mathbf{F}$ together with a map $^*\colon \mathbf{F} \to \mathbf{F}$ such that for all x and y in $\mathbf{F}$:

(1) $(x+y)^* = x^* + y^*$;

(2) $(xy)^* = y^*x^*$;

(3) $1^* = 1$;

(4) $(x^*)^* = x$.

Suppose that $\mathbf{F}$ is a *-field and contains ordered subfield $\mathbf{E}$ such that $x^* = x$ for all $x \in \mathbf{E}$. Then for every $\mathbf{F}$-vector space V it is possible to define inner products over V in a similar fashion as we did for complex vector spaces in Definition 4.1.11. That is, we ask $\langle v, v\rangle \in \mathbf{E}_{\geq 0}$ for all $v \in V$. In this general context, every statement about complex inner products remains true for $\mathbf{F}$ inner products.

Once again, to be able to define a norm on V, we need $\mathbf{F}$ to contain all $\sqrt{\langle v, v\rangle}$. But if V is an inner product space over $\mathbf{F}$ and $\mathbf{E}$ contains $\{\sqrt{x} \mid x \in \mathbf{E}_{\geq 0}\}$, then it is possible to define the norm by $\|v\| = \sqrt{\langle v, v\rangle}$. In this case, all statements of this chapter about complex inner product spaces remain true for $\mathbf{F}$-inner product spaces.

As we have seen, the theory of inner product spaces can be generalised to fields other than $\mathbf{R}$ and $\mathbf{C}$. However, for a general ordered field F spaces of functions might be really strange and difficult to understand. This is why we usually stick to $\mathbf{F} = \mathbf{R}$ or $\mathbf{C}$.

5 Eigen-theory beyond $\mathbf{C}$

In Chapter 4, we saw many results that were true only for complex vector spaces, but not for real vector spaces. All these results use that $\mathbf{F} = \mathbf{C}$ only to guarantee that any operator on a complex vector space has at least one eigenvalue (Theorem 5.1.13). But this only relies on the fact that all polynomials with complex coefficients have a root in $\mathbf{C}$. Therefore, all results of this chapter remain true for fields $\mathbf{F}$ satisfying a similar criterion.

5.1 Algebraically closed fields

In the proof of Theorem 5.1.13, we only used $\mathbf{F} = \mathbf{C}$ to ensure that any polynomial in $\mathcal{P}(\mathbf{F})$ of degree at least 1 has at least 1 root in $\mathbf{F}$. This is true for $\mathbf{C}$ (and is sometimes called the fundamental theorem of algebra), but not true for $\mathbf{R}$ (think of $p(x) = x^2 + 1$).

If a field $\mathbf{F}$ satisfies "the fundamental theorem of algebra", then Theorem 5.1.13 and all its consequences will also be true for $\mathbf{F}$.

Definition 5.1.

A field $\mathbf{F}$ is **algebraically closed fields** if any polynomial $p \in \mathcal{P}(\mathbf{F})$ has at least one root in $\mathbf{F}$.

For example, $\mathbf{C}$ is algebraically closed, but $\mathbf{R}$ is not. For another example of algebraically closed fields, start with $\mathbf{Q}$ and add all complex numbers that are roots of polynomials with rational coefficients to obtain a new field $\overline{\mathbf{Q}}$ with $\mathbf{Q} \subsetneq \overline{\mathbf{Q}} \subsetneq \mathbf{C}$. So

$$\overline{\mathbf{Q}} = \{z \in \mathbf{C} \mid \exists p \in \mathcal{P}(\mathbf{Q}) : p(z) = 0\}.$$

This new field $\overline{\mathbf{Q}}$ contains $\sqrt{2}$ (root of $x^2 - 2$), i (root of $x^2 + 1$), but does not contains π. The field $\overline{\mathbf{Q}}$ does not only contain all roots of polynomials with coefficients in $\mathbf{Q}$, one can shows that it also also contains roots of polynomials with coefficients in $\overline{\mathbf{Q}}$ and that it is algebraically closed.

The main result of the theory of algebraically closed field is that for any field $\mathbf{F}$, there exists a smallest algebraically closed field $\mathbf{K}$ containing $\mathbf{F}$. Such a field is called the **algebraic closure** of $\mathbf{F}$ and written $\overline{\mathbf{F}}$. So a field is algebraically closed if and only if $\mathbf{F} = \overline{\mathbf{F}}$.

If $\mathbf{F}$ is algebraically closed, then all results of Chapter 5 that were stated for $\mathbf{C}$ remain true for $\mathbf{F}$.

Proposition 5.2 (Theorems 5.1.13 and 5.1.48, Corollary 5.1.15, Proposition 5.1.51)**.** *Let $\mathbf{F}$ be an algebraically closed field, let V be an $\mathbf{F}$-vector space and let $T \in \mathcal{L}(V)$ be an operator. Then:*

1. *If $V \neq \{0\}$, then T has at least one eigenvalue;*
2. *If $\dim(V) \geq 2$, then T has an invariant subspace that is neither $\{0\}$ nor V;*
3. *If $\dim(V)$ is finite, there exists a basis of V consisting of generalised eigenvectors of T;*
4. *If 0 is the only eigenvalue of T, then T is nilpotent.*

Proposition 5.3 (Propositions 5.1.38 and 5.1.51 and Corollary 5.2.14)**.** *Let $\mathbf{F}$ be an algebraically closed field, let $V \neq \{0\}$ be a non-trivial finite dimensional $\mathbf{F}$-vector space and let $T \in \mathcal{L}(V)$ be an operator. Then the following are equivalent:*

I. *T is nilpotent;*

II. *0 is the only eigenvalue of T;*

III. $\chi_T(t) = t^{\dim(V)}$.

Proposition 5.4 (Proposition 5.1.53, Lemma 5.1.55, and Corollary 5.3.13)**.** *Let* $\mathbf{F}$ *be an algebraically closed field, let* $V \neq \{0\}$ *be a non-trivial finite dimensional* $\mathbf{F}$*-vector space, and let* $T \in \mathcal{L}(V)$ *be an operator. Then the following are equivalent;*

I. T *is diagonalisable;*

II. $\mathrm{E}(\lambda, T) = \mathrm{G}(\lambda, T)$ *for all* $\lambda \in \mathbf{F}$*;*

III. $\mathrm{m}_{\mathrm{geo}}(\lambda, T) = \mathrm{m}_{\mathrm{alg}}(\lambda, T)$.

IV. $\mathrm{M}_T(t) = (t - \lambda_1) \cdots (t - \lambda_l)$ *where* $\lambda_1, \dots, \lambda_l$ *are the distinct eigenvalues of* T.

Theorem 5.5 (Theorem 5.1.49 and Proposition 5.2.18)**.**

Let $\mathbf{F}$ *be an algebraically closed field, let* V *be a finite dimensional* $\mathbf{F}$*-vector space, and let* $T \in \mathcal{L}(V)$ *be an operator. Let* $\lambda_1, \dots, \lambda_l$ *be the distinct eigenvalues of* T*. Then*

1. *Each of the* $\mathrm{G}(\lambda_j, T)$ *is a* T*-invariant subspace;*
2. $V = \mathrm{G}(\lambda_1, T) \oplus \cdots \oplus \mathrm{G}(\lambda_k, T)$*;*
3. *The operator* $T_j := (T - \lambda_j \mathrm{Id}_V)\big|_{\mathrm{G}(\lambda_j, T)}$ *is a nilpotent operator on* $\mathrm{G}(\lambda_j, T)$*;*
4. $\chi_T(t) = (\lambda_1 - t)^{\mathrm{m}_{\mathrm{alg}}(\lambda_1)} \cdots (\lambda_k - t)^{\mathrm{m}_{\mathrm{alg}}(\lambda_k)}$.

Proposition 5.1.56 (there exists a basis $\mathscr{B}$ such that $[T]_{\mathscr{B}}^{\mathscr{B}}$ is diagonal by block) remains true for algebraically closed fields $\mathbf{F}$, this is mostly an intermediate result.

Proposition 5.6 (Lemma 5.3.14 and Corollary 5.3.15)**.** *Let* $\mathbf{F}$ *be an algebraically closed field. Then*

1. *For every square matrix* $A \in \mathbf{F}^{m,m}$ *there exists an invertible matrix* $P \in \mathbf{F}^{m,m}$ *such that* $P^{-1}AP$ *is the Jordan form of* A*;*
2. *Two square matrices* $A, B \in \mathbf{F}^{m,m}$ *are similar if and only if they have the same Jordan form.*

5.2 Cayley–Hamilton Theorem for arbitrary fields

In this short subsection, we will finish the proof of the Cayley–Hamilton Theorem for an arbitrary field. Actually, the Cayley–Hamilton remains true for matrices over commutative rings $(R, +, -, \cdot, 0, 1)$, which are "fields without division", see Appendix 2.2.

Theorem 5.7 (Cayley–Hamilton Theorem for operators)**.**

Let V *be a finite dimensional vector space and let* $T \in \mathcal{L}(V)$*. Then* $\chi_T(T) = 0_{\mathcal{L}(V)}$.

Proof. The original proof of Theorem 5.2.19 given page 166 works for all algebraically closed fields $\overline{\mathbf{F}}$.

Now, if $\mathbf{F}$ is an arbitrary field, then it is contained in its algebraic closure $\overline{\mathbf{F}}$ and the matrix trick for $\mathbf{R} \subseteq \mathbf{C}$ in the original proof of Theorem 5.2.19 still works for $\mathbf{F} \subseteq \overline{\mathbf{F}}$. □

Theorem 5.8 (Cayley–Hamilton Theorem for matrices)**.**

Let R be a commutative ring and let $A \in R^{m,m}$ be a square matrix with coefficients in R. Then $\chi_A(A) = 0_{m\times m}$ is the zero matrix.

Proof. Since R (think $\mathbf{Z}$) is a commutative ring, then it is a subring of its field of fractions $\mathbf{F} = \mathrm{Frac}(R)$ (think $\mathbf{Z} \subseteq \mathbf{Q}$). This field is itself contained in its algebraic closure $\overline{\mathrm{Frac}(R)}$ (think $\mathbf{Z} \subseteq \mathbf{Q} \subseteq \overline{\mathbf{Q}}$). So every square matrix A with coefficients in R is a matrix with coefficients in $\overline{\mathrm{Frac}(R)}$ and therefore satisfies $\chi_A(A) = 0$. □

To go further

The Cayley–Hamilton Theorem also works for the quaternion division ring $\mathbf{H}$, see Appendix 2.2, which is a non-commutative division ring. It is however false for general division rings.

6 Alternative proof of the existence of Jordan form

We conclude this appendix with a "short" abstract proof that every nilpotent operator admits a Jordan normal form (Lemma 5.3.7). While this proof is totally correct, it is not the most useful one when it comes to actually find a Jordan basis. The main idea is similar to the proof on page 174, but this time we use induction.

Alternative proof of Lemma 5.3.7. The proof is done by induction on $m = \dim(V)$. If $m = 1$, the only nilpotent operator is the zero operator, which has matrix representation $[T]_{\mathscr{B}}^{\mathscr{B}} = \begin{bmatrix}0\end{bmatrix}$ in any basis, so we are done.

Now, suppose that $m \geq 2$ and that the theorem has been proven for every vector space of dimension strictly smaller than m. If T is the zero operator, then its matrix representation is a 0 matrix in any basis, and hence a Jordan form. So one can suppose that $T \neq 0$. Our aim is to find a direct sum decomposition $V = U \oplus W$ such that both U and W are of dimension strictly less than V and T-invariant. Indeed, in this case one can apply the induction hypothesis to U and obtain a Jordan basis $\mathscr{B}_U$ for $T|_U$. One also obtain a Jordan basis $\mathscr{B}_W$ for $T|_W$. Altogether, $\mathscr{B} = \mathscr{B}_U \cup \mathscr{B}_W$ is a basis of V in which $[T]_{\mathscr{B}}^{\mathscr{B}}$ is diagonal by blocks (this follows from the T-invariance), with blocks $[T|_U]_{\mathscr{B}_U}^{\mathscr{B}_U}$ and $[T|_W]_{\mathscr{B}_W}^{\mathscr{B}_W}$:

$$[T]_{\mathscr{B}}^{\mathscr{B}} = \begin{bmatrix} [T|_U]_{\mathscr{B}_U}^{\mathscr{B}_U} & 0 \\ 0 & [T|_W]_{\mathscr{B}_W}^{\mathscr{B}_W} \end{bmatrix}.$$

In particular, $[T]_{\mathscr{B}}^{\mathscr{B}}$ is a Jordan form for T and B is a Jordan basis.

We first describe U. Let k be the smallest integer such that $T^k = 0$. Therefore, we have

$$\{0\} \subsetneq \ker(T) \subsetneq \ker(T^2) \subsetneq \cdots \subsetneq \ker(T^{k-1}) \subsetneq \ker(T^k) = V.$$

Then there exists $u_k \in V$ but not in $\ker(T^{k-1})$. For such an u_k, $u_{k-1} \coloneqq Tu_k$ is in $\ker(T^{k-1})$ but not in $\ker(T^{k-2})$ and so on, until we have $u_1 \coloneqq T^{k-1}u \in \ker(T)$ but $u_1 \neq 0$. In particular, the list $u_k, u_{k-1}, \dots, u_1$ is linearly independent by Exercise 3.2.35. Let $U \coloneqq \operatorname{span}(u_k, u_{k-1}, \dots, u_1)$. This is a k-dimensional subspace of V with basis $\mathscr{B}_U \coloneqq (u_1, \dots, u_k)$. We have $Tu_j = u_{j-1}$ for $j \in \{2, \dots, k\}$ and $Tu_1 = 0$. This implies both that U is T-invariant and that $[T|_U]_{\mathscr{B}_U}^{\mathscr{B}_U}$ is a single Jordan block of eigenvalue 0 and size k. If $U = V$, then $\mathscr{B}_U$ is a Jordan basis of V and we are done. Thus we can assume that $U \neq V$ is of dimension strictly less than m. Moreover, $U \neq 0$, so any direct sum complement W will have dimension strictly less than m.

All that remind to do is to find a direct sum complement $W \subseteq V$ of U, which is also T-invariant. Let $X = \operatorname{span}(u_1)$ and let Y be any direct sum complement: $X \oplus Y = V$. (For example, one can take $Y = X^\perp$ if V is an inner product space). So we have a map $P\colon V \to \mathbf{F}$ defined by $P(\lambda u_1, y) \coloneqq \lambda$. ($P$ is the projection onto X followed by the isomorphism $X \cong \mathbf{F}$.) One can hence define a map $S\colon V \to \mathbf{F}^k$ by

$$Sv \coloneqq (P(v), P(Tv), \dots, P(T^{k-1}v)).$$

Finally, we let $W \coloneqq \ker(S) \subseteq V$. We want to prove that W is T-invariant and a direct sum complement of U. So let $w \in W$ and look at Tw. Then

$$S(Tw) = (P(Tw), P(T^2w), \dots, P(T^{k-1}w), P(T^kw)).$$

Since w is in $\ker(S)$ we have $P(Tw) = P(T^2w) = \dots = P(T^{k-1}w) = 0)$, while $T^k = 0$ implies $T^kw = 0$. Altogether, $S(Tw) = (0, \dots, 0)$, which proves that Tw is still in $W = \ker(S)$. So we have just proven the T-invariance of W. Now, let $u \in U$. Then $u = \lambda_1 u_1 + \cdots \lambda_k u_k$. Therefore, $Su = (\lambda_1, \lambda_2, \dots, \lambda_k)$. If $u \neq 0$, then at least one of the λ_j is non zero and therefore $Su \neq 0$. We conclude $U \cap W = \{0\}$. Therefore, the sum $U + W$ is direct. Finally, by the rank-nullity theorem we have $\dim(W) = \dim(\ker(S)) = \dim(V) - \dim(\operatorname{Im}(S)) \geq m - k$. But then, $\dim(U \oplus W) = \dim(U) + \dim(W) \geq k + m - k = m$, which implies $U \oplus W = V$.

The proof of unicity is similar as what we did in the other proof. □