An introduction to linear algebra

Edoardo Provenzi

Contents

Introduction

The objective of this course is to familiarize you with the fundamental concepts of linear algebra.

Linear algebra, initially devised to tackle practical problems, has evolved into an abstract mathematical discipline with its own terminology and symbolism. Even students specializing in pure mathematics may find it challenging if not approached properly.

In these notes I wanted to avoid as much as possible the use of definitions that appear to come out of nowhere. Instead, I have introduced them through *motivations*, drawn from a real-world problems or computational mathematical needs.

This approach aims to foster an appreciation for linear algebra as an elegant and powerful theory with broad applications across scientific domains.

We begin by delving into the cornerstone of linear algebra: the notion of vector space. Rather than abstractly defining it, we draw parallels with familiar vectors in the real plane $\mathbb{R}^2$ and space $\mathbb{R}^3$ to provide tangible grounding.

Once vector spaces are established, we explore their subspaces and associated operations, progressing to concepts like generators and linear independence, culminating in the pivotal notion of a basis.

Next, we delve into the realm of linear maps between vector spaces, emphasizing the unique association between a linear map and its corresponding matrix, and how each informs the study of the other.

Lastly, we conclude our journey by exploring one of the earliest and most significant applications of linear algebra: the efficient resolution of systems of linear equations.

To show the usefulness of the topics discussed in these notes, each chapter will end up with the discussion of at least one application of linear algebra techniques to real-world problems in diverse fields such as color perception, cryptography, biology, chemistry and physics.

The author.

Chapter 1

Vector spaces

Let us start with a little bit of history. The person who ignited the construction of modern linear algebra is unanimously considered to be Hermann **Grassmann** (1809-1877), depicted in Figure 1.1, a German polymath much ahead of his time who worked in several scientific and humanistic disciplines.

Figure 1.1: Hermann Günter Graßmann.

In 1842, Grassmann published the book '*Die lineale Ausdehnungslehre, ein neuer Zweig der Mathematik*' (Linear expansion theory, a new branch of mathematics) in which, crucially, he shows (among many other things) that the concept of *vector*, until then treated only as a geometric entity and embedded in

- a line (1 dimension)
- a plane (2 dimensions)
- or a volume (3 dimensions)

can be redefined through algebraic operations which happen to be **independent of the dimension**.

This was a huge conceptual step which, nowadays, is of fundamental importance in science: we can visualize and understand geometry only up to three dimensions, sometimes geometric constructions can help us and other times can be difficult both to draw and to interpret. However, if we 'algebrize' a geometric problem we can avoid being stuck to the three dimensions, increase their number and even make sense of vectors in infinite dimensions. Paramount important examples of theories in which we deal with vectors in more that 3 dimensions are:

- Einstein's theory of **relativity**, essential to understand the movement of objects which travel at very high speed, where 3D space and 1D time are fused together into an entity called **4-dimensional spacetime**
- **quantum mechanics**, the theory of microscopic particles with far-reaching applications in many applied scientific fields, in which we may have to deal with vectors in **infinite dimensions**, we will see later what that means.

As it often happened in the history of humanity, groundbreaking ideas need time to be digested, this was also the case for the incredible amount of novel and profound mathematical content of Grassmann's book. So, it is not surprising that it was only 80 years later that, thanks to another great German mathematician, Hermann Weyl (1885-1955), the ideas of Grassmann found a fertile ground to be rediscovered and to grow into the discipline that nowadays we call linear algebra.

The most fundamental concept in linear algebra is that of vector (or linear) space. The mathematical notion of **space** is not to be confused with the physical one.

Using a single sentence, we could say that:

'a (mathematical) space is **a set equipped with a structure**',

where

- a **set** is a **collection** of elements lumped together by the fact of **sharing a property**, e.g. the set of cats, the set of dogs, the set of natural numbers $0, 1, 2, 3, \ldots$, and so on
- a **structure**, roughly speaking, is **a list of operations and properties** that must be **defined on and fulfilled by all the elements of the set**.

The structure that defines the topic of this chapter, i.e. a vector space, is called *linear structure* and it is characterized by the rules associated to just two simple operations: the sum of two vectors and the multiplication of a vector by a numerical coefficient.

The following section is devoted to make this sentence precise.

1.1 The concept of vector space

Let us start this section by analyzing the operation of multiplication of a vector by a numerical coefficient. We will see in section 1.2.2 that vector theory is tightly intertwined with that of systems of linear equations, hence the numerical coefficients that make sense to consider are those for which linear equations can be solved.

Luckily, to single out what kind of coefficients we have to consider, it is enough to examine the simplest linear equation, i.e.

$$ax + b = 0,$$

where a and b are the numerical coefficients and x is the variable of the equation.

The solution of this equation amounts at performing two operations:

1. the first is subtracting b from each side of the equation, or, equivalently, summing $-b$, the **opposite** of b:

$$ax + \cancel{b} + \cancel{(-b)} = 0 + (-b) \iff ax = -b,$$

where the symbol $\iff$ is used to denote equivalence and it is read 'if and only if';

2. the second operation is the division by a or, equivalently, the multiplication by $a^{-1} = \frac{1}{a}$, the **inverse** of a:

$$ax = -b \iff \cancel{a} \cdot \frac{1}{\cancel{a}} x = -b \cdot \frac{1}{a} \iff x = -\frac{b}{a}.$$

We see that, in order to solve even the easiest linear equation, we need the **existence of the opposite and the inverse** of a numerical coefficient.

This simple remark shows that we cannot use numerical coefficients that belong to

- the set of natural numbers $\mathbb{N} = \{0, 1, 2, \dots\}$, because the opposite of a natural number different than 0 does not belong to $\mathbb{N}$
- or to the set of integer numbers $\mathbb{Z} = \{0, \pm 1, \pm 2, \dots\}$, because the inverse of an integer number different than ± 1 does not belong to $\mathbb{Z}$.

At least, the numerical coefficients that we can consider must belong to the set of *rational numbers*, i.e. all possible fractions:

$$\mathbb{Q} = \left\{ \frac{p}{q} : p, q \in \mathbb{Z},\ q \neq 0 \right\}.$$

However, the most common numerical sets used in the theory of vector spaces are two larger sets that contain $\mathbb{Q}$ as a subset, they are:

- $\mathbb{R}$: the set of **real numbers**, which contains $\mathbb{Q}$ and also the so-called irrational numbers, i.e. numbers that cannot be expressed as fractions, as e.g., $\sqrt{2}, \pi, \dots$ By the Pythagorean theorem, $\sqrt{2}$ is the length of the diagonal of a square with side 1, and π appears in the formula for the circumference and area of a circle, thus proving that irrational numbers are extremely important and useful.

- $\mathbb{C}$: the set of **complex numbers**, which can be written as $z = a + ib$, where $a, b \in \mathbb{R}$ and i is the *imaginary unit*, a special entity defined by the property $i^2 = -1$, something that could not happen if i were real. The need of such an entity was put in evidence when mathematicians tried to solve quadratic equations, in fact we know that the solution of $ax^2 + bx + c = 0$ is
$$x_{1,2} = \frac{-b \pm \sqrt{\Delta}}{2a},$$
if the *discriminant* $\Delta = b^2 - 4ac$ is negative, then $x_{1,2}$ cannot be real numbers, but they are the following complex numbers:
$$x_{1,2} = \frac{-b \pm i\sqrt{(-\Delta)}}{2a}.$$

More generally, mathematicians call the sets that provide the coefficients to vector spaces **fields** and indicate them with $\mathbb{F}$. For the scopes of this course, there is no need to enter in the formal definition of the concept of field, just keep in mind that $\mathbb{Q}, \mathbb{R}$ and $\mathbb{C}$ are all fields.

Once understood that we will need to consider numbers belonging to a field $\mathbb{F}$, let us follow the path traced by Grassmann and try to single out what are the algebraic properties that characterize vectors and operations on them in the usual 2-dimensional real plane.

In order to do that, we first have to agree on what a vector is in geometrical terms. A vector, symbolized with the letter v, is an *oriented segment* depicted with an arrow, as in Figure 1.2, that allows us to perform a *translation* from the origin of the arrow to its endpoint.

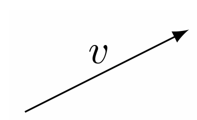


Figure 1.2: A vector v as an oriented segment. Courtesy of Francesco Bottacin.

In doing so, a vector defines (and it is defined by) three qualities:

- the magnitude of the translation, indicated with $|v|$ and called **modulus** of v
- the **direction** of the translation, i.e. the unique straight line on which v lies
- the **sense of pointing**, from left to right or from right to left.

On the set of all vectors, we can naturally define two operations.

1. The **multiplication** of v **by a coefficient** λ, that for now we suppose to belong to $\mathbb{R}$, simply written as λv, which can be interpreted as the dilation or shrinking of the modulus of v by the factor λ, see Figure 1.3 for a graphical representation. Notice that multiplying a vector by 1 leaves it unaffected, i.e. $1v = v$.

2. The **sum** of two vectors u and v, depicted in Figure 1.4, is implemented by following sequential translations: from the point A to B thanks to u and then from B to C thanks to v. If write $w = u + v$, then the translation implemented by w is from the point A to C in one shot.

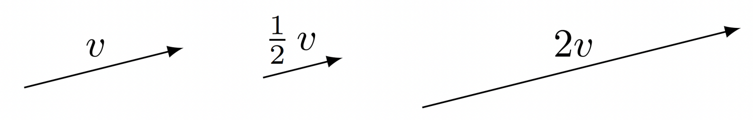


Figure 1.3: A vector can be shrunk or dilated, while preserving its direction and sense of pointing, by multiplying it with a positive real coefficient λ belonging to $(0, 1)$, e.g. $\lambda = 1/2$, or to $(1, +\infty)$, e.g. $\lambda = 2$, respectively. If $\lambda = 0$, then the vector collapses to its origin. Courtesy of Francesco Bottacin.

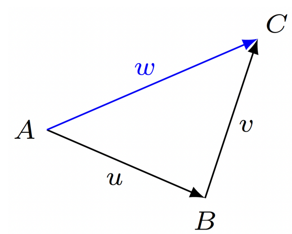


Figure 1.4: The geometric sum of two vectors. Courtesy of Francesco Bottacin.

Notice that, as shown in Figure 1.5, the order of the sum of two vectors is not important, i.e. $w = u + v = v + u$. In mathematical jargon, we say that *the sum of two vectors is commutative*. It can also be seen that, geometrically, the sum of two vectors agrees with the diagonal of the parallelogram that has the vector as edges.

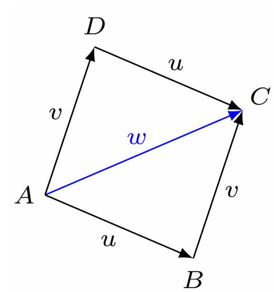


Figure 1.5: The geometric sum of two vectors. Courtesy of Francesco Bottacin.

Now let us consider negative coefficients $\lambda \in \mathbb{R}$, for example $\lambda = -1$, what happens if we multiply a vector by such a coefficient? Geometrically, the vector keeps its magnitude and direction unaltered, but it flips its sense of pointing, as shown in Figure 1.6. The vector $(-1)v$, simply written $-v$, is called the **opposite** of v.

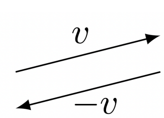


Figure 1.6: The vectors v and its opposite $-v$. Courtesy of Francesco Bottacin.

By mixing the sum and the opposite we can build a novel operation on vectors called **difference** and defined as follows

$$u - v := u + (-1)v.$$

In particular, if we perform the difference between a vector and itself we nullify the vector, i.e. the resulting vector reduces to a point with zero magnitude.

This special vector is called for obvious reasons the **null vector** and it is indicated with $\mathbf{0}$. There are two ways to obtain the null vectors:

1. $v - v = \mathbf{0}$ (difference between a vector and itself)
2. $0v = \mathbf{0}$ (multiplication of a vector by zero).

If we now fix a Cartesian system of coordinates such that its origin is set at the initial point of a vector v, then we can uniquely associate to v a couples of components, indicated with v_x and v_y, obtained by considering the *orthogonal projections of the endpoint of* v on the Cartesian axes X and Y, respectively, as in Figure 1.7. The expression of v in terms of its components is written as $v = (v_x, v_y)$, in particular, $\mathbf{0} = (0, 0)$.

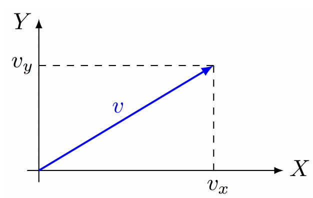


Figure 1.7: 2-dimensional components of a vector in a Cartesian system. Courtesy of Francesco Bottacin.

It is well-known (and if nobody has shown you that so far, it is a very (very!) instructive exercise to verify it) that the previous operations on vectors can all be performed through their components, namely, if $u = (u_x, u_y)$ and $v = (v_x, v_y)$, then:

$$\begin{cases} \lambda u = (\lambda u_x, \lambda u_y),\ \lambda v = (\lambda v_x, \lambda v_y) \implies -u = (-u_x, -u_y),\ -v = (-v_x, -v_y) \\ u + v = (u_x + v_x, u_y + v_y) \\ u - v = (u_x - v_x, u_y - v_y). \end{cases} \tag{1.1}$$

Thanks to these expressions it is very simple to prove by direct computation that the product between a coefficient and a vector satisfies the properties of *associativity* and *distributivity*, i.e., for all coefficients $\lambda, \mu \in \mathbb{R}$ and vectors $u, v \in \mathbb{R}^2$, we have

$$\begin{cases} (\lambda\mu)v = \lambda(\mu v) \\ \lambda(u + v) = \lambda u + \lambda v \\ (\lambda + \mu)v = \lambda v + \mu v. \end{cases} \tag{1.2}$$

Similarly, it can be verified that also *the vector sum is associative*, i.e.

$$(u + v) + w = u + (v + w) \tag{1.3}$$

and, since the null vector has both components equal to 0, it holds that

$$\mathbf{0} + v = v + \mathbf{0} = v. \tag{1.4}$$

Now, let us increase the difficulty by considering a vector v belonging to the real 3D space instead of the real 2D plane. As shown in Figure 1.8, it is still possible to construct a coordinate system with origin in the initial point of the vector v such that v is uniquely associated to its Cartesian components v_x, v_y, v_z by orthogonal projections onto the X, Y, Z.

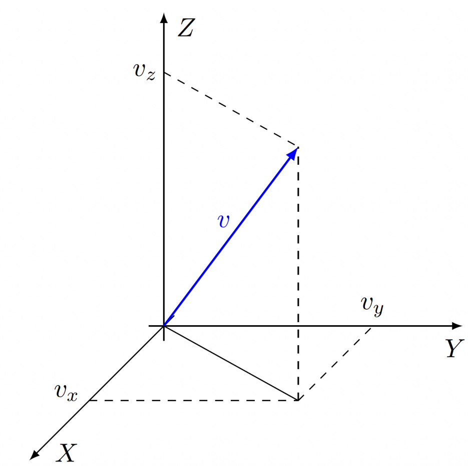


Figure 1.8: 3-dimensional components of a vector in a Cartesian system. Courtesy of Francesco Bottacin.

From a geometrical point of view, if we want to perform the multiplication of a 3D vector by a real coefficient λ or the the sum of two 3D vectors, the corresponding diagrams that we have to draw are more complicated than in 2D.

Instead, if we want to perform the same operations using the Cartesian components, we simply have to add a third one, but *the algebraic rules remain exactly the same*: if $u = (u_x, u_y, u_z)$ and $v = (v_x, v_y, v_z)$, then (1.1), (1.2), (1.3) and (1.4) keep the same structure, the only difference being that now there is a third component relative to the axis Z.

It follows that all the algebraic properties satisfied by the vectors of the real plane are also satisfied by those of the real space.

In fact, these algebraic properties happen to be those that *define the linear structure that we were searching for*!

Remark. The word *vector* comes from the same Latin word, which meant ‘carrier’, it was wisely chosen by mathematician to express the fact that a vector carries a point to another point. However, modern mathematicians prefer to use the wording *linear structure* than vector structure to avoid the misleading interpretation of objects belonging to the *abstract* vector spaces that we are going to define as ‘carriers’.

The only two concepts that are left to recall before formalizing the definition of vector space are those of *Cartesian product* and *function*.

Let us start with the first: given any two sets S and T, their Cartesian product is symbolized as $S \times T$ and it is given by

$$S \times T = \{(s,t) : s \in S, t \in T \text{ in that order}\},$$

i.e. the elements of the Cartesian product are *ordered couples*, in which the first element belongs to S and the second to T.

For example, if $H = \{0,1,\ldots,23\}$ and $M = \{0,1,\ldots,59\}$, then the Cartesian product $H \times M$ represents *the clock* because each ordered couple specifies the hour and the minute of a day. The importance of the order should be clear: while $(12,45)$ is 45 minutes past noon, $(45,12)$ does not define any moment of the day!

Now let us recall the concept of function: given any two non empty sets X and Y, a function f between them, written

$$\begin{array}{rccc} f: & X & \longrightarrow & Y \\ & x & \longmapsto & y = f(x), \end{array}$$

is a law that assigns to every element x of X (called **domain** of f) *one and only one* element $y = f(x)$ of Y. For example, the function

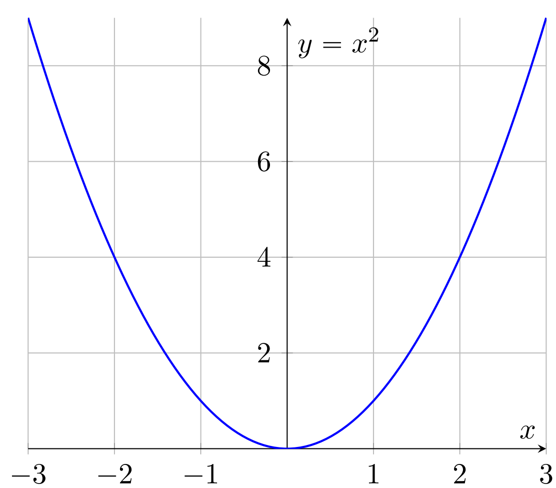
$$\begin{array}{rccc} f: & \mathbb{R} & \longrightarrow & [0,+\infty) \\ & x & \longmapsto & y = x^2, \end{array}$$

assigns to every real number its square, which is a non-negative real number.

Cartesian product and functions merge together in the definition of *graph* of a function f, which is the subset of the Cartesian product $X \times Y$ given by

$$G_f := \{(x,y),\ x \in X,\ y = f(x)\}.$$

The graph of the function in the example above is set $G_f = \{(x,x^2),\ x \in \mathbb{R}\} \subset \mathbb{R} \times [0,+\infty)$, geometrically represented by the parabola with vertex in the origin of the Cartesian plane depicted in the figure below.



We are now ready to meaningfully define the concept of vector space in a way that should not appear as catapulted from a galaxy far far away...

Def. 1.1.1 (Vector space) *A vector space over a field* $\mathbb{F}$ *is a not empty set* V *endowed with two operations, the first called sum*

$$\begin{array}{ccc} V \times V & \longrightarrow & V \\ (v, w) & \longmapsto & v + w, \end{array}$$

the second called multiplication by an element of $\mathbb{F}$

$$\begin{array}{ccc} \mathbb{F} \times V & \longrightarrow & V \\ (\lambda, v) & \longmapsto & \lambda v, \end{array}$$

which satisfy the following properties for all $v, v_1, v_2 \in V, \ \lambda, \mu \in \mathbb{F}$:

1. $v_1 + v_2 = v_2 + v_1$
2. $(v_1 + v_2) + v_3 = v_1 + (v_2 + v_3)$
3. *there exists a neutral element for the sum called null vector, i.e.* $\mathbf{0} \in V$ *such that* $\mathbf{0} + v = v + \mathbf{0} = v$
4. *there exists an opposite vector for the sum, i.e.* $-v \in V$ *such that* $v + (-v) = (-v) + v = \mathbf{0}$
5. $\lambda(v_1 + v_2) = \lambda v_1 + \lambda v_2$
6. $(\lambda + \mu)v = \lambda v + \mu v$
7. $(\lambda\mu)v = \lambda(\mu v)$
8. *there exists a neutral element for the multiplication by a coefficient of* $\mathbb{F}$*, i.e.* $1_{\mathbb{F}}$ *such that* $1_{\mathbb{F}} v = v$.

The previous properties define the ***linear structure*** *of* V*. The elements of* V *are called* ***vectors*** *and those of* $\mathbb{F}$ *are called* ***coefficients*** *or* ***scalars****.*

- If $\mathbb{F} = \mathbb{R}$, V is a **real vector space**
- If $\mathbb{F} = \mathbb{C}$, V is a **complex vector space**.

$1_{\mathbb{R}}$ and $1_{\mathbb{C}}$ will be denoted simply as 1.

1.1.1 Examples of vector spaces

As a generalization of the real plane $\mathbb{R}^2$ and the real space $\mathbb{R}^3$, we can consider the **Cartesian power of the field itself**, i.e.

$$\mathbb{F}^n = \mathbb{F} \times \cdots \times \mathbb{F} \quad (n \text{ times}),$$

where $n \in \mathbb{N}$. So $\mathbb{R}^n$ and $\mathbb{C}^n$, $n \geqslant 1$, are both vector spaces. $\mathbb{R}^2$ and $\mathbb{R}^3$ are simply particular cases of the vector space $\mathbb{R}^n$ with $n = 2, 3$.

The vectors of $\mathbb{F}^n$ are called $n-$**tuples** and the sum and product by an element of $\mathbb{F}$ are defined as those for $\mathbb{R}^2$ and $\mathbb{R}^3$, i.e.

$$(a_1, \ldots, a_n) + (b_1, \ldots, b_n) := (a_1 + b_1, \ldots, a_n + b_n),$$

$$\lambda(a_1, \ldots, a_n) := (\lambda a_1, \ldots, \lambda a_n),$$

where $\lambda, a_1, \ldots, a_n, b_1, \ldots, b_n \in \mathbb{F}$.

The neutral element for the sum is the null vector $\mathbf{0} = (0, \ldots, 0)$, the opposite of a vector $(a_1, \ldots, a_n)$ is then $(-a_1, \ldots, -a_n)$ because

$$(a_1, \ldots, a_n) + (-a_1, \ldots, -a_n) = (a_1 - a_1, \ldots, a_n - a_n) = (0, \ldots, 0) = \mathbf{0}$$

and the neutral element for the multiplication by a scalar is clearly the number 1.

The second example is provided by the set of **polynomials of degree $\leqslant n$ in an indeterminate X with coefficients in a field** $\mathbb{F}$, indicated with the symbol $\mathbb{F}_n[X]$. Each element of $\mathbb{F}_n[X]$ is written as

$$p(X) = a_0 + a_1 X + a_2 X^2 + \cdots + a_n X^n = \sum_{j=0}^{n} a_j X^j,$$

for some $n \in \mathbb{N}$ and $a_j \in \mathbb{F}$ for all $j = 0, 1, \ldots, n$.

Given two arbitrary polynomials $p(X) = \sum_{j=0}^{n} a_j X^j$ and $q(X) = \sum_{j=0}^{n} b_j X^j$, the operations that make $\mathbb{F}_n[X]$ a vector field over $\mathbb{F}$ are

$$p(X) + q(X) = \sum_{j=0}^{n} (a_j + b_j) X^j,$$

$$\lambda p(X) = \sum_{j=0}^{n} (\lambda a_j) X^j.$$

We can see that, despite the fact that the elements of $\mathbb{F}_n[X]$ are different to those of $\mathbb{F}^n$, their linear structures are practically identical: in fact the operations of sum and multiplication by a scalar for $\mathbb{F}_n[X]$ involve only the coefficients of the polynomials, which are n-tuples of scalars as in $\mathbb{F}^n$!

Coherently with this remark, the neutral element for the sum is the polynomial $\mathbf{0} = \sum_{j=0}^{n} 0X^j$, i.e. the polynomial with all null coefficients, so the opposite of a polynomial with coefficients $(a_1, \ldots, a_n)$ is the polynomial with coefficients $(-a_1, \ldots, -a_n)$ and the neutral element for the multiplication by a scalar is again the number 1.

The third example is given by a so-called **functional space**.

Given any non empty set X and a vector space V over the field $\mathbb{F}$, let us consider the set $\mathcal{F} := \{f : X \to V, f \text{ is a function}\}$, then $\mathcal{F}$ becomes a vector space over $\mathbb{F}$ when we endow it with the so-called **point-wise linear structure**, i.e. for all $f, g \in \mathcal{F}$ and $\lambda \in \mathbb{F}$

$$\begin{array}{rccl} f+g: & X & \longrightarrow & V \\ & x & \longmapsto & (f+g)(x) := f(x) + g(x), \end{array} \tag{1.5}$$

$$\begin{array}{rccl} \lambda f: & X & \longrightarrow & V \\ & x & \longmapsto & (\lambda f)(x) := \lambda f(x). \end{array} \tag{1.6}$$

Notice that $f(x)$ and $g(x)$ belong to the vector space V, so it makes perfect sense to sum them and to multiply them by $\lambda \in \mathbb{F}$.

The neutral element for the sum is the so-called null function,

$$\begin{array}{rccl} \mathbf{0}_{\mathcal{F}}: & X & \longrightarrow & V \\ & x & \longmapsto & \mathbf{0}_{\mathcal{F}}(x) := \mathbf{0}_V, \end{array}$$

because $f + \mathbf{0}_{\mathcal{F}}$ is the function such that $(f + \mathbf{0}_{\mathcal{F}})(x) = f(x) + \mathbf{0}_V = f(x)$, so $f + \mathbf{0}_{\mathcal{F}} = f$.

The opposite of a function $f \in \mathcal{F}$ is $-f$, defined as $(-f)(x) := -f(x)$ and the neutral element for the multiplication by a scalar is also in this case the number 1 because $(1f)(x) = 1f(x) = f(x)$.

1.2 Vector subspaces

Let's motivate our interest in vector subspaces with an analogy: if you are interested in buying a house, you go there and look at its exterior, the facade, the windows, hopefully the garden, and so on... however you would never buy a house without taking a good look at its interior: the bedroom, the kitchen, and so on... because the interior of a house provides very valuable information on the house itself.

Also in mathematics, each time we define a space, some of its subspaces are a source of important information, as we will detail in chapter 2.

A subspace is a 'smaller' part a space which 'behaves well' with respect to the structure that defines the whole space, where for a good behavior we mean that if we restrict the space structure to the smaller part, all the requests that define the structure are still fulfilled.

For the case of a vector space V, a subspace should be a part $W \subset V$ for which the properties of sum and multiplication by a scalar given by 1 to 8 of Def. 1.1.1 are all still valid and the results of these operations applied to elements of W produce again elements of W. If W satisfies this last feature we say that W is **stable** or **closed** with respect to those operations.

Naively, we may think that considering only a bunch of elements of a vector space V and throwing out some others would not change that much, however we can have an immediate example of a *subset* S of V which surely does not fulfill the properties of a linear structure: imagine that S is obtained from V just by eliminating the null vector $\mathbf{0}$, then S will not satisfy the request 3. of Def. 1.1.1 and so it cannot be considered a vector space itself! This very simple example shows that there may be obstructions to the fulfillment of all the requests of a linear structure when we reduce the elements of a vector space.

The following definition translates in rigorous mathematical language what discussed above.

Def. 1.2.1 (Vector subspace) *Let V be a vector space over the field $\mathbb{F}$ and $W \subseteq V$ a subset of V. W is a vector subspace of V if the operations of sum and multiplication by a scalar of $\mathbb{F}$ defined on V restricted to the elements of W still verify the axioms of a linear structure, i.e. properties 1. to 8. of Def. 1.1.1, and W is stable with respect to them.*

Since the elements of W are also elements of V, the associativity and distributivity of the linear operations are still valid because they are, by definition, valid for all the elements of V, and so also for those of W. What is essential to test is if, given $w, w_1, w_2 \in W$ and $\lambda \in \mathbb{F}$, we have

1. $w_1 + w_2 \in W$
2. $-w \in W$
3. $\lambda w \in W$
4. $\mathbf{0} \in W$.

Example 1.2.1 $\mathbb{R} \subset \mathbb{R}^2$ is a real vector subspace of $\mathbb{R}^2$, but $[0, +\infty) \subset \mathbb{R}$ is not a vector subspace of $\mathbb{R}$ because, for instance, given $w = 2 \in [0, +\infty)$, clearly $-w = -2 \notin [0, +\infty)$.

The previous four conditions can be reduced to a single one.

Theorem 1.2.1 *Let V be a vector space over the field $\mathbb{F}$ and $W \subset V$ a subset of V. W is a vector subspace of V if and only if*

$$\lambda_1 w_1 + \lambda_2 w_2 \in W, \qquad \forall \lambda_1, \lambda_2 \in \mathbb{F},\ w_1, w_2 \in W.$$

Proof.

- By taking $\lambda_1 = \lambda_2 = 1$, we describe condition 1.
- By taking either $\lambda_1 = -1$ and $\lambda_2 = 0$ or the opposite choice, we describe condition 2.
- By taking either $\lambda_1 = \lambda$ and $\lambda_2 = 0$ or the opposite choice, we describe condition 3.
- By taking $\lambda_1 = 1$, $\lambda_2 = -1$ and $w_1 = w_2 = w$, we have

  $$\lambda_1 w_1 + \lambda_2 w_2 \in W \iff w - w = \mathbf{0} \in W,$$

  which is condition 4.

□

The expression that appears in the theorem is a particular case of a more general one that has a fundamental importance in linear algebra, for this reason it deserves a special name.

Def. 1.2.2 (Linear combination) *Let V be a vector space over the field $\mathbb{F}$ and let $n \in \mathbb{N}$ be finite. An expression of the type*

$$\lambda_1 v_1 + \cdots + \lambda_n v_n = \sum_{j=1}^{n} \lambda_j v_j$$

is called a linear combination of the vectors v_j with the coefficients λ_j.

Thus, in terms of the definition just given, we can say that, in order to test if W is a vector subspace of V it must be verified if the generic linear combination of two vectors of W belongs to W.

1.2.1 Special examples of vector subspaces

V and $\{\mathbf{0}\}$ are called the *trivial vector subspaces* for self-explanatory reasons. A non-trivial example of vector subspace is provided by the intersection of all the vector subspaces of V. We recall that the intersection of two sets X and Y, denoted with $X \cap Y$ is defined as the set of all the elements that are contained in both X and Y. For instance, if $X = \{1, 2, 3, 4, 5\}$ and $Y = \{1, 3, 5, 7\}$, then $X \cap Y = \{1, 3, 5\}$. Notice that $X \cap Y$ is always smaller or, at best, equal to the smallest set. Where 'smallest' is intended with respect to the ordering relation given by the inclusion of sets.

Theorem 1.2.2 *Let V be a vector space over the field $\mathbb{F}$ and W_j an arbitrary vector subspace of V. If J is the set that contains all the indices j, then*

$$W = \bigcap_{j \in J} W_j$$

is a vector subspace of V. W is ***the smallest non-trivial vector subspace of*** *V.*

Proof. Thanks to the previous theorem, in order to prove that W is a vector subspace of V, we have to verify that, given $w_1, w_2 \in W$ and $\lambda_1, \lambda_2 \in \mathbb{F}$, $\lambda_1 w_1 + \lambda_2 w_2 \in W$.

By definition of intersection, w_1 and w_2 belong to all the vector subspaces W_j, so also the linear combination $\lambda_1 w_1 + \lambda_2 w_2$ belongs to all the vector subspaces W_j (otherwise we could not call them vector subspaces!), hence $\lambda_1 w_1 + \lambda_2 w_2 \in W_j$ for all $j \in J$, which, by definition of intersection, means that $\lambda_1 w_1 + \lambda_2 w_2 \in W$. □

One may naturally wonder if the same property holds for the *union* of vector subspaces, but the answer is, in general, negative. A very instructive way to see why is by considering the case of the vector space given by the real space $V = \mathbb{R}^3$ and the two vector subspaces

$$W_x := \{(x, 0, 0) : x \in \mathbb{R}\} \quad \text{and} \quad W_y := \{(0, y, 0) : y \in \mathbb{R}\},$$

since two elements of the ordered triple are fixed to 0, it is quite easy to recognize in W_x the x-axis and in W_y the y-axis. Both can be identified with the real line $\mathbb{R}$, which is of course a real vector space, so W_x and W_y are vector subspaces of $\mathbb{R}^3$.

The union $W_x \cup W_y$ is the set

$$W = W_x \cup W_y = \{(x, 0, 0) \text{ or } (0, y, 0),\ x \in \mathbb{R},\ y \in \mathbb{R}\}.$$

Let us check if W is a vector subspace of $\mathbb{R}^3$. If we take for instance the vectors $(1, 0, 0) \in W_x$ and $(0, 1, 0) \in W_y$, then of course both of them belong to W. Every dilation or contraction by a scalar creates another vector that belongs to W_x and W_y and so also to W, however the problem is created by their sum, which is the vector $(1, 0, 0) + (0, 1, 0) = (1, 1, 0)$ and it does not belong to W, because both its first two coordinates are non-zero *simultaneously*. Figure 1.9 gives a graphical representation of this fact in 2-dimensions.

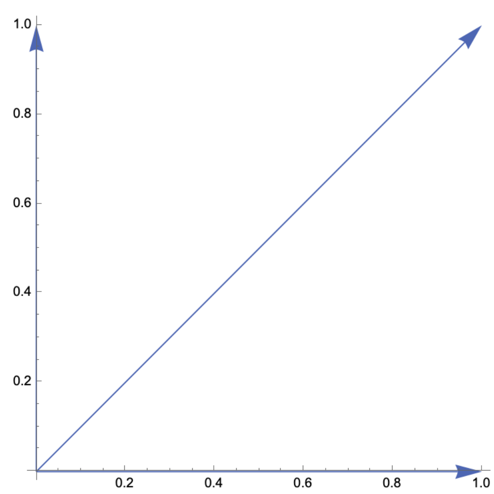


Figure 1.9: The vector $(1, 1, 0)$, depicted in the plane $\mathbb{R}^2$ embedded in the space $\mathbb{R}^3$, does not belong to the union of the horizontal and the vertical axes.

The problem showed by this example implicitly suggests its solution: in fact, since it is the sum of vectors belonging to the vector subspaces which creates the problem, we can try to replace the union of two subspaces by their sum, in the sense defined below.

Def. 1.2.3 (Sum of vector subspaces) *Let V be a vector space and U and W two vector subspaces of V. The set*

$$U + W := \{u + w : u \in U, \ w \in W\},$$

is called the sum of U and W.

Example 1.2.2 To highlight the difference between union and sum, let us consider again the subspaces W_x and W_y above, we have:

$$W_x + W_y = \{w = (x, 0, 0) + (0, y, 0) = (x, y, 0) : x, y \in \mathbb{R}\}.$$

With such a definition, the vector $(1, 0, 0) + (0, 1, 0) = (1, 1, 0) \in W_x + W_y$!

It turns out that, not only $U + W$ is a vector subspace of V, but it has a special property stated in the following theorem.

Theorem 1.2.3 *Let V be a vector space over $\mathbb{F}$ and U and W two vector subspaces of V. Then, $U + W$ is the smallest vector subspace of V that contains $U \cup W$.*

Proof. Let us first prove that $U+W$ is a vector subspace of V. If $v_1 = u_1+w_1$ and $v_2 = u_2+w_2$ are two generic vectors of $U + W$ and $\lambda \in \mathbb{F}$, then[1]

$$\begin{aligned} v_1 + v_2 &= (u_1 + w_1) + (u_2 + w_2) \\ &\underset{\text{associativity of } +}{=} u_1 + (w_1 + u_2) + w_2 \\ &\underset{\text{commutativity of } +}{=} u_1 + (u_2 + w_1) + w_2 \\ &\underset{\text{associativity of } +}{=} (u_1 + u_2) + (w_1 + w_2) \in U + W. \end{aligned}$$

Similarly, $\lambda(u + w) = \lambda u + \lambda w \in U + W$, so $U + W$ is stable with respect to the sum and the multiplication by a scalar.

It is very simple to show that $U \cup W$ is contained in $U + W$: in fact every $u \in U$ can be written as $u = u + \mathbf{0}$ and $\mathbf{0} \in W$ because W is a vector subspace of V, so it must contain the null vector, hence $u = u + \mathbf{0} \in U + W$. Analogously, every $w \in W$ can be written as $w = \mathbf{0} + w$ and $\mathbf{0} \in U$, so $w \in U + W$.

Finally, we have to show that $U + W$ is the smallest vector subspace of V that contains $U \cup W$. Let $L \subseteq V$ be a vector subspace of V that contains $U \cup W$, then $U \subseteq L$ and $W \subseteq L$, we must show that $U + W \subseteq L$. Take any $u \in U$, then, since $U \subset L$, we have that $u \in L$, analogously, for all $w \in W$, $w \in L$, so $u + w$ is the sum of two vectors of L, which is a vector subspace, so $u + w \in L$. This proves that, for all $u \in U$ and $w \in W$, $\{u + w : u \in U, \ w \in W\} = U + W \subset L$. Hence, $U + W$ is contained in all the vector subspaces of V that contain $U \cup W$ and so it is the smallest one with this characteristic. □

[1]Notice how important are the properties of associativity and commutativity of the sum!

The sum of vector subspaces can of course be iterated to more than two of them, if W_j, $j \in J$ are all vector subspaces of V, then we write their sum as:

$$W = \mathop{+}_{j\in J} W_j = \sum_{j\in J} W_j,$$

both symbols are used in the mathematical literature.

In the following definition we single out a special type of sum of subspaces.

Def. 1.2.4 (Direct sum of vector subspaces) *Let V be a vector space and U and W two vector subspaces of V. We say that the sum of U and W is direct if $U \cap W = \{\mathbf{0}\}$. We write:*

$$U \oplus W.$$

More generally, if $W_1, \ldots, W_n$ are vector subspaces of V such that $W_i \cap W_j = \{\mathbf{0}\}$ for all couple of indices $i \neq j$, then we say that their sum is direct and we write

$$\bigoplus_{j=1}^{n} W_j.$$

Since direct sums are subjected to a constraint, we expect them to have stronger properties than 'normal' sums, the following theorem confirms that this is actually the case.

Theorem 1.2.4 *Every vector $v \in U \oplus W$ can be written **uniquely** as $v = u + w$, where u and w are two specific vectors of U and W, respectively, i.e. there are no other vectors than u and w such that their sum reconstructs v.*

Proof. Suppose that the two expressions $v = u + w$ and $v = u' + w'$ hold, then, since v is the same vector in both expressions, we have $u + w = u' + w'$, i.e. $u - u' = w' - w$, but $u - u' \in U$ and $w' - w \in W$, so the equality between these vectors means that they belong to the intersection between U and W!

However, by definition of direct sum, this intersection is reduced to the null vector, so $u - u' = \mathbf{0}$, i.e. $u = u'$ and, similarly, $w' = w$. Hence, any vector of the direct sum admits a unique decomposition. □

Example 1.2.3 Consider the following subspaces of $V = \mathbb{R}^3$:

$$U := \{(x, y, 0) : x, y \in \mathbb{R}\} \quad \text{and} \quad W := \{(0, w, z) : w, z \in \mathbb{R}\},$$

it is easy to recognize in U the Cartesian plane XY and in W the Cartesian plane YZ, hence $U \cap W$ is the entire Y axis, and so the sum of and U and W is not direct.

We can verify that the decomposition of a vector $v \in \mathbb{R}^3$ as sum of one vector of U and one of W is not unique by considering, for example, $v = (2, 3, -1)$, which can be written both as

$$v = (2, 1, 0) + (0, 2, -1),$$

with $(2, 1, 0) \in U$ and $(0, 2, -1) \in W$, and also as

$$v = (2, 4, 0) + (0, -1, -1),$$

with $(2, 4, 0) \in U$ and $(0, -1, -1) \in W$.

1.2.2 The span of a subset of a vector space

We have seen that the sum is the smallest vector subspace that contains the union of *at least two* vector subspaces. A natural question that can be asked is the following: imagine that we have *one subset* S of a vector space V that *is not a vector subspace*. Of course, there is for sure a vector subspace of V that contains S and it is the trivial subspace given by V itself. However, V is the largest subspace that contains S, what about the smallest one? Does it exist? If so, can we characterize it in a simple way?

The answer to both questions is affirmative and is contained in the following definition and theorem.

Def. 1.2.5 (Span of a subset of a vector space) *Let S be a subset of a vector space V over the field $\mathbb{F}$. Then*

$$\text{span}(S) := \left\{ \sum_{j=1}^{n} \lambda_j v_j \ : \ v_j \in S,\ \lambda_j \in \mathbb{F},\ n \in \mathbb{N} \textit{ finite} \right\},$$

i.e. the span *of S is simply the set of all the linear combinations of vectors of S.*

Since the condition that must be verified by a subset of a vector space to be a vector subspace is to be stable with respect to linear combinations, it is self-evident that span(S) *is a vector subspace of V*, being built exactly by linear combinations of vectors!

However, span(S) has a finer property, as the following theorem states.

Theorem 1.2.5 *Let V be a vector space over $\mathbb{F}$ and S a subset of V. Then,* span(S) *is the smallest vector subspace of V that contains S.*

Proof. Clearly, span(S) contains S because every $v \in S$ can be written as the trivial linear combination $v = 1v \in \text{span}(S)$. Moreover, every vector subspace W_j of V which contains the vectors of S contains also every linear combination of these vectors, i.e. $\text{span}(S) \subseteq W_j$ for all $j \in J$, hence $\text{span}(S) \subseteq \bigcap_{j \in J} W_j$. However, since span$(S)$ is itself a vector subspace of V, and $\bigcap_{j \in J} W_j$ is the smallest vector space of V we have that $\bigcap_{j \in J} W_j \subseteq \text{span}(S)$. The two opposite improper inclusions imply that $\text{span}(S) = \bigcap_{j \in J} W_j$ and so it is the smallest vector subspace of V containing S. □

If span(S) is the smallest vector subspace of V that contains S and V is the largest vector subspace of V that contains S, we can ask ourselves what happens when the two coincide, i.e. when $\text{span}(S) = V$. This is a particularly important condition that deserves a specific name.

Def. 1.2.6 (Family of generators of a vector space) *The subset $S \subset V$ of a vector space V is called a family of generators of V if*

$$\text{span}(S) = V.$$

*V is **finitely generated** if it admits a family of generators with a finite number of vectors.*

By making the definition of span(S) explicit, we see that S is a family of generators of V if every $v \in V$ can be written as a linear combination of vectors of S, i.e. if for all $v \in V$ there exist a finite number $n \in \mathbb{N}$ of scalars $\lambda_1, \dots, \lambda_n$ and of vectors $v_1, \dots, v_n \in S$ such that

$$v = \lambda_1 v_1 + \cdots + \lambda_n v_n = \sum_{j=1}^{n} \lambda_j v_j.$$

A family of generators always exists, in fact V is, by definition of vector space, a family of generators of itself. Of course, this is the largest family of generators that one can imagine and it would be interesting to find out if there is a minimal family of generators without redundant vectors.

To have a simple example at hand, consider again the real plane $\mathbb{R}^2$, then

$$S_1 = \{w_1 = (1,0), w_2 = (0,1)\}$$

is a family of generators of $\mathbb{R}^2$. To see why, consider the generic linear combination of w_1 and w_2 with scalars $\mu_k \in \mathbb{R}$, $k = 1, 2$, i.e.

$$\sum_{k=1}^{2} \mu_k w_k = (\mu_1, 0) + (0, \mu_2) = (\mu_1, \mu_2).$$

Then, given a arbitrary vector $v = (x, y) \in \mathbb{R}^2$, we have that the *vector equation*

$$v = (x, y) = (\mu_1, \mu_2)$$

is satisfied by $\mu_1 = x$ and $\mu_2 = y$.

Consider now the family

$$S_2 = \{u_1 = (1,0), u_2 = (2,0), u_3 = (0,-1)\},$$

let us prove that also S_2 is families of generators of $\mathbb{R}^2$: $\lambda_j \in \mathbb{R}$, $j = 1, 2, 3$ and $\mu_k \in \mathbb{R}$, $k = 1, 2$, the linear combination of the vectors of S_2 gives rise to the vector

$$\sum_{j=1}^{3} \lambda_j u_j = (\lambda_1, 0) + (2\lambda_2, 0) + (0, -\lambda_3) = (\lambda_1 + 2\lambda_2, -\lambda_3)$$

and the vector equation

$$v = (x, y) = (\lambda_1 + 2\lambda_2, -\lambda_3)$$

can be re-written as the following system of linear equations

$$\begin{cases} x = \lambda_1 + 2\lambda_2 \\ y = -\lambda_3 \end{cases} \tag{1.7}$$

which admits not only a solution, but actually an infinite amount of them. An explicit example will help understand why.

Consider $v = (1, -1)$, then the linear system (1.7) with $x = 1, y = -1$ becomes

$$\begin{cases} 1 = \lambda_1 + 2\lambda_2 \\ -1 = -\lambda_3 \end{cases},$$

which is solved when $\lambda_3 = 1$ and $\lambda_1 + 2\lambda_2 = 1$, i.e. $\lambda_1 = 1 - 2\lambda_2$, *one* equation with *two* variables that has infinite solutions, e.g. $\lambda_1 = 1$ and $\lambda_2 = 0$ or $\lambda_1 = 1/2$ and $\lambda_2 = 1/4$, just to quote two possibilities.

S_1 is a family of 2 vectors and S_2 a family of 3 vectors, so the latter has a *redundant vector* with respect to the former.

The practical consequence of this redundancy manifests itself through the multiple choices of the scalars λ_j in the reconstruction of the same vector. This is not the case for the family of vectors S_1, where every reconstruction is unique.

If we consider a family of 4 or more vectors, we have even more freedom in the choice of the scalars to reconstruct the vectors of $\mathbb{R}^2$ via linear combination, so also for families of 4 or more vectors we will lack the uniqueness.

Let us see what happens if we consider a family given by only one vector, e.g. $S_3 = \{(a, b)\}$, with $a, b \in \mathbb{R}$ *fixed*. In this case it is impossible to generate the whole $\mathbb{R}^2$, because the only linear combination that we can perform is the multiplication of the vector (a, b) by a real scalar λ and the result is a vector that has the same direction of (a, b), so all the other vectors of $\mathbb{R}^2$ with different direction will never be written as $\lambda(a, b)$!

Let us recap:

- a family with just 1 vector of $\mathbb{R}^2$ *cannot generate* $\mathbb{R}^2$
- a family of 2 vectors of $\mathbb{R}^2$ *can*[2] generate $\mathbb{R}^2$ and, if it does, the decomposition of any vector of $\mathbb{R}^2$ as a linear combination of the vectors of this family is *unique*
- a family of 3 or more vectors of $\mathbb{R}^2$ *can* generate $\mathbb{R}^2$ but, if it does, the decomposition of any vector of $\mathbb{R}^2$ as a linear combination of the vectors of this family is *non-unique.*

This suggests that the minimal number of vectors of a family of generators is related to the uniqueness of the decomposition of a vector as a linear combination of the generators.

This intuition is actually correct and, in the following section, we will investigate what is the condition that guarantees this uniqueness.

Important remark. Confirming what stated at the beginning of section 1.1, we have shown that **the investigation of the theory of vector spaces leads naturally to linear equations**!

[2] S_1 generates $\mathbb{R}^2$, but, for example, the family $\{(1, 0), (2, 0)\}$ cannot generate $\mathbb{R}^2$, it is an instructive exercise to work out explicitly why.

1.3 Linear dependence and independence of vectors

Let us consider two *non-null vectors* v and w of the real plane $\mathbb{R}^2$.

- If v and w are *collinear*, i.e. they lie on the same straight line, then there exists $\lambda \in \mathbb{R}$, $\lambda \neq 0$, such that $w = \lambda v$, which can be written also as $w - \lambda v = \mathbf{0}$. On the left-hand side of the last equation we have a linear combination of v and w with coefficients $-\lambda$ and 1, respectively, and on the right-hand side we have the null vector. This means that *two collinear vectors can give rise to* $\mathbf{0}$ *through a linear combination with coefficients which are non-null.*

- Let us suppose now that v and w are *not collinear* and let us see what happens when we impose a generic linear combination of them with non-null coefficients to be the null vector:
$$\lambda v + \mu w = \mathbf{0} \iff \mu w = -\lambda v \iff w = -\frac{\lambda}{\mu} v, \tag{1.8}$$
but the last equation means that v and w are collinear with a coefficient of proportionality given by $-\lambda/\mu$ and this contradicts the hypothesis that v and w are not collinear.

  The consequence is that *a linear combination of two non-collinear vectors gives rise to the null vector if and only if the coefficients of the linear combination are both null.*

If we now increase of one dimension and we consider the real space $\mathbb{R}^3$, then, repeating the same reasoning, we discover that the linear combination of three non-null vectors $u, v, w \in \mathbb{R}^3$ can give rise to $\mathbf{0}$ with coefficients which are not all null if and only if the three vectors belong to the same plane, i.e. if there exist $\lambda, \mu \in \mathbb{R}$ such that $w = \lambda u + \mu v$. Otherwise, the only way to give rise to $\mathbf{0}$ with a linear combination of u, v, w is to use all null coefficients.

$\mathbb{R}^2$ and $\mathbb{R}^3$ allow us to have a nice geometrical representation in terms of collinearity and coplanarity. However, when we consider an abstract vector space V *this geometric interpretation is lost, but the algebraic properties that we have highlighted remain intact* and we can use them to define the concepts of linearly dependent and independent vectors.

Def. 1.3.1 (Linear dependence and independence) *Let V be a vector space over the field $\mathbb{F}$. A family of vectors $S = \{v_1, \ldots, v_n\} \subset V$ is said to be **free** and the vectors are said to be **linearly independent** if the vector equation*

$$\lambda_1 v_1 + \ldots \lambda_n v_n = \mathbf{0}$$

*has $\lambda_1 = \cdots = \lambda_n = 0$ as only solution. Otherwise, if at least one of the coefficients λ_j is non null, the vectors are said to be **linearly dependent**.*

Notice that if S is composed only by one vector v, then the only linear combination that we can write is λv and saying that $\lambda v = \mathbf{0}$ is solved only by $\lambda = 0$ means that v is not null. So, *a one-vector family is free if and only if the vector is non null.*

Moreover, *the null vector cannot appear in a family of linearly independent vectors* because we can multiply the null vector by any scalar obtaining again the null vector! As a consequence, *a family of vectors containing the null vector is always linearly dependent.*

A family of linearly dependent vectors can be characterized as described in the following theorem.

Theorem 1.3.1 *A set of vectors $v_1, \dots, v_n$ of V is linearly dependent if and only if there is at least one vector that can be written as a linear combination of the others.*

Proof.

$\boxed{\Longrightarrow}$: suppose that $v_1, \dots, v_n$ are linearly dependent, we must prove that at least one of them can be written as a linear combination of the others. By hypothesis, we can write

$$\lambda_1 v_1 + \lambda_2 v_2 + \cdots + \lambda_n v_n = \mathbf{0}$$

with at least one of the coefficients $\lambda_j \neq 0$. For the sake of simplicity, we can reorder the indices so that the non-null coefficients is λ_1, then we can write

$$v_1 = -\frac{\lambda_2}{\lambda_1} v_2 - \cdots - \frac{\lambda_n}{\lambda_1} v_n,$$

hence v_1 is written as a linear combination of the other $n-1$ vectors.

$\boxed{\Longleftarrow}$: up to a permutation of the indices, we can still concentrate our attention on just one vector, which we choose again to be v_1. Suppose that v_1 that is written as a linear combination of the other vectors, i.e.

$$v_1 = \lambda_2 v_2 + \cdots + \lambda_n v_n,$$

then

$$\mathbf{0} = -v_1 + \lambda_2 v_2 + + \cdots + \lambda_n v_n,$$

and the coefficients of v_1 is $-1 \neq 0$, so we can reconstruct $\mathbf{0}$ with a linear combination of vectors in which at least one of the coefficients is non null, hence $v_1, \dots, v_n$ is a linearly dependent family. $\square$

We can now state and prove the link between the linear independence and the uniqueness of a linear combination.

Theorem 1.3.2 *Let $v_1, \dots, v_n$ be linearly independent vectors of the vector space V over the field $\mathbb{F}$. If $v \in V$ can be written as a linear combination of $v_1, \dots, v_n$, i.e.*

$$v = \lambda_1 v_1 + \cdots + \lambda_n v_n,$$

then the scalars $\lambda_1, \dots, \lambda_n \in \mathbb{F}$ are uniquely determined.

Proof. Suppose that we can write the linear combination in two ways:

$$v = \lambda_1 v_1 + \cdots + \lambda_n v_n \quad \text{and} \quad v = \mu_1 v_1 + \cdots + \mu_n v_n,$$

with of course $\mu_1, \dots, \mu_n \in \mathbb{F}$, then, since v is the same vector we have

$$\lambda_1 v_1 + \cdots + \lambda_n v_n = \mu_1 v_1 + \cdots + \mu_n v_n \iff (\lambda_1 - \mu_1) v_1 + \cdots + (\lambda_n - \mu_n) v_n = \mathbf{0},$$

but $v_1, \dots, v_n$ are linearly independent, so $\lambda_j - \mu_j = 0$, i.e. $\lambda_j = \mu_j$ for all $j = 1, \dots, n$. $\square$

1.4 Bases of a vector space

Consider a family of vectors $S = \{v_1, \dots, v_n\}$ in a vector space V over the field $\mathbb{F}$. In the previous section we have discussed two concepts related to S:

1. S can be a family of generators of V
2. S can be a free family, i.e. the vectors of S can be linearly independent.

We can naturally ask ourselves what happens if we mix the two concepts together, i.e. if S is a free family of generators of V. By definition of family of generators we have that every vector $v \in V$ can be written as a linear combination of the vectors of S. Moreover, from Theorem 1.3.2, we get that the linear combination in uniquely determined. We can resume this by saying that *if S is a free family of generators, then every $v \in V$ can be uniquely written as*

$$v = \lambda_1 v_1 + \cdots + \lambda_n v_n,$$

i.e. the scalars $\lambda_1, \dots, \lambda_n$ are uniquely associated to v once the family S is specified.

In the sequel, we will see that the order of the vectors in S is important, for this reason, in the following definition we explicitly add the request of ordering.

Def. 1.4.1 (Basis of a vector space) *A basis of a vector space V is an ordered family of vectors B which has the property of being free and to generate V.*

To distinguish between a non-ordered set of vectors and an ordered one, in the literature it is usual to replace the notation $\{v_1, \dots, v_n\}$ with $(v_1, \dots, v_n)$, i.e. the curly brackets denote a non-ordered set, while the parenthesis indicate an ordered one.

A basis B of V is then an ordered family of linearly independent vectors $(v_1, \dots, v_n)$ that generate all the vectors of V through linear combinations. Every vector of V has its own set of scalars appearing in the combination: given $v, w \in V$, $v \neq w$, we have

$$v = \lambda_1 v_1 + \cdots + \lambda_n v_n \qquad \text{and} \qquad w = \mu_1 v_1 + \cdots + \mu_n v_n,$$

with $(\lambda_1, \dots, \lambda_n) \neq (\mu_1, \dots, \mu_n)$. It is convenient to have a precise name for these scalars.

Def. 1.4.2 (Components of a vector with respect to a basis) *The scalar appearing in the linear combination that expresses a vector v in terms of the vectors of a basis B are called components of v with respect to B.*

The easiest and one of the most used example of basis of a vector space is the so-called **canonical basis of** $\mathbb{F}^n$, $\mathbb{F} = \mathbb{R}$ or $\mathbb{C}$, which is given by the vectors

$$\begin{cases} e_1 := (1, 0, 0, \dots, 0) \\ e_2 := (0, 1, 0, \dots, 0) \\ \vdots \\ e_n := (0, 0, 0, \dots, 1) \end{cases}$$

so, the coordinates of the j-th vector of the canonical basis of $\mathbb{F}^n$ are all zero, except for the one at the position j, whose value is 1.

To avoid cumbersome computations, let us consider $\mathbb{R}^3$ and show that every vector of this space can be written uniquely as a linear combination of the vectors of the basis

$$B = (e_1 = (1,0,0),\ e_2 = (0,1,0),\ e_3 = (0,0,1))$$

and that two different vectors have a distinct decomposition on B. Notice that e_1, e_2, e_3 are nothing but the unit vectors of the axes X, Y, Z of the Cartesian diagram of Figure 1.8.

Let us indicate with $v = (x, y, z)$ a generic vector of $\mathbb{R}^3$, with $x, y, z \in \mathbb{R}$, then the vector equation

$$v = (x, y, z) = \lambda_1 e_1 + \lambda_2 e_2 + \lambda_3 e_3 = (\lambda_1, 0, 0) + (0, \lambda_2, 0) + (0, 0, \lambda_3) = (\lambda_1, \lambda_2, \lambda_3),$$

is clearly solved for $\lambda_1 = x$, $\lambda_2 = y$, $\lambda_3 = z$. Hence, *the components of a vector with respect to the canonical basis are nothing but the Cartesian coordinates of that vector.*

Let us now consider the basis

$$B' = (e_3 = (0,0,1),\ e_2 = (0,1,0),\ e_1 = (1,0,0)),$$

obtained by exchanging the first and the last vector of the canonical basis of $\mathbb{R}^3$. In this case we have

$$v = (x, y, z) = \mu_1 e_3 + \mu_2 e_2 + \mu_3 e_1 = (0, 0, \mu_1) + (0, \mu_2, 0) + (\mu_3, 0, 0) = (\mu_3, \mu_2, \mu_1),$$

which is solved for $\mu_1 = z$, $\mu_2 = y$, $\mu_3 = x$. This shows that the order of the vectors in a basis matters.

Let us now examine an example with a less simple basis of $\mathbb{R}^3$, e.g.

$$B'' = (u_1 = (1,1,0), u_2 = (1,0,1), u_3 = (0,2,0)).$$

First of all, we have to verify that B'' is indeed a basis for $\mathbb{R}^3$, i.e. that u_1, u_2, u_3 are linearly independent and they generate $\mathbb{R}^3$.

We start with the linear independence: by definition, we have to show that

$$au_1 + bu_2 + cu_3 = \mathbf{0} \iff a = b = c = 0.$$

We have

$$au_1+bu_2+cu_3 = (a,a,0)+(b,0,b)+(0,2c,0) = (a+b, a+2c, b) = (0,0,0) \iff \begin{cases} a+b=0 \\ a+2c=0 \\ b=0 \end{cases},$$

introducing $b = 0$ in the first equation we find $a = 0$ and introducing $a = 0$ in the second equation we get $2c = 0$, i.e. $c = 0$. So, a linear combination of the vectors of B'' can be the null vector if and only if all the coefficients of linear combination are 0, thence B'' is free.

Now we must prove that B'' is a family of generators, i.e. that, given a generic vector $v = (x, y, z) \in \mathbb{R}^3$ there exist $\lambda_1, \lambda_2, \lambda_3 \in \mathbb{R}$ such that $v = \lambda_1 u_1 + \lambda_2 u_2 + \lambda_3 u_3$. Taking advantage of the calculation just made we have

$$(x, y, z) = (\lambda_1 + \lambda_2, \lambda_1 + 2\lambda_3, \lambda_2),$$

which corresponds to the linear system of equations

$$\begin{cases} \lambda_1 + \lambda_2 = x \\ \lambda_1 + 2\lambda_3 = y \\ \lambda_2 = z \end{cases} \iff \begin{cases} \lambda_2 = z \\ \lambda_1 + z = x \\ \lambda_1 + 2\lambda_3 = y \end{cases} \iff \begin{cases} \lambda_2 = z \\ \lambda_1 = x - z \\ x - z + 2\lambda_3 = y \end{cases} \iff \begin{cases} \lambda_1 = x - z \\ \lambda_2 = z \\ \lambda_3 = \frac{y-x+z}{2} \end{cases}.$$

It is a good exercise to verify that the linear combination of the vectors of B'' with the coefficients just found gives back the generic vector $v = (x, y, z)$ of $\mathbb{R}^3$:

$$\begin{aligned} \lambda_1 u_1 + \lambda_2 u_2 + \lambda_3 u_3 &= (x - z)(1, 1, 0) + z(1, 0, 1) + \frac{y - x + z}{2}(0, 2, 0) \\ &= (x - z, x - z, 0) + (z, 0, z) + (0, y - x + z, 0) \\ &= (x - \cancel{z} + \cancel{z}, \cancel{x} - \cancel{z} + y - \cancel{x} + \cancel{z}, z) \\ &= (x, y, z) \\ &= v. \end{aligned} \tag{1.9}$$

This shows that B'' is indeed a basis for $\mathbb{R}^3$. Let us compute, for instance, the components of the vector $v = (1, 2, -1)$ with respect to B''. We already know that the components of v with respect to the canonical basis B are its Cartesian coordinates, i.e. $a = 1$, $b = 2$ and $c = -1$, in that order. To verify that each decomposition of a vector on a basis is unique, we must find at least a different component or a different order.

Using (1.9) we have that

$$(1, 2, -1) = \lambda_1 u_1 + \lambda_2 u_2 + \lambda_3 u_3 \iff \begin{cases} \lambda_1 = 1 - (-1) = 2 \\ \lambda_2 = -1 \\ \lambda_3 = \frac{2-1-1}{2} = 0 \end{cases},$$

hence, the components of the vector $v = (1, 2, -1)$ with respect to the basis B'' are $\lambda_1 = 2$, $\lambda_2 = -1$ and $\lambda_3 = 0$. Let us verify that:

$$2u_1 - u_2 + 0u_3 = (2, 2, 0) + (-1, 0, -1) + (0, 0, 0) = (2 - 1, 2, -1) = (1, 2, -1) = v.$$

Notice that the components of v with respect to B'' are different than the components of v with respect to the canonical basis, as highlighted below

$$\begin{cases} a = 1 \\ b = 2 \\ c = -1 \end{cases} \quad \text{vs.} \quad \begin{cases} \lambda_1 = 2 \\ \lambda_2 = -1 \\ \lambda_3 = 0 \end{cases}.$$

At this point, a natural question may be asked: since it is immediate to find the components of a vector of $\mathbb{R}^n$ with respect to its canonical basis, why do we have to bother investigating other kind of bases? The answer is that, as we will see later on, when we will deal with linear maps and matrices, there exist bases different than the canonical one, with respect to which the expression of a linear map, and the shape of the corresponding matrix, is particularly simple to analyze.

The bases B, B' and B'' are all composed by 3 vectors. We may wonder if this is a coincidence or if it is a general property of bases and if this feature is shared also by other vector spaces than $\mathbb{R}^3$. The answer to these questions is affirmative and it consists in the most important result regarding the bases of a finitely generated vector space.

Theorem 1.4.1 *Let V a finitely generated vector space, then:*

- *all the bases of V have the same number of vectors*
- *a family with less vectors than those of a basis can be free but cannot generate V*
- *a family with more vectors than those of a basis can generate V but cannot be free.*

The proof of this theorem, even though not complicated, is too long to be reported in an introductory course on linear algebra.

Thanks to this theorem, the following definition is well-posed.

Def. 1.4.3 (Dimension of a finitely generated vector space) *The dimension of a finitely generated vector space V, denoted $\dim(V)$, is the number of vectors belonging any basis of V.*

Examples.

- $\dim(\mathbb{R}^n) = n$ because, for example, the canonical basis has exactly n vectors
- The dimension of $\mathbb{F}_n[X]$, the vector space over $\mathbb{F}$ of polynomials of degree $\leqslant n$ in an indeterminate X with coefficients in $\mathbb{F}$ has dimension $n+1$. The analogue of the canonical basis of $\mathbb{R}^n$ for $\mathbb{F}_n[X]$ is

$$\begin{cases} e_0[X] := 1 \\ e_1[X] := X \\ e_2[X] := X^2 \\ \quad\vdots \\ e_n[X] := X^n \end{cases}.$$

  In fact, every polynomial $p \in \mathbb{F}_n[X]$ can be written as a linear combination of theses polynomials with coefficients $a_j \in \mathbb{F}$, $j = 0, 1, \dots, n$:

$$p(X) = a_0 1 + a_1 X + a_2 X^2 + \cdots + a_n X^n.$$

- Consider a vector space V and its **null vector subspace** defined by the sole null vector $N := \{\mathbf{0}\}$. We have that $\dim(N) = 0$ for all V and N *is the only vector space with zero dimension.* To understand why observe that a basis of N can contain at best the null vector of V, but we know the family $\{\mathbf{0}\}$ is not free, so it cannot be a basis of N and the only alternative that remains is the empty set $\varnothing$.

  Let us show that $\varnothing$ **is a basis for** N. $\varnothing$ is a free subset of V because there are no vectors that we can multiply by a non-null scalar to obtain $\mathbf{0}$! To see why $\varnothing$ can be considered a family of generators of N we use Theorem 1.2.5 to identify $\text{span}(\varnothing)$ as the smallest subspace of V that contains the empty set, i.e. the smallest subspace of V at all, which we know to be N. So, by Def. 1.2.6, $\varnothing$ generates N. To recap, $\varnothing$ is a free family of generators of N, i.e. a basis of N, with 0 vectors, so $\dim(N) = 0$.

- An example of non finitely-generated vector space is provided by $\mathcal{F}$, the space of functions $f : X \to \mathbb{F}$, where X is a non empty set and $\mathbb{F}$ is a field.

  Functional spaces are actually among the *most interesting and important infinite-dimensional vector spaces* of mathematics and, for example, quantum mechanics could not be formulated without this kind of spaces.

Let us now just quote without proof two important theorems.

Theorem 1.4.2 *Let V be a vector space of dimension n and $v_1, \ldots, v_n$ a family of n vectors of V. Then:*

- *if $v_1, \ldots, v_n$ are linearly independent, then they are also a family of generators for V, i.e. they are a basis for V*
- *if $v_1, \ldots, v_n$ generate V, then they are also linearly independent, i.e. they are a basis for V.*

The consequence of this theorem is that when we have a family of vectors of V whose number equals that of the dimension of V, we have a *strong advantage in the task of determining if those vectors form a basis* for V: we can either check if they are linearly independent or if they generate V, *without having to check both of them.*

Recall now that we have analyzed the concept of vector subspace, so we can ask ourselves what can we say about its dimension. In the following theorem we give some information about that.

Theorem 1.4.3 *Let V a vector space and W, W_1, W_2 vector subspaces of V.*

- *If W is strictly contained in V, i.e. there are vectors of V that do not belong to W, then* $\dim(W) < \dim(V)$.
- **Grassmann's formula***:*

$$\dim(W_1 + W_2) = \dim(W_1) + \dim(W_2) - \dim(W_1 \cap W_2).$$

The Grassmann formula is actually quite intuitive: if we sum the vectors of a basis of W_1 with those of a basis of W_2 without taking off those belonging to the intersection between W_1 and W_2, then we count them twice!

By definition of direct sum, Grassmann's formula implies

$$\dim(W_1 \oplus W_2) = \dim(W_1) + \dim(W_2).$$

1.5 The first practical application of linear algebra: the space of perceived colors

The earliest applications of the concept of linear combination was provided by Grassmann himself in 1854. In order to describe it, we must recall that the human visual system is not sensible to all the electromagnetic spectrum, but only to a very tiny portion of it. In fact, only the electromagnetic waves oscillating within a certain range of frequencies $[\nu_{\min}, \nu_{\max}]$ are perceived as visual signals.

In general, it is preferred to discuss wavelengths λ instead of frequencies ν, using the relation

$$\nu = \frac{c}{\lambda},$$

where c is the speed of light. The range of wavelengths corresponding to the **visible spectrum** is the very small interval

$$\Lambda := [380, 780]\text{nm},$$

where nm means 'nanometer', i.e. 10^{-9}m, or one billionth of a meter.

As shown in Figure 1.10, light with different wavelengths is perceived with different colors, from red to violet.

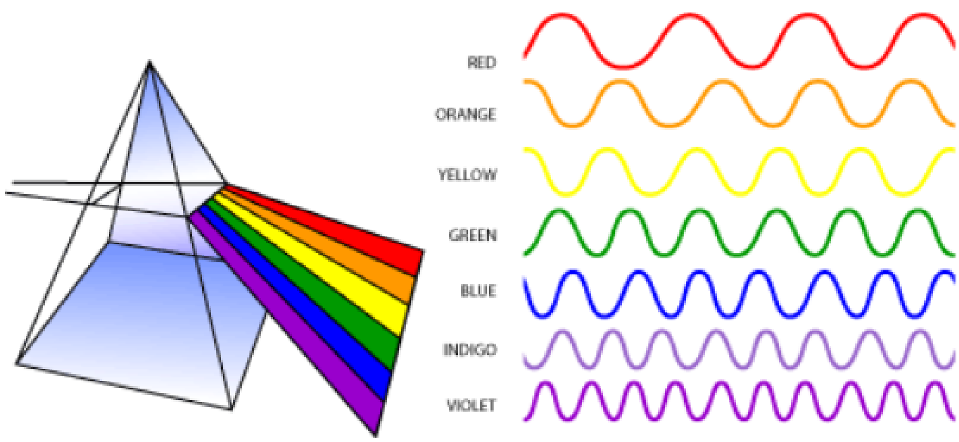


Figure 1.10: Spectral colors from red to violet.

The intensity of a generic luminous signal, however, does not depend only on one single wavelength, but on all wavelengths of Λ and can be modeled as a function like this, called *light spectrum*:

$$\begin{aligned} \mathcal{L} : \quad \Lambda &\longrightarrow (0, +\infty) \\ \lambda &\longmapsto \mathcal{L}(\lambda). \end{aligned}$$

If our color perception would be based solely on the physics of light spectra, then the space of perceivable colors will be the functional space of light spectra. As we have seen in this chapter, functional spaces are infinite-dimensional space. If that were the case, then color pictures, cinema, TV and printing would probably be impossible to realize, or at least much more difficult than they actually are.

However, the photoreceptors in human retina that respond to light to produce colors are not sensitive to all the wavelength is the same way. In fact, they can be categorized in three types: those with a sensitivity peak on the long (L), middle (M) and short (S) wavelengths, see Figure 1.11.

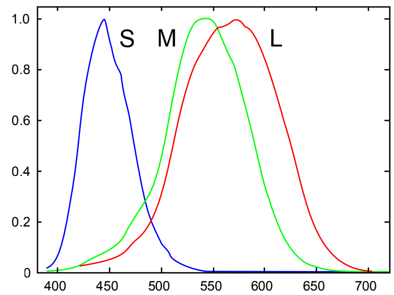


Figure 1.11: The average spectral sensitivity curves of the daylight photoreceptors in the human retina.

This sort of '*physiological flaw*' is actually very welcome, because, perceptually speaking, it has the effect of reducing the infinite-dimensional space of light spectra to a 3-dimensional one.

Grassmann was the first one to discuss this huge dimensional reduction in terms of his invention, linear algebra, pointing out that the space of perceivable colors must be contained in a vector space of dimension 3 instead of infinite dimensions.

If you approach (very close) an old TV screen, you will see three little squares or rectangles side-by-side which appear having red, green and blue color with different intensities. The reason is that the first colorimetric standard for color TV, proposed in 1953 and called NTSC for 'National Television System Committee', was called RGB, for red, green and blue, where RGB are monochromatic light wave with wavelengths

- 700nm for R
- 546.1nm for G
- 435.8nm for B,

chosen with these values because they were experimentally found to be linearly independent, and also due to the technological limitations of that time.

The RGB model must be considered as a useful way to reproduce color stimuli, but it is not the end of the story: color perception is a very complicated phenomenon and the research about it is still ongoing.

However, the fact that Grassmann, the creator of linear algebra, contributed to provide such a useful insight of his theory only 12 years after the publication of his treatise should already make you realize **the important linear algebra is in real-life applications**. We will discuss other interesting examples in the following chapters.

1.6 The link between the theory of vector spaces and that of linear maps between them

In the following chapter we are going to study particular transformations between vector spaces called *linear*. We can understand why the study of such transformations is natural by analyzing the what happens to the components of a vector if we multiply it by a scalar or if we sum two vectors.

Theorem 1.6.1 *Let V be a vector space of dimension n over the field $\mathbb{F}$ and B a basis of V. If $\lambda_1, \ldots, \lambda_n$ and $\mu_1, \ldots, \mu_n$ are the components of the vectors v and w of V, respectively, then:*

- *the components of $v + w$ are $\lambda_1 + \mu_1, \ldots, \lambda_n + \mu_n$*
- *the components of av, where $a \in \mathbb{F}$, are $a\lambda_1, \ldots, a\lambda_n$.*

The proof of this theorem is an easy, but very tedious, direct computation, and it is omitted.

Maintaining the notations of this last theorem, the fact that the components are *uniquely associated* to a vector once the basis B is chosen induces naturally a function between V and $\mathbb{F}^n$ represented as follows

$$\begin{array}{rccl} f_B: & V & \longrightarrow & \mathbb{F}^n \\ & v & \longmapsto & f_B(v) = (\lambda_1, \ldots, \lambda_n), \end{array} \tag{1.10}$$

i.e. f_B is the function that associates v to the vector of $\mathbb{F}^n$ built with the components of v with respect to the basis B (this is the reason why B appears as a subscript of f).

Thanks to Theorem 1.6.1, we can immediately establish two properties of the function f_B:

1. $f_B(av) = a(\lambda_1, \ldots, \lambda_n) = af_B(v)$, for all $a \in \mathbb{F}$
2. $f_B(v + w) = (\lambda_1 + \mu_1, \ldots, \lambda_n + \mu_n) = f_B(v) + f_B(w)$, for all $v, w \in V$.

Properties 1 and 2 constitute precisely what defines a **linear map**! So, we see **that the study of linear maps is connatural with the study of vector spaces**.

1.7 Questions about chapter 1

In order to check if you have understood the concepts that have been introduced in this chapter, it is of paramount importance that you are able to give a correct and precise answer to the following questions. If you are not able to respond, it means that you need to review the concepts that you have forgotten or misunderstood. An optimal (and nicer) way to check this is to test each other. We will not repeat this disclaimer for the next chapters, but of course the previous suggestions will remain valid for them too.

1. Why, in general, a linear equation $y = ax + b$ cannot be solved if the coefficients a, b belong to the set of natural numbers $\mathbb{N}$ or to that of the integer numbers $\mathbb{Z}$? What is the mathematical name to describe numerical sets as $\mathbb{Q}, \mathbb{R}, \mathbb{C}$?
2. What are the two algebraic operation that every vector space must equipped with? Write them explicitly.
3. What is the defining property of the null vector of a vector space? And that of the opposite of a vector?
4. How can be characterized the vector subspace W of a vector space V?
5. What is a linear combination of vectors of a vector space?
6. What is the smallest non-trivial vector subspace of a vector space?
7. Given a subset S (not a vector subspace) of a vector space, what is the smallest vector subspace that contains S?
8. What is the difference between the sum and the direct sum of two vector subspaces?
9. What is a family of generators of a vector space?
10. When n vectors are linearly independent? and linearly dependent?
11. What is the characteristic of a vector written as a linear combination of linearly independent vectors?
12. How is it defined a basis of a vector space?
13. What does it mean that a vector space is finitely generated?
14. What is a basis of a finitely generated vector space?
15. Quote the Grassmann formula and deduce from it the dimension of the direct sum of two subspaces.
16. How does linear maps between vector spaces emerge naturally from the study of vector spaces and their bases?

1.8 Exercises of chapter 1

The following exercises have the aim of testing the comprehension of the most important concepts that have been introduced in chapter 1.

1. Let E be the set of all polynomials with real coefficients in the indeterminate X with degree equal to $n \in \mathbb{N}$, $n \geqslant 1$. Is E a real vector space with respect to the polynomial sum and multiplication by a real scalar?

2. In the functional vector space of functions $f : \mathbb{R} \to \mathbb{R}$, determine if the vectors given by $f_1(x) = \sin(x)$, $f_2(x) = \sin(2x)$, $f_3(x) = \sin(3x)$ are linearly independent.

3. Establish if this family of vectors

$$B = ((1, 1, 1), (3, 0, -1), (-1, 1, -1))$$

   is a basis for $\mathbb{R}^3$.

4. Establish if the sum of these vector subspaces of $\mathbb{R}^4$ is direct:

$$U = \mathrm{span}((1, 0, 1, 0), (1, 2, 3, 4)), \quad V = \mathrm{span}((0, 1, 1, 1), (0, 0, 0, 1)).$$

1.8.1 Solutions of the exercises of chapter 1

The reader is *strongly encouraged* not to look at the solution of the exercises proposed in the previous page before trying to solve them.

1. No, it is not, because it is not stable with respect to the sum. As an example, consider the polynomials of degree n given by $p(X) = 2X^n - 1$ and $q(X) = -2X^n + 2$, then $p(X) + q(X) = 2X^n - 1 - 2X^n + 2 = 1$, which is a polynomial of degree 0 because $1 = 1 \cdot X^0$, so it has not degree $n \geqslant 1$.

2. To determine if the given vectors are linearly independent we have to write a generic linear combination of them and equate it to the null vector of the vector space of functions $f : \mathbb{R} \to \mathbb{R}$, which is the null function $0 : \mathbb{R} \to \mathbb{R}$, $x \mapsto 0$. Thus, given $a, b, c \in \mathbb{R}$ we have to check if

$$af_1(x) + bf_2(x) + cf_3(x) = a\sin(x) + b\sin(2x) + c\sin(3x) = 0 \quad \forall x \in \mathbb{R},$$

implies that $a = b = c = 0$. Since a, b, c are constants, their value is independent of the choice of $x \in \mathbb{R}$, so we can choose particular values of x that suit our scope, for instance:

$$x = \frac{\pi}{2}: \quad a \cdot 1 + b \cdot 0 + c \cdot (-1) = 0 \iff a - c = 0 \iff a = c$$

$$x = \frac{\pi}{3}: \quad a \cdot \frac{\sqrt{3}}{2} + b \cdot \frac{\sqrt{3}}{2} + c \cdot (0) = 0 \iff \frac{\sqrt{3}}{2}(a + b) = 0 \iff a = -b$$

$$x = \frac{\pi}{4}: \quad a \cdot \frac{\sqrt{2}}{2} + b \cdot 1 + c \cdot \frac{\sqrt{2}}{2} = 0 \iff \frac{\sqrt{2}}{2}(a + c) = 0 \iff a = -c.$$

But $a = c$ and $a = -c$ can be simultaneously true if and only if $a = c = 0$, so, since $a = -b$, it follows that also $b = 0$, so all three constants are 0 and thus the three functions are linearly independent.

3. We have 3 vectors and the dimension of $\mathbb{R}^3$ is 3, since all the bases of $\mathbb{R}^3$ thanks to Theorem 1.4.2, if we prove that they are either linearly independent or that they generate $\mathbb{R}^3$, then they constitute a basis. We choose arbitrarily to check if they are linearly independent. Setting

$$a(1, 1, 1) + b(3, 0, -1) + c(-1, 1, -1) = (0, 0, 0)$$

we have to find that $a = b = c = 0$. The previous vector equation is equivalent to the system of linear equations

$$\begin{cases} a + 3b - c = 0 \\ a + c = 0 \\ a - b - c = 0 \end{cases} \iff \begin{cases} a = -c \\ 2a + 3b = 0 \\ 2a - b = 0 \end{cases}$$

subtracting both sides of the second and the third equation we find $4b = 0$, i.e. $b = 0$, so, eliminating the terms with b in either the second or the third equation we find $a = 0$, so $c = -a = 0$, thence the vectors are linearly independent and so they are a basis for $\mathbb{R}^3$.

4. A sum is direct if and only if the intersection of the two vector subspaces is reduced to the null vector of $\mathbb{R}^4$, i.e. $\mathbf{0} = (0,0,0,0)$. A vector $w \in \mathbb{R}^4$ belongs to the intersection of U and V if and only if it can be written both as a linear combination of the vectors generating U and of those generating V, i.e. if there exist $a, b, c, d \in \mathbb{R}$ such that

$$w = a(1,0,1,0) + b(1,2,3,4) = c(0,1,1,1) + d(0,0,0,1),$$

a vector equation which corresponds to the system of linear equations given by

$$\begin{cases} a + b = 0 \\ 2b = c \\ a + 3b = c \\ 4b = c + d \end{cases} \iff \begin{cases} a = -b \\ c = 2b \\ a + 3b = 2b \iff a = -b \\ 4b = 2b + d \iff d = 2b \end{cases} \iff \begin{cases} a = -b \\ b \in \mathbb{R} \\ c = d = 2b \end{cases}$$

Let us choose the simplest possible non zero value for b: $b = 1$, then $a = -1$ and $c = d = 2$, then

$$(-1,0,-1,0) + (1,2,3,4) = (0,2,2,4)$$

and

$$(0,2,2,2) + (0,0,0,2) = (0,2,2,4)$$

thus $w = (0,2,2,4) \in U \cap V$, so the sum $U + V$ is not direct.

Chapter 2

Linear maps and matrices

In this chapter we will develop the theory of linear maps between two vector spaces. We will introduce the concept of matrix and describe the tight link that exists between matrices and linear maps. The most important results of matrix theory will be discusses.

2.1 Linear maps

DISCLAIMER. In the mathematical literature, the word *map, function, application, transformation* and *operator* are used as synonyms. It must be kept in mind that they all refer to the same thing, i.e. a correspondence between a domain and a codomain which relates all the elements of the domain to one and only one element of the codomain. In linear algebra of finite-dimension vector spaces, it is custom to use the words map or application, instead, when infinite-dimensional vector spaces are involved, the word operator is more common. Finally, the word function is more frequent in real analysis. *In this notes, I have chosen to use map for brevity.*

Linear maps are the functions that 'passes through' linear combinations, let us see what this means. Consider two vector spaces V and W, not necessarily different but both defined over the same field $\mathbb{F}$, and the linear combination

$$v = \lambda_1 v_1 + \cdots + \lambda_n v_n = \sum_{j=1}^{n} \lambda_j v_j,$$

$\lambda_j \in \mathbb{F}$ and $v_j \in V$, for all $j = 1, \ldots, n$.

Consider then a map $f : V \to W$ and apply it to v:

$$f(v) = f\left(\sum_{j=1}^{n} \lambda_j v_j\right),$$

since f acts of vectors, the only way in which f can 'pass through' the linear combination is that we can exchange the position of the sum and of the scalars λ_j with that of f, i.e. f passes through the linear combination if it happens that

$$f\left(\sum_{j=1}^{n} \lambda_j v_j\right) = \sum_{j=1}^{n} \lambda_j f(v_j). \tag{2.1}$$

By expanding the sum, the last equality can be written as

$$f(\lambda_1 v_1 + \cdots + \lambda_n v_n) = \lambda_1 f(v_1) + \cdots + \lambda_n f(v_n), \tag{2.2}$$

the defining features of this equality can be understood by considering two special cases:

1. suppose $n = 1$, then (2.2) gives $f(\lambda_1 v_1) = \lambda_1 f(v_1)$, a feature called *homogeneity* of f
2. suppose $n = 2$ and $\lambda_1 = \lambda_2 = 1$, then (2.2) gives $f(v_1 + v_2) = f(v_1) + f(v_2)$, a feature called *additivity* of f.

The following definition formalized what just discussed.

Def. 2.1.1 (Linear map) *Let V and W be two, not necessarily different, vector spaces over the same field $\mathbb{F}$. A map $f : V \to W$ is said to be linear if*

1. *f is additive: $f(v_1 + v_2) = f(v_1) + f(v_2)$ for all $v_1, v_2 \in V$*
2. *f is homogeneous: $f(\lambda v) = \lambda f(v)$, for all $\lambda \in \mathbb{F}$ and $v \in V$.*

Together, the two properties of a linear map lead to formula (2.1) by extending the sum and the product with a scalar to a linear combination of vectors of V with coefficients in $\mathbb{F}$.

Let us immediately see what is the behavior of a linear map when it is applied to the null vector $\mathbf{0}_V$ of V: since, for every $v \in V$, we have that $v = v + \mathbf{0}_V$, by the additivity of f we have

$$f(v) = f(v + \mathbf{0}_V) \underset{\text{additivity}}{=} f(v) + f(\mathbf{0}_V),$$

but $f(v) = f(v) + f(\mathbf{0}_V)$ if and only if $f(\mathbf{0}_V)$ is the null vector $\mathbf{0}_W$ of the vector space W (recall that f sends any vector of V, and so also the null vector $\mathbf{0}_V$ to vectors of W!). Hence:

$$f(\mathbf{0}_V) = \mathbf{0}_W,$$

i.e., *a linear map transforms the null vector of its domain vector space to the null vector of its codomain vector space.*

We have concluded the first chapter by showing that the properties of a basis B of a vector space V lead naturally to consider a linear map, that we have defined in (1.10). Let us now show that this map is not only linear, but it has the property defined below.

Def. 2.1.2 *If a linear map $f : V \to W$ is one-to-one[1] and onto[2], then it is called an isomorphism[3] between V and W, which are said to be isomorphic via f.*

Theorem 2.1.1 *Fixed a basis B of a vector space V of dimension n over the field $\mathbb{F}$, the linear map f_B defined in (1.10), i.e.*

$$\begin{array}{rccl} f_B : & V & \longrightarrow & \mathbb{F}^n \\ & v & \longmapsto & f_B(v) = (\lambda_1, \ldots, \lambda_n), \end{array}$$

is an isomorphism.

[1] *one-to-one* means that, if $v \neq w$, then $f(v) \neq f(w)$.

[2] *onto* means that, for all $w \in W$ it exists at least a $v \in V$ such that $w = f(v)$.

[3] thus, an *isomorphism* is a linear map linear $f : V \to W$ such that, for all $w \in W$ it *exists one and only one* $v \in V$ such that $w = f(v)$.

Notice that $\mathbb{F}^n$ is always the same independently of V, for this reason we say that $\mathbb{F}^n$ is the prototype of any vector space over the field $\mathbb{F}$ of dimension n.

So, $\mathbb{R}^n$ and $\mathbb{C}^n$ are the prototypes of all real and complex, respectively, vector spaces of dimension n. However, it is important to highlight that the isomorphism with $\mathbb{F}^n$ is subjected to the choice of a basis of V, hence it is not a 'canonical' isomorphism.

Despite not being canonical, the isomorphism established by f_B, when B is chosen once and for all, allows us to transfer the analysis of any vector space to that of $\mathbb{F}^n$, which is *the easiest non trivial vector space*, explains the particular interest dedicated to this kind of vector space in linear algebra.

Proof. We have already stated in chapter 1 that the function f_B is linear. We now prove that, thanks to the fact that B is a basis, f_B is both one-to-one and onto.

f_B is one-to-one because every v can be *uniquely* written as a linear combination of the basis vectors with coefficients that are not shared with any other vector different than v. This follows from the fact that the basis vectors are *linearly independent* and so theorem 1.3.2 can be applied.

f_B is onto because a basis is also a *family of generators* and so $V = \text{span}(B)$, thus each different ordered sequence of scalars $(\lambda_1, \dots, \lambda_n)$ defines a different vector $v \in V$, hence, as v varies in V, $f_B(v)$ represents all possible n-tuple of scalars of $\mathbb{F}$. $\square$

The previous theorem has a very important consequence. Before discussing it, we must recall the concept of **composition** and **inversion** of functions. Given any two sets X and Y and $f_1 : X \to Y$, $f_2 : Y \to Z$, we write their *composition* as the function $f_2 \circ f_1 : X \to Z$ (notice the order!) as follows

$$\begin{array}{rccl} f_2 \circ f_1 : & X & \longrightarrow & Z \\ & x & \longmapsto & (f_2 \circ f_1)(x) := f_2(f_1(x)), \end{array}$$

with makes perfect sense because $y = f_1(x) \in Y$ and f_2 is defined on Y, so $z = f_2(y)$ belongs to Z. The composite function $f_2 \circ f_1$ allows us to skip the intermediate transformations $X \to Y$ and $Y \to Z$ and it does it in just one shot $X \to Z$ as depicted in Figure 2.1.

$$\begin{tikzcd} X \arrow[r, "f_1"] \arrow[rr, bend left, "f_2 \circ f_1"] \arrow[d, dotted, no head] & Y \arrow[r, "f_2"] \arrow[d, dotted, no head] & Z \arrow[d, dotted, no head] \\ x & y = f_1(x) & z = f_2(y) \end{tikzcd}$$

Figure 2.1: Composition of functions.

Example 2.1.1 Consider

- $f_1 : \mathbb{R} \to [1, +\infty)$, $x \mapsto y = f_1(x) := 1 + x^2$
- $f_2 : [1, +\infty) \to [0, +\infty)$, $y \mapsto z = f_2(y) := \log(y)$, substituting the explicit expression of $y = 1 + x^2$ we find $z = \log(1 + x^2)$
- Then, the composite function is $f_2 \circ f_1 : \mathbb{R} \to [0, +\infty)$, $x \to (f_2 \circ f_1)(x) = \log(1 + x^2)$.

If a function $f : X \to Y$ is *one-to-one and onto*, then we can construct its *inverse function* $f^{-1} : Y \to X$ defined in this way: for all $y \in Y$, $f^{-1}(y) = x$, where $x \in X$ is the only element of X such that $f(x) = y$. x exists because f is onto and x is unique because f is one-to-one.

The composition between f and f^{-1} has a special name: $f^{-1} \circ f : X \to X$ is called **identity function** on X and indicated with id_X, while $f \circ f^{-1} : Y \to Y$ is called identity function on Y and indicated with id_Y. Both identity function leave all the elements of the set on which they are defined unchanged.

Let us see why analyzing for instance $f^{-1} \circ f : X \to X$:

$$\begin{array}{rccccc} f^{-1} \circ f : & X & \longrightarrow & Y & \longrightarrow & X \\ & x & \longmapsto & y = f(x) & \longmapsto & f^{-1}(y) = x, \end{array}$$

thus, the global action of $f^{-1} \circ f$ on any $x \in X$ is to leave it as it is, for this reason $f^{-1} \circ f = id_X$.

Example 2.1.2 Consider:

- $f : \mathbb{R} \to \mathbb{R}$, $x \mapsto y = x^3$
- $f^{-1} : \mathbb{R} \to \mathbb{R}$, $y \mapsto \sqrt[3]{y}$
- $f^{-1} \circ f : \mathbb{R} \to \mathbb{R}$, $x \mapsto \sqrt[3]{y} = \sqrt[3]{x^3} = x$.

Having recalled these concepts, we can now state and prove the following consequence of the previous theorem.

Corollary 2.1.1 *Two vector spaces V and W defined over the same field $\mathbb{F}$ are isomorphic if and only if they have the same dimension.*

Proof. Suppose $\dim(V) = \dim(W) = n$, fix a basis B_1 of V and a basis B_2 of W and then consider the following diagram:

$$\begin{tikzcd} V \arrow[rr, dashed, leftrightarrow, "\sim"] \arrow[dr, "f_{B_1}"] & & W \arrow[dl, "f_{B_2}"'] \\ & \mathbb{F}^n \arrow[ul, bend left, "f_{B_1}^{-1}"] \arrow[ur, bend right, "f_{B_2}^{-1}"'] & \end{tikzcd}$$

We can build two isomorphisms between V and W: the first is

$$\begin{array}{rccl} f_{V,W} = f_{B_2}^{-1} \circ f_{B_1} : & V & \longrightarrow & W \\ & v & \longmapsto & f_{V,W}(v) = f_{B_2}^{-1}(f_{B_1}(v)) \end{array}$$

while the second is:

$$\begin{array}{rccl} f_{W,V} = f_{B_1}^{-1} \circ f_{B_2} : & W & \longrightarrow & V \\ & w & \longmapsto & f_{W,V}(w) = f_{B_1}^{-1}(f_{B_2}(w)) \end{array}$$

Both are isomorphisms because they are built by composition of isomorphisms. $\square$

The last result is the reason why in many books about linear algebra it is said that *the only important information to know about a vector space are its dimension and the field that contains its scalars*. Indeed, once we know that, up to an isomorphism, the vector space V can be identified with $\mathbb{F}^{\dim(V)}$.

2.2 Kernel and image of a linear map

In this section we introduce and analyze two extremely important vector subspaces related to a linear map.

Def. 2.2.1 *Let $f : V \to W$ be a linear map.*

- *The kernel*[4] *of f is the subset of V given by*

$$\ker(f) := \{v \in V : f(v) = \mathbf{0}_W\}.$$

- *The image of f is the subset of W given by*

$$\mathrm{Im}(f) := \{w \in W : \exists v \in V \text{ such that } w = f(v)\}.$$

Recalling that a linear map $f : V \to W$ transforms $\mathbf{0}_V$ into $\mathbf{0}_W$, we have that $\ker(f)$ is never empty because, at least, it contains $\mathbf{0}_V$. The opposite situation is when f is the *null map*, in this case all the vectors of V are mapped to $\mathbf{0}_W$, so $\ker(f) = V$.

Theorem 2.2.1 *Given the linear map $f : V \to W$, $\ker(f)$ is a vector subspace of V and $\mathrm{Im}(f)$ is a vector subspace of W.*

Proof. Recall that, in order to prove that a subset of a vector space is a vector subspace, we must prove that a generic linear combination of elements of the subset remains in the subset.

Let us start with the kernel. Let $v_1, v_2 \in \ker(f)$, which means that $f(v_1) = f(v_2) = \mathbf{0}_W$, $\lambda_1, \lambda_2 \in \mathbb{F}$ and apply f to the linear combination $\lambda_1 v_1 + \lambda_2 v_2$: using the linearity of f we find

$$f(\lambda_1 v_1 + \lambda_2 v_2) = \lambda_1 f(v_1) + \lambda_2 f(v_2) = \lambda_1 \mathbf{0}_W + \lambda_2 \mathbf{0}_W = \mathbf{0}_W,$$

so $f(\lambda_1 v_1 + \lambda_2 v_2) = \mathbf{0}_W$ and then, by definition, $\lambda_1 v_1 + \lambda_2 v_2 \in \ker(f)$.

Now we consider the image. Let $w_1, w_2 \in W$ such that $w_1 = f(v_1)$ and $w_2 = f(v_2)$, with $v_1, v_2 \in V$, then, by applying first the homogeneity and then the additivity of the linear map f we have

$$\lambda_1 w_1 + \lambda_2 w_2 = \lambda_1 f(v_1) + \lambda_2 f(v_2) = f(\lambda_1 v_1) + f(\lambda_2 v_2) = f(\lambda_1 v_1 + \lambda_2 v_2),$$

so $\lambda_1 w_1 + \lambda_2 w_2 = f(\lambda_1 v_1 + \lambda_2 v_2)$, hence $\lambda_1 w_1 + \lambda_2 w_2 \in \mathrm{Im}(f)$. □

Since $\ker(f)$ and $\mathrm{Im}(f)$ are subspaces, it makes sense to talk about their dimensions, which have specific names.

Def. 2.2.2 (Nullity and rank) *Given the linear map $f : V \to W$,*

- $\dim(\ker(f)) \leqslant \dim(V)$ *is called nullity of f and indicated with* $\mathrm{null}(f)$
- $\dim(\mathrm{Im}(f)) \leqslant \dim(W)$ *is called rank of f and indicated with* $\mathrm{rank}(f)$.

It turns out that the nullity and rank of f characterize its properties as a one-to-one and onto linear map, respectively.

[4] certain authors prefer **null space** instead of kernel.

Theorem 2.2.2 *The linear map $f : V \to W$ is onto if and only if* $\mathrm{Im}(f) = W$*, i.e. if and only if its rank is maximal:* $\mathrm{rank}(f) = \dim(W)$*.*

It is because of this theorem that an onto linear map is also called **full-rank**.

Proof. f is onto if and only if every $w \in W$ can be written as $w = f(v)$ for a certain $v \in V$, so $\mathrm{Im}(f) = W$. In this case $\mathrm{rank}(f) = \dim(\mathrm{Im}(f)) = \dim(W)$. □

Theorem 2.2.3 *The linear map $f : V \to W$ is one-to-one if and only if* $\ker(f) = \{\mathbf{0}_V\}$*, i.e. if and only if its nullity is* 0*.*

Proof.

$\boxed{\Longrightarrow}$: suppose f is one-to-one, then, since we already know that $\mathbf{0}_V \in \ker(f)$, and so $f(\mathbf{0}_V) = \mathbf{0}_W$, no other vector is mapped into $\mathbf{0}_W$ other than $\mathbf{0}_V$, hence $\ker(f) = \{\mathbf{0}_V\}$.

$\boxed{\Longleftarrow}$: suppose $\ker(f) = \{\mathbf{0}_V\}$, then, if $v_1, v_2 \in V$ are such that $f(v_1) = f(v_2)$ we have $f(v_1) - f(v_2) = \mathbf{0}_W$, but, thanks to the linearity of f, this implies $f(v_1 - v_2) = \mathbf{0}_W$, i.e. $v_1 - v_2 \in \ker(f) = \{\mathbf{0}_V\}$, so $v_1 - v_2 = \mathbf{0}_V$, which means that $v_1 = v_2$. If follows that f is one-to-one. □

Since a linear map is an isomorphism when it is one-to-one and onto, the previous two theorems imply immediately the next result.

Corollary 2.2.1 *The linear map $f : V \to W$ is an isomorphism if and only if it has full rank and zero nullity.*

The following theorem relates the dimension of the domain of a linear map with its nullity and rank.

Theorem 2.2.4 (Nullity+rank) *Given the linear map $f : V \to W$ we have*

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

At first glance, the thesis of this theorem can be surprising because the dimension of W does not play any role. Only by looking at the proof one can understand why is that, however, the proof is a bit technical and it would take too much time to discuss it properly, for this reason we omit it. Instead, we prefer to analyze an important consequence of this theorem on linear maps for which domain and codomain coincide. These maps bear a special name.

Def. 2.2.3 *A linear map $f : V \to V$, i.e. for which $V = W$, is called **endomorphism**.*

Theorem 2.2.5 *Let $f : V \to V$ be an endomorphism. f one-to-one $\Longrightarrow$ f also onto. Vice-versa, f onto $\Longrightarrow$ f also one-to-one. So, for an endomorphism to be an isomorphism it is enough to be either one-to-one or onto.*

Proof. The proof relies solely on the nullity+rank theorem... try to figure out why... □

Example 2.2.1 Determine if the following linear map is one-to-one, onto or an isomorphism.

$$\begin{array}{rccl} f_1 : & \mathbb{R}^2 & \longrightarrow & \mathbb{R}^2 \\ & v=(x,y) & \longmapsto & f_1(v)=f_1(x,y):=(x-y,x+y). \end{array}$$

First of all notice that f_1 acts on the components of v through linear combinations, so it is indeed linear.

To determine if f_1 is one-to-one let us study its kernel by imposing

$$f_1(x,y)=(0,0) \iff (x-y,x+y)=(0,0) \iff \begin{cases} x-y=0 \\ x+y=0 \end{cases},$$

the first equation implies that $x=y$, which, introduced in the second, implies $2y=0$, i.e. $y=0$ and so also $x=0$. It follows that (x,y) is nullified by f_1 if and only if it is $\mathbf{0}=(0,0)$, so f_1 is one-to-one.

To study if f_1 is also onto would be redundant, because we recognize that the domain and codomain of f_1 are the same, hence f_1 is an endomorphism, so the fact that it is one-to-one implies that it also onto and, in turn, that f_1 is an isomorphism of $\mathbb{R}^2$ with itself.

Example 2.2.2 Determine if the following linear map is one-to-one, onto or an isomorphism.

$$\begin{array}{rccl} f_2 : & \mathbb{R}^2 & \longrightarrow & \mathbb{R}^2 \\ & v=(x,y) & \longmapsto & f_2(v)=f_2(x,y):=(x-y,x-y). \end{array}$$

Let us study again the kernel of f_2 by we imposing

$$f_2(x,y)=(0,0) \iff (x-y,x-y)=(0,0) \iff \begin{cases} x-y=0 \\ x-y=0 \end{cases},$$

this time both equations are the same and they imply that $x=y$. This means that all the vectors of $\mathbb{R}^2$ written as follows $v=(x,x)$, with $x\in\mathbb{R}$ are nullified by f_2. Hence, f_2 is not one-to-one and so it cannot be an isomorphism.

Let us check if f_2 is at least onto. We have to check if, for all $w=(a,b)\in\mathbb{R}^2$ there exists $v=(x,y)\in\mathbb{R}^2$ such that $(a,b)=f_2(x,y)$:

$$(a,b)=f_2(x,y) \iff (a,b)=(x-y,x-y) \iff \begin{cases} a=x-y \\ b=x-y \end{cases}.$$

We see quite easily that f_2 cannot be onto: in fact it is enough to consider $a\neq b$ to see that the previous system cannot be solved, in fact two different numbers cannot be equal to the same number $x-y$.

So, f_2 provides us the example of an endomorphism which is neither one-to-one nor onto.

2.3 Linear maps and bases

In this section we study the relation between linear maps and bases of vector spaces. We start with this fundamental theorem.

Theorem 2.3.1 *Let $f : V \to W$ be a linear map and $B = (v_1, \ldots, v_n)$ a basis for V. Then $\{f(v_1), \ldots, f(v_n)\}$ is a family of generators (in general non-free) for $\mathrm{Im}(f)$. So, linear maps transform bases of their domains into families of generators of their images.*

Proof. For every $w \in \mathrm{Im}(f)$ there exists $v \in V$ such that $w = f(v)$, since B is a basis, $v = \sum_{j=1}^{n} \lambda_j v_j$, hence, by the linearity of f, $w = f(v) = \sum_{j=1}^{n} \lambda_j f(v_j)$.

This means that every $w \in \mathrm{Im}(f)$ can be written as a linear combination of the vectors belonging to the family $\{f(v_1), \ldots, f(v_n)\}$, so, by definition, this family generates $\mathrm{Im}(f)$. □

We now show that a linear map $f : V \to W$ is completely determined by the knowledge of the images of the vectors of a basis of V, which can be arbitrarily chosen in W.

Theorem 2.3.2 (Generic expression of a linear map) *Let $f : V \to W$ be a linear map and let $B = (v_1, \ldots, v_n)$ be a basis of V.*

1. *f is uniquely determined by the way it transforms the vectors of B, i.e. by the knowledge of the vectors of W given by $f(v_1), \ldots, f(v_n)$.*

2. *Once n vectors $w_1, \ldots, w_n$ are arbitrarily chosen in W, there exists a unique linear map $f : V \to W$ such that $w_j = f(v_j)$, $j = 1, \ldots, n$.*

f is uniquely associated to the basis B, so, if another basis is chosen, then f changes.

Proof.

1. Consider any vector $v \in V$, then we know that there exist unique scalars λ_j, $j = 1, \ldots, n$, such that
$$v = \sum_{j=1}^{n} \lambda_j v_j.$$
By linearity, f acts on v as follows
$$f(v) = \sum_{j=1}^{n} \lambda_j f(v_j). \tag{2.3}$$
Since the scalars are uniquely determined by v and the basis, the only action that is left to f is the way in which it transforms the basis vectors. Hence, once we know the vectors $f(v_j)$, $j = 1, \ldots, n$, we automatically know the action of f.

2. Define the linear map f on the basis vectors as follows $f(v_j) := w_j$, then for every $v \in V$ there is a unique set $(\lambda_j)_{j=1}^{n}$ such that $v = \sum_{j=1}^{n} \lambda_j v_j$ so, by linearity, $f(v) = \sum_{j=1}^{n} \lambda_j f(v_j)$. Thanks to the statement of item 1., this defines f uniquely.

□

We can highlight the results of this last theorem as follows.

PRACTICAL METHOD TO EXTEND A LINEAR MAP $f : V \to W$ FROM THE KNOWLEDGE OF ITS ACTION ON THE VECTOR OF A BASIS OF V TO THE WHOLE SPACE V

1. Let the basis of V be $B = (v_1, \ldots, v_n)$
2. Suppose $f(v_1), \ldots, f(v_n)$ are known
3. Decompose any v on B: $v = \sum_{j=1}^{n} \lambda_j v_j$
4. Then, the action of f on v is

$$\boxed{f(v) = \sum_{j=1}^{n} \lambda_j f(v_j)}\,. \tag{2.4}$$

PRACTICAL METHOD TO BUILT A LINEAR MAP $f : V \to W$ FROM THE RANDOM CHOICE OF $n = \dim(V)$ NUMBER OF VECTORS OF W

1. Fix arbitrarily the vectors $w_1, \ldots, w_n$ of W
2. Fix a basis $B = (v_1, \ldots, v_n)$ of V
3. Define $f(v_1) := w_1, \ldots, f(v_n) := w_n$
4. Decompose any v on B: $v = \sum_{j=1}^{n} \lambda_j v_j$
5. Then, the action of f on v is

$$\boxed{f(v) = \sum_{j=1}^{n} \lambda_j w_j}\,. \tag{2.5}$$

The expressions (2.4) (2.5) reveal that **all linear maps are written as linear combinations of vectors belonging to their codomain**.

Example 2.3.1 Let $V = W = \mathbb{R}^3$ and consider the canonical basis of $\mathbb{R}^3$. Let $f : V \to W$ be the linear map that transforms the canonical basis vectors as follows:

$$\begin{cases} f((1,0,0)) = (1,1,2) \\ f((0,1,0)) = (0,0,-1) \\ f((0,0,1)) = (-1,2,0) \end{cases} . \tag{2.6}$$

To find the expression of f on the general vector $v = (x, y, z) \in \mathbb{R}^3$, we use the first practical method. Since we have fixed the canonical basis, the decomposition of v on it is simply

$$v = x(1,0,0) + y(0,1,0) + z(0,0,1) = (x, y, z),$$

then, using formula (2.4) we have

$$\begin{aligned} f((x,y,z)) &= xf((1,0,0)) + yf((0,1,0)) + zf((0,0,1)) \\ &= x(1,1,2) + y(0,0,-1) + z(-1,2,0) \\ &= (x,x,2x) + (0,0,-y) + (-z,2z,0) = (x-z, x+2z, 2x-y). \end{aligned}$$

So, the extension of f on the whole $\mathbb{R}^3$ is

$$f((x,y,z)) = (x-z, x+2z, 2x-y), \quad x,y,z \in \mathbb{R}.$$

Example 2.3.2 Consider now the basis of $\mathbb{R}^3$ examined in exercise 3. of chapter 1, i.e.

$$B = ((1,1,1),(3,0-1),(-1,1,-1))$$

and define the linear map $g : \mathbb{R}^3 \to \mathbb{R}^3$ by imposing that the vectors of B are mapped to the same vectors as in (2.6), i.e.

$$\begin{cases} g((1,1,1)) = (1,1,2) \\ g((3,0,-1)) = (0,0,-1) \\ g((-1,1,-1)) = (-1,2,0) \end{cases} . \tag{2.7}$$

g maps different vectors than those of the canonical basis of $\mathbb{R}^3$ to the same vectors used to define f in (2.6), so, by the uniqueness property established by Theorem 2.3.2, g cannot be the same linear map as f, we will verify that this is indeed the case.

This time, since we are not using the canonical basis, in order to find the expression of the general vector $v = (x,y,z) \in \mathbb{R}^3$ with respect to B, we have to write the vector equation

$$(x,y,z) = a(1,1,1) + b(3,0,-1) + c(-1,1,-1) = (a+3b-c, a+c, a-b-c),$$

which can be equivalently expressed by the following system of linear equations

$$\begin{cases} a+3b-c = x & (1) \\ a+c = y & (2) \\ a-b-c = z & (3) \end{cases} \underset{(1)\mapsto(1)-(3)}{\iff} \begin{cases} 4b = x-z \\ a = y-c \\ y-c-b-c = z \end{cases} \iff \begin{cases} b = \frac{x}{4} - \frac{z}{4} \\ a = y-c \\ 2c = y - (\frac{x}{4} - \frac{z}{4}) - z \end{cases}$$

so,

$$\begin{cases} b = \frac{x}{4} - \frac{z}{4} \\ a = y-c \\ c = \frac{y}{2} - \frac{x}{8} - \frac{3z}{8} \end{cases} \iff \begin{cases} a = \frac{y}{2} + \frac{x+3z}{8} \\ b = \frac{x-z}{4} \\ c = \frac{y}{2} - \frac{x+3z}{8} \end{cases} . \tag{2.8}$$

Thus

$$(x,y,z) = \left(\frac{y}{2} + \frac{x+3z}{8}\right)(1,1,1) + \left(\frac{x-z}{4}\right)(3,0,-1) + \left(\frac{y}{2} - \frac{x+3z}{8}\right)(-1,1-1),$$

and so

$$\begin{aligned} g((x,y,z)) &= \left(\frac{y}{2} + \frac{x+3z}{8}\right) g((1,1,1)) + \left(\frac{x-z}{4}\right) g((3,0,-1)) + \left(\frac{y}{2} - \frac{x+3z}{8}\right) g((-1,1-1)) \\ &= \left(\frac{y}{2} + \frac{x+3z}{8}\right)(1,1,2) + \left(\frac{x-z}{4}\right)(0,0,-1) + \left(\frac{y}{2} - \frac{x+3z}{8}\right)(-1,2,0) \\ &= \left(\left(\frac{y}{2} + \frac{x+3z}{8}, \frac{y}{2} + \frac{x+3z}{8}, y + \frac{x+3z}{4}\right) + \left(0,0,\frac{z-x}{4}\right) + \left(\frac{x+3z}{8} - \frac{y}{2}, y - \frac{x+3z}{4}, 0\right)\right) \\ &= \left(\frac{x+3z}{4}, \frac{3}{2}y - \frac{x+3z}{8}, y+z\right), \end{aligned}$$

so the extension of g on the whole $\mathbb{R}^3$ is:

$$g((x,y,z)) = \left(\frac{x+3z}{4}, \frac{3}{2}y - \frac{x+3z}{8}, y+z\right), \quad x,y,z \in \mathbb{R}.$$

Let us check that this expression is coherent with the vectors assigned in (2.7):

$$\begin{cases} g((1,1,1)) = \left(\frac{1+3}{4}, \frac{3}{2} - \frac{1+3}{8}, 1+1\right) = (1,1,2) \\ g((3,0,-1)) = \left(\frac{3-3}{4}, 0 - \frac{3-3}{8}, 0-1\right) = (0,0,-1) \\ g((-1,1,-1)) = \left(\frac{-1-3}{4}, \frac{3}{2} - \frac{-1-3}{8}, 1-1\right) = (-1,2,0) \end{cases}.$$

Example 2.3.3 This example is about the second practical method to build a linear map. We select arbitrarily three vectors of $W = \mathbb{R}^3$, for instance:

$$w_1 = (0,1,2),\ w_2 = (1,1,1),\ w_3 = (2,0,0).$$

We can fix for instance the canonical basis of $V = \mathbb{R}^3$ and define the linear map $\varphi : \mathbb{R}^3 \to \mathbb{R}^3$ to verify these equations:

$$\begin{cases} \varphi((1,0,0)) = w_1 = (0,1,2) \\ \varphi((0,1,0)) = w_2 = (1,1,1) \\ \varphi((0,0,1)) = w_3 = (2,0,0) \end{cases}.$$

We know that the decomposition of the generic vector $v = (x,y,z) \in \mathbb{R}^3$ on the canonical basis of $\mathbb{R}^3$ is $v = (x,y,z)$, so, using eq. (2.5), the action of φ on v is

$$\varphi((x,y,z)) = xw_1 + yw_2 + zw_3 = x(0,1,2) + y(1,1,1) + z(2,0,0) = (y+2z, x+y, 2x+y).$$

To highlight the dependence on the choice of the basis, let us now chose, instead of the canonical basis of $\mathbb{R}^3$, the basis B of Example 2.3.2 to build a linear map, which we already know that it will be different than φ, so that we denote it with ψ:

$$\begin{cases} \psi((1,1,1)) = w_1 = (0,1,2) \\ \psi((3,0,-1)) = w_2 = (1,1,1) \\ \psi((-1,1,-1)) = w_3 = (2,0,0) \end{cases}.$$

From Example 2.3.2 we know that the decomposition of the generic vector $v = (x,y,z) \in \mathbb{R}^3$ on B is:

$$(x,y,z) = a(1,1,1) + b(3,0,-1) + c(-1,1,-1)$$

with $a = \frac{y}{2} + \frac{x+3z}{8}$, $b = \frac{x-z}{4}$, $c = \frac{y}{2} - \frac{x+3z}{8}$. Hence, this time eq. (2.5) implies that the action of ψ on v is

$$\begin{aligned} \psi((x,y,z)) &= \left(\frac{y}{2} + \frac{x+3z}{8}\right) w_1 + \left(\frac{x-z}{4}\right) w_2 + \left(\frac{y}{2} - \frac{x+3z}{8}\right) w_3 \\ &= \left(\frac{y}{2} + \frac{x+3z}{8}\right)(0,1,2) + \left(\frac{x-z}{4}\right)(1,1,1) + \left(\frac{y}{2} - \frac{x+3z}{8}\right)(2,0,0) \\ &= \left(\frac{x-z}{4} + y - \frac{x+3z}{4}, \frac{y}{2} + \frac{x+3z}{8} + \frac{x-z}{4}, y + \frac{x+3z}{4} + \frac{x-z}{4}\right) \\ &= \left(y - z, \frac{y}{2} + \frac{3x+z}{8}, y + \frac{x+z}{2}\right). \end{aligned}$$

As expected, φ and ψ are different linear maps.

Since $f : V \to W$ is completely determined by its action on the vectors $v_1, \ldots, v_n$ of any fixed basis of V, it comes with no surprise that the properties of f can be studied by the properties of the family of vectors $f(v_1), \ldots, f(v_n)$.

Theorem 2.3.3 *Let $f : V \to W$ be a linear map and $B = (v_1, \ldots, v_n)$ a basis for V.*

1. *f is one-to-one if and only if $\{f(v_1), \ldots, f(v_n)\}$ is a free family in W*
2. *f is onto if and only if $\{f(v_1), \ldots, f(v_n)\}$ is a family of generators of W*
3. *f is and isomorphism if and only if $\{f(v_1), \ldots, f(v_n)\}$ is a basis of W.*

Proof.

1. We will prove the two opposite implications separately.

$\boxed{\Longrightarrow}$: let us suppose that f is one-to-one, then we know that $\ker(f) = \mathbf{0}_V$. We have to prove that $f(v_1), \ldots, f(v_n)$ is a family of linearly independent vectors of W, i.e. that if a linear combination of these vectors is $\mathbf{0}_W$, then all the scalars of the linear combination are 0. Let us write this linear combination as

$$\lambda_1 f(v_1) + \cdots + \lambda_n f(v_n) = \mathbf{0}_W \iff \sum_{j=1}^{n} \lambda_j f(v_j) = \mathbf{0}_W \underset{f \text{ linear}}{\iff} f\left(\sum_{j=1}^{n} \lambda_j v_j\right) = \mathbf{0}_W,$$

remember now that we are under the hypothesis that $\ker(f) = \mathbf{0}_V$, which implies that $\sum_{j=1}^{n} \lambda_j v_j = \mathbf{0}_V$, but the vectors $v_1, \ldots, v_n$ are a basis of V, so they are linearly independent, which means that $\lambda_j = 0$ for all $j = 1, \ldots, n$, and so $\{f(v_1), \ldots, f(v_n)\}$ is a free family in W.

$\boxed{\Longleftarrow}$: now we suppose that $\{f(v_1), \ldots, f(v_n)\}$ is a free family in W and we must prove that this implies that f in one-to-one, i.e. that $\ker(f) = \mathbf{0}_V$. Consider a generic vector $v \in \ker(f)$ and decompose it on the basis B:

$$v = \sum_{j=1}^{n} \lambda_j v_j \underset{f \text{ linear}}{\Longrightarrow} f(v) = \sum_{j=1}^{n} \lambda_j f(v_j) = \mathbf{0}_W \quad \text{because } v \in \ker(f).$$

However, $f(v_1), \ldots, f(v_n)$ is a family of linearly independent vectors of W, so $\lambda_j = 0$ for all $j = 1, \ldots, n$, i.e. $v = \sum_{j=1}^{n} 0 v_j = \mathbf{0}_V$ and thus $\ker(f) = \{\mathbf{0}_V\}$, i.e. f is one-to-one.

2. Recall that f is onto if and only if $\mathrm{Im}(f) = W$ and recall from Theorem 2.3.1 that if $B = (v_1, \ldots, v_n)$ is a basis for V, then $\{f(v_1), \ldots, f(v_n)\}$ is a family of generators for $\mathrm{Im}(f)$. So, f is onto if and only if $\{f(v_1), \ldots, f(v_n)\}$ is a family of generators for the whole W.

3. By mixing together 1. and 2. we have that f is both one-to-one and onto, i.e. it is an isomorphism, if and only if $\{f(v_1), \ldots, f(v_n)\}$ is both free and it generates W, i.e. if and only if $\{f(v_1), \ldots, f(v_n)\}$ is a basis of W. $\square$

Example 2.3.4 Let us consider the linear maps φ and ψ of 2.3.3. In both cases, the images of the vectors of either the canonical basis of $\mathbb{R}^3$ or of the basis $((1,1,1),(3,0,-1),(-1,1,-1))$ are $w_1 = (0,1,2),\ w_2 = (1,1,1),\ w_3 = (2,0,0)$.

Let us determine if these vectors are linearly independent, a family of generators or a basis of $\mathbb{R}^3$. Since we are dealing with three vectors of a vector space of dimension 3, by Theorem 1.4.2, it is enough to establish, for instance, if w_1, w_2, w_3 are linearly independent to assure that they are also a family of generators and so a basis of $\mathbb{R}^3$. If this is the case, then, by virtue of Theorem 2.3.3, both φ and ψ are isomorphisms.

To check if w_1, w_2, w_3 are linearly independent, we write as usual

$$aw_1+bw_2+cw_3 = \mathbf{0} \iff (a,a,a)+(3b,0,-c)+(-a,b,-c) = \mathbf{0} \iff (a+3b,a+b,a-2c) = \mathbf{0},$$

which corresponds to the system of linear equations

$$\begin{cases} a+3b=0 \\ a+b=0 \\ a-2c=0 \end{cases} \iff \begin{cases} a=-b \\ -b+3b=0 \implies b=0 \\ -b-2c=0 \end{cases} \iff \begin{cases} a=0 \\ b=0 \\ c=0 \end{cases}.$$

So w_1, w_2, w_3 are linearly independent and, thank to the argument discussed above, both φ and ψ are isomorphisms.

Corollary 2.3.1 *Let $f : V \to W$ be a linear map and* $\dim(V) < \dim(W)$*, then f cannot be onto.*

Proof. By item 2. of Theorem 2.3.3, we have that f is onto if and only if the images of the vectors of a basis of V form a family of generators of W. By the number of vectors in a basis of V is exactly $\dim(V)$, hence also the number of images of these vectors via f will be $\dim(V)$. Thus, if $\dim(V) < \dim(W)$, we do not have enough vectors to generate W and so f cannot be onto. $\square$

2.4 The matrix associated to a linear map

This section is one of the most important of the entire course.

We have seen that, given two vector spaces V and W over the same field $\mathbb{F}$, of dimension $\dim(V) = n$ and $\dim(W) = m$, once a basis

$$B_V = (v_1, \dots, v_n) = (v_j)_{j=1}^n$$

of V is fixed, we can uniquely know the action of a linear map $f : V \to W$ on all the vectors of V if we know how f transforms the vectors of the basis B_V.

The vectors $f(v_1), \dots, f(v_n)$ belong to W, so, we can wonder what happens if we fix also a basis

$$B_W = (w_1, \dots, w_m) = (w_i)_{i=1}^m$$

of W. The most natural thing that we can do is to expand the vectors $f(v_1), \dots, f(v_n)$ on the basis B_W. Let us write the first two expansions:

$$f(v_1) = \sum_{i=1}^m a_i w_i,$$

$$f(v_2) = \sum_{i=1}^m b_i w_i,$$

we immediately recognize that using the letters $a_i, b_i, \dots$ is not a smart choice: in fact, if n is larger than the number of letters of the alphabet that we want to use, at some point we will have to introduce other symbols. It is a much better strategy to fix just one letter with the sum suffix i, for example a_i, and replace the following letters by adding another suffix to a represented by a natural number. With such a choice, there is no possibility to exhaust the natural numbers, and so *one letter with two natural indices* is a much wiser choice.

Let us see how the previous expansions of $f(v_1)$ and $f(v_2)$ will become if introduce scalars with a double index:

$$f(v_1) = \sum_{i=1}^m a_{i1} w_i,$$

$$f(v_2) = \sum_{i=1}^m a_{i2} w_i,$$

and so on. The generic j-th vector $f(v_j)$ will have the following expansion on the vectors of the basis B_W:

$$f(v_j) = \sum_{i=1}^m a_{ij} w_i = a_{1j} w_1 + \dots + a_{mj} w_m, \tag{2.9}$$

- the suffix $i = 1, \dots, m = \dim(W)$ represents the index that runs over the vectors of the basis B_W
- the suffix $j = 1, \dots, n = \dim(V)$ represents the index that runs over the vectors of the basis B_V.

These indices can be arranged in an ordered tabular array, called **matrix**, which can be explicitly written as follows:

$$A := \begin{pmatrix} a_{11} & \dots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{m1} & \dots & a_{mn} \end{pmatrix}.$$

As always, having a more compact notation comes in handy and one usually writes:

$$A = (a_{ij})^{i=1,\dots,m}_{j=1,\dots,n}.$$

Three features must be highlighted:

1. A can be represented by rows, i.e.

$$A = \begin{pmatrix} \longleftarrow R_1 \longrightarrow \\ \vdots \\ \longleftarrow R_m \longrightarrow \end{pmatrix}$$

   or by columns, i.e.

$$A = \begin{pmatrix} \uparrow & & \uparrow \\ C_1 & \cdots & C_n \\ \downarrow & & \downarrow \end{pmatrix}.$$

2. A has m **rows**, as the *dimension of the codomain* of f, which are vectors of n components belonging to $\mathbb{F}^n$, labeled by the **row index** $i = 1, \dots, m$:

$$\begin{aligned} R_1 &= (a_{11}, \dots, a_{1n}) \\ &\vdots \\ R_m &= (a_{m1}, \dots, a_{mn}). \end{aligned}$$

   The **generic i-th row** is

$$R_i = (a_{i1}, \dots, a_{in}) \in \mathbb{F}^n, \qquad i = 1, \dots, m.$$

3. Analogously, A has n **columns**, as the *dimension of the domain* of f, which are vectors of m components belonging to $\mathbb{F}^m$, labeled by the **column index** $j = 1, \dots, n$:

$$C_1 = \begin{pmatrix} a_{11} \\ \vdots \\ a_{m1} \end{pmatrix}, \cdots, C_n = \begin{pmatrix} a_{1n} \\ \vdots \\ a_{mn} \end{pmatrix}.$$

   The **generic j-th column** is

$$C_j = \begin{pmatrix} a_{1j} \\ \vdots \\ a_{mj} \end{pmatrix} \in \mathbb{F}^m, \qquad j = 1, \dots, n,$$

   C_j has a very important meaning: if we compare the elements of C_j with eq. (2.9), we can see that C_j **contains the components of the expansion of the vector** $f(v_j)$ **on the basis** B_W.

Practical method to associate a matrix to a linear map $f : V \to W$ w.r.t. two bases B_V and B_W

- Fix a basis $B_V = (v_1, \dots, v_n)$ of V and a basis $B_W = (w_1, \dots, w_m)$ of W
- Apply f to all the vectors of B_V, obtaining n vectors of W
- Expand $f(v_1), \dots, f(v_n)$ as linear combinations of vectors of the basis B_W
- Place the coefficients of the j-th linear combination in the j-th column of the matrix.

Theorem 2.4.1 *Given a linear map $f : V \to W$, once bases B_V and B_W of the vector spaces V and W, respectively, are arbitrarily chosen, the association between f and its matrix A is unique.*

Proof. The uniqueness follows from the fact that both the coefficients that compose A and their ordering are uniquely determined by the choice of the bases B_V and B_W. □

Because of this theorem, the matrix A should be more rigorously written as $A_{B_V}^{B_W}(f)$, because A depends on f, B_V and B_W. However, when it is not strictly needed to avoid confusion, we will simply write the symbol A.

Remark on the importance of matrices in linear algebra

In general, in mathematics, when an object appears naturally in a theory, that object is the source of many useful information. The matrix A associated to a linear map f through the choice of bases is no exception to this non-written rule: in fact, we can more easily study the properties of f through its associated matrix: for instance, we can establish if f is one-to-one, onto or an isomorphism by studying A. More generally, matrix theory is fundamental to solve efficiently systems of linear equations or to characterize algebraically geometric transformations as, e.g., rotations. These are among the most important reasons why linear algebra of finitely generated vector spaces is so tightly related to matrices.

Let us immediately see examples of how we can associate a linear map to a matrix and how the choice of different bases affects the matrix.

Example 2.4.1 Let $f : \mathbb{R}^3 \to \mathbb{R}^2$ be the linear map defined as follows

$$f((x, y, z)) = (x + y, x - z).$$

We know that the matrix A associated to f with respect to any choice of the bases of $\mathbb{R}^3$ and $\mathbb{R}^2$ will have 2 rows given by vectors with 3 components and 3 columns given by vectors of 2 components. The entries of this matrix, instead, will depend on the choice of the bases.

For this first example, let us fix for simplicity the canonical basis $\mathcal{C}_3$ of $\mathbb{R}^3$ and $\mathcal{C}_2$ of $\mathbb{R}^2$. Following the rules of how to associate a matrix to a linear map, the first thing to do is to transform the 3 vectors of the canonical basis of $\mathbb{R}^3$:

$$\begin{cases} f((1,0,0)) = (1+0, 1-0) = (1,1) \\ f((0,1,0)) = (0+1, 0-0) = (1,0) \\ f((0,0,1)) = (0+0, 0-1) = (0,-1). \end{cases}$$

Now we should express these vectors as a linear combination of the basis vectors of $\mathbb{R}^2$ and place the components on the columns of A. However, since we have selected the canonical basis, the components that we get are exactly those appearing in the vectors. To convince ourselves of this fact, let us consider, for instance, the third vector $(0, -1)$:

$$(0, -1) = a_{13}(1, 0) + a_{23}(0, 1) = (a_{13}, a_{23}),$$

so $a_{13} = 0$ and $a_{23} = -1$.

Hence, in the particular case in which W is $\mathbb{F}^n$ and the basis B_W is the canonical basis, we can simply place the vectors of B_V transformed by f on the columns of A (this is not true for other vector spaces and other bases!). So,

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

Example 2.4.2 Let $f : V \to W$, $V = \mathbb{R}^3$ and $W = \mathbb{R}^3$ be the linear map of Example 2.3.1 of section 2.3, i.e.

$$f((x, y, z)) = (x - z, x + 2z, 2x - y).$$

We saw that, if we fix B_V to be the canonical basis of $\mathbb{R}^3$, denoted with $\mathcal{C}_3$, then the images of the basis vectors of $\mathcal{C}_3$ via f are:

$$\begin{cases} f((1,0,0)) = (1,1,2) = w_1 \\ f((0,1,0)) = (0,0,-1) = w_2 \\ f((0,0,1)) = (-1,2,0) = w_2 \end{cases}.$$

If we fix the basis B_W to be again the canonical basis $\mathcal{C}_3$ of $\mathbb{R}^3$, then, as we know, the components of w_1, w_2, w_3 with respect to $\mathcal{C}_3$ will not change, hence the matrix associated to f with respect to the canonical basis of $\mathbb{R}^3$, chosen both for the domain and the codomain of f, will simply be the matrix whose *columns* are given by the components of w_1, w_2, w_3, in that order, i.e.

$$A_{\mathcal{C}_3}^{\mathcal{C}_3}(f) = \begin{pmatrix} 1 & 0 & -1 \\ 1 & 0 & 2 \\ 2 & -1 & 0 \end{pmatrix}.$$

Example 2.4.3 Consider now the basis $B_V = ((1,1,1),(3,0-1),(-1,1,-1))$ of $\mathbb{R}^3$ examined in Example 2.3.2 of section 2.3 and the linear map $g : \mathbb{R}^3 \to \mathbb{R}^3$ defined by imposing that the vectors of B_V are mapped to the same vectors as in the previous example:

$$\begin{cases} g((1,1,1)) = (1,1,2) = w_1 \\ g((3,0,-1)) = (0,0,-1) = w_2 \\ g((-1,1,-1)) = (-1,2,0) = w_3 \end{cases}.$$

In Example 2.3.2 we saw that the extension of g on the whole $\mathbb{R}^3$ was

$$g((x,y,z)) = \left(\frac{x+3z}{4}, \frac{3}{2}y - \frac{x+3z}{8}, y+z\right). \tag{2.10}$$

If we fix the basis B_W to be the canonical basis $\mathcal{C}_3$ of $\mathbb{R}^3$, then, as before, the components of w_1, w_2, w_3 with respect to $\mathcal{C}_3$ will not change, and so the matrix associated to g with respect to the basis B_V of V and $\mathcal{C}_3$ of W is

$$A^{\mathcal{C}_3}_{B_V}(g) = \begin{pmatrix} 1 & 0 & -1 \\ 1 & 0 & 2 \\ 2 & -1 & 0 \end{pmatrix}.$$

It can be seen that $A^{\mathcal{C}_3}_{\mathcal{C}_3}(f) = A^{\mathcal{C}_3}_{B_V}(g)$ in spite of the fact that f and g are two different linear maps, this is of course possible because of the fact that the matrices are written with respect to different choices of the bases.

To verify this claim, let us write the matrix associated to g with respect to the bases $B_V = B_W = \mathcal{C}_3$, as we did for the matrix associated to f. Since $f \neq g$ and, this time, the choice of the basis is the same, we must find a different matrix.

Using the expression of g given by eq. (2.10) we find that the images of the vectors of the canonical basis $\mathcal{C}_3$ are

$$\begin{cases} g((1,0,0)) = (\frac{1}{4}, -\frac{1}{8}, 0) = w_1' \\ g((0,0,1)) = (\frac{3}{4}, \frac{3}{2}, 1) = w_2' \\ g((0,0,1)) = (\frac{3}{4}, -\frac{3}{8}, 1) = w_3' \end{cases},$$

so

$$A^{\mathcal{C}_3}_{\mathcal{C}_3}(g) = \begin{pmatrix} \frac{1}{4} & \frac{3}{4} & \frac{3}{4} \\ -\frac{1}{8} & \frac{3}{2} & -\frac{3}{8} \\ 0 & 1 & 1 \end{pmatrix}.$$

Coherently with what expected, we see that $A^{\mathcal{C}_3}_{\mathcal{C}_3}(f) \neq A^{\mathcal{C}_3}_{\mathcal{C}_3}(g)$ and that $A^{\mathcal{C}_3}_{\mathcal{C}_3}(g) \neq A^{\mathcal{C}_3}_{B_V}(g)$.

Example 2.4.4 . Let us now compute the matrix associated to g when we fix the bases $B_V = B_W = B = ((1,1,1),(3,0-1),(-1,1,-1))$. In this case we have to expand the vectors

$$\begin{cases} g((1,1,1)) = (1,1,2) = w_1 \\ g((3,0,-1)) = (0,0,-1) = w_2 \\ g((-1,1,-1)) = (-1,2,0) = w_3 \end{cases}.$$

on the basis B in order to find out the coefficients that will place in the matrix columns.

$(1,1,2) = a_{11}(1,1,1) + a_{21}(3,0,-1) + a_{31}(-1,1,-1) = (a_{11} + 3a_{21} - 3a_{31}, a_{11} + a_{31}, a_{11} - a_{21} - a_{31})$, which corresponds to the system of linear equations

$$\begin{cases} a_{11}+3a_{21}-3a_{31}=1 \\ a_{11}+a_{31}=1 \implies a_{11}=1-a_{31} \\ a_{11}-a_{21}-a_{31}=2 \end{cases} \iff \begin{cases} a_{11}=1-a_{31} \\ a_{31}=\frac{3}{4}a_{21} \\ a_{21}=-\frac{2}{5} \end{cases} \iff \begin{cases} a_{11}=\frac{13}{10} \\ a_{21}=-\frac{2}{5} \\ a_{31}=-\frac{3}{10} \end{cases},$$

so, the first column of $A^B_B(g)$ will be

$$C_1=\begin{pmatrix} \frac{13}{10} \\ -\frac{2}{5} \\ -\frac{3}{10} \end{pmatrix}.$$

To compute the other two columns we have to solve the remaining two vector equations

$$(0,0,-1)=a_{12}(1,1,1)+a_{22}(3,0,-1)+a_{32}(-1,1,-1)=(a_{12}+3a_{22}-3a_{32},a_{12}+a_{32},a_{12}-a_{22}-a_{32}),$$

$$(-1,2,0)=a_{13}(1,1,1)+a_{23}(3,0,-1)+a_{33}(-1,1,-1)=(a_{13}+3a_{23}-3a_{33},a_{13}+a_{33},a_{13}-a_{23}-a_{33}),$$

transforming them into systems of linear equations and solving them with respect to the unknown coefficients. This task is left as a (very useful!) exercise and you can check that the result is the following matrix:

$$A^B_B(g)=\begin{pmatrix} \frac{13}{10} & -\frac{3}{10} & \frac{11}{10} \\ -\frac{2}{5} & \frac{2}{5} & \frac{1}{5} \\ -\frac{3}{10} & \frac{3}{10} & \frac{9}{10} \end{pmatrix}.$$

Notice two things: the first is that, as it should be, $A^B_B(g) \neq A^{\mathcal{C}_3}_B(g) \neq A^{\mathcal{C}_3}_{\mathcal{C}_3}(g)$. The second is that the canonical basis simplifies dramatically the computations, however, the matrix associated to the canonical basis may not be the easiest one to deal with.

So, there is a sort of *trade-off*: associating a matrix to a linear map between $\mathbb{F}^n$ and $\mathbb{F}^m$ with respect to their canonical bases is *computationally* very easy, however, there may be other bases of $\mathbb{F}^n$ and $\mathbb{F}^m$ with respect to which the matrix associated to the same linear map has an easier expression, e.g., it has *many zeros.*

Example 2.4.5 ***Every matrix can be identified with a matrix associated to a linear map.*** Here we reverse the direction of the previous examples and we show how, given any matrix, two vector spaces and the choice of a basis for each of them, we can recover the linear map uniquely associated to the matrix.

Consider again $V=W=\mathbb{R}^3$, the canonical bases on both spaces and the matrix

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

what if the linear map $f:\mathbb{R}^3\to\mathbb{R}^3$ such that $A=A^{\mathcal{C}_3}_{\mathcal{C}_3}(f)$?

To answer this question we have to recall that, *having chosen the canonical basis of* $\mathbb{R}^3$ *interpreted as the range vector space of* f, the entries of each columns of A are the images of the canonical basis vectors by f, i.e.

$$\begin{cases} f((1,0,0)) = (1,0,0) \\ f((0,1,0)) = (1,1,0) \\ f((0,0,1)) = (2,0,3) \end{cases} .$$

Thus, we explicitly have the information about how f transforms the vectors of a basis (in this case the canonical one), which, as we know, it is enough to find the expression of f on the generic vector of the whole space.

Again, the coefficients of the generic vector $v = (x, y, z) \in \mathbb{R}^3$ on the canonical basis are (x, y, z), so

$$(x,y,z) = x(1,0,0)+y(0,1,0)+z(0,0,1) \implies f((x,y,z)) = xf(1,0,0)+yf(0,1,0)+zf(0,0,1),$$

i.e. $f((x, y, z)) = x(1, 0, 0) + y(1, 1, 0) + z(2, 0, 3) = (x + y + 2z, y, 3z)$.

It is interesting to put A and f side-by-side:

$$f((x,y,z)) = (x+y+2z, y, 3z) \qquad \text{vs.} \qquad A = \begin{pmatrix} 1 & 1 & 2 \\ 0 & 1 & 0 \\ 0 & 0 & 3 \end{pmatrix}.$$

Think about how the coefficients appearing in the expression of f and in the matrix A are related *when the canonical basis is chosen in the domain and codomain of* f...

If the bases are not the canonical ones, the computations are of course more complicated. Let us choose the basis B of the Example 2.4.4 for both the domain and the codomain of f. Then, by definition of A, we have that the elements of each column are the scalars that appear in the decomposition of the vectors of B transformed by f as a linear combination of the same vectors of B (because B is chosen as basis for both V and W!). Hence:

$$\begin{cases} f(1,1,1) = 1(1,1,1) + 0(3,0,-1) + 0(-1,1,-1) = (1,1,1) \\ f(3,0,-1) = 1(1,1,1) + 1(3,0,-1) + 0(-1,1,-1) = (4,1,0) \\ f(-1,1,-1) = 2(1,1,1) + 0(3,0,-1) + 3(-1,1,-1) = (-1,5-1) \end{cases} .$$

Now we know the action of f on the vectors of the basis B, we extend f by linearity on the whole $\mathbb{R}^3$ as usual. Using (2.8) we have:

$$(x,y,z) = \left(\frac{y}{2} + \frac{x+3z}{8}\right)(1,1,1) + \frac{x-z}{4}(3,0,-1) + \left(\frac{y}{2} - \frac{x+3z}{8}\right)(-1,1,-1)$$

so

$$\begin{aligned} f(x,y,z) &= \left(\frac{y}{2} + \frac{x+3z}{8}\right) f(1,1,1) + \frac{x-z}{4} f(3,0,-1) + \left(\frac{y}{2} - \frac{x+3z}{8}\right) f(-1,1,-1) \\ &= \left(\frac{y}{2} + \frac{x+3z}{8}\right)(1,1,1) + \frac{x-z}{4}(4,1,0) + \left(\frac{y}{2} - \frac{x+3z}{8}\right)(-1,5,-1) \\ &= \left(\frac{5x-z}{4}, 3y - \frac{x+7z}{4}, \frac{x+3z}{4}\right). \end{aligned}$$

This confirms that the same matrix can correspond to very different linear maps depending on the basis with respect to which it is associated.

2.5 Operations on linear maps and their matrix representations

As we have seen, given a linear map $f : V \to W$ an fixed arbitrarily a basis of V and a basis of W, the association between f and its matrix A is natural: after all, only linear combinations of suitable vectors appear in this association, and there is no more natural operation in linear algebra than a linear combination!

Due to this remark, we expect that operations on linear maps can be easily translated into analogous operations on the associated matrices. We are going to see that this is exactly what happens, but to do that we need to define the vector space where linear maps live.

For this, we need to recall one of the first examples of vector spaces that we have introduced in section 1.1.1, i.e. the *infinite-dimensional* functional space $\mathcal{F}(X, E)$, that is the set of all functions from a set X to a vector space E endowed with the point-wise linear structure defined by eqs. (1.5), (1.6).

A linear map f is a particular example of function, characterized by two facts:

- both its domain and range are vector spaces
- f has the property of passing through linear combinations in the sense that we have defined.

So, linear maps constitute a subset of the vector space $\mathcal{F}(V, W)$. Thanks to the linear behavior, it is very easy to check that the set of linear maps is not only a subset of $\mathcal{F}(V, W)$, but it is actually *a vector subspace of* $\mathcal{F}(V, W)$. To underline the linearity of the maps contained in this vector subspace the letter $\mathcal{F}$ is changed to $\mathcal{L}$, as formalized in the next definition.

Def. 2.5.1 (The vector space of linear maps) *Given two vector spaces V and W over the same field $\mathbb{F}$, we indicate with $\mathcal{L}(V, W)$ the vector space given by all the linear maps $f : V \to W$ endowed with the point-wise linear structure, i.e., if $f, g \in \mathcal{L}(V, W)$ and $\lambda \in \mathbb{F}$,*

$$f + g : V \to W, \ (f + g)(x) := f(x) + g(x), \quad \text{for all } x \in V$$

$$\lambda f : V \to W, \ (\lambda f)(x) := \lambda f(x), \quad \text{for all } x \in V.$$

Remarkably, the request of linearity for the functions living in $\mathcal{L}(V, W)$ reduce the dimension of this vector space from infinity to a very precise finite number specified in the following result.

Theorem 2.5.1 (Dimension of $\mathcal{L}(V, W)$) *It holds that*

$$\dim(\mathcal{L}(V, W)) = \dim(V) \cdot \dim(W).$$

To resume, given two vector spaces V and W over the same field, we can always construct another vector space, $\mathcal{L}(V, W)$, whose dimension is the product of the dimensions of the vector spaces V and W.

Let us now see how the operations of the linear structure of $\mathcal{L}(V, W)$ can be translated on the matrices associated to the linear maps that belong to $\mathcal{L}(V, W)$. As said at the beginning, we expect a straightforward relation, and we will find exactly that.

We start with the sum: consider

- $f, g \in \mathcal{L}(V, W)$
- $\dim(V) = n$, $\dim(W) = m$
- $B_V = (v_j)_{j=1}^n$ is a basis of V and $B_W = (w_i)_{i=1}^m$ is a basis of W
- $A = (a_{ij})$ and $B = (b_{ij})$ are the matrices associated to the linear maps f and g, respectively, with respect to the bases B_V and B_W.

If we apply the sum of f and g to the j-th vector of the basis B_V we have, by definition of A and B,

$$(f+g)(v_j) = f(v_j) + g(v_j) = \sum_{i=1}^m a_{ij} w_i + \sum_{i=1}^m b_{ij} w_i = \sum_{i=1}^m (a_{ij} + b_{ij}) w_i,$$

this computation implies that if we *define* the sum of the two matrices A and B as follows:

$$A + B := (a_{ij} + b_{ij})_{j=1,\dots,n}^{i=1,\dots,m},$$

then $A + B$ becomes the matrix associated to the linear map $f + g$ with respect to the bases B_V and B_W! The matrix $A + B$ is obtained simply by adding together the entries of A and B which have the same position, i.e. the same row and column. For instance:

$$A = \begin{pmatrix} 5 & 1 & 0 \\ -1 & 0 & 1 \\ 0 & -3 & 1 \end{pmatrix}, \; B = \begin{pmatrix} -4 & 0 & 2 \\ -1 & 1 & 1 \\ 2 & 2 & 0 \end{pmatrix} \implies A + B = \begin{pmatrix} 1 & 1 & 2 \\ -2 & 1 & 2 \\ 2 & -1 & 1 \end{pmatrix}.$$

Clearly, the zero element for the matrix sum is the **null matrix**, i.e. the matrix $m \times n$ with all 0. So, the **opposite matrix** of $A = (a_{ij})_{j=1,\dots,n}^{i=1,\dots,m}$ is the matrix $-A = (-a_{ij})_{j=1,\dots,n}^{i=1,\dots,m}$.

Repeating the same argument, it is easy to check (and it is a good exercise to actually do it!) that if we define the product of a scalar $\lambda \in \mathbb{F}$ by the matrix A as follows:

$$\lambda A := (\lambda a_{ij})_{j=1,\dots,n}^{i=1,\dots,m},$$

then λA becomes the matrix associated to the linear map λf with respect to the bases B_V and B_W. The matrix λA is obtained simply by multiplying by λ all the entries of A. For example:

$$A = \begin{pmatrix} 5 & 1 & 0 \\ -1 & 0 & 1 \\ 0 & -3 & 1 \end{pmatrix} \implies -3A = \begin{pmatrix} -15 & -3 & 0 \\ 3 & 0 & -3 \\ 0 & 9 & -3 \end{pmatrix}.$$

Now that we have the definition of the two linear operations, sum and product by a scalar, on the set of matrices, we can ask ourselves if this set is a vector space with respect to these operations. The answer is affirmative and it is convenient to introduce a special symbol for this vector space.

Def. 2.5.2 *Given $n, m \in \mathbb{N}$, $n, m \geqslant 1$,*

$$M_{m,n}(\mathbb{F}) := \{A : A \text{ is a } m \times n \text{ matrix with entries in } \mathbb{F}\},$$

i.e., A has m rows, n columns and the scalars that appear in it belong to the field $\mathbb{F}$.

- *If $\mathbb{F} = \mathbb{R}$, the matrix is said to be real, if $\mathbb{F} = \mathbb{C}$, the matrix is said to be complex.*
- *If $n = m = 1$, then the matrix is just a scalar in $\mathbb{F}$.*

Theorem 2.5.2 *$M_{m,n}(\mathbb{F})$ is a vector space over $\mathbb{F}$ of dimension $n \cdot m$. Thus, given two vector spaces V, W over $\mathbb{F}$ of dimension n and m, respectively, $M_{m,n}(\mathbb{F})$ is isomorphic to $\mathcal{L}(V, W)$.*

In particular, the vector space of endomorphisms of V, i.e. $\mathcal{L}(V) := \mathcal{L}(V, V)$ is isomorphic to $M_n(\mathbb{F}) := M_{n,n}(\mathbb{F})$, as they both have dimension n^2.

$M_{m,n}(\mathbb{F})$ can be endowed with a special basis which is **the analogous of the canonical basis for matrices**. This basis is given by the matrices E_{ij}, which have all null entries, except for the one with position (i, j), i.e. belonging to the row i and the column j, whose value is 1. For instance, in the vector space $M_{5,4}(\mathbb{R})$, the matrix $E_{2,3}$ is

$$E_{2,3} = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix},$$

in fact, it is a matrix with 5 rows and 4 columns with all null entries, except for the entry of position $(2, 3)$ located at the intersection between the second row and the third column, whose value is 1.

By direct computation, we have that

$$A = \sum_{i=1}^{m} \sum_{j=1}^{n} a_{ij} E_{ij}.$$

Let us show explicitly this equality for a matrix of $M_{2,2}(\mathbb{R})$:

$$A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix},$$

in this case the basis is given by:

$$E_{11} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \; E_{12} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \; E_{21} = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \; E_{22} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix},$$

so

$$\begin{aligned} \sum_{i=1}^{2} \sum_{j=1}^{2} a_{ij} E_{ij} &= \sum_{j=1}^{2} a_{1j} E_{1j} + \sum_{j=1}^{2} a_{2j} E_{2j} = a_{11}E_{11} + a_{12}E_{12} + a_{21}E_{21} + a_{22}E_{22} \\ &= \begin{pmatrix} a_{11} & 0 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & a_{12} \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 0 \\ a_{21} & 0 \end{pmatrix} + \begin{pmatrix} 0 & 0 \\ 0 & a_{22} \end{pmatrix} \\ &= \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \\ &= A. \end{aligned}$$

2.6 The matrix product

In this subsection we investigate the possibility to associate a matrix operation to the composition between linear maps. This is indeed possible and it will gives rise to the definition of matrix product.

Besides this theoretical motivation, there is also a practical motivation to study matrix product: this is the most important operation that is involved in the functioning of neural networks, which are the building blocks of artificial intelligent systems.

Let us consider:

- three vector spaces U, V and W over the same field $\mathbb{F}$
- $\dim(U) = r$, $\dim(V) = n$ and $\dim(W) = m$
- $\mathscr{B}_U = (u_1, \ldots, u_r) = (u_j)_{j=1}^r$: basis of U
- $\mathscr{B}_V = (v_1, \ldots, v_n) = (v_k)_{k=1}^n$: basis of V
- $\mathscr{B}_W = (w_1, \ldots, w_m) = (w_i)_{i=1}^m$: basis of W
- $f : V \to W$, $g : U \to V$, $f \circ g : U \to W$: linear maps
- we visualize the previous objects as follows:

$$
\begin{tikzcd}
\text{Bases:} & \mathscr{B}_U \arrow[d, dotted, no head] & \mathscr{B}_V \arrow[d, dotted, no head] & \mathscr{B}_W \arrow[d, dotted, no head] \\
\text{Vector spaces and linear maps:} & U \arrow[r, "g"] \arrow[rr, bend right, "f\circ g"'] & V \arrow[r, "f"] & W
\end{tikzcd}
$$

- A: matrix associated to f with respect to $\mathscr{B}_V$ and $\mathscr{B}_W$, $A = (a_{ik})_{k=1,\ldots,n}^{i=1,\ldots,m} \in M_{m,n}(\mathbb{F})$
- B: matrix associated to g with respect to $\mathscr{B}_U$ and $\mathscr{B}_V$, $B = (b_{kj})_{j=1,\ldots,r}^{k=1,\ldots,n} \in M_{n,r}(\mathbb{F})$
- C: matrix associated to $f \circ g$ with respect to $\mathscr{B}_U$ and $\mathscr{B}_W$, $C = (c_{ij})_{j=1,\ldots,r}^{i=1,\ldots,m} \in M_{m,r}(\mathbb{F})$.

By definition, the matrix elements of A appear in the linear combination of the images via f of the basis vectors belonging to $\mathscr{B}_V$ with respect to B_W, i.e.

$$f(v_k) = \sum_{i=1}^{m} a_{ik} w_i, \qquad k = 1, \ldots, n,$$

instead, the matrix elements of B appear in the linear combination of the images via g of the basis vectors belonging to $\mathscr{B}_U$ with respect to B_V, i.e.

$$g(u_j) = \sum_{k=1}^{n} b_{kj} v_k, \qquad j = 1, \ldots, r.$$

Finally, the matrix elements of C appear in the linear combination of the images via $f \circ g$ of the basis vectors belonging to B_U with respect to B_W, i.e.

$$(f \circ g)(u_j) = \sum_{i=1}^{m} c_{ij} w_i, \qquad j = 1, \ldots, r.$$

However,

$$(f \circ g)(u_j) = f(g(u_j)) = f\left(\sum_{k=1}^{n} b_{kj} v_k\right) \underset{f \text{ linear}}{=} \sum_{k=1}^{n} b_{kj} f(v_k)$$

$$= \sum_{k=1}^{n} b_{kj} \sum_{i=1}^{m} a_{ik} w_i \quad \text{(we can rearrange the finite sums as follows ...)}$$

$$= \sum_{i=1}^{m} \left(\sum_{k=1}^{n} a_{ik} b_{kj}\right) w_i$$

$$= \sum_{i=1}^{m} c_{ij} w_i, \qquad j = 1, \ldots, r$$

Notice that the coefficients c_{ij} of the matrix C associated to the linear map $f \circ g$ are expressed as a sum of products of coefficients belonging to the matrices A and B, associated to the linear maps f and g. It is therefore natural to define the matrix C as the product of A and B, because, in this way, the matrix product will be automatically associated to the composition of linear maps.

Def. 2.6.1 (Matrix product) *Given the matrices*

- $A = (a_{ik})_{k=1,\ldots,n}^{i=1,\ldots,m} \in M_{m,n}(\mathbb{F})$
- $B = (b_{kj})_{j=1,\ldots,r}^{k=1,\ldots,n} \in M_{n,r}(\mathbb{F})$,

their product is the matrix $C = (c_{ij})_{j=1,\ldots,r}^{i=1,\ldots,m} \in M_{m,r}(\mathbb{F})$, *where the coefficients are defined by the formula*

$$c_{ij} = \sum_{k=1}^{n} a_{ik} b_{kj}, \qquad i = 1, \ldots, m, \ j = 1, \ldots, r. \tag{2.11}$$

Theorem 2.6.1 *If* $A \in M_{m,n}(\mathbb{F})$ *and* $B \in M_{n,r}(\mathbb{F})$ *are the matrices associated to the linear maps* $f : V \to W$ *and* $g : U \to V$ *with respect to some fixed bases, then their product* $C = AB$ *is the matrix associated to the linear map* $f \circ g : U \to W$ *with respect to the same bases chosen for* U *and* W*.*

The matrix product is often called **rows times columns product**, let us see why. To compute the matrix element c_{ij}, located at the intersection between the row i and the column j of the matrix C, we must select:

- the row i from the matrix A, i.e. $(a_{i1}, \ldots, a_{in})$
- the column j from the matrix B, i.e. $\begin{pmatrix} b_{1j} \\ \vdots \\ b_{nj} \end{pmatrix}$

and the 'multiply' that row and that column as indicated in formula (2.11), i.e. adding the product of the elements of the row and the column with the same explicit index, from 1 to n:

$$c_{ij} = (a_{i1}, \ldots, a_{in}) \begin{pmatrix} b_{1j} \\ \vdots \\ b_{nj} \end{pmatrix} = a_{i1} b_{1j} + \cdots + a_{in} b_{nj}.$$

Notice that **the matrix product makes sense if and only if the length of the rows of A coincides with the length of the columns of B.** If we think in terms of composition of linear maps this is obvious: it is not possible to compose two functions unless the codomain of the first coincides with the domain of the second!

The resulting product matrix $C = AB$ will then have a number of rows equal to that of the matrix A and a number of columns equal to that of the matrix B.

In the mathematical jargon, when we have a behavior like the following

$$(m \times n)(n \times r) = m \times r,$$

we say that the intermediate index n is *saturated*.

Example 2.6.1 Multiply the matrices

$$A = \begin{pmatrix} 1 & 0 & 1 & -2 \\ 0 & -2 & 1 & 0 \\ -1 & 0 & -\frac{1}{2} & 3 \end{pmatrix}, \quad B = \begin{pmatrix} 3 & 1 \\ 0 & 0 \\ 1 & -1 \\ \frac{1}{2} & -3 \end{pmatrix}.$$

First of all we notice that the product can be computed because A is 3×4 and B is 4×2, so $C = AB$ will be 3×2.

We will detail the computation only for two matrix elements and leave the others as useful exercise:

$$c_{11} = \begin{pmatrix} 1 & 0 & 1 & -2 \end{pmatrix} \begin{pmatrix} 3 \\ 0 \\ 1 \\ \frac{1}{2} \end{pmatrix} = 1 \cdot 3 + 0 \cdot 0 + 1 \cdot 1 - 2 \cdot \frac{1}{2} = 3,$$

$$c_{32} = \begin{pmatrix} -1 & 0 & -\frac{1}{2} & 3 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ -1 \\ -3 \end{pmatrix} = -1 \cdot 1 + 0 \cdot 0 - \frac{1}{2} \cdot (-1) + 3 \cdot (-3) = -\frac{19}{2},$$

calculating all the other entries, we find

$$C = \begin{pmatrix} 3 & 6 \\ 1 & -1 \\ -2 & -\frac{19}{2} \end{pmatrix}.$$

Since matrix product is associated to composition of linear functions, which is not a **commutative** operation, i.e. it is not always true that $f \circ g = g \circ f$, whenever this composition makes sense, it would be not coherent if the matrix product were commutative, i.e. if $AB = BA$ for all matrices A and B for which the product makes sense.

Consider, for example, the linear maps $f, g : \mathbb{R}^2 \to \mathbb{R}^2$, $f(v, w) = (2v + w, v - 3)$ and $g(x, y) = (x - 1, y + 1)$, we have that their compositions give

$$(f \circ g)(x, y) = f(g(x, y)) = f(v = x-1, w = y+1) = (2(x-1)+(y+1), (x-1)-3) = (2x+y-1, x-4)$$

and

$$(g \circ f)(v, w) = g(f(v, w)) = g(x = 2v + w, y = v - 3) = ((2v + w) - 1, (v - 3) + 1) = (2v + w - 1, v - 2),$$

we can see that the second component of $f \circ g$ and $g \circ f$ are not the same, so f and g do not commute. Accordingly, if we compute the matrices A and B associated to f and g, respectively, with respect to the canonical basis of $\mathbb{R}^2$, to minimize the calculations, we find:

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

and

$$AB = \begin{pmatrix} 1 & 0 \\ -3 & -7 \end{pmatrix}, \; BA = \begin{pmatrix} -1 & 3 \\ 4 & -5 \end{pmatrix},$$

so, coherently with the fact that $f \circ g \neq g \circ f$, we have confirmed that $AB \neq BA$.

2.6.1 Particular cases of matrix product

We discuss here particular cases of matrix product which can help us highlighting some important features of linear algebra and introducing new interesting objects.

1. Matrix product AB of the type $(m \times n)(n \times 1)$, i.e. $r = 1$. In this case the matrix B coincides with a **column vector** v with n rows belonging to $\mathbb{F}^n$, the resulting matrix $C = AB$ is of type $(m \times 1)$, hence it is again a column vector w, but this time with m rows and so it belongs to $\mathbb{F}^m$:

$$AB = \begin{pmatrix} a_{11} & \dots & a_{1n} \\ \vdots & & \vdots \\ a_{m1} & \dots & a_{mn} \end{pmatrix} \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix} = w = \begin{pmatrix} w_1 \\ \vdots \\ w_m \end{pmatrix}.$$

2. Matrix product AB of the type $(1 \times n)(n \times r)$, i.e. $m = 1$. In this case the matrix A coincides with a **row vector** v with n columns belonging to $\mathbb{F}^n$, the resulting matrix $C = AB$ is of type $(1 \times r)$, hence it is again a row vector w, but this time with r columns and so it belongs to $\mathbb{F}^r$:

$$AB = (v_1, \dots, v_n) \begin{pmatrix} b_{11} & \dots & b_{1r} \\ \vdots & & \vdots \\ b_{n1} & \dots & b_{nr} \end{pmatrix} = w = (w_1, \dots, w_r).$$

3. Matrix product AB of the type $(1 \times n)(n \times 1)$, i.e. $m = r = 1$. In this case, applying the rules of the matrix product, we obtain a scalar, in fact:

$$AB = (a_1, \dots, a_n) \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix} = a_1 b_1 + \dots a_n b_n \in \mathbb{F}.$$

   This particular scalar is called the **scalar product** of the two vectors and it will be studied in the course of **Euclidean spaces**. Notice that the matrix product allows us to make sense, via the scalar product, of the product of two vectors, an operation otherwise impossible to define. This shows another reason why it is interesting and useful to study matrices!

Important remark. The case (1.), i.e. the product of a matrix $A \in M_{m,n}(\mathbb{F})$ times a column vector $v \in \mathbb{F}^n$, deserves a particular attention. In fact, we have seen that this product gives rise to a vector $w \in \mathbb{F}^m$ and so it defines following the linear map

$$\begin{array}{rccl} f_A : & \mathbb{F}^n & \longrightarrow & \mathbb{F}^m \\ & v & \longmapsto & f_A(v) := Av = w. \end{array}$$

As a nice and straightforward exercise, it can be checked that the matrix associated to f_A w.r.t. the canonical bases of $\mathbb{F}^n$ and $\mathbb{F}^m$ respectively, is exactly A!

In the following, we will assume that, in these circumstances, we can write equivalently:

$$\boxed{f(v) = w = Av}.$$

2.6.2 Transposition of a matrix

Another important operation on matrices is the swap between rows and columns, which bears a particular name.

Def. 2.6.2 (Transpose of a matrix) *Given the matrix* $A = (a_{ik})^{i=1,\dots,m}_{k=1,\dots,n} \in M_{m,n}(\mathbb{F})$, *its transpose is the matrix* $A^t = (a_{ki})^{k=1,\dots,n}_{i=1,\dots,m} \in M_{n,m}(\mathbb{F})$ *in which the role of rows and columns of* A *has been exchanged.*

Explicitly:

$$\begin{pmatrix} a_{11} & \dots & a_{1n} \\ \vdots & & \vdots \\ a_{m1} & \dots & a_{mn} \end{pmatrix}^t = \begin{pmatrix} a_{11} & \dots & a_{m1} \\ \vdots & & \vdots \\ a_{1n} & \dots & a_{mn} \end{pmatrix}.$$

The properties of transposition are listed below.

Theorem 2.6.2 *Let* $A, B \in M_{m,n}(\mathbb{F})$ *and* $\lambda \in \mathbb{F}$, *then:*

1. *the transposition is an involution:* $(A^t)^t = A$
2. *the transposition is a linear operation:*
$$(A+B)^t = A^t + B^t, \quad (\lambda A)^t = \lambda A^t$$
3. *if* $A \in M_{m,n}(\mathbb{F})$ *and* $B \in M_{n,r}(\mathbb{F})$, *then*
$$(AB)^t = B^t A^t,$$
so, the transposed of a matrix product is the product of the transposed matrices in the reverse order, so it has dimension $(r \times n)(n \times m) = r \times m$.

Regarding the third property, notice that, dimensionally, the product of the transposed matrices would not have matched because the inner dimensions do not agree: $(n \times m)(r \times n)$.

2.7 The nullity and rank of a matrix

We recall that in section 2.2 we have defined the rank of a linear map $f : V \to W$, $\dim(V) = n$ and $\dim(W) = m$, as the dimension of its image $\mathrm{Im}(f)$, which is the vector subspace of W given by the images $f(v)$ of the all the vectors $v \in V$ via f.

If we fix bases B_V of V and B_W of W, then we can associate f to a matrix $A \in M_{m,n}(\mathbb{F})$ and we can transform any vector $v \in V$ into a column vector belonging to $\mathbb{F}^n$ whose entries are the components of $v \in V$ with respect to the basis B_V.

The vector $f(v) = w \in W$ can be decomposed on the basis B_W and its components form a column vector w that coincides with the matrix product Av:

$$f(v) = w \in W \iff Av = \begin{pmatrix} a_{11} & \dots & a_{1n} \\ \vdots & & \vdots \\ a_{m1} & \dots & a_{mn} \end{pmatrix} \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix} = w \in \mathbb{F}^m.$$

For this reason, we define the image of A as follows.

Def. 2.7.1 (Image and rank of a matrix) *The image of a matrix $A \in M_{m,n}(\mathbb{F})$ is*

$$\mathrm{Im}(A) = \{w \in \mathbb{F}^m : \exists v \in \mathbb{F}^n : Av = w\}.$$

The rank of A, written $\mathrm{rank}(A)$*, is the dimension of* $\mathrm{Im}(A)$*.*

We are now going to show that the image of A can be characterized in a more explicit way. The key to do that is contained in the following computation:

$$\begin{aligned} Av &= \begin{pmatrix} a_{11} & \dots & a_{1n} \\ \vdots & & \vdots \\ a_{m1} & \dots & a_{mn} \end{pmatrix} \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix} = \begin{pmatrix} a_{11}v_1 + \ldots + a_{1n}v_n \\ \vdots \\ a_{m1}v_1 + \ldots + a_{mn}v_n \end{pmatrix} = \begin{pmatrix} a_{11}v_1 \\ \vdots \\ a_{m1}v_1 \end{pmatrix} + \ldots + \begin{pmatrix} a_{1n}v_n \\ \vdots \\ a_{mn}v_n \end{pmatrix} \\ &= \begin{pmatrix} a_{11} \\ \vdots \\ a_{m1} \end{pmatrix} v_1 + \ldots + \begin{pmatrix} a_{1n} \\ \vdots \\ a_{mn} \end{pmatrix} v_n \\ &= C_1 v_1 + \cdots + C_n v_n, \end{aligned}$$

where, for all $j = 1, \ldots, n$, C_j represents the j-th column of A:

$$C_j = \begin{pmatrix} a_{1j} \\ \vdots \\ a_{mj} \end{pmatrix}, \quad C_j \in \mathbb{F}^m.$$

To resume, we have proven that

$$Av = C_1 v_1 + \ldots + C_n v_n,$$

i.e., the image of a vector v via A can be written as a linear combination of the columns of A with coefficients given by the components of the vector v itself. So, by letting v vary in V, we can reconstruct $\mathrm{Im}(A)$ through linear combinations of the columns of A. We formalize what we have found in the following theorem.

Theorem 2.7.1 $\mathrm{Im}(A) = \mathrm{span}(C_1, \ldots, C_n)$.

So, the rank of (A), i.e. the dimension of $\mathrm{Im}(A)$, is the number of linearly independent columns of A. The following theorem, that we report without proof, says that this number characterized the rank of the linear map associated to A.

Theorem 2.7.2 *The rank of a linear map $f : V \to W$ coincides with the number of linearly independent columns of the matrix A associated to f with respect to any choice of bases of V and W.*

Since for a matrix $A \in M_{m,n}(\mathbb{F})$ the number of columns is n, $\mathrm{rank}(A) \leqslant n$. However, we can give a more precise information about the rank of A thanks to the following theorem, which states a very surprising property of matrices.

Theorem 2.7.3 *Given a matrix $A \in M_{m,n}(\mathbb{F})$, the number of its linearly independent rows is equal to the number of its linearly independent columns, hence*

$$\mathrm{rank}(A) \leqslant \min\{m, n\}.$$

The proof of this theorem would take us too much time, so we omit it, but it is worthwhile highlighting how counter-intuitive this result is: if a matrix has 10^9 columns and 3 rows, then it has at best 3 linearly independent columns!

Since the transpose matrix A^t is A with row and columns exchanged, the next result follows immediately.

Corollary 2.7.1 *Given a matrix $A \in M_{m,n}(\mathbb{F})$,* $\mathrm{rank}(A) = \mathrm{rank}(A^t)$.

Inspired by how we have defined the rank of a matrix, we define its kernel and nullity analogously.

Def. 2.7.2 (Kernel and nullity of a matrix) *Given a matrix $A \in M_{m,n}(\mathbb{F})$, its kernel and nullity are*

$$\ker(A) := \{v \in \mathbb{F}^n : Av = \mathbf{0}_{\mathbb{F}^m}\}, \quad \mathrm{null}(A) := \dim(\ker(A)).$$

The following theorem guarantees that this definition is coherent with that of kernel of a linear map.

Theorem 2.7.4 *Given a matrix $A \in M_{m,n}(\mathbb{F})$, $\ker(A)$ and $\ker(f)$ are isomorphic, where f is any linear map associated to A, independently of the choice of the bases of $\mathbb{F}^n$ and $\mathbb{F}^m$. Hence, $\mathrm{null}(A) = \mathrm{null}(f)$.*

Thanks to this result, the nullity+rank theorem can be applied on matrices: given $A \in M_{m,n}(\mathbb{F})$,

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

So,

- if $n \leqslant m$ and $\mathrm{rank}(A) = n$, then $\mathrm{null}(A) = 0$ and A represents a one-to-one linear map
- if $n = m$ and $\mathrm{rank}(A) = n$, i.e. A is full rank, then $\mathrm{null}(A) = 0$ and $\mathrm{rank}(A) = n$, so A represents an isomorphism.

The case $n = m$ is that of a matrix A associated to an endomorphisms $f : V \to V$. A is called a **square matrix** because the table of its scalar entries forms a square.

Example 2.7.1 The matrix

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

belongs to $M_{4,3}(\mathbb{R})$ and so it represents a linear map $f : \mathbb{R}^3 \to \mathbb{R}^4$ with respect to any bases of $\mathbb{R}^3$ and $\mathbb{R}^4$ that we may choose.

The nullity+rank theorem applied to A gives

$$3 = \text{null}(A) + \text{rank}(A),$$

and we can already say that $\text{rank}(A)$ is at best 3 because A has 3 columns. Let's check if the columns are linearly independent or not. Given $\alpha, \beta, \gamma \in \mathbb{R}$, the generic linear combination of the column vectors is

$$\alpha(1,0,0,2) + \beta(2,1,0,0) + \gamma(3,4,1,0) = (\alpha + 2\beta + 3\gamma, \beta + 4\gamma, \gamma, 2\alpha).$$

The vector equation

$$(\alpha + 2\beta + 3\gamma, \beta + 4\gamma, \gamma, 2\alpha) = (0,0,0,0)$$

is equivalent to the system

$$\begin{cases} \alpha + 2\beta + 3\gamma = 0 \\ \beta + 4\gamma = 0 \\ \gamma = 0 \\ 2\alpha = 0 \end{cases} \quad \Longleftrightarrow \quad \alpha = \beta = \gamma = 0,$$

this shows the three column vectors are linearly independent and so $\text{rank}(A) = 3$. By the nullity+rank theorem we have that $\text{null}(A) = 0$, and so every linear map $f : \mathbb{R}^3 \to \mathbb{R}^4$ whose associated matrix is A will be one-to-one but not onto.

2.8 Square matrices associated to endomorphisms

Endomorphisms play a particularly important role in linear algebra, so it is worth underlying some of their features. Let $f, g : V \to V$, $\dim(V) = n$, be two endomorphisms and A, B their associated matrices, respectively, with respect to any bases of V.

- We denote with $M_n(\mathbb{F}) = M_{n,n}(\mathbb{F})$ the vector space of square matrices with n rows and columns and we say that n is the **order** or **dimension** of the square matrix.

- All the elements of $A \in M_n(\mathbb{F})$ of the type a_{jj}, $j = 1, \dots, n$, form the **diagonal** of A.

- The matrix products AB and BA are always defined for all $A, B \in M_n(\mathbb{F})$, in fact the inner dimensions always match, because $(n \times n)(n \times n)$, so $AB, BA \in M_n(\mathbb{F})$.

- The null element of $M_n(\mathbb{F})$ with respect to the operation of sum is the zero matrix $\mathbf{0}_n$, which has all null entries. It *represents the null linear map* $f : V \to V$, $v \mapsto \mathbf{0}_V$.

- The unit element of $M_n(\mathbb{F})$ with respect to the operation of matrix product is the so-called **identity matrix**:

$$I_n := \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \dots & 0 & 1 \end{pmatrix},$$

  so I_n has 0 everywhere and all 1 along its diagonal. It *represents the identity map* id_V, in fact, for all $v \in \mathbb{F}^n$

$$I_n v = \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \dots & 0 & 1 \end{pmatrix} \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix} = \begin{pmatrix} 1 \cdot v_1 + 0 \cdot v_2 + \dots + 0 \cdot v_n \\ \vdots \\ 0 \cdot v_1 + 0 \cdot v_2 + \dots + 1 \cdot v_n \end{pmatrix} = \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix} = v.$$

- If we multiply the identity matrix by a scalar $\lambda \in \mathbb{F}$ we obtain a so-called **scalar matrix**:

$$\lambda I_n = \begin{pmatrix} \lambda & 0 & \dots & 0 \\ 0 & \lambda & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \dots & 0 & \lambda \end{pmatrix},$$

  λI_n corresponds to the endomorphism $f(v) = \lambda v$ for all $v \in \mathbb{F}^n$ with respect to the canonical bases of $\mathbb{F}^n$, these endomorphisms play a crucial role in linear algebra.

- More generally, we call $A \in M_n(\mathbb{F})$ a **diagonal matrix** if the only non-null entries of A are located on its diagonal and we write

$$A = \operatorname{diag}(a_{11}, \dots, a_{nn}),$$

  so I_n and λI_n are special diagonal matrices with all 1 or λ, respectively, on the diagonal.

- The *identity matrix and all scalar matrices commute with all other matrices.*
- Any *two diagonal matrices commute with each other*, but it is *not true that diagonal matrices commute with any other matrix*, e.g.

$$\begin{pmatrix} 0 & 2 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 2 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} 0 & -2 \\ 2 & 1 \end{pmatrix}, \quad \text{but} \quad \begin{pmatrix} 2 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} 0 & 2 \\ 1 & -1 \end{pmatrix} = \begin{pmatrix} 0 & 4 \\ -1 & 1 \end{pmatrix}.$$

- A matrix $A \in M_n(\mathbb{F})$ is called **upper triangular** or **lower triangular** if it has the following form, respectively:

$$A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ 0 & a_{22} & \dots & a_{2n} \\ \vdots & \ddots & \ddots & \vdots \\ 0 & \dots & 0 & a_{nn} \end{pmatrix},$$

$$A = \begin{pmatrix} a_{11} & 0 & \dots & 0 \\ a_{21} & a_{22} & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ a_{n1} & \dots & a_{nn-1} & a_{nn} \end{pmatrix},$$

  i.e. if the only non-null elements of A are those contained in its diagonal and in the entries above it (upper triangular), or below it (lower triangular).

- In $\mathbb{R}$ and $\mathbb{C}$ the *cancellation law* holds: the product of two real or complex scalars a, b is 0 if and only if one of them, or both of them, is 0. For matrices this is not guaranteed: given two matrices $A, B \in M_n(\mathbb{F})$ it may happen that $AB = \mathbf{0}_n$, but neither A nor B are the null matrix! For instance, by performing the matrix product of the following two matrices (do it…), we obtain:

$$\begin{pmatrix} 2 & -1 \\ -4 & 2 \end{pmatrix} \begin{pmatrix} 1 & 3 \\ 2 & 6 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} = \mathbf{0}_2.$$

  Thus, $M_n(\mathbb{F})$ does not have the cancellation law! Non-null matrices $A, B \in M_n(\mathbb{F})$ that satisfy $AB = \mathbf{0}_n$ are called **divisors of zero**.

- Another peculiar behavior of square matrices is that there may be non-null matrices which become null when elevated to a certain power r (i.e. when they are multiplied by themselves r times), something that cannot happen in $\mathbb{R}$ or $\mathbb{C}$.

  If $A \in M_n(\mathbb{F})$ is such that $A^r = \mathbf{0}_n$, then A is called **nilpotent** of order r. For instance

$$A = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}, \quad A^2 = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \quad A^3 = \mathbf{0}_3 \implies A: \text{ nilpotent of order 3.}$$

- Importantly, *for a square matrix it makes sense to talk about its inverse*: to introduce the concept of matrix inversion, let us recall that if $a \in \mathbb{R}$, $a \neq 0$, then the inverse of a is the real number b such that $ab = ba = 1$, and we write $b = a^{-1} = 1/a$.

Since the unit with respect to the matrix product is I_n we say that a matrix $B \in M_n(\mathbb{F})$ is the **inverse** of a non-null matrix $A \in M_n(\mathbb{F})$ if

$$AB = BA = I_n,$$

and we write $B = A^{-1}$. Differently from $\mathbb{R}$, not all square matrices admit an inverse. In fact, $A \in M_n(\mathbb{F})$ represents an endomorphism and not all endomorphisms are invertible because only one-to-one and onto endomorphisms, i.e. isomorphisms, have an inverse!

A class of matrices that do not admit inverse is given by divisors of zero. To understand why, suppose that two non-null matrices $A, B \in M_n(\mathbb{F})$, are divisors of zero, i.e. $AB = \mathbf{0}_n$. If there exists $A^{-1} \in M_n(\mathbb{F})$ such that $A^{-1}A = I_n$, then

$$B = I_n B = (A^{-1}A)B = A^{-1}(AB) = A^{-1}\mathbf{0}_n = \mathbf{0}_n,$$

which contradicts the fact that $B \neq \mathbf{0}_n$, so A cannot be invertible. We can repeat the same argument by exchanging A with B and we find that also B cannot be invertible. We deduce that **divisors of zero cannot be invertible**.

- An endomorphism $f : V \to V$ which is also an isomorphism is called an **automorphism** of V. The set of automorphisms of a vector space V is denoted with $\mathrm{Aut}(V)$.
- The set of invertible matrices of $M_n(\mathbb{F})$ is denoted with $\mathrm{GL}(n, \mathbb{F})$ and it is called the **general linear group**[5].
- Thanks to the nullity+rank theorem, $A \in M_n(\mathbb{F})$ belongs to $\mathrm{GL}(n, \mathbb{F})$ if and only if it has *full rank*, i.e. if $\mathrm{rank}(A) = n$.

For square matrices, one can define a very important quantity called determinant, which plays a fundamental role in the analysis of endomorphisms and systems of linear equations. We will dedicate the next section to this concept.

[5] The reason why it is called in this way is that $\mathrm{GL}(n, \mathbb{F})$ forms a group with respect to matrix product. In general, a group is set G endowed with an associative operation called product, $\cdot : G \times G \to G$, for which it exists a neutral element $e \in G$, i.e. $e \cdot g = g \cdot e = g$ for all $g \in G$, and an inverse element g^{-1}, i.e. $g^{-1} \cdot g = g \cdot g^{-1}$, for all $g \in G$.

2.9 The determinant of a square matrix and its properties

The determinant of a square matrix $A = (a_{ij})_{i,j=1,\ldots,n} \in M_n(\mathbb{F})$ is a scalar that belongs to $\mathbb{F}$, written either as $\det(A)$ or $|A|$, that can be defined through a *very general, yet very abstract formula* which deals with *permutations*, i.e. one-to-one and onto maps over a set of indices.

This definition is *computationally useless* because, even with modern days computers, one would need years to compute the determinant of even a very small matrix by translating that formula into an algorithm. Plus, when the size of the matrix increases, the computational time becomes soon enormous (literally... for a matrix of order 30, the time needed to compute its determinant using the algorithm corresponding to the defining formula would be around 10000 times the age of the universe, which is ≈13.7 billion years!).

Why then even bother considering such a formula? The answer is that, *thanks to this formula, it is relatively easy to prove several important properties of the determinant.* So, even though it is never used in practice, it is of great theoretical importance.

We do not have the time to go through the proofs of the determinant properties, hence we will do not introduce its defining formula (because we would also need to spend time discussing permutations). What we will do instead is to redefine the determinant through a formula, due to the French polymath Pierre Simon de **Laplace** (1749-1827), which is computationally much more useful, and then we will just quote its properties, replacing their proofs by concrete examples.

We need a few definitions that will make our next discussion much easier.

Def. 2.9.1 *Consider a square matrix $A = (a_{ij})_{i,j=1,\ldots,n} \in M_n(\mathbb{F})$.*

- *A_{ij} is the matrix belonging to $M_{n-1}(\mathbb{F})$, obtained from A by removing the i-th row and the j-th column*
- *$\det(A_{ij}) = |A_{ij}|$ is called the (i,j)-**minor** of the matrix A. In the particular case of $A_{ij} \in M_1(\mathbb{F})$ we set $\det(A_{ij}) = A_{ij}$*
- *$(-1)^{i+j}\det(A_{ij}) = (-1)^{i+j}|A_{ij}|$ is called the **cofactor** of the element $a_{ij} \in A$. The matrix whose entries are the cofactors of the elements of A is called **cofactor matrix** and it is indicated with C:*

$$C = (c_{ij})_{i,j=1,\ldots,n},\ c_{ij} = (-1)^{i+j}|A_{ij}|.$$

Example 2.9.1 Given the matrix

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

the matrix A_{23} is obtained from A by removing the second row and the third column, i.e.

$$A = \begin{pmatrix} 1 & 0 & \color{red}{4} \\ \color{red}{0} & \color{red}{-2} & \color{red}{1} \\ -1 & 0 & \color{red}{0} \end{pmatrix} \Longrightarrow A_{23} = \begin{pmatrix} 1 & 0 \\ -1 & 0 \end{pmatrix}.$$

We cannot write neither the $(2,3)$-minor of A nor the cofactor of the element a_{23} and the cofactor matrix because we need to know how to compute the determinant. The following theorem gives a the most used way to calculate the determinant of a matrix.

Theorem 2.9.1 (Laplace development along a row or a column) *The determinant of $A \in M_n(\mathbb{F})$ is the scalar* $\det(A) \in \mathbb{F}$ *which can be computed as follows:*

$$\det(A) = \sum_{k=1}^{n} (-1)^{i+k} a_{ik} |A_{ik}|$$

or as follows:

$$\det(A) = \sum_{k=1}^{n} (-1)^{k+j} a_{kj} |A_{kj}|$$

The former formula is called Laplace development of the determinant along the i-th row, the latter is called Laplace development of the determinant along the j-th column.

In words, Laplace theorem says that the determinant of a square matrix can be computed:

- by adding all the cofactors of the elements a_{ik}, where i is a *fixed row index* and k is the sum index, running from column 1 to column n, each one multiplied by a_{ik}
- by adding all the cofactors of the elements a_{kj}, where j is a *fixed column index* and k is the sum index, running from row 1 to row n, each one multiplied by a_{kj}.

Of course, if a_{ik}, or a_{kj}, is null, there is no need to compute the minor associated to it, because, independently of its value, the corresponding term in the sum will be 0. Thanks to this observation we have this **golden rule** for the optimal application of the Laplace formulae: **it is convenient to compute the determinant by performing a Laplace development along either the row or the column which has the largest amount of zeros in it**!

In the next explicit examples we show how to use the Laplace formula for a square matrix of order 2,3 and 4, this should be enough to understand how to use it in general.

Example 2.9.2 *Determinant of a 2×2 generic matrix.* Let us consider the generic 2×2 matrix

$$A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix},$$

we develop the determinant of A along, e.g., the first row

$$\det(A) = (-1)^{1+1} a_{11}|A_{11}| + (-1)^{1+2} a_{12}|A_{12}| = a_{11}|A_{11}| - a_{12}|A_{12}|.$$

$|A_{11}|$ is the determinant of the matrix $(2-1) \times (2-1) = 1 \times 1$ obtained from A by deleting its first row and first column, i.e. $|A_{11}| = a_{22}$.

Likewise, $|A_{12}|$ is the determinant of the matrix 1×1 obtained from A by deleting its first row and second column, i.e. $|A_{12}| = a_{21}$.

So,

$$\det(A) = a_{11}a_{22} - a_{12}a_{21},$$

i.e. *the determinant of a 2×2 matrix is obtained by multiplying together the elements of the diagonal and then subtracting the product of the off-diagonal elements.*

In order to have a numerical example, consider

$$A = \begin{pmatrix} 2 & -1 \\ 3 & \frac{1}{2} \end{pmatrix} \implies \det(A) = 2 \cdot \frac{1}{2} - (-1) \cdot 3 = 1 + 3 = 4.$$

Example 2.9.3 *Determinant of a* 3×3 *generic matrix.* The generic 3×3 matrix is

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

this time, we arbitrarily choose to develop the determinant along the first column:

$$\begin{aligned} \det(A) &= (-1)^{1+1} a_{11}|A_{11}| + (-1)^{2+1} a_{21}|A_{21}| + (-1)^{3+1} a_{31}|A_{31}| \\ &= a_{11}|A_{11}| - a_{21}|A_{21}| + a_{31}|A_{31}|, \end{aligned}$$

but

$$|A_{11}| = \det \begin{pmatrix} a_{22} & a_{23} \\ a_{32} & a_{33} \end{pmatrix} = a_{22}a_{33} - a_{23}a_{32},$$

$$|A_{21}| = \det \begin{pmatrix} a_{12} & a_{13} \\ a_{32} & a_{33} \end{pmatrix} = a_{12}a_{33} - a_{13}a_{32},$$

$$|A_{31}| = \det \begin{pmatrix} a_{12} & a_{13} \\ a_{22} & a_{23} \end{pmatrix} = a_{12}a_{23} - a_{13}a_{22},$$

so

$$\det(A) = a_{11}a_{22}a_{33} - a_{11}a_{23}a_{32} - a_{21}a_{12}a_{33} + a_{21}a_{13}a_{32} + a_{31}a_{12}a_{23} - a_{31}a_{13}a_{22}.$$

In order to have a numerical example, consider

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

following the golden rule provided above, it is convenient to develop the determinant either along the third row or the third column, let us do both so we can confirm that the result is the same.

Development along the third row:

$$\det(A) = (-1)^{3+2}(-2)|A_{32}| = 2|A_{32}| = 2 \begin{vmatrix} -1 & 0 \\ 3 & 1 \end{vmatrix} = 2(-1 \cdot 1 - 0 \cdot 3) = -2.$$

Development along the third column:

$$\det(A) = (-1)^{2+3} \cdot 1 \cdot |A_{23}| = -|A_{23}| = -\begin{vmatrix} -1 & 2 \\ 0 & -2 \end{vmatrix} = -((-1) \cdot (-2) - 2 \cdot 0) = -2.$$

Example 2.9.4 *Determinant of a* 4×4 *numerical matrix. Consider the matrix*

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

it is convenient to develop the determinant either along the third row or along the fourth column, we choose arbitrarily to do it along the third row:

$$\det(A) = (-1)^{3+2} \cdot 2 \cdot |A_{32}| + (-1)^{3+3}(-3)|A_{33}| = -2 \begin{vmatrix} 2 & 1 & 1 \\ -1 & 0 & 2 \\ 1 & -1 & 0 \end{vmatrix} - 3 \begin{vmatrix} 2 & 0 & 1 \\ -1 & 3 & 2 \\ 1 & 4 & 0 \end{vmatrix},$$

we develop the first minor along the second column, which has only unitary coefficients:

$$\begin{vmatrix} 2 & 1 & 1 \\ -1 & 0 & 2 \\ 1 & -1 & 0 \end{vmatrix} = (-1)^{1+2} \cdot 1 \cdot \begin{vmatrix} -1 & 2 \\ 1 & 0 \end{vmatrix} + (-1)^{3+2}(-1) \begin{vmatrix} 2 & 1 \\ -1 & 2 \end{vmatrix} = -(-2) + 5 = 7,$$

we develop the second minor along the first row:

$$\begin{vmatrix} 2 & 0 & 1 \\ -1 & 3 & 2 \\ 1 & 4 & 0 \end{vmatrix} = (-1)^{1+1} \cdot 2 \cdot \begin{vmatrix} 3 & 2 \\ 4 & 0 \end{vmatrix} + (-1)^{1+3} \cdot 1 \cdot \begin{vmatrix} -1 & 3 \\ 1 & 4 \end{vmatrix} = 2(-8) + 1 \cdot (-7) = -16 - 7 = -23,$$

in conclusion

$$\det(A) = -2 \cdot 7 - 3 \cdot (-23) = -14 + 69 = 55.$$

It can be seen in the previous examples that the signs to put in front of the minors in order to create the cofactors have a regular pattern. Since we will not consider square matrices of order greater than 4, we hereby show this pattern for 4×4 matrices and we will implicitly use it from now on:

$$\begin{pmatrix} + & - & + & - \\ - & + & - & + \\ + & - & + & - \\ - & + & - & + \end{pmatrix}.$$

The pattern show above can be used to also for matrices 2×2 and 3×3 just by considering the first two (three) rows and columns (respectively).

Let us immediately state the relation between the determinant of the matrix associated to an endomorphism and its inversibility, so that we can understand why the determinant is so important in linear algebra.

Theorem 2.9.2 *The endomorphism $f : V \to V$ is invertible if and only the matrix A associated to f with respect to any choice of bases of V is invertible and this happens if and only if* $\det(A) \neq 0$.

Recalling that a matrix $A \in M_n(\mathbb{F})$ is inversible if and only if it has full rank, the following corollary follows immediately.

Corollary 2.9.1 *A matrix $A \in M_n(\mathbb{F})$ has full rank if and only if* $\det(A) \neq 0$.

We collect in the following theorem the most important properties of the determinant, which will be very useful in the the theory of systems of linear equations.

Theorem 2.9.3 (Properties of the determinant) *Let $A, B \in M_n(\mathbb{F})$ and $\lambda, \mu \in \mathbb{F}$.*

1. $\det(A) = \det(A^t)$.

2. *If A is an upper or lower triangular matrix, and so, in particular, if it is a diagonal matrix, then*
$$\det(A) = a_{11}a_{22}\cdots a_{nn}.$$

3. $\det(\lambda A) = \lambda^n \det(A)$, *so the determinant is not a linear function of matrices because it is not homogeneous. Moreover, in general, the determinant it is not additive either, i.e.* $\det(A+B) \neq \det(A) + \det(B)$.

4. *The only linear behavior of* $\det$ *is with respect to linear combinations of rows or columns, i.e., if the k-th row R_k of A is written as $R_k = \lambda R_i + \mu R_j$, $i, j \in \{1, \ldots, n\}$, then*
$$\det(A) = \lambda \det \begin{pmatrix} R_1 \\ R_2 \\ \vdots \\ R_i \\ \vdots \\ R_n \end{pmatrix} + \mu \det \begin{pmatrix} R_1 \\ R_2 \\ \vdots \\ R_j \\ \vdots \\ R_n \end{pmatrix}.$$
Analogously, if the k-th column C_k of A is written as $C_k = \lambda C_i + \mu C_j$, $i, j \in \{1, \ldots, n\}$, then
$$\det(A) = \lambda \det \left(\begin{array}{c:c:c:c:c:c} C_1 & C_2 & \cdots & C_i & \cdots & C_n \end{array} \right) + \mu \det \left(\begin{array}{c:c:c:c:c:c} C_1 & C_2 & \cdots & C_j & \cdots & C_n \end{array} \right).$$

5. *If the matrix B is obtained by A by exchanging two rows or two columns, then we have* $\det(B) = -\det(A)$.

6. *From the previous property, it follows that if A has two identical rows or two identical columns, then* $\det(A) = 0$ (*in fact, if we exchange the identical rows* (*or columns*), *the matrix remains the same, but the determinant switches sign, so* $\det(A) = -\det(A)$, *which implies* $\det(A) = 0$).

7. *If A has at least a null row or a null column, then* $\det(A) = 0$.

8. *The determinant of A does not change if we sum to a row* (*or a column*) *of A a linear combination of the remaining ones, i.e. if we replace the generic row R_i, $i \in \{1, \ldots, n\}$, with this one*
$$R_i' = R_i + \sum_{k \in \{1,\ldots,n\},\ k \neq i} \lambda_k R_k, \qquad \lambda_k \in \mathbb{F}$$
or the generic column C_j, $j \in \{1, \ldots, n\}$, with this one
$$C_j' = C_j + \sum_{k \in \{1,\ldots,n\},\ k \neq j} \lambda_k C_k, \qquad \lambda_k \in \mathbb{F}.$$

9. *The previous two properties imply immediately that if A has two linearly dependent rows (or two columns), then* $\det(A) = 0$.

   In fact, suppose that $R_j = \lambda R_i$, $\lambda \neq 0$, then using 8. we have that $\det(A)$ does not change if we replace R_i with the row

$$R_i' = R_i - \frac{1}{\lambda} R_j + \sum_{k \in \{1,\ldots,n\},\, k \neq i,j} 0 \cdot R_k = R_i - R_i = \mathbf{0},$$

   so, 7. implies $\det(A) = 0$ because one row is null. Of course, an analogous argument can be repeated for columns.

10. **Binet's theorem**:

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

11. If A is invertible, then

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

12. If B is invertible, then

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

   the operation BAB^{-1} is called **conjugation** of the matrix A by the matrix B, so the previous property established the invariance of the determinant with respect to conjugation.

2.9.1 Inversion of a matrix

Since the non-nullity of determinant determines when a matrix is invertible, it is not so surprising that the determinant appears also in the formula for computing the inverse of a matrix. Before giving the formula we need a definition.

Def. 2.9.2 (Adjugate matrix) *Given $A \in M_n(\mathbb{F})$, its adjugate matrix, indicated with* $\mathrm{adj}(A)$*, is the transpose of the cofactor matrix, i.e.*

$$\mathrm{adj}(A) = C^t,\ \mathrm{adj}(A)_{ij} = ((-1)^{i+j}|A_{ij}|)^t_{i,j} = ((-1)^{i+j}|A_{ji}|)_{i,j}$$

For example, given a generic 2×2 matrix:

$$A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix},$$

the cofactors are

$$c_{11} = +a_{22},\ c_{12} = -a_{21},\ c_{21} = -a_{12},\ c_{22} = +a_{11},$$

so the cofactor matrix is

$$C = \begin{pmatrix} a_{22} & -a_{21} \\ -a_{12} & a_{11} \end{pmatrix},$$

and thus the adjugate matrix is

$$\mathrm{adj}(A) = C^t = \begin{pmatrix} a_{22} & -a_{12} \\ -a_{21} & a_{11} \end{pmatrix}.$$

The shape of the adjugate matrix 2×2 can be better visualized if we write the original matrix as follows

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \implies \operatorname{adj}(A) = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}.$$

Let us now see how the inverse of a matrix with non null determinant can be computed.

Theorem 2.9.4 (Computation of the inverse of a matrix) *Given a matrix $A \in M_n(\mathbb{F})$ with $\det(A) \neq 0$, its inverse is given by*

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

The computation of the inverse of a matrix is a very time consuming operation and, nowadays, we perform it with computers. However, it must be kept in mind that, *whenever it is possible, it should be avoided to inverse a large order square matrix with and use different strategies.*

Let us see an example of computation of the inverse of a 3×3 matrix to see how many operations are involved. We consider a matrix that we have analyzed in the previous section:

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

because we have already computed its determinant to be $\det(A) = -2 \neq 0$, so A can be inverted. The cofactors of A are

$$c_{11} = +\det \begin{pmatrix} 4 & 1 \\ -2 & 0 \end{pmatrix} = 2,\ c_{12} = -\det \begin{pmatrix} 3 & 1 \\ 0 & 0 \end{pmatrix} = 0,\ c_{13} = +\det \begin{pmatrix} 3 & 4 \\ 0 & -2 \end{pmatrix} = -6,$$

$$c_{21} = -\det \begin{pmatrix} 2 & 0 \\ -2 & 0 \end{pmatrix} = 0,\ c_{22} = +\det \begin{pmatrix} -1 & 0 \\ 0 & 0 \end{pmatrix} = 0,\ c_{23} = -\det \begin{pmatrix} -1 & 2 \\ 0 & -2 \end{pmatrix} = -2,$$

$$c_{31} = +\det \begin{pmatrix} 2 & 0 \\ 4 & 1 \end{pmatrix} = 2,\ c_{32} = -\det \begin{pmatrix} -1 & 0 \\ 3 & 1 \end{pmatrix} = 1,\ c_{33} = +\det \begin{pmatrix} -1 & 2 \\ 3 & 4 \end{pmatrix} = -10,$$

so

$$C = \begin{pmatrix} 2 & 0 & -6 \\ 0 & 0 & -2 \\ 2 & 1 & -10 \end{pmatrix}$$

and

$$A^{-1} = \frac{C^t}{\det(A)} = -\frac{1}{2} \begin{pmatrix} 2 & 0 & 2 \\ 0 & 0 & 1 \\ -6 & -2 & -10 \end{pmatrix} = \begin{pmatrix} -1 & 0 & -1 \\ 0 & 0 & -\frac{1}{2} \\ 3 & 1 & 5 \end{pmatrix}.$$

As a useful exercise, you can check that $AA^{-1} = A^{-1}A = I_3$.

In the next chapter, we will exploit what we have learned about vector spaces and linear maps to solve linear systems efficiently.

2.10 A practical application of matrix theory: the early days of cryptography

When we want to send a secret message to someone, we need to modify its content in order to be readable only by the receiver.

In order to do that, since the English alphabet is composed by 26 letters, we start by assigning to every letter of the alphabet an integer number between 0 and 25:

- A becomes 0
- B becomes 1
- ...
- Z becomes 25.

The message then is encrypted by changing the number associated to each letter with other one on the basis of any arbitrary rule.

For example, we can change the number n with $n+3$, so A will be encrypted by 3, B by 4, and so on. There is of course a problem when we reach 23 because 23+3=26> 25. We can easily remedy this problem by using the convention that, if $n+3>25$, then we replace $n+3$ by its **cyclic extension**, as depicted in Figure 2.2.

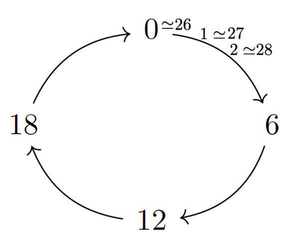


Figure 2.2: The cyclic extension.

To compute the cyclic extension corresponding to $n+3$ one can follow this very simple rule: divide $n+3$ by 26, then the remainder of the division is its cyclic extension. For example:

- X has position $n=23$, so $n+3=26$ and $26=1\cdot 26+0$, so X will be encrypted by 0
- Y has position $n=24$, so $n+3=27$ and $27=1\cdot 26+1$, so Y will be encrypted by 1
- Z has position $n=25$, so $n+3=28$ and $28=1\cdot 26+2$, so Z will be encrypted by 2.

With this encryption rule the word 'HELLO' will undergo this encryption:

$$7 \quad 4 \quad 11 \quad 11 \quad 14 \quad \longmapsto \quad 10 \quad 7 \quad 14 \quad 14 \quad 17,$$

which the received will read in letters as 'KHOOR'. If the the receiver knows the **encryption code** (or **key**), the reconstruction the original word will be operated by $k \mapsto k-3$ together with the cyclic extension.

Clearly, this encryption is very basic and simple to decipher, for this reason more refined techniques have been developed. The standard nowadays consists in having to find the decomposition of a very large number n into the product of prime numbers, something that even for a supercomputer would take a huge amount of time.

Instead of entering in the quite complicated details of this encryption algorithm, we discuss an intermediate one, which has the advantage of showing the usefulness of matrices.

Let us consider again the basic encryption algorithm discussed above and, instead of considering each letter one by one, we join together two of them in a couple, with the convention that if we remain with only one letter alone, we add Z to form a couple. So, for example,

HELLO becomes HE LL OZ,

which, codified in numbers with the rule $n \mapsto n+3$ with cyclic extension becomes

7 4 11 11 14 2.

The reason why we take couple is to have the possibility to build column vectors using the two numbers of the couple as follows

$$X_1 = \begin{pmatrix} 7 \\ 4 \end{pmatrix}, \quad X_2 = \begin{pmatrix} 11 \\ 11 \end{pmatrix}, \quad X_3 = \begin{pmatrix} 14 \\ 2 \end{pmatrix},$$

The core of this encryption method is the selection of an *invertible* 2×2 matrix, e.g.

$$M = \begin{pmatrix} 2 & 1 \\ 1 & -1 \end{pmatrix}, \quad \text{with inverse} \quad M^{-1} = \frac{1}{3}\begin{pmatrix} 1 & 1 \\ 1 & -2 \end{pmatrix}.$$

By matrix multiplication we can scramble the previous vectors, obtaining

$$\tilde{X}_1 = MX_1 = \begin{pmatrix} 18 \\ 3 \end{pmatrix}, \quad \tilde{X}_2 = MX_2 = \begin{pmatrix} 33 \\ 0 \end{pmatrix}, \quad \tilde{X}_3 = MX_3 = \begin{pmatrix} 30 \\ 12 \end{pmatrix},$$

and we use the cyclic extension to bring back to the set $\{0, \ldots, 25\}$ the numbers that fell out of it[6], so: $33 = 1 \cdot 26 + 7$ and $30 = 1 \cdot 26 + 4$, so

$$\tilde{X}_1 = \begin{pmatrix} 18 \\ 3 \end{pmatrix}, \quad \tilde{X}_2 = \begin{pmatrix} 7 \\ 0 \end{pmatrix}, \quad \tilde{X}_3 = \begin{pmatrix} 4 \\ 12 \end{pmatrix}.$$

Finally, we turn back to letters and the novel encryption of HELLO will be

PA EX BJ.

To decode the encrypted word and understand the original one that has been sent, the receiver must first apply the inverse matrix M^{-1} to each pair, in fact, using the fact that $\tilde{X}_j = MX_j$ we get

$$X_j = M^{-1}\tilde{X}_j = M^{-1}MX_j = I_2X_j = X_j.$$

Finally, the receiver must undo the original encryption with the operation $k \mapsto k-3$ and using the cyclic extension if needed. This encryption method is more difficult to be deciphered than the previous one and, of course, it becomes more and more efficient as we increase the dimension of the matrix M, which, of course, implies also to adapt the convention of adding a letter at the end of the word correspondingly to the new dimension of the matrix.

[6] If we had found a negative number, e.g. -15, that would not have been a problem, because in our case the remainder is always a positive integer number between 0 and 25: $-15 = (-1) \cdot 26 + 11$, so $-15 \simeq 11$.

2.11 Questions about chapter 2

In the following questions, unless explicitly specified, $f : V \to W$ is a linear map between two vector spaces V and W over the same field $\mathbb{F}$.

1. What are the two properties that define a linear map $f : V \to W$? What does it mean that f passes through linear combinations?
2. What is the image of $\mathbf{0}_V$ via the linear map f?
3. What is the prototype of a vector space V over the field $\mathbb{F}$? Can you write down the isomorphism between V and its prototype?
4. Do you remember a necessary and sufficient condition for two vector spaces over the same field to be isomorphic via a linear map?
5. What are the kernel and the image of f? Are they simply sets or something more?
6. Define the nullity and rank of f and relate them to the property of being one-to-one and onto.
7. What does it mean that f is full-rank?
8. Quote the nullity+rank theorem.
9. When does f is an endomorphism?
10. When an endomorphism is also an isomorphism?
11. If $B = (v_1, \ldots, v_n)$ is a basis of V, what is the set $(f(v_1), \ldots, f(v_n))$?
12. How can a linear map be extended to the whole V by knowing a basis $B = (v_1, \ldots, v_n)$ and the set $(f(v_1), \ldots, f(v_n))$?
13. How can a linear map $f : V \to W$ be defined from the knowledge of a basis $B = (v_1, \ldots, v_n)$ of V and a random set $(w_1, \ldots, w_n)$ of vectors of W?
14. If you had to describe with a simple sentence what is the explicit expression of a linear map, what would you say?
15. Do you remember how to classify the property of a linear map of being one-to-one, onto and an isomorphism on the basis of how it transforms the vectors of a generic basis of its domain?
16. Do you recall how to associate a matrix to a linear map $f : V \to W$ once a basis B_V of V and a basis B_W of W have been chosen? Moreover, can you tell why this association is unique?
17. What is $\mathcal{L}(V, W)$ and how does it become a vector space? What is its dimension?
18. What is $M_{mn}(\mathbb{F})$ and how does it become a vector space? What is its dimension? How is it related to $\mathcal{L}(V, W)$?
19. What is the analogous of the canonical basis of $\mathbb{F}^n$ for $M_{m,n}(\mathbb{F})$?

20. Define the matrix product and specify when it makes sense. To what operation between linear maps is it related?
21. What is the transpose of a matrix and what are its properties?
22. Is it possible to express the rank of a linear map in terms of a property verified by the matrix associated to it with respect to any bases?
23. Define a matrix that is square, diagonal, upper and lower triangular, the identity and the zero matrix.
24. What are the divisors of zero of $M_n(\mathbb{F})$?
25. What does it mean that the matrix $B \in M_n(\mathbb{F})$ is the inverse of $A \in M_n(\mathbb{F})$?
26. Tell two conditions on $A \in M_n(\mathbb{F})$ to guarantee that A admits an inverse. What does that imply for the linear map associated to A with respect a fixed choice of bases?
27. Define the (i, j)-minor of a matrix $A \in M_n(\mathbb{F})$, the cofactor of the element a_{ij} of A and the cofactor matrix.
28. Write down the Laplace formula for the development of the determinant of a matrix along a row and along a column.
29. What is the 'golden rule' to apply each time we want to use the Laplace formula to compute the determinant of a matrix?
30. Is the determinant a linear function?
31. Can you quote Binet's theorem?
32. Can you tell some conditions which assure that the determinant of a matrix is zero without computing it?
33. What is the determinant of the inverse of a(n invertible) matrix A?
34. What is the adjugate of a matrix and how does it appear in the formula for the explicit computation of the inverse of a(n invertible) matrix?

2.12 Exercises of chapter 2

The following exercises have the aim of testing the comprehension of the most important concepts that have been introduced in chapter 2.

1. Establish if the following linear map

$$\begin{array}{rccl} f: & \mathbb{R}^3 & \longrightarrow & \mathbb{R}^4 \\ & (x,y,z) & \longmapsto & f((x,y,z)) = (x-y-z, -2x+z, y-3z, x+y+z) \end{array}$$

is one-to-one, onto or an isomorphism.

2. Given the real matrix

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

find the linear map f associated to it with respect to the canonical bases of $\mathbb{R}^3$ and establish if it is one-to-one or onto.

3. Given the endomorphisms

$$f : \mathbb{R}^3 \to \mathbb{R}^3, \quad (x,y,z) \mapsto f((x,y,z)) = (x-y, -z, x+y+z)$$

$$g : \mathbb{R}^3 \to \mathbb{R}^3, \quad (u,v,w) \mapsto g((u,v,w)) = (u-v, w, -u-v-w)$$

establish if they are one-to-one, onto or automorphisms of $\mathbb{R}^3$ using their associated matrices. Are the endomorphisms $g \circ f$ and $f \circ g$ automorphisms of $\mathbb{R}^3$ or not?

2.12.1 Solutions of the exercises of chapter 2

The reader is *strongly encouraged* not to look at the solution of the exercises proposed in the previous page before trying to solve them.

1. Given the linear map $f : \mathbb{R}^3 \to \mathbb{R}^4$, $f((x, y, z)) = (x - y - z, -2x + z, y - 3z, x + y + z)$, it cannot be an isomorphism because we know that there can be an isomorphism between vector spaces if and only if they have the same dimension, which is not the case for us. Moreover, $\dim(\mathbb{R}^3) = 3 < 4 = \dim(\mathbb{R}^4)$, hence, by Corollary 2.3.1, f cannot be onto either. For this reason, f *can* only be one-to-one.

   We can check that property by using Theorem 2.3.3 which, applied to our case, says that f is one-to-one if and only if the images of the vectors of a basis is a free family in $\mathbb{R}^4$.

   To minimize the computations, we choose of course the canonical basis of $\mathbb{R}^3$ and we find

   $$f((1,0,0)) = (1,-2,0,1),\ f((0,1,0)) = (-1,0,1,1),\ f((0,0,1)) = (-1,1,-3,1).$$

   Now we impose that a linear combination of the three image vectors is $\mathbf{0}_{\mathbb{R}^4}$. f is one-to-one if and only if the coefficients of the linear combinations are all 0:

   $$a(1,-2,0,1) + b(-1,0,1,1) + c(-1,1,-3,1) = (0,0,0,0)$$

   or

   $$(a - b - c, -2a + c, b - 3c, a + b + c) = (0,0,0,0),$$

   i.e.

   $$\begin{cases} a - b - c = 0 & (1) \\ -2a + c = 0 & (2) \\ b - 3c = 0 & (3) \\ a + b + c = 0 & (4) \end{cases} \iff \begin{cases} (2) \implies c = 2a \\ (3) \implies b = 3c = 6a \\ (1) \implies a - 6a - 2a = 0 \implies a = 0 \\ (4) \implies a + 6a + 2a = 0 \implies a = 0 \end{cases} \iff \begin{cases} a = 0 \\ b = 0 \\ c = 0 \end{cases},$$

   so f is indeed one-to-one.

2. The matrix

   $$A = \begin{pmatrix} 3 & 1 & 2 \\ 0 & -1 & 1 \\ -6 & -2 & -4 \end{pmatrix} \in M_3(\mathbb{R}),$$

   can be associated only to an endomorphism $f : \mathbb{R}^3 \to \mathbb{R}^3$. Following the indication of the exercise, the columns of A are the images via f of the vectors of the canonical basis of $\mathbb{R}^3$, i.e.

   $$f((1,0,0)) = (3,0,-6),\ f((0,1,0)) = (1,-1,-2),\ f((0,0,1)) = (2,1,-4).$$

   Now we must extend f to the whole $\mathbb{R}^3$ with the technique that we have learned in section 2.3:

   $$f((x,y,z)) = xf((1,0,0)) + yf((0,1,0)) + zf((0,0,1)),$$

   i.e.

   $$f((x,y,z)) = x(3,0,-6)+y(1,-1,-2)+z(2,1,-4) = (3x+y+2z, -y+z, -6x-2y-4z).$$

Since we are dealing with an endomorphism, we can establish its properties by computing the determinant of the associated matrix A. In fact, thanks to the nullity+rank theorem, f is an isomorphism if and only if $\det(A) \neq 0$, and if $\det(A) = 0$ then f is neither one-to-one nor onto.

By the property 9. of Theorem 2.9.3, we can immediately say that $\det(A) = 0$ because the first and the third row are linearly dependent, in fact:

$$R_3 = -2R_1.$$

So f is neither one-to-one, nor onto.

In order to practice the Laplace formula, we can develop the determinant of A along the second row, because it contains a 0, obtaining

$$\det(A) = -\det\begin{pmatrix} 3 & 2 \\ -6 & -4 \end{pmatrix} - \det\begin{pmatrix} 3 & 1 \\ -6 & -2 \end{pmatrix} = 0.$$

3. Let us consider first

$$f : \mathbb{R}^3 \to \mathbb{R}^3, \quad (x, y, z) \mapsto f((x, y, z)) = (x - y, -z, x + y + z)$$

and fix the canonical bases of $\mathbb{R}^3$, then

$$f((1,0,0)) = (1,0,1),\ f((0,1,0)) = (-1,0,1),\ f((0,0,1)) = (0,-1,1),$$

so the matrix A associated to f is

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

Its determinant can be computed using the Laplace development along the second row, which has two zeros:

$$\det(A) = \det\begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix} = 2 \neq 0,$$

so f is an automorphism of $\mathbb{R}^3$.

Now we consider

$$g : \mathbb{R}^3 \to \mathbb{R}^3, \quad (u, v, w) \mapsto g((u, v, w)) = (u - v, w, -u - v - w)$$

and fix the canonical bases of $\mathbb{R}^3$, then

$$g((1,0,0)) = (1,0,-1),\ g((0,1,0)) = (-1,0,-1),\ g((0,0,1)) = (0,1,-1),$$

so the matrix B associated to g is

$$B = \begin{pmatrix} 1 & -1 & 0 \\ 0 & 0 & 1 \\ -1 & -1 & -1 \end{pmatrix}.$$

Using again the Laplace development along the second row, which has two zeros, we find

$$\det(B) = -\det \begin{pmatrix} 1 & -1 \\ -1 & -1 \end{pmatrix} = 2 \neq 0,$$

so, also g is an automorphism of $\mathbb{R}^3$.

The composition of automorphisms is again an automorphism, so also $g \circ f$ and $f \circ g$ are automorphisms.

Coherently with that, the matrices associated to them with respect to the canonical bases of $\mathbb{R}^3$ are BA and AB, respectively, and it can be checked as a useful exercise that their determinant is different than 0.

Chapter 3

Resolution of linear systems through linear algebra techniques

In both applied science and pure mathematics, systems of linear equations frequently arise very frequently. The next section shows why.

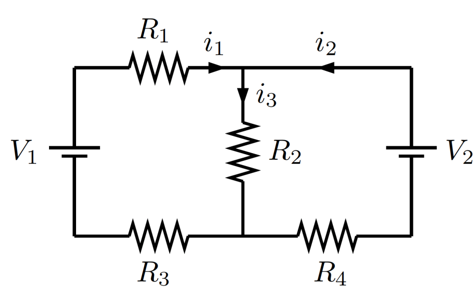
3.1 Motivations to study linear systems

In this section we provide both practical and theoretical reasons to study systems of linear equations or, more briefly, *linear systems*.

3.1.1 Practical motivations

The following worked problems have been proposed by Prof. Joel Feldman of the University of British Columbia, to whom I am very grateful.

Example 3.1.1 Consider the electrical network below.



Question: knowing that all of the all the resistors have an electric resistance of 10Ω ('ohms') and both generators produce an electromotive force by creating a difference of electric potential of $5V$ ('volts'), what is the current flowing through the resistor R_2?

Solution. To answer the question we must consider both the currents and the voltages in the network.

The *law of conservation of currents at a node* says that the algebraic sum of currents at a node is 0, i.e. the incoming currents into a node must be equal to the outgoing currents.

If we consider the top node in the network we have:

$$i_1 + i_2 - i_3 = 0. \tag{3.1}$$

Kirchhoff's voltage law says that in a closed path of the network the difference of electric potential due the generators must be equal to the voltages through the resistors. The last ones can be found thanks to Ohm law: $V = Ri$.

In the network under analysis we have two closed paths: the one on the left in which we have V_1, R_1, R_2 and R_3, and the one of the right composed by V_2, R_2, R_4, hence we can write the system

$$\begin{cases} R_1 i_1 + R_2 i_3 + R_3 i_1 = V_1 \\ R_2 i_3 + R_4 i_2 = V_2 \end{cases}, \tag{3.2}$$

having used the fact that the current flowing into a series of resistors is the same.

If we join eq. (3.1) with eqs. (3.2) and introduce the numerical data given in the exercise statement, we find the following linear system with *unknown currents*:

$$\begin{cases} 20i_1 + 10i_3 = 5 \\ 10i_3 + 10i_2 = 5 \\ i_1 + i_2 - i_3 = 0 \end{cases} \iff \begin{cases} i_1 = -i_2 - i_3 & (1) \\ -20i_2 + 30i_3 = 5 & (2) \\ 10i_2 + 10i_3 = 5 & (3) \end{cases} \underset{(2)\mapsto(2)+2\cdot(3)}{\iff} \begin{cases} i_1 = -i_2 - i_3 \\ 50i_3 = 15 \\ 10i_3 + 10i_2 = 5 \end{cases},$$

so

$$\begin{cases} i_3 = \frac{3}{10} \\ i_2 = \frac{2}{10} \\ i_1 = -\frac{2}{10} \end{cases},$$

so the current flowing through R_2, i.e. i_3 is equal to $0.3A$ ('ampères').

Notice that the current i_1 appears to be negative just for a convention of signs: since it is flowing clockwise and i_2, i_3 are flowing counterclockwise and we were interested in finding i_3, we arbitrary selected the plus sign for currents flowing counterclockwise.

Example 3.1.2 In the process of photosynthesis plants use energy from sunlight to convert carbon dioxide, CO_2, and water, H_2O, into glucose, $C_6H_{12}O_6$, and oxygen, O_2. The equation of the chemical reaction is of the form

$$x_1 CO_2 + x_2 H_2O \mapsto x_3 O_2 + x_4 C_6H_{12}O_6.$$

Question. What kind of values of x_j, $j = 1, \ldots, 4$ make sense (taking into account the conservation of mass)?

Solution. The number of atoms of hydrogen, H, carbon, C, and oxygen, O, on the left-hand side of the chemical reaction must equal that on the right-hand side. Thus, we must impose the following system

$$\begin{cases} \mathrm{H}: & 2x_2 = 12x_4 \\ \mathrm{C}: & x_1 = 6x_4 \iff x_4 = x_1/6 \\ \mathrm{O}: & 2x_1 + x_2 = 2x_3 + 6x_4 \end{cases} \iff \begin{cases} 2x_2 = 2x_1 \iff x_1 = x_2 \\ 6x_4 = x_1 \\ 2x_1 + x_1 = 2x_3 + x_1 \iff x_3 = x_1 \end{cases},$$

so, setting $x_4 = n \in \mathbb{N}$, because the number of atoms is of course a natural number, we have

$$\begin{cases} x_1 = x_2 = x_3 = 6n \end{cases},$$

and the chemical reaction can be explicitly written as follows:

$$6nCO_2 + 6nH_2O \mapsto 6nO_2 + nC_6H_{12}O_6, \quad n = 0, 1, 2, \ldots$$

$n = 0$ corresponds to the absence of molecules, while for $n = 1$ we find the canonical chemical reaction for photosynthesis

$$6CO_2 + 6H_2O \mapsto 6O_2 + C_6H_{12}O_6,$$

which means that we plants need at least 6 molecules of carbon dioxide and 6 molecules of water to perform photosynthesis, releasing 6 molecules of oxygen and 1 of glucose.

3.1.2 Theoretical motivation

Besides applied problems, we have also encountered many times in the first two chapters systems of linear equations that pop out from the theoretical study of linear spaces and maps between them. In particular, given two vector spaces V and W over the same field $\mathbb{F}$, and a linear map $f \in \mathcal{L}(V, W)$, we know that each time we fix a basis $B_V = (v_1, \ldots, v_n)$ of V and $B_W = (w_1, \ldots, w_m)$ of W, then f is uniquely associated to a matrix $A = (a_{ij})_{j=1,\ldots,n}^{i=1,\ldots,m}$ with coefficients in $\mathbb{F}$ such that, for all vector

$$v = \sum_{j=1}^{n} \lambda_j v_j \ \in V$$

if we express $f(v)$ as a linear combination of the vectors of B_W, i.e.

$$f(v) = \sum_{i=1}^{m} \mu_i w_i,$$

then we have

$$\begin{pmatrix} a_{11} & \ldots & a_{1n} \\ \vdots & & \vdots \\ a_{m1} & \ldots & a_{mn} \end{pmatrix} \begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_n \end{pmatrix} = \begin{pmatrix} \mu_1 \\ \vdots \\ \mu_m \end{pmatrix}.$$

Knowing the rules of matrix product, we can write the previous matrix equation as the following system of linear equations:

$$\begin{cases} a_{11}\lambda_1 + \cdots + a_{1n}\lambda_n = \mu_1 \\ \qquad \vdots \\ a_{m1}\lambda_1 + \cdots + a_{mn}\lambda_n = \mu_m \end{cases}.$$

In the previous chapters we had to deal only with systems of linear equations of small size, typically with three equations, which are relatively easy to solve.

However, when the number of equations and that of variables increase, it is evident that a more systematic method to solve a linear system, which *can be turned into a computer algorithm*, is needed.

Linear algebra provides such methods and this will show a first application of how important this branch of mathematics is both in theory and in practice.

3.2 General information about linear systems

Def. 3.2.1 (Linear system) *A system of linear equations, or a linear system, with m equations and n unknowns is written as follows*

$$\begin{cases} a_{11}x_1 + \dots + a_{1n}x_n = b_1 \\ \qquad\qquad \vdots \\ a_{m1}x_1 + \dots + a_{mn}x_n = b_m \end{cases}$$

and it can be rearranged in the so-called ***matrix form:***

$$AX = B,$$

where

$$A = \begin{pmatrix} a_{11} & \dots & a_{1n} \\ \vdots & & \vdots \\ a_{m1} & \dots & a_{mn} \end{pmatrix} \in M_{m,n}(\mathbb{F})$$

is called ***coefficient matrix****,*

$$X = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \in \mathbb{F}^n$$

is called ***vector of unknowns****, and*

$$B = \begin{pmatrix} b_1 \\ \vdots \\ b_m \end{pmatrix} \in \mathbb{F}^m$$

is called ***vector of known data****. Setting $B = \mathbf{0}_{\mathbb{F}^m}$, we obtain $AX = \mathbf{0}_{\mathbb{F}^m}$, which is called the* ***homogeneous linear system*** *associated to $AX = B$.*

Example 3.2.1 Given the linear system

$$\begin{cases} 3x + 2y - w - z = 0 \\ 2y + w = 4 \\ -x + -y - w + 5z = -2 \\ 5w - z = 1 \\ x - y + w = 3 \end{cases}$$

can be written as $AX = B$ with

$$A = \begin{pmatrix} 3 & 2 & -1 & -1 \\ 0 & 2 & 1 & 0 \\ -1 & -1 & -1 & 5 \\ 0 & 0 & 5 & -1 \\ 1 & -1 & 1 & 0 \end{pmatrix} \in M_{5,4}(\mathbb{F}), \quad X = \begin{pmatrix} x \\ y \\ w \\ z \end{pmatrix} \in \mathbb{F}^4, \quad B = \begin{pmatrix} 0 \\ 4 \\ -2 \\ 1 \\ 3 \end{pmatrix} \in \mathbb{F}^5.$$

By setting $B = \mathbf{0}_{\mathbb{F}^5}$ we find the homogeneous linear system $AX = \mathbf{0}_{\mathbb{F}^5}$ associated to $AX = B$.

Def. 3.2.2 (Resolution of a linear system) *To solve a linear system $AX = B$ means finding at least an explicit vector $\overline{X}$, which, inserted into the matrix equation $AX = B$, transforms it into an identity, i.e. the vector $A\overline{X} \in \mathbb{F}^m$ coincides with the vector $B \in \mathbb{F}^m$.*

If $AX = B$ has at least one solution, we say that it is ***solvable****.*

An explicit example may clarify this definition: the solution of the linear system

$$\begin{cases} x - y = 2 \\ 2x + y = 1 \end{cases} \iff \begin{pmatrix} 1 & -1 \\ 2 & 1 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 2 \\ 1 \end{pmatrix}$$

is the vector

$$\overline{X} = \begin{pmatrix} 1 \\ -1 \end{pmatrix},$$

in fact

$$\begin{pmatrix} 1 & -1 \\ 2 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ -1 \end{pmatrix} = \begin{pmatrix} 2 \\ 1 \end{pmatrix}.$$

Recalling the definitions of image and kernel of a matrix, Defs. 2.7.1 and 2.7.2, respectively, the following theorem follows immediately.

Theorem 3.2.1 *The following assertions hold.*

- *The linear system $AX = B$ has a solution if and only if $B \in \mathrm{Im}(A)$, i.e. if and only if B is a linear combination of the columns of A.*
- *The solution of the associated homogeneous linear system $AX = \mathbf{0}_{\mathbb{F}^m}$ coincide with* $\ker(A)$ *and so it is a vector subspace of $\mathbb{F}^n$.*

This theorem shows a first concrete example of why the investigation of the vector subspaces of a given vector space is so useful in linear algebra.

It turns out that the solutions of the linear system $AX = B$ and of its associated homogeneous one $AX = \mathbf{0}_{\mathbb{F}^m}$ are strictly related, as detailed in the following theorem.

Theorem 3.2.2 *If $\overline{X} \in \mathbb{F}^n$ is a particular solution of the linear system $AX = B$, then the set containing all the solutions agrees with*

$$\overline{X} + \ker(A) := \{\overline{X} + K : K \in \ker(A)\}.$$

In mathematical jargon, we say that the set of all solutions of a linear system is obtained by translating $\ker(A)$ with any particular solution $\overline{X}$.

So, *in order to know all the solutions of $AX = B$, it is enough to know just one of it and all the solutions of the associated homogeneous linear system.*

A generic solution of $AX = B$ will be expressed as $\overline{X} + K$, for a suitable $K \in \ker(A)$.

Proof.

$\boxed{\subseteq}$: let us show that $\overline{X} + K$, with *any* $K \in \ker(A)$, is a solution of $AX = B$. For that, it is sufficient to apply A to $\overline{X} + K$ and use the additivity to obtain:

$$A(\overline{X} + K) = A\overline{X} + AK = B + \mathbf{0}_{\mathbb{F}^m} = B.$$

So, the kernel of A translated by a particular solution $\overline{X}$ of $AX = B$ is subset of the set of all solutions of $AX = B$.

$\boxed{\supseteq}$: conversely, suppose that X' *is any solution of* $AX = B$, we must prove that X' can be written as $X' = \overline{X} + K$. To this aim, we consider the difference $X' - \overline{X}$ and we apply A to it, obtaining:

$$A(X' - \overline{X}) = AX' - A\overline{X} = B - B = \mathbf{0}_{\mathbb{F}^m},$$

hence $X' - \overline{X} \in \ker(A)$, i.e. it exists $K \in \ker(A)$ such that $X' - \overline{X} = K$, i.e. $X' = \overline{X} + K$, so the set of all solutions of $AX + B$ is a subset of the kernel of A translated by a particular solution of $AX = B$.

$\boxed{=}$: having proven the two opposite inclusions, we have shown that the sets coincide. □

We can now give a famous characterization of solvability for linear system through a pure matrix feature, thanks to which we can also determine whether the system has a unique solution or not. To state the theorem in a clear way we need to introduce a definition first.

Def. 3.2.3 (Augmented (or complete) matrix) *Let $AX = B$ be a linear system, then we call augmented (or complete) matrix of the system the $m \times (n+1)$ matrix*

$$\left(A \;\vdots\; B \right) = \left(\begin{array}{cccc:c} a_{11} & a_{12} & \cdots & a_{1n} & b_1 \\ a_{21} & a_{22} & \cdots & a_{2n} & b_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ a_{m1} & a_{n2} & \cdots & a_{mn} & b_m \end{array}\right)$$

obtained by providing A with a novel column, at the position $n+1$, given by the column vector B containing the known data of the linear systems.

Theorem 3.2.3 (Rouché-Capelli) [1] *Let $AX = B$ be a linear system of m equations in n unknowns. $AX = B$ is solvable if and only if*

$$\operatorname{rank}(A) = \operatorname{rank}\left(A \;\vdots\; B \right).$$

If $AX = B$ is solvable, then, denoted with r the common rank of A and $\left(A \;\vdots\; B \right)$, we have

1. *if $r = n$, then $AX = B$ has only one solution*
2. *if $r < n$, then $AX = B$ has infinite solutions which depend on $n - r$ parameters*[2]*, free to vary in $\mathbb{F}$.*

[1] Eugène Rouché 1832-1910, French mathematician; Alfredo Capelli 1855-1910, Italian mathematician.

[2] in the mathematical jargon, we say that $AX = B$ has ∞^{n-r} solution, which is just a compact symbolic way to highlight how many free parameters the solutions have.

From the theorem of Rouché-Capelli, it follows that **a linear system has**:

- **1) no solution**
- **2) a unique solution**
- **3) an infinite number of solutions**.

Proof. We first prove the characterization of solvability through the equality of the rank of the system matrix and the complete matrix.

$\boxed{\Longrightarrow}$: if $AX = B$ is solvable, then, thanks to the previous theorem, B is a linear combination of the columns of A. We recall that the rank of a matrix is the number of linearly independent columns. It follows that $\operatorname{rank}(\, A \mid B \,) = \operatorname{rank}(A)$, because enlarging a family C of vectors (the columns of A) with a vector (B) that is a linear combination of the vectors of C does not alter the number of linearly independent vectors in the family C.

$\boxed{\Longleftarrow}$: if $\operatorname{rank}(\, A \mid B \,) = \operatorname{rank}(A)$, then it means that B is not linearly independent from the column vectors of A, i.e. B is a linear combination of the columns of A and so, by the previous theorem, $AX = B$ is solvable.

Now let us suppose that $AX = B$ is solvable, the common rank of A and $(\, A \mid B \,) = \operatorname{rank}(A)$ is r and the number of unknown in n. Thanks to Theorem 3.2.2, the set of solutions of $AX = B$ is given by a particular solution $\overline{X}$ of $AX = B$ plus the elements of $\ker(A)$, hence $AX = B$ has only one solution if and only if $\ker(A) = \{\mathbf{0}_{\mathbb{F}^n}\}$. But the nullity+rank theorem guarantees that

$$n = r + \dim(\ker(A)),$$

so $AX = B$ if and only if $n = r$.

Finally, if $r < n$, then $\dim(\ker(A)) = n - r$, i.e. the elements of $\ker(A)$ can be obtained through linear combinations of $n - r$ basis vectors. In such a combination there appear exactly $n - r$ scalar coefficients, which can take any value in the field $\mathbb{F}$. $\square$

We hereby provide examples of the three possible cases that can happen when trying to solve linear systems. We will not prove the our statements for the moment, postponing the demonstrations to section 3.4 after learning the Gauss reduction method for solving linear systems.

Example 3.2.2 (Non-solvable linear system)

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

This linear system turns out to be not solvable.

Example 3.2.3 (Solvable linear system with a unique solution)

$$\begin{cases} 2x - 2y + 8z = 5 \\ 2y + 6z = 1 \\ x - 2y + 4z = -1 \\ x + 10z = 0 \end{cases} \iff \begin{cases} x = 10 \\ y = 7/2 \\ z = -1 \end{cases} .$$

The solution shown is the unique one that the system has.

Example 3.2.4 (Solvable linear system with a infinite solutions)

$$\begin{cases} 2x + 5z = 1 \\ 4x - 3y + 4z = 5 \\ 2x - y + 3z = 2 \end{cases} \iff \begin{cases} x = 1/2 - 5z/2 \\ y = -1 - 2z \\ z \text{ free to vary in } \mathbb{F}. \end{cases}$$

This time, the system has ∞^1 solutions: any value of $z \in \mathbb{F}$ provides a solution. Let us check it for just three values chosen arbitrarily: $z = 0$ and $z = 1$, $z = -2$.

If $z = 0$, then $x = 1/2$ and $y = -1$, so the system becomes

$$\begin{cases} 2(1/2) = 1 \\ 4(1/2) - 3(-1) = 5 \\ 2(1/2) - (-1) = 2 \end{cases} ,$$

all these equations are identities.

If $z = 1$, then $x = -2$ and $y = -3$, so the system becomes

$$\begin{cases} 2(-2) + 5 = 1 \\ 4(-2) - 3(-3) + 4 = 5 \\ 2(-2) - (-3) + 3 = 2 \end{cases} ,$$

all these equations are identities.

If $z = -2$, then $x = 11/2$ and $y = 3$, so the system becomes

$$\begin{cases} 2(11/2) + 5(-2) = 1 \\ 4(11/2) - 9 + 4(-2) = 5 \\ 2(11/2) - 3 + 3(-2) = 2 \end{cases} ,$$

again, all there equations are identities.

3.3 Reduction of matrices and computation of the rank

The Roché-Capelli theorem underlines once more the importance of being able to compute the rank of a matrix. In this section, we show a technique, first used by Carl Friedrich Gauss (1777-1855), the German polymath considered by many to be the greatest mathematician of all times, which is an efficiently way solve linear systems and that later turned out to be also a systematic method to compute the rank of a matrix. One of the great features of this method is that it can be run by a computer and thus automatized.

We will present the method step-by-step and with several examples.

Def. 3.3.1 (Matrix reduced by rows) *A matrix $A = (a_{ij})_{j=1,\dots,n}^{i=1,\dots,m} \in M_{mn}(\mathbb{F})$ is said to be reduced by rows if, apart from the last row, in every non-null row there exists a non-null element below which there are only zeros in the same column.*

In mathematical language, we can restate this as follows: given $i \in \{1, \dots, m-1\}$, if the i-th row is non-null, then there exists $j \in \{1, \dots, n\}$ such that $a_{ij} \neq 0$ and $a_{(i+1)j} = \cdots = a_{mj} = 0$.

Every element of a non-null row with this property is called ***special****. Every non-zero element of the last row is special.*

Example 3.3.1 The matrix

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

is reduced by rows because $a_{12} = 3$ and $a_{14} = 1$ have only 0 below them (in their corresponding columns), the second row is null and $a_{31} = 1$ has only 0 below it in the same column.

The special element of the first row are a_{12}, a_{14}, the second row does not have special elements because it is null, the only special element of the third row is a_{31} an the special elements of the fourth row are a_{43}, a_{45}.

Example 3.3.2 On the contrary, the following matrix

$$B = \begin{pmatrix} 1 & 0 & 2 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

is not reduced by rows.

The rank of a matrix reduced by rows can be computed immediately thanks to the following theorem.

Theorem 3.3.1 *The non-null rows of a matrix A reduced by rows are linearly independent. Hence, the rank of a matrix reduced by rows is the number of its non-null rows.*

To show the power of this result, without performing a single calculation, we can say that the rank of matrix of Example 3.3.1 is 3 because it is reduced by row and has 3 non-null rows.

Proof. Let A be reduced by rows. Up to a re-ordering of the rows, which of course does not affect the rank, we can suppose that the non-null rows of A are the first $r \leqslant m$. We must show that they are linearly independent, i.e. that the vector equation

$$\lambda_1(a_{11}, \ldots, a_{1n}) + \cdots + \lambda_r(a_{r1}, \ldots, a_{rn}) = \mathbf{0} \tag{3.3}$$

holds if and only if $\lambda_1 = \cdots = \lambda_r = 0$.

Let a_{1j_1} be a special elements of the first rows. Then, since all the elements below it in the same column are null, eq. (3.3) implies

$$\lambda_1 a_{1j_1} + \lambda_2 \cancelto{0}{a_{2j_1}} + \cdots + \lambda_r \cancelto{0}{a_{rj_1}} = 0 \iff \lambda_1 a_{1j_1} = 0 \underset{a_{1j_1} \neq 0}{\iff} \lambda_1 = 0.$$

By repeating this exact argument for all special elements until the row r, we find that $\lambda_1 = \cdots = \lambda_r = 0$, hence the non-null rows of a matrix reduced by rows are linearly independent. □

Def. 3.3.2 (Reduction of a matrix by rows) *Let $A \in M_{m,n}(\mathbb{F})$. To reduce A by rows means finding a matrix $A' \in M_{m,n}(\mathbb{F})$ reduced by rows such that* rank(A) =rank(A').

The reduction of a matrix by rows is *highly non-unique* and can be achieved through 3 kind of operations called **elementary transformations**. The first kind is the most important one, the other two help simplify the computations.

3.3.1 Elementary transformations on the rows of a matrix

Let $A \in M_{m,n}(\mathbb{F})$ and let $R_1, \ldots, R_m \in \mathbb{F}^n$ be its rows.

Def. 3.3.3 (E1) *The elementary transformations of the first kind on the rows of A consist in adding to a row a <u>different one</u> multiplied by a non-null coefficient.*

The notation for the E1 transformations is the following:

$$R_i \mapsto R_i + \alpha R_k, \quad i, k \in \{1, \ldots, m\},\ i \neq k,\ \alpha \in \mathbb{F},\ \alpha \neq 0.$$

Def. 3.3.4 (E2) *The elementary transformations of the second kind on the rows of A consist in exchanging one row with another.*

The notation for the E2 transformations is the following:

$$R_i \leftrightarrow R_k, \quad i, k \in \{1, \ldots, m\},\ i \neq k.$$

Def. 3.3.5 (E3) *The elementary transformations of the third kind on the rows of A consist in multiplying one row by a non null scalar $\alpha \in \mathbb{F}$.*

The notation for the E3 transformations is the following:

$$R_i \mapsto \alpha R_i, \quad i \in \{1, \ldots, m\},\ \alpha \in \mathbb{F},\ \alpha \neq 0.$$

While it is clear that E2 and E3 do not modify the linear independence of the rows, this fact is not so trivial for E1 and it must be proven.

Theorem 3.3.2 *The E1 transformations do not modify the linear independence of the rows of a matrix, i.e. the vector space generated by the original rows and the E1-transformed ones is exactly the same.*

Proof. Up to a reordering of the row indices, we can suppose that we modify R_1 in $R_1 + \alpha R_2$, $\alpha \neq 0$. We must prove that

$$\mathrm{span}(R_1, R_2, \dots, R_m) = \mathrm{span}(R_1', R_2, \dots, R_m),$$

where $R_1' = R_1 + \alpha R_2$. We will prove that the two opposite inclusions hold.

$\boxed{\supseteq}$: since $R_1' = R_1 + \alpha R_2$, R_1' is a linear combination of two rows belonging to the family $\{R_1, \dots, R_m\}$, hence $R_1' \in \mathrm{span}(R_1, R_2, \dots, R_m)$, so the vector space that $R_1', R_2, \dots, R_m$ generate cannot be larger than that generated by the family $\{R_1, \dots, R_m\}$, thus:

$$\mathrm{span}(R_1', R_2, \dots, R_m) \subseteq \mathrm{span}(R_1, R_2, \dots, R_m).$$

$\boxed{\supseteq}$: since $R_1' = R_1 + \alpha R_2$, $R_1 = R_1' - \alpha R_2$, so R_1 is a linear combination of two rows belonging to the family $\{R_1', \dots, R_m\}$. Using the same argument as before we have that:

$$\mathrm{span}(R_1, R_2, \dots, R_m) \subseteq \mathrm{span}(R_1', R_2, \dots, R_m).$$

As a consequence:

$$\mathrm{span}(R_1, R_2, \dots, R_m) = \mathrm{span}(R_1', R_2, \dots, R_m).$$

If other E1 transformations are performed, then the previous argument can be applied to them and so, no matter how many of them are performed, the vector space generated by the E1-transformed rows and the original ones will be the same. □

Now we arrive to the most important property of the E1 transformations, which explains why they are so vital for the procedure of matrix reduction.

Practical method to nullify the matrix entries below a special element with E1 transformations

- Let a_{ij} a special element of the row R_i
- All the matrix entries below a_{ij} in the same column can be written as a_{kj}, $k = i+1, \dots, m$
- To nullify the entry a_{kj}, the following E1 transformation must be applied:

$$\boxed{R_k \mapsto R_k - \frac{a_{kj}}{a_{ij}} R_i}, \quad k = i+1, \dots, m.$$

In fact:

$$\begin{aligned}
R_k - \frac{a_{kj}}{a_{ij}} R_i &= (a_{k1}, a_{k2}, \dots, a_{kj}, \dots, a_{km}) - \frac{a_{kj}}{a_{ij}} (a_{i1}, a_{i2}, \dots, a_{ij}, \dots, a_{im}) \\
&= (a_{k1}, a_{k2}, \dots, a_{kj}, \dots, a_{km}) - \left(\frac{a_{kj}}{a_{ij}} a_{i1}, \frac{a_{kj}}{a_{ij}} a_{i2}, \dots, \frac{a_{kj}}{\cancel{a_{ij}}} \cancel{a_{ij}}, \dots, \frac{a_{kj}}{a_{ij}} a_{im} \right) \\
&= (a_{k1} - \frac{a_{kj}}{a_{ij}} a_{i1}, a_{k2} - \frac{a_{kj}}{a_{ij}} a_{i2}, \dots, \cancelto{0}{a_{kj} - a_{kj}}, \dots, a_{km} - \frac{a_{kj}}{a_{ij}} a_{im}).
\end{aligned}$$

Example 3.3.3 Consider the matrix

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

A it is not reduce by rows, but we can apply the E1 transformation $R_2 \mapsto R_2 - \frac{1}{2}R_1$ obtaining

$$A' = \begin{pmatrix} 2 & 1 \\ 1 - \frac{1}{2} \cdot 2 & 3 - \frac{1}{2} \cdot 1 \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 0 & \frac{5}{2} \end{pmatrix},$$

with is reduced by rows and has 2 non-null linearly independent rows, hence its rank is 2.

PRACTICAL METHOD TO REDUCE A MATRIX BY ROWS AND COMPUTE ITS RANK

- If the matrix A has null rows, then apply the E2 transformations to set all of them as the final rows of a new matrix A_1
- Choose a non-null element of the first row of A_1 and nullify all the entries below it, in the same column, by applying the E1 transformations as described before, obtaining another matrix A_2
- Choose a non-null element of the second row of A_2 and nullify all the entries below it in the same column, obtaining another matrix A_3
- Iterate this process until it is possible. The non-null rows of the final matrix are linearly independent and their number is the rank of A.

Example 3.3.4 Reduce by rows the matrix

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

There are no null rows. We choose 2 as special element of the first row, hence we apply the E1 transformations $R_2 \mapsto R_2 - \frac{1}{2}R_1$ and $R_3 \mapsto R_3 - \frac{3}{2}R_1$, this gives rise to the matrix

$$A_1 = \begin{pmatrix} 2 & 1 & 0 \\ 1 - \frac{1}{2} \cdot 2 & 2 - \frac{1}{2} \cdot 1 & 1 - \frac{1}{2} \cdot 0 \\ 3 - \frac{3}{2} \cdot 2 & 1 - \frac{3}{2} \cdot 1 & 2 - \frac{3}{2} \cdot 0 \end{pmatrix} = \begin{pmatrix} 2 & 1 & 0 \\ 0 & \frac{3}{2} & 1 \\ 0 & -\frac{1}{2} & 2 \end{pmatrix}.$$

As we have said before, the elementary transformations E2 and E3 can simplify the computations, here we can use two times E3 to multiply the row R_2 and R_3 of A_1 by 4 and 2, respectively, thus obtaining

$$A_2 = \begin{pmatrix} 2 & 1 & 0 \\ 0 & 6 & 4 \\ 0 & -1 & 4 \end{pmatrix}.$$

We have chosen those coefficients because now we can make the entry of position $(2, 3)$ of A_2 a special element of the second row by operation the E1 transformation $R_3 \mapsto R_3 - R_2$:

$$A_3 = \begin{pmatrix} 2 & 1 & 0 \\ 0 & 6 & 4 \\ 0 & -1 - 6 & 4 - 4 \end{pmatrix} = \begin{pmatrix} 2 & 1 & 0 \\ 0 & 6 & 4 \\ 0 & -7 & 0 \end{pmatrix}.$$

A_3 is reduced by rows with 3 non-null rows, hence the rank of A is 3.

Example 3.3.5 Reduce by rows the matrix

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

Here we show how we can combine the elementary transformations to achieve a reduction more rapidly. We see that the entry of position $(1, 2)$ of A has already one 0 below it in C_2, so it is convenient to nullify the entry immediately below it in C_2. To do that we can multiply R_2 by 2 with a E3 transformation and then subtract R_1 with a E1 transformation. So, in one shot, we perform the transformation $R_2 \mapsto 2R_2 - R_1$:

$$A_1 = \begin{pmatrix} 1 & 2 & 0 & 1 \\ 2-1 & 2-2 & 2-0 & 2-1 \\ 1 & 0 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 0 & 1 \\ 1 & 0 & 2 & 1 \\ 1 & 0 & 2 & 1 \end{pmatrix}.$$

Now we simply perform $R_3 \mapsto R_3 - R_2$ in A_1, obtaining:

$$A_2 = \begin{pmatrix} 1 & 2 & 0 & 1 \\ 1 & 0 & 2 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix}.$$

A_2 is reduced by row with only two non-null rows, thence the rank of A is 2.

Since the number of linearly independent rows equals that of linearly independent columns, it should not be surprising that all we have said about matrices reduced by rows can be said about matrices reduced by columns.

Def. 3.3.6 (Matrix reduced by columns) *The matrix A is reduced by columns if A^t is reduced by rows.*

It follows that in a matrix reduced by columns there is always one non-zero element of a non-null column *at the right of which*, in the same row, there are only zeros.

Mathematicians usually prefer to apply the row reduction, for this reason, *if the number of columns of A is considerably smaller than the number of rows, then consider A^t and reduce it by rows.*

3.3.2 Reduction to row echelon form

The reduction to row echelon form is an *improvement of the row reduction method*, which, as we will soon see, *it speeds up the resolution* of linear systems.

The name echelon comes from the French word 'échelon', which means 'step of a staircase', in fact, as we are going to show, the non-null entries of a row echelon matrix form a staircase. If the matrix is square, then the row echelon form coincides with an upper triangular matrix, if not, is the most similar version of it. To reduce to row echelon form a matrix we

1. set all the null rows at the end of the matrix

2. create a special element, **normalized to 1**, in every nonzero row, called the **pivot**, which is on the right (not necessarily the immediate right) of the pivot of the previous row.

Example 3.3.6 Reduce to row echelon form the matrix

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

To have 1 at the position $(1,1)$ we can exchange the row R_3 and R_1:

$$A_1 = \begin{pmatrix} 1 & -2 & -1 & -2 \\ 3 & -6 & 3 & -3 \\ 2 & -4 & 0 & -4 \end{pmatrix}.$$

Now we have to nullify the entries below 1 appearing in the first column of A_1, we do it with the E1 transformations $R_2 \mapsto R_2 - 3R_1$ and $R_3 \mapsto R_3 - 2R_2$:

$$A_2 = \begin{pmatrix} 1 & -2 & -1 & -2 \\ 0 & 0 & 6 & 3 \\ 0 & 0 & 2 & 0 \end{pmatrix}.$$

The first row of A_2 has a normalized pivot in the position $(1,1)$, so now we start back from the second row of A_2 by dividing it by 6: $R_2 \mapsto R_2/6$:

$$A_3 = \begin{pmatrix} 1 & -2 & -1 & -2 \\ 0 & 0 & 1 & 1/2 \\ 0 & 0 & 2 & 0 \end{pmatrix}.$$

Finally, we perform $R_3 \mapsto R_3 - 2R_2$ on A_3:

$$A_4 = \begin{pmatrix} \boxed{1} & -2 & -1 & -2 \\ 0 & 0 & \boxed{1} & 1/2 \\ 0 & 0 & 0 & -1 \end{pmatrix}.$$

In the row echelon matrix above we have underlined the staircase and the two pivots.

The fact that a pivot is not necessarily at the immediate right of the pivot of the previous row implies that the steps of the staircase are not necessarily of the same size.

Let us now use the computations of the previous example to show how easy it is to establish if a linear system is solvable or not when its augmented matrix is reduced to row echelon form.

Example 3.3.7 Consider the following linear system:

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

The matrices A, X and B are

$$A = \begin{pmatrix} 2 & -4 & 0 \\ 3 & -6 & 3 \\ 1 & -2 & -1 \end{pmatrix}, \quad X = \begin{pmatrix} x \\ y \\ z \end{pmatrix}, \quad B = \begin{pmatrix} -4 \\ -3 \\ -2 \end{pmatrix}.$$

The augmented matrix of the linear system is

$$\left(A \,\vdots\, B \right) = \left(\begin{array}{ccc:c} 2 & -4 & 0 & -4 \\ 3 & -6 & 3 & -3 \\ 1 & -2 & -1 & -2 \end{array} \right),$$

which coincides with the matrix examined in Example 3.3.6, so we can take advantage of the row echelon form found in that example, which is

$$\left(\begin{array}{ccc:c} 1 & -2 & -1 & -2 \\ 0 & 0 & 1 & 1/2 \\ 0 & 0 & 0 & -1 \end{array} \right).$$

From this expression it follows that the rank of $\left(A \,\vdots\, B \right)$ is 3, but the rank of A is just 2 because the last row of the 'A part' is null. So, *the system is not solvable.*

Another way to see this is to translate the last row of the augmented matrix into a linear equation:

$$0 \cdot x + 0 \cdot y + 0 \cdot z = -1 \iff 0 = -1,$$

which is of course impossible and so the system cannot be solved.

What happens in the previous example is a specific instance of a general property.

Theorem 3.3.3 *If the augmented matrix of a linear system is reduced to row echelon form and its null rows coincide with the null rows of the A part, then* $\mathrm{rank}(A) = \mathrm{rank}\left(A \,\vdots\, B \right)$ *and the system is solvable, otherwise, the system is not solvable.*

3.4 Solution of linear systems through the Gauss reduction (or elimination) method

Now we can take advantage of the method described before to reduce a matrix to row echelon form in order to efficiently solve linear systems.

In order to do that, we need a definition and a theorem.

Def. 3.4.1 (Equivalent linear systems) *Two linear systems are said to be equivalent if they have the same set of solutions, including the empty set, which means that the systems are not solvable.*

Theorem 3.4.1 *If A' is a reduced version of the matrix A, then the linear systems $A'X = B$ and $AX = B$ are equivalent.*

Notice that the row echelon form of a matrix is a particular form of reduction, so the previous result holds also in that case.

The proof of the theorem is not difficult but quite long, so we prefer to omit it and show immediately how to find the solutions of a linear system via the method described in the examples that follow.

Example 3.4.1 Consider the following linear system:

$$\begin{cases} 2x - 2y + 8z = 5 \\ 2y + 6z = 1 \\ x - 2y + 4z = -1 \\ x + 10z = 0 \end{cases},$$

$$A = \begin{pmatrix} 2 & -2 & 8 \\ 0 & 2 & 6 \\ 1 & -2 & 4 \\ 1 & 0 & 10 \end{pmatrix}, \quad X = \begin{pmatrix} x \\ y \\ z \end{pmatrix}, \quad B = \begin{pmatrix} 5 \\ 1 \\ -1 \\ 0 \end{pmatrix}, \quad \left(A \mid B \right) = \left(\begin{array}{ccc|c} 2 & -2 & 8 & 5 \\ 0 & 2 & 6 & 1 \\ 1 & -2 & 4 & -1 \\ 1 & 0 & 10 & 0 \end{array}\right).$$

To reduce $\left(A \mid B \right)$ to row echelon form, we exchange R_1 with R_3 in order to start with 1:

$$\left(\begin{array}{ccc|c} 1 & -2 & 4 & -1 \\ 0 & 2 & 6 & 1 \\ 2 & -2 & 8 & 5 \\ 1 & 0 & 10 & 0 \end{array}\right),$$

then we operate the following E1 transformations: $R_3 \mapsto R_3 - 2R_1$, $R_4 \mapsto R_4 - R_1$, obtaining

$$\left(\begin{array}{ccc|c} 1 & -2 & 4 & -1 \\ 0 & 2 & 6 & 1 \\ 0 & 2 & 0 & 7 \\ 0 & 2 & 6 & 1 \end{array}\right).$$

We notice that $R_4 = R_2$, so we perform the E1 transformations $R_3 \mapsto R_3 - R_2$, $R_4 \mapsto R_4 - R_2$, obtaining

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

Finally, we divide R_2 by 2 and R_3 by -6:

$$\left(\begin{array}{ccc:c} 1 & -2 & 4 & -1 \\ 0 & 1 & 3 & 1/2 \\ 0 & 0 & 1 & -1 \\ 0 & 0 & 0 & 0 \end{array}\right).$$

Since the null row of the echelon reduced augmented matrix agrees with that of its A part, $\text{rank}(A) = \text{rank}(\ A \,\vdots\, B\ ) = 3 =$ number of unknowns, *the linear system is solvable and has a unique solution.*

To find it, we transform back the echelon reduced augmented matrix into a linear system without writing the last equation (which gives the identity $0 = 0$), and we solve it with a bottom-up strategy:

$$\begin{cases} x - 2y + 4z = -1 \\ y + 3z = 1/2 \\ z = -1 \end{cases} \iff \begin{cases} z = -1 \\ y + 3 \cdot (-1) = 1/2 \iff y = 7/2 \\ x - 2 \cdot (7/2) + 4 \cdot (-1) = -1 \iff x = 10 \end{cases} \iff \begin{cases} x = 10 \\ y = 7/2 \\ z = -1 \end{cases}.$$

It should now be clear *why we normalize the value of the pivot to 1*: in this way we can avoid spurious coefficients in front of the variables and we save time.

Example 3.4.2 Consider the following linear system:

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

The matrices A, X and B are

$$A = \begin{pmatrix} 2 & 0 & 5 \\ 4 & -3 & 4 \\ 2 & -1 & 3 \end{pmatrix}, \quad X = \begin{pmatrix} x \\ y \\ z \end{pmatrix}, \quad B = \begin{pmatrix} 1 \\ 5 \\ 2 \end{pmatrix}.$$

The augmented matrix of the linear system is

$$(\ A \,\vdots\, B\ ) = \left(\begin{array}{ccc:c} 2 & 0 & 5 & 1 \\ 4 & -3 & 4 & 5 \\ 2 & -1 & 3 & 2 \end{array}\right).$$

By operating $R_2 \mapsto R_2 - 2R_1$ and $R_3 \mapsto R_3 - R_1$, we find

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

Then we divide R_1 by 2 and R_2 by -3, obtaining

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

Finally, we perform $R_3 \mapsto R_3 + R_2$ and we get

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

The linear system is again solvable because the null row of the reduced echelon form of the augmented matrix coincides with the null row of the A part. The rank of A and that of the augmented matrix are both equal to 2.

However, since the number of unknowns is 3, the system will have ∞^1 solutions and the nullity of A, i.e. $\dim(\ker(A))$, will be exactly 1 by the nullity+rank theorem.

If we discard the final row of the last reduced echelon augmented matrix and we transform it back to a linear system, we find three unknowns and just two equations:

$$\begin{cases} x + 5z/2 = 1/2 \\ y + 2z = -1 \end{cases} \iff \begin{cases} y = -1 - 2z \\ x = 1/2 - 5z/2 \end{cases} \iff \begin{cases} x = 1/2 - 5z/2 \\ y = -1 - 2z \\ z \text{ free to vary in } \mathbb{F}. \end{cases}$$

We see that the solutions depend on the free parameter z.

We take this occasion to show how to compute $\ker(A)$ by studying the homogeneous system associated to $AX = B$, i.e. by considering

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

In this case the augmented matrix is

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

By repeating the sequence of operations performed before of the augmented matrix of the original linear system, we arrive to the row echelon matrix

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

corresponding to the homogeneous linear system

$$\begin{cases} x + 5z/2 = 0 \\ y + 2z = 0 \end{cases} \iff \begin{cases} x = -5z/2 \\ y = -2z \\ z \in \mathbb{F} \end{cases}.$$

Hence, all the vectors belonging to $\ker(A)$ are of the form

$$(-5z/2, -2z, z) = z(-5/2, -2, 1),$$

if we let z vary in $\mathbb{F}$, we see that all these vectors are proportional, i.e. collinear and so they are *linearly dependent*. For this reason, it is sufficient to consider just one of them, typically by choosing a (non zero!) value of z which makes the vector look 'nice', and this will constitute a basis for $\ker(A)$.

For example, we can choose $z = -2$, so that a basis of $\ker(A)$ is given by the vector $(5, 4, -2)$ and

$$\ker(A) = \text{span}((5, 4, -2)),$$

but we can also choose, e.g. $z = -1$, thus obtaining the basis vector $(5/2, 2, -1)$.

In any case, since there is one non-null vector in the basis of $\ker(A)$, we have that $\dim(\ker(A)) = 1 = \text{null}(A)$, confirming what we had previously deduced.

What we have learned in the two previous examples can be written in a general form.

Practical method to establish the solvability of the linear system $AX = B$ and then to solve it

1. Reduce the augmented matrix $\left(A \,\vdots\, B \right)$ to row echelon form.

2. Establish if the system is solvable using theorem 3.3.3.

3. If the system is solvable, then it can be solved by substitution *starting from the last equation* of the linear system corresponding to the row echelon form of $\left(A \,\vdots\, B \right)$.

   (a) First of all, the null equations are discarded.

   (b) We solve the last equation with respect to one of the unknowns.

   (c) We solve the penultimate equation with respect to one of the unknowns that do not appear in the last equation and by introducing the value of the unknown previously found

   (d) We iterate the process until arriving to the first equation.

4. In the case of solvability, by the Roché-Capelli theorem,

   - if $\text{rank}(A)$ =number of unknowns, then the solution is unique
   - if $\text{rank}(A)$ <number of unknowns, then there are infinite solutions, precisely $\infty^{\text{null}(A)}$ solutions, where $\dim(\ker(A)) = \text{null}(A) =$ number of unknowns$-\text{rank}(A)$.

3.4.1 The Cramer rule

The Cramer rule is a formula that allows us to compute the unique solution of a solvable system of n equations with n unknowns, thus represented by a *square coefficient matrix* A. Since A is square, we can compute its determinant, and it is thanks to $\det(A)$ that the Cramer rule is expressed.

Theorem 3.4.2 (Cramer rule) *Let* $AX = B$*, with*

$$A = \begin{pmatrix} a_{11} & \dots & a_{1n} \\ \vdots & & \vdots \\ a_{n1} & \dots & a_{nn} \end{pmatrix}, \quad X = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}, \quad B = \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix},$$

be a system of n *linear equations with* n *unknowns. If* $\det(A) \neq 0$*, then the system has a unique solution given by*

$$x_i = \frac{\Delta_i}{\det(A)}, \quad i = 1, \dots, n,$$

where Δ_i *is the determinant of the matrix obtained by replacing the* $i-th$ *column of* A *with* B*.*

We omit the proof of this theorem in favor of an example that shows how to apply it and how it compares to the Gauss method of reduction.

Example 3.4.3 Consider the linear system

$$\begin{cases} x + 2z = 9 \\ 2y + z = 8 \\ 4x - 3y = -2 \end{cases},$$

which can be written as $AX = B$ with

$$A = \begin{pmatrix} 1 & 0 & 2 \\ 0 & 2 & 1 \\ 4 & -3 & 0 \end{pmatrix}, \quad X = \begin{pmatrix} x \\ y \\ z \end{pmatrix}, \quad B = \begin{pmatrix} 9 \\ 8 \\ -2 \end{pmatrix}.$$

We compute the determinant of A through the Laplace development along the first row:

$$\det(A) = \det \begin{pmatrix} 2 & 1 \\ -3 & 0 \end{pmatrix} + 2 \det \begin{pmatrix} 0 & 2 \\ 4 & -3 \end{pmatrix} = 3 - 16 = -13,$$

since $\det(A) \neq 0$, the system has a unique solution that we can find using the Cramer rule:

- $\Delta_1 = \det \begin{pmatrix} 9 & 0 & 2 \\ 8 & 2 & 1 \\ -2 & -3 & 0 \end{pmatrix} = 2 \det \begin{pmatrix} 8 & 2 \\ -2 & -3 \end{pmatrix} - \det \begin{pmatrix} 9 & 0 \\ -2 & -3 \end{pmatrix} = 2(-24 + 4) - (-27) = -13$
- $\Delta_2 = \det \begin{pmatrix} 1 & 9 & 2 \\ 0 & 8 & 1 \\ 4 & -2 & 0 \end{pmatrix} = \det \begin{pmatrix} 8 & 1 \\ -2 & 0 \end{pmatrix} + 4 \det \begin{pmatrix} 9 & 2 \\ 8 & 1 \end{pmatrix} = 2 + 4(9 - 16) = -26$
- $\Delta_3 = \det \begin{pmatrix} 1 & 0 & 9 \\ 0 & 2 & 8 \\ 4 & -3 & -2 \end{pmatrix} = \det \begin{pmatrix} 2 & 8 \\ -3 & -2 \end{pmatrix} + 4 \det \begin{pmatrix} 0 & 9 \\ 2 & 8 \end{pmatrix} = -4 + 24 + 4(-18) = 20 - 72 = -52,$

so

$$x = \frac{\Delta_1}{\det(A)} = 1, \quad y = \frac{\Delta_2}{\det(A)} = 2, \quad z = \frac{\Delta_3}{\det(A)} = 4.$$

Let us compare this method with the Gauss reduction technique. The augmented matrix of the system is

$$\left(\begin{array}{ccc|c} 1 & 0 & 2 & 9 \\ 0 & 2 & 1 & 8 \\ 4 & -3 & 0 & -2 \end{array}\right).$$

We apply $R_3 \mapsto R_3 - 4R_1$:

$$\left(\begin{array}{ccc|c} 1 & 0 & 2 & 9 \\ 0 & 2 & 1 & 8 \\ 0 & -3 & -8 & -38 \end{array}\right),$$

then we divide R_2 by 2:

$$\left(\begin{array}{ccc|c} 1 & 0 & 2 & 9 \\ 0 & 1 & 1/2 & 4 \\ 0 & -3 & -8 & -38 \end{array}\right),$$

finally we apply $R_3 \mapsto R_3 + 3R_2$:

$$\left(\begin{array}{ccc|c} 1 & 0 & 2 & 9 \\ 0 & 1 & 1/2 & 4 \\ 0 & 0 & -13/2 & -26 \end{array}\right),$$

which, converted back to a linear system, gives

$$\begin{cases} x + 2z = 9 \\ y + z/2 = 4 \\ -13z/2 = -26 \implies z = 4 \end{cases} \iff \begin{cases} z = 4 \\ y + 2 = 4 \implies y = 2 \\ y + 8 = 9 \implies x = 1 \end{cases} \iff \begin{cases} x = 1 \\ y = 2 \\ z = 4 \end{cases}.$$

Thus, for linear systems with equal number of unknowns and equations the Cramer rule and the Gauss reduction methods are equivalent and one can use one or the other depending on personal taste.

However, it is important to keep in mind that, *for linear systems where the number of equations and that of the unknown do not match, the Cramer rule cannot be applied* anymore.

As a final note, recalling property 8. of Theorem 2.9.3 on the determinant, we have immediately the following result.

Theorem 3.4.3 *The determinant of a matrix is invariant under E1 transformations.*

It is useful to keep in mind this property to compute the determinant of a matrix much more easily by nullifying as many entries as possible.

Remark: *the determinant is not invariant under E2 and E3 transformations*, can you say why by looking at the properties listed in Theorem 2.9.3?

3.5 Questions about chapter 3

1. Can you invent a linear system and write the coefficient matrix, the vector of unknowns, the vector of known data and the homogeneous linear system associated to it?

2. What does precisely mean to solve a linear system? And that a linear system is solvable?

3. Given $AX = B$, can you quote a necessary and sufficient condition that involves B and A that guarantees the solvability of the linear system?

4. Given the homogeneous system $AX = 0$, can you characterize its solution space in terms of A?

5. Imagine to know a solution $\overline{X}$ of $AX = B$, how can you find all the other solutions?

6. What is the augmented matrix of a linear system?

7. Can you quote the Roché-Capelli theorem? What are the consequences of it on the number of solutions of a linear system?

8. What does it mean for a matrix to be reduced by rows?

9. What's so special about the rows of a matrix reduced by rows? What's their relation with the rank of the matrix?

10. Can you quote what are the three kinds of elementary transformations that permit to reduce a matrix by rows?

11. What is the characteristic of a matrix reduced to row echelon form?

12. Do you remember the Cramer rule? What can it be applied?

13. Why does the Cramer rule is less general than the Gauss reduction method to solve linear systems?

3.6 Exercises of chapter 3

The following exercises have the aim of testing the comprehension of the most important concepts that have been introduced in chapter 3.

1. Solve the following linear system

$$\begin{cases} x_1 + 2x_2 + x_3 + 2_x 4 + x_5 = 1 \\ 2x_1 + 4x_2 + 4x_3 + 6x_4 + x_5 = 2 \\ 3x_1 + 6x_2 + x_3 + 4x_4 + 5x_5 = 4 \\ x_1 + 2x_2 + 3x_3 + 5x_4 + x_5 = 4 \end{cases}$$

   by first guessing how many solutions the system can have.

2. Use the Cramer rule to solve the linear system

$$\begin{cases} 2x_1 + x_2 + 3x_3 = 1 \\ 4x_1 + 5x_2 + 7x_3 = 7 \\ 2x_1 - 5x_2 + 5x_3 = -7 \end{cases}$$

   trying to make the computation of the determinants as easy as possible...

3. The following table gives the number of milligrams of vitamins A, B, C contained in one gram of each of the foods F_1, F_2, F_3, F_4.

	F_1	F_2	F_3	F_4
A	1	1	1	1
B	1	3	2	1
C	4	0	1	1

   E.g., 1g of the food F_2 contains 1mg of vitamin A, 3mg of vitamin B and no vitamin C.

   A mixture is to be prepared containing precisely (for each gram):

   - 14 mg of vitamin A
   - 29 mg of vitamin B
   - 23 mg of vitamin C.

   What is the greatest amount of F_2 that can be used in the mixture?

3.6.1 Solutions of the exercises of chapter 3

The reader is *strongly encouraged* not to look at the solution of the exercises proposed in the previous page before trying to solve them.

1. Solve the following linear system

$$\begin{cases} x_1 + 2x_2 + x_3 + 2x_4 + x_5 = 1 \\ 2x_1 + 4x_2 + 4x_3 + 6x_4 + x_5 = 2 \\ 3x_1 + 6x_2 + x_3 + 4x_4 + 5x_5 = 4 \\ x_1 + 2x_2 + 3x_3 + 5x_4 + x_5 = 4 \end{cases}$$

First of all notice that: number of unknowns= 5, maximal rank =4, so there will surely be at least ∞^1 solutions, if the system is solvable.

Augmented matrix:

$$\left(A \,\vdots\, B \right) = \left(\begin{array}{ccccc:c} 1 & 2 & 1 & 2 & 1 & 1 \\ 2 & 4 & 4 & 6 & 1 & 2 \\ 3 & 6 & 1 & 4 & 5 & 4 \\ 1 & 2 & 3 & 5 & 1 & 4 \end{array}\right),$$

$R_2 \mapsto R_2 - 2R_1$, $R_3 \mapsto R_2 - 3R_1$, $R_4 \mapsto R_4 - R_1$:

$$\left(A \,\vdots\, B \right) = \left(\begin{array}{ccccc:c} 1 & 2 & 1 & 2 & 1 & 1 \\ 0 & 0 & 2 & 2 & -1 & 0 \\ 0 & 0 & -2 & -2 & 2 & 1 \\ 0 & 0 & 2 & 3 & 0 & 3 \end{array}\right),$$

$R_3 \mapsto R_3 + R_2$, $R_4 \mapsto R_4 - R_2$:

$$\left(A \,\vdots\, B \right) = \left(\begin{array}{ccccc:c} 1 & 2 & 1 & 2 & 1 & 1 \\ 0 & 0 & 2 & 2 & -1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 3 \end{array}\right),$$

$R_2 \mapsto R_2/2$, $R_3 \leftrightarrow R_4$:

$$\left(A \,\vdots\, B \right) = \left(\begin{array}{ccccc:c} 1 & 2 & 1 & 2 & 1 & 1 \\ 0 & 0 & 1 & 1 & -1/2 & 0 \\ 0 & 0 & 0 & 1 & 1 & 3 \\ 0 & 0 & 0 & 0 & 1 & 1 \end{array}\right).$$

We can now 'backsolve' because the matrix is in row echelon form and the last equation is an identity:

$$\begin{cases} x_5 = 1 \\ x_4 + 1 = 3 \iff x_4 = 2 \\ x_3 + 2 - 1/2 = 0 \iff x_3 = -3/2 \\ x_1 + 2x_2 - 3/2 + 4 + 1 = 1 \iff x_1 = -5/2 - 2x_2 \\ x_2 = \lambda \in \mathbb{F} \end{cases} \iff \begin{cases} x_1 = -5/2 - 2\lambda \\ x_2 = \lambda \\ x_3 = -3/2 \\ x_4 = 2 \\ x_5 = 1 \end{cases}.$$

So, there are indeed ∞^1 solutions.

2. Use the Cramer rule to solve the linear system

$$\begin{cases} 2x_1 + x_2 + 3x_3 = 1 \\ 4x_1 + 5x_2 + 7x_3 = 7 \\ 2x_1 - 5x_2 + 5x_3 = -7 \end{cases} .$$

Coefficient matrix:

$$A = \begin{pmatrix} 2 & 1 & 3 \\ 4 & 5 & 7 \\ 2 & -5 & 5 \end{pmatrix},$$

it has no zeros, let us make them appear by using E1 transformations, which do not change the determinant. By performing $R_2 \mapsto R_2 - 2R_1$ and $R_3 \mapsto R_3 - R_1$ we find

$$A_1 = \begin{pmatrix} 2 & 1 & 3 \\ 0 & 3 & 1 \\ 0 & -6 & 2 \end{pmatrix},$$

finally $R_3 \mapsto R_3 + 2R_2$

$$A_2 = \begin{pmatrix} 2 & 1 & 3 \\ 0 & 3 & 1 \\ 0 & 0 & 4 \end{pmatrix},$$

so

$$\det(A) = \det(A_2) = 2 \det \begin{pmatrix} 3 & 1 \\ 0 & 4 \end{pmatrix} = 24 \neq 0,$$

so A is invertible and we can use the Cramer rule.

- $\Delta_1 = \det \begin{pmatrix} 1 & 1 & 3 \\ 7 & 5 & 7 \\ -7 & -5 & 5 \end{pmatrix} \underset{\substack{R_2 \mapsto R_2 - 7R_1 \\ R_3 \mapsto R_3 + R_2}}{=} \det \begin{pmatrix} 1 & 1 & 3 \\ 0 & -2 & -14 \\ 0 & 0 & 12 \end{pmatrix} = -24$
- $\Delta_2 = \det \begin{pmatrix} 2 & 1 & 3 \\ 4 & 7 & 7 \\ 2 & -7 & 5 \end{pmatrix} \underset{\substack{R_2 \mapsto R_2 - 2R_1 \\ R_3 \mapsto R_3 - R_1}}{=} \det \begin{pmatrix} 2 & 1 & 3 \\ 0 & 5 & 1 \\ 0 & -8 & 2 \end{pmatrix} = 36$
- $\Delta_3 = \det \begin{pmatrix} 2 & 1 & 1 \\ 4 & 5 & 7 \\ 2 & -5 & -7 \end{pmatrix} \underset{\substack{R_2 \mapsto R_2 - 2R_1 \\ R_3 \mapsto R_3 - R_1}}{=} \det \begin{pmatrix} 2 & 1 & 1 \\ 0 & 3 & 5 \\ 0 & -6 & -8 \end{pmatrix} = 12.$

In the computation of Δ_i, $i = 1, 2, 3$, we have used the Laplace development along the first column at the end.

We have:

$$x = \frac{\Delta_1}{\det(A)} = -\frac{24}{24} = -1, \quad y = \frac{\Delta_2}{\det(A)} = \frac{36}{24} = 3/2, \quad z = \frac{\Delta_3}{\det(A)} = \frac{12}{24} = 1/2.$$

3. This question may seem odd at first sight, but we will soon understand its meaning by calling x_j the amount of food F_j used in the mixture, $j = 1, \ldots, 4$. Since we have to use all the foods in order to create the mixture, the data assigned requires that the following linear system has to be solved

$$\begin{cases} x_1 + x_2 + x_3 + x_4 = 14 \\ x_1 + 3x_2 + 2x_3 + x_4 = 29 \\ 4x_1 + x_3 + x_4 = 23 \end{cases} .$$

Let us reduce in row echelon form the augmented matrix of the linear system:

$$\left(\begin{array}{cccc|c} 1 & 1 & 1 & 1 & 14 \\ 1 & 3 & 2 & 1 & 29 \\ 4 & 0 & 1 & 1 & 23 \end{array}\right) \underset{\substack{R_2 \mapsto R_1 \\ R_3 \mapsto R_3 - 4R_1}}{\mapsto} \left(\begin{array}{cccc|c} 1 & 1 & 1 & 1 & 14 \\ 0 & 2 & 1 & 0 & 15 \\ 0 & -4 & -3 & -3 & -33 \end{array}\right) \underset{R_3 \mapsto R_3 + 2R_2}{\mapsto} \left(\begin{array}{cccc|c} 1 & 1 & 1 & 1 & 14 \\ 0 & 2 & 1 & 0 & 15 \\ 0 & 0 & -1 & -3 & -3 \end{array}\right),$$

the rank is 3 and the number of unknown is 4, so we have ∞^1 solutions. To find them we write:

$$\begin{cases} x_1 + x_2 + x_3 + x_4 = 14 \\ 2x_2 + x_3 = 15 \\ -x_3 - 3x_4 = -3 \end{cases} \iff \begin{cases} x_4 \in \mathbb{R} \\ x_3 = 3 - 3x_4 \\ 2x_2 + 3 - 3x_4 = 15 \iff x_2 = 6 + \frac{3}{2}x_4 \\ x_1 + 6 + \frac{3}{2}x_4 + 3 - 3x_4 + x_4 = 14 \iff x_1 = 5 + \frac{x_4}{2} \end{cases},$$

hence the *mathematical solutions* of the system are

$$\begin{cases} x_1 = 5 + \frac{\alpha}{2} \\ x_2 = 6 + \frac{3}{2}\alpha \\ x_3 = 3 - 3\alpha \\ x_4 = \alpha \in \mathbb{R} \end{cases} .$$

We have underlined that the ones above are the mathematical solutions of the system, however, when we deal with real-world problems, we must always *interpret* the solutions in a meaningful way. In our case, the amount of foods x_j must be strictly positive, and we see that, if $\alpha > 0$, then $x_1, x_2 > 0$, but x_3 may be negative, hence we must impose the constraint

$$x_3 = 3 - 3\alpha > 0 \iff x_3 = 3(1 - \alpha) > 0 \iff \alpha \in (0, 1),$$

since we are considering $\alpha > 0$.

So, the answer to the question is that the maximal amount of food F_2 that can be used in the mixture is

$$x_2 \underset{\alpha \to 1}{\to} 6 + \frac{3}{2} = \frac{15}{2} = 7.5\text{mg}.$$

Actually, in order to avoid $x_3 = 0$, we should use a little less of 7.5mg of F_2. For example, if we set $\alpha = 0.99$, our mixture would be

$$(5 + 0.99/2)F_1 + (6 + 3/2 \cdot 0.99)F_2 + (3 - 3 \cdot 0.99)F_3 + 0.99F_4,$$

i.e. the required mixture with the largest amount of food F_2 is:

$$5.495\, F_1 + 7.485\, F_2 + 0.03\, F_3 + 0.99\, F_4.$$