# Linear Algebra

E. Kowalski

ETH Zürich – Fall 2015 and Spring 2016
Version of September 15, 2016
kowalski@math.ethz.ch

# Contents

CHAPTER 1

# Preliminaries

We assume knowledge of:

- Proof by induction and by contradiction
- Complex numbers
- Basic set-theoretic definitions and notation
- Definitions of maps between sets, and especially injective, surjective and bijective maps
- Finite sets and cardinality of finite sets (in particular with respect to maps between finite sets).

We denote by $\mathbf{N} = \{1, 2, \ldots\}$ the set of all natural numbers. (In particuler, $0 \notin \mathbf{N}$).

CHAPTER 2

# Vector spaces and linear maps

Before the statement of the formal definition of a field, a field $\mathbf{K}$ is either $\mathbf{Q}$, $\mathbf{R}$, or $\mathbf{C}$.

## 2.1. Matrices and vectors

Consider a system of linear equations

$$\begin{cases} a_{11}x_1 + \cdots + a_{1n}x_n = b_1 \\ \cdots \\ a_{m1}x_1 + \cdots + a_{mn}x_n = b_m \end{cases}$$

with $n$ unknowns $(x_1, \ldots, x_n)$ in $\mathbf{K}$ and coefficients $a_{ij}$ in $\mathbf{K}$, $b_i$ in $\mathbf{K}$. It is represented concisely by the equation

$$f_A(x) = b$$

where $A = (a_{ij})_{\substack{1\leqslant i\leqslant m \\ 1\leqslant j\leqslant n}}$ is the *matrix*

$$A = \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \cdots & \cdots & \cdots \\ a_{m1} & \cdots & a_{mn} \end{pmatrix}$$

with $m$ rows and $n$ columns, $b$ is the column vector

$$b = \begin{pmatrix} b_1 \\ \vdots \\ b_m \end{pmatrix},$$

$x$ is the column vector with coefficients $x_1, \ldots, x_n$, and $f_A$ is the map $f_A : \mathbf{K}^n \to \mathbf{K}^m$ defined by

$$f_A\Big(\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}\Big) = \begin{pmatrix} a_{11}x_1 + \cdots + a_{1n}x_n \\ \cdots \\ a_{m1}x_1 + \cdots + a_{mn}x_n \end{pmatrix}.$$

We use the notation $M_{m,n}(\mathbf{K})$ for the set of all matrices with $m$ rows and $n$ columns and coefficients in $\mathbf{K}$, and $\mathbf{K}^n$ or $M_{n,1}(\mathbf{K})$ for the set of all columns vectors with $n$ rows and coefficients in $\mathbf{K}$. We will also use the notation $\mathbf{K}_n$ for the space of row vectors with $n$ columns.

We want to study the equation $f_A(x) = b$ by composing with other maps: if $f_A(x) = b$, then $g(f_A(x)) = g(b)$ for any map $g$ defined on $\mathbf{K}^m$. If $g$ is bijective, then conversely if $g(f_A(x)) = g(b)$, we obtain $f_A(x) = b$ by applying the inverse map $g^{-1}$ to both sides. We do this with $g$ also defined using a matrix. This leads to matrix products.

## 2.2. Matrix products

THEOREM 2.2.1. *Let $m$, $n$, $p$ be natural numbers. Let $A \in M_{m,n}(\mathbf{K})$ be a matrix with $m$ rows and $n$ columns, and let $B \in M_{p,m}(\mathbf{K})$ be a matrix with $p$ rows and $m$ columns. Write*

$$A = (a_{ij})_{\substack{1\leqslant i\leqslant m,\\ 1\leqslant j\leqslant n}} \qquad B = (b_{ki})_{\substack{1\leqslant k\leqslant p.\\ 1\leqslant i\leqslant m}}$$

*Consider the map $f$ obtained by composition*

$$\mathbf{K}^n \xrightarrow{f_A} \mathbf{K}^m \xrightarrow{f_B} \mathbf{K}^p,$$

*that is, $f = f_B \circ f_A$. Then we have $f = f_C$ where $C \in M_{p,n}(\mathbf{K})$ is the matrix $C = (c_{kj})_{\substack{1\leqslant k\leqslant p\\ 1\leqslant j\leqslant n}}$ with*

$$\begin{aligned} c_{kj} &= b_{k1}a_{1j} + b_{k2}a_{2j} + \cdots + b_{km}a_{mj} \\ &= \sum_{i=1}^{m} b_{ki}a_{ij}. \end{aligned}$$

PROOF. Let $x = (x_j)_{1\leqslant j\leqslant n} \in \mathbf{K}^n$. We compute $f(x)$ and check that this is the same as $f_C(x)$. First we get by definition

$$f_A(x) = y,$$

where $y = (y_i)_{1\leqslant i\leqslant m}$ is the row vector such that

$$y_i = a_{i1}x_1 + \cdots + a_{in}x_n = \sum_{j=1}^{n} a_{ij}x_j.$$

Then we get $f(x) = f_B(y)$, which is the row vector $(z_k)_{1\leqslant k\leqslant p}$ with

$$z_k = b_{k1}y_1 + \cdots + b_{km}y_m = \sum_{i=1}^{m} b_{ki}y_i.$$

Inserting the value of $y_i$ in this expression, this is

$$z_k = \sum_{i=1}^{m} b_{ki} \sum_{j=1}^{n} a_{ij}x_j = \sum_{j=1}^{n} c_{kj}x_j$$

where

$$c_{kj} = b_{k1}a_{1j} + \cdots + b_{km}a_{mj} = \sum_{i=1}^{m} b_{ki}a_{ij}.$$

□

EXERCISE 2.2.2. Take $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ and $B = \begin{pmatrix} x & y \\ z & t \end{pmatrix}$ and check the computation completely.

DEFINITION 2.2.3 (Matrix product). For $A$ and $B$ as above, the matrix $C$ is called the **matrix product** of $B$ and $A$, and is denoted $C = BA$.

EXAMPLE 2.2.4. (1) For $A \in M_{m,n}(\mathbf{K})$ and $x \in \mathbf{K}^n$, if we view $x$ as a column vector with $n$ rows, we can compute the product $Ax$ corresponding to the composition

$$\mathbf{K} \xrightarrow{f_x} \mathbf{K}^n \xrightarrow{f_A} \mathbf{K}^m.$$

Using the formula defining $f_x$ and $f_A$ and the matrix product, we see that

$$Ax = \begin{pmatrix} a_{11}x_1 + \cdots + a_{1n}x_n \\ \cdots \\ a_{m1}x_1 + \cdots + a_{mn}x_n \end{pmatrix} = f_A(x).$$

This means that $f_A$ can also be interpreted as the map that maps a vector $x$ to the matrix product $Ax$.

(2) Consider $B \in M_{k,m}(\mathbf{K})$, $A \in M_{m,n}(\mathbf{K})$. Let $C = BA$, and write $A = (a_{ij})$, $B = (b_{kj})$, $C = (c_{ki})$. Consider an integer $j$, $1 \leqslant j \leqslant n$ and let $A_j$ be the $j$-th column of $A$:

$$A_j = \begin{pmatrix} a_{1j} \\ \vdots \\ a_{nj} \end{pmatrix}.$$

We can then compute the matrix product $BA_j$, which is an element of $M_{k,1}(\mathbf{K}) = \mathbf{K}^k$:

$$BA_j = \begin{pmatrix} b_{11}a_{1j} + b_{12}a_{2j} + \cdots + b_{1n}a_{nj} \\ \vdots \\ b_{p1}a_{1j} + b_{p2}a_{2j} + \cdots + b_{pn}a_{nj} \end{pmatrix}.$$

Comparing with the definition of $C$, we see that

$$BA_j = \begin{pmatrix} c_{1j} \\ \vdots \\ c_{pj} \end{pmatrix}$$

is the $j$-th column of $C$. So the columns of the matrix product are obtained by products of matrices with column vectors.

PROPOSITION 2.2.5 (Properties of the matrix product). (1) *Given positive integers $m$, $n$ and matrices $A$ and $B$ in $M_{m,n}(\mathbf{K})$, we have $f_A = f_B$ if and only if $A = B$. In particular, if a map $f : \mathbf{K}^n \to \mathbf{K}^m$ is of the form $f = f_A$ for some matrix $A \in M_{m,n}(\mathbf{K})$, then this matrix is unique.*

(2) *Given positive integers $m$, $n$, $p$ and $q$, and matrices*

$$A = (a_{ij})_{\substack{1\leqslant i\leqslant m,\\ 1\leqslant j\leqslant n}} \qquad B = (b_{ki})_{\substack{1\leqslant k\leqslant p,\\ 1\leqslant i\leqslant m}} \qquad C = (c_{lk})_{\substack{1\leqslant l\leqslant q,\\ 1\leqslant k\leqslant p}}$$

*defining maps*

$$\mathbf{K}^n \xrightarrow{f_A} \mathbf{K}^m \xrightarrow{f_B} \mathbf{K}^p \xrightarrow{f_C} \mathbf{K}^q,$$

*we have the equality of matrix products*

$$C(BA) = (CB)A.$$

In particular, for any $n \geqslant 1$, the product of matrices is an operation on $M_{n,n}(\mathbf{K})$ (the product of matrices $A$ and $B$ which have both $n$ rows and $n$ columns is a matrix of the same size), and it is associative: $A(BC) = (AB)C$ for all matrices $A$, $B$, $C$ in $M_{n,n}(\mathbf{K})$.

PROOF. (1) For $1 \leqslant i \leqslant n$, consider the particular vector $e_i$ with all coefficients 0, except that the $i$-th coefficient is 1:

$$e_1 = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \quad e_2 = \begin{pmatrix} 0 \\ 1 \\ 0 \\ \vdots \end{pmatrix}, \quad \cdots, \quad e_n = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix}.$$

Computing the matrix product $f_A(e_i) = Ae_i$, we find that

$$f_A(e_i) = \begin{pmatrix} a_{1i} \\ \vdots \\ a_{mi} \end{pmatrix}, \tag{2.1}$$

which is the $i$-th column of the matrix $A$. Therefore, if $f_A = f_B$, the $i$-column of $A$ and $B$ are the same (since $f_A(e_i) = f_B(e_i)$), which means that $A$ and $B$ are the same (since this is true for all columns).

(3) Since composition of maps is associative, we get

$$(f_C \circ f_B) \circ f_A = f_C \circ (f_B \circ f_A),$$

or $f_{CB} \circ f_A = f_C \circ f_{BA}$, or even $f_{(CB)A} = f_{C(BA)}$, which by (1) means that $(CB)A = C(BA)$. ☐

Exercise 2.2.6. Check directly using the formula for the matrix product that $C(BA) = (CB)A$.

Now we define two additional operations on matrices and vector: (1) addition; (2) multiplication by an element $t \in \mathbf{K}$.

Definition 2.2.7 (Operations and special matrices). (1) For $m$, $n$ natural numbers and $A = (a_{ij})_{\substack{1 \leqslant i \leqslant m \\ 1 \leqslant j \leqslant n}}$, $B = (b_{ij})_{\substack{1 \leqslant i \leqslant m \\ 1 \leqslant j \leqslant n}}$ matrices in $M_{m,n}(\mathbf{K})$, the **sum** $A + B$ is the matrix

$$A + B = (a_{ij} + b_{ij})_{\substack{1 \leqslant i \leqslant m \\ 1 \leqslant j \leqslant n}} \in M_{m,n}(\mathbf{K}).$$

(2) For $t \in \mathbf{K}$, for $m$, $n$ natural numbers and $A = (a_{ij})_{\substack{1 \leqslant i \leqslant m \\ 1 \leqslant j \leqslant n}}$ a matrix in $M_{m,n}(\mathbf{K})$, the **product** $tA$ is the matrix

$$tA = (ta_{ij})_{\substack{1 \leqslant i \leqslant m \\ 1 \leqslant j \leqslant n}} \in M_{m,n}(\mathbf{K}).$$

(3) For $m$, $n$ natural numbers, the **zero matrix** $0_{mn}$ is the matrix in $M_{m,n}(\mathbf{K})$ with all coefficients 0.

(4) For $n$ a natural number, the **unit matrix** $1_n \in M_{n,n}(\mathbf{K})$ is the matrix with coefficients $a_{ij} = 0$ if $i \neq j$ and $a_{ii} = 1$ for $1 \leqslant i \leqslant n$.

Example 2.2.8. For instance:

$$1_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \qquad 1_3 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

One computes that for any $n \geqslant 1$, we have

$$f_{1_n}(x) = x$$

for all $x \in \mathbf{K}^n$. This means that $f_{1_n}$ is the identity map $\mathrm{Id}_{\mathbf{K}^n}$.

PROPOSITION 2.2.9. *For $m$, $n$ natural numbers, the following rules apply:*

$$0_{m,n} + A = A + 0_{m,n} = A, \quad (A \in M_{m,n}(\mathbf{K}))$$
$$1_m A = A, \qquad A 1_n = A, \quad (A \in M_{m,n}(\mathbf{K}))$$
$$0_{p,m} A = 0_{p,n}, \qquad A 0_{n,p} = 0_{m,p}, \quad (A \in M_{m,n}(\mathbf{K}))$$
$$A_1 + A_2 = A_2 + A_1, \quad (A_1 + A_2) + A_3 = A_1 + (A_2 + A_3), \quad (A_i \in M_{m,n}(\mathbf{K}))$$
$$0 \cdot A = 0_{m,n}, \quad (A \in M_{m,n}(\mathbf{K}))$$
$$(t_1 t_2) A = t_1(t_2 A), \quad (A \in M_{m,n}(\mathbf{K}),\ t \in \mathbf{K})$$
$$A_1(tA_2) = t(A_1A_2) = (tA_1)A_2, \quad (A_1 \in M_{m,n}(\mathbf{K}),\ A_2 \in M_{p,n}(\mathbf{K}),\ t \in \mathbf{K})$$
$$t(A_1 + A_2) = tA_1 + tA_2, \quad (A_i \in M_{m,n}(\mathbf{K}),\ t \in \mathbf{K})$$
$$(t_1 + t_2)A = t_1 A + t_2 A, \quad (A \in M_{m,n}(\mathbf{K}),\ t_i \in \mathbf{K})$$
$$(B_1 + B_2)A = B_1 A + B_2 A, \quad (B_i \in M_{p,m}(\mathbf{K}), \quad A \in M_{m,n}(\mathbf{K})),$$
$$B(A_1 + A_2) = BA_1 + BA_2, \quad (B \in M_{p,m}(\mathbf{K}), \quad A_i \in M_{m,n}(\mathbf{K})).$$

PROOF. We check only the last property, which is the most complicated in notation. We write $B = (b_{ki})_{\substack{1 \leqslant k \leqslant p \\ 1 \leqslant i \leqslant m}}$ and

$$A_1 = (a_{ij})_{\substack{1 \leqslant i \leqslant m, \\ 1 \leqslant j \leqslant n}}, \qquad A_2 = (a'_{ij})_{\substack{1 \leqslant i \leqslant m. \\ 1 \leqslant j \leqslant n}}$$

The matrix $A_1 + A_2$ has coefficients $c_{ij} = a_{ij} + a'_{ij}$. The matrix $B(A_1 + A_2)$ has $(k, j)$-coefficient equal to

$$\begin{aligned} b_{k1}c_{1j} + \cdots + b_{km}c_{mj} &= b_{k1}(a_{1j} + a'_{1j}) + \cdots + b_{km}(a_{mj} + a'_{mj}) \\ &= (b_{k1}a_{1j} + \cdots + b_{km}a_{mj}) + (b_{k1}a'_{1j} + \cdots + b_{km}a'_{mj}) \end{aligned}$$

which is the same as the sum of the $(k, j)$-coefficient of $BA_1$ and that of $BA_2$. This means that $B(A_1 + A_2) = BA_1 + BA_2$. ☐

For $n$ a natural number, $k \geqslant 0$ integer and $A \in M_{n,n}(\mathbf{K})$, we write $A^0 = 1_n$ and $A^k = A \cdot A \cdots A$ (with $k$ factors) for $k \geqslant 1$. We then have $A^{k+l} = A^k A^l$ for all $k$, $l \geqslant 0$.

We also write $-A = (-1) \cdot A$ and $A_1 - A_2 = A_1 + (-A_2)$, so that for instance $A - A = (1-1)A = 0 \cdot A = 0_{mn}$.

EXAMPLE 2.2.10. Warning! The rules of multiplication of numbers are not always true for matrices!

(1) It can be that a non-zero matrix $A \in M_{m,n}(\mathbf{K})$ does not have an “inverse” $B$ such that $AB = BA = 1$. For instance, the matrix

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

is such that $A^2 = 0_{2,2}$. If there was a matrix with $BA = 1_2$, then we would get $0_{2,2} = B0_{2,2} = BA^2 = (BA)A = 1_2 A = A$, which is not the case.

(2) It may be that $AB \neq BA$.

## 2.3. Vector spaces and linear maps

Let $\mathbf{K}$ be a field.

Definition 2.3.1 (Vector space). A **K-vector space**, or **vector space over K**, is a set $V$ with a special element $0_V$ (the zero vector in $V$) and with two operations

$$+_V \begin{cases} V \times V \to V \\ (v_1, v_2) \mapsto v_1 +_V v_2 \end{cases}$$

("addition of vectors") and

$$\cdot_V \begin{cases} \mathbf{K} \times V \to V \\ (t, v) \mapsto t \cdot_V v, \end{cases}$$

("multiplication by elements of **K**") such that the following rules are valid:

$$0_V + v = v + 0_V = v \quad (v \in V) \tag{2.2}$$

$$0 \cdot_V v = 0_V, \quad 1 \cdot_V v = v \quad (v \in V) \tag{2.3}$$

$$v_1 +_V v_2 = v_2 +_V v_1 \quad (v_i \in V) \tag{2.4}$$

$$v_1 +_V (v_2 +_V v_3) = (v_1 +_V v_2) +_V v_3 \quad (v_i \in V) \tag{2.5}$$

$$(t_1 t_2) \cdot_V v = t_1 \cdot_V (t_2 \cdot_V v) \quad (t_i \in \mathbf{K},\ v \in V) \tag{2.6}$$

$$t \cdot_V (v_1 +_V v_2) = t \cdot_V v_1 +_V t \cdot_V v_2 \quad (t \in \mathbf{K},\ v_i \in V) \tag{2.7}$$

$$(t_1 + t_2) \cdot_V v = t_1 \cdot_V v +_V t_2 \cdot_V v \quad (t_i \in \mathbf{K},\ v \in V). \tag{2.8}$$

We write $-v = (-1) \cdot_V v$ and $v_1 - v_2 = v_1 +_V (-v_2)$. In particular we get $v - v = (1 + (-1)) \cdot_V v = 0 \cdot_V v = 0$ using (2.8) and (2.3). For any integer $n \in \mathbf{Z}$ and $v \in V$, we write

$$nv = v +_V v +_V \cdots +_V v \text{ (with } n \text{ summands), if } n \geqslant 0, \quad nv = (-n)(-v) \text{ if } n < 0.$$

We then have $(n + m)v = nv +_V mv$ for all $n$ and $m$ in $\mathbf{Z}$, and $nv = n \cdot_V v$, where $n$ is viewed as an element of **K**.

Exercise 2.3.2. Check these last assertions.

Lemma 2.3.3. *In a* **K***-vector space, for* $t \in \mathbf{K}$ *and* $v \in V$*, we have* $t \cdot_V v = 0$ *if and only if either* $t = 0$ *or* $v = 0_V$*.*

Proof. If $t \neq 0$, we can multiply the formula $t \cdot_V v = 0$ by $t^{-1} \in \mathbf{K}$, and we get

$$t^{-1} \cdot_V (t \cdot_V v) = t^{-1} \cdot 0_V = 0_V$$

(by (2.3)). On the other hand, by (2.5) followed by the second part of (2.3), this is $(t^{-1}t) \cdot_V v = 1 \cdot_V v = v$. This means that if $t \neq 0$, the vector $v$ is $0_V$. ☐

Definition 2.3.4 (Linear map). Let $V$ and $W$ be vector spaces over **K**. A map

$$f : V \to W$$

is called a **linear map** (or a **K**-linear map) if for all $t_1$ and $t_2 \in \mathbf{K}$ and all $v_1$, $v_2 \in V$, we have

$$f(t_1 \cdot_V v_1 +_V t_2 \cdot_V v_2) = t_1 \cdot_W f(v_1) +_W t_2 \cdot_W f(v_2).$$

Once we abbreviate the notation to remove the subscripts in the operations, this becomes simply

$$f(t_1 v_1 + t_2 v_2) = t_1 f(v_1) + t_2 f(v_2).$$

We also get then $f(v_1 - v_2) = f(1 \cdot v_1 + (-1) \cdot v_2) = 1 \cdot f(v_1) + (-1) \cdot f(v_2) = f(v_1) - f(v_2)$. Furthermore, by induction, we get

$$f(t_1 v_1 + \cdots + t_n v_n) = t_1 f(v_1) + \cdots + t_n f(v_n)$$

for any $n \geqslant 1$ and elements $t_i \in \mathbf{K}$, $v_i \in V$.

LEMMA 2.3.5. *If $f : V \to W$ is linear, then $f(0_V) = 0_W$.*

PROOF. Fix any vector $v \in V$. Then

$$\begin{aligned} f(0_V) = f(v - v) &= f(1 \cdot v + (-1) \cdot v) \\ &= 1 \cdot f(v) + (-1) \cdot f(v) = (1 + (-1))f(v) = 0 \cdot f(v) = 0_W. \end{aligned}$$

□

EXAMPLE 2.3.6. (1) A vector space is never empty since it contains the zero vector. If $V = \{x\}$ is a set with one element, defining

$$0_V = x, \qquad a +_V b = x, \qquad t \cdot_V a = x$$

for all $a$ and $b \in V$ and $t \in \mathbf{K}$, we see that the conditions of the definition holds (because they all state that two elements of $V$ should be equal, and $V$ has only one element, which means that any equality between elements of $V$ holds). This vector space is called the *zero space*, and usually we will write $V = \{0\}$ for this space.

(2) Let $m$, $n \geqslant 1$ be integers. The set $V = M_{m,n}(\mathbf{K})$ of matrices with $m$ rows and $n$ columns is a vector space with the zero matrix $0_{m,n}$ as zero vector, and the addition of matrices and multiplication by elements of $\mathbf{K}$ defined in Section 2.2 as operations. Indeed, Proposition 2.2.9 gives all desired conditions.

In particular (taking $n = 1$) the space $\mathbf{K}^m$ of column vectors with $m$ rows is a vector space with addition of vectors and multiplication by elements of $\mathbf{K}$. If $m = n = 1$, we see that $\mathbf{K}$ itself is a $\mathbf{K}$-vector space. The operations on $\mathbf{K}$ are then the same as the usual operations (addition of elements of $\mathbf{K}$ and multiplication of elements of $\mathbf{K}$).

Fix a matrix $A \in M_{m,n}(\mathbf{K})$. The map

$$f_A : \mathbf{K}^n \longrightarrow \mathbf{K}^m$$

is then *linear*: indeed, we have seen that $f_A(x) = Ax$, and therefore

$$f_A(t_1x_1 + t_2x_2) = A(t_1x_1 + t_2x_2) = t_1Ax_1 + t_2Ax_2 = t_1f_A(x_1) + t_2f_A(x_2)$$

for all $t_i \in \mathbf{K}$ and $x_i \in \mathbf{K}^n$.

(3) Let $X$ be an arbitrary set and let $V$ be a fixed $\mathbf{K}$-vector space (for instance, $V = \mathbf{K}$). Define

$$W = \{f : X \longrightarrow V\},$$

the set of all possible maps from $X$ to $V$, with no conditions or restrictions on the values of $f$.

Define in $W$ the zero vector $0_W$ as the function $f$ such that $f(x) = 0$ for all $x \in X$. Define the sum $f_1 + f_2$ of two functions $f_i \in W$ by

$$(f_1 + f_2)(x) = f_1(x) +_V f_2(x) \text{ for all } x \in X,$$

and the product $tf$ of a number $t \in \mathbf{K}$ and a function $f \in W$ by

$$(tf)(x) = t \cdot_V f(x)$$

for all $x \in X$.

PROPOSITION 2.3.7. *The set $W$ with $0_W$, this addition and this multiplication by elements of $\mathbf{K}$, is a $\mathbf{K}$-vector space.*

PROOF. All the verifications of the conditions in the definition proceed in the same way, so we only check for instance that associativity $f_1 + (f_2 + f_3) = (f_1 + f_2) + f_3$ of addition.

Let $g_1 = f_1 + (f_2 + f_3)$ and $g_2 = (f_1 + f_2) + f_3$. Two maps from $X$ to $V$ are equal if and only if they take the same value for all $x \in X$. For $x \in X$, the definition of addition shows that

$$g_1(x) = f_1(x) +_V (f_2 + f_3)(x) = f_1(x) +_V (f_2(x) +_V f_3(x)).$$

Applying condition (2.5) for the vector space $V$ and the vectors $f_i(x)$, and then the definitions again, we get

$$g_1(x) = (f_1(x) +_V f_2(x)) +_V f_3(x) = (f_1 + f_2)(x) +_V f_3(x) = g_2(x).$$

Since this is true for all $x \in X$, this means that $g_1 = g_2$. Since $f_1$, $f_2$, $f_3$ were arbitrary in $W$, this then means that (2.5) is true for $W$. $\square$

For instance, if $X = \mathbf{N}$ and $V = \mathbf{K}$, the vector space $W$ becomes the space of *sequences* of elements of $\mathbf{K}$: an element of $W$ is a function $\mathbf{N} \to \mathbf{K}$, and corresponds to the sequence $(f(1), \ldots, f(n), \ldots)$.

Consider now a subset $Y \subset X$, and let $W_Y = \{f : Y \longrightarrow V\}$ be the vector space of functions from $Y$ to $V$ (with the operations as above, but applied to functions on $Y$ instead of $X$). Consider the maps

$$T : W_Y \longrightarrow W, \qquad S : W \longrightarrow W_Y$$

defined as follows: (1) for $f \in W_Y$, we define $T(f) = g$, where $g$ is the function on $X$ such that

$$g(x) = \begin{cases} f(x) & \text{if } x \in Y \\ 0 & \text{otherwise,} \end{cases}$$

("extension of $f$ by zero to $Y$"); (2) for $f \in W$, we define $S(f) = g$ by $g(y) = f(y)$ for all $y \in Y$ ("restriction of $f$ to $Y$"). Then $T$ and $S$ are both linear maps (this is left as exercise to check).

PROPOSITION 2.3.8. (1) *Let $V$ be a $\mathbf{K}$-vector space. The identity map $\mathrm{Id}_V$ is linear.*

(2) *Let $V_1$, $V_2$ and $V_3$ be $\mathbf{K}$-vector spaces and let*

$$V_1 \xrightarrow{f} V_2 \xrightarrow{g} V_3$$

*be linear maps. The composition $g \circ f$ is then a linear map.*

(3) *Let $f : V_1 \longrightarrow V_2$ be a bijective linear map. Then the reciprocal bijection $f^{-1}$ is linear.*

PROOF. (1) is easy and left as exercise.

(2) We just use the definition: for $t_1$, $t_2 \in \mathbf{K}$ and $x_1$, $x_2 \in V_1$, we have

$$\begin{aligned}(g \circ f)(t_1x_1 + t_2x_2) &= g(f(t_1x_1 + t_2x_2)) = g(t_1f(x_1) + t_2f(x_2)) \\ &= t_1g(f(x_1)) + t_2g(f(x_2)) = t_1(g \circ f)(x_1) + t_2(g \circ f)(x_2).\end{aligned}$$

(3) Let $t_1$, $t_2 \in \mathbf{K}$ and $y_1$, $y_2 \in V_2$ be given. Let

$$x = f^{-1}(t_1y_1 + t_2y_2).$$

This element $x$ is, by definition, the *unique* element in $V_1$ such that $f(x) = t_1y_1 + t_2y_2$. Now define

$$x' = t_1f^{-1}(y_1) + t_2f^{-1}(y_2) \in V_1.$$

Since $f$ is linear, we have

$$f(x') = t_1 f(f^{-1}(y_1)) + t_2 f(f^{-1}(y_2)) = t_1 y_1 + t_2 y_2$$

(since $f(f^{-1}(y)) = y$ for all $y \in V_2$). Using the uniqueness property of $x$, this means that $x' = x$, which states that

$$f^{-1}(t_1 y_1 + t_2 y_2) = t_1 f^{-1}(y_1) + t_2 f^{-1}(y_2).$$

This shows that $f^{-1}$ is linear. □

DEFINITION 2.3.9 (Isomorphism). A bijective linear map from $V_1$ to $V_2$ is called an **isomorphism** from $V_1$ to $V_2$. If there exists an isomorphism between vector spaces $V_1$ and $V_2$, they are said to be **isomorphic**.

EXAMPLE 2.3.10. We consider the special case of linear maps from $\mathbf{K}^n$ to $\mathbf{K}^m$ of the form $f = f_A$ for some matrix $A$.

PROPOSITION 2.3.11. *Consider the linear map $f_A : \mathbf{K}^n \to \mathbf{K}^m$ associated to a matrix $A \in M_{m,n}(\mathbf{K})$. Then $f_A$ is bijective if and only if there exists a matrix $B \in M_{n,m}(\mathbf{K})$ such that $BA = 1_n$ and $AB = 1_m$. If this is the case, the matrix $B$ is unique. We say that $A$ is* invertible *and we denote by $A^{-1}$ the matrix $B$, called the* inverse *of $A$.*

We will also write $A^{-n} = (A^{-1})^n$ for $n \geqslant 0$.

LEMMA 2.3.12. *Any linear map $g : \mathbf{K}^m \longrightarrow \mathbf{K}^n$ is of the form $g = f_B$ for some matrix $B \in M_{n,m}(\mathbf{K})$.*

PROOF. Define the elements $e_i \in \mathbf{K}^m$ for $1 \leqslant i \leqslant m$ as in the proof of Proposition 2.2.5: all coefficients of $e_i$ are zero, except that the $i$-th coefficient is 1. Define the vectors $f_i = g(e_i) \in \mathbf{K}^n$, and consider the matrix $B$ obtained by putting together the vectors $(f_1, \ldots, f_m)$ in order: if

$$f_i = \begin{pmatrix} b_{1i} \\ \vdots \\ b_{ni} \end{pmatrix}$$

then

$$B = \begin{pmatrix} b_{11} & \cdots & b_{1m} \\ \cdots & \cdots & \cdots \\ b_{n1} & \cdots & b_{nm} \end{pmatrix}$$

The matrix $B$ has $m$ columns and $n$ rows.

Computing $f_B(e_i) = Be_i$, we see that $f_B(e_i) = f_i = g(e_i)$ for $1 \leqslant i \leqslant m$ (this is similar to the proof of Proposition 2.2.5 (1)). Now note that if $x = (x_i)_{1 \leqslant i \leqslant m} \in \mathbf{K}^m$ is any vector, then we can write

$$x = x_1 e_1 + \cdots + x_m e_m,$$

and therefore

$$g(x) = x_1 g(e_1) + \cdots + x_m g(e_m)$$

since $g$ is linear, and this becomes

$$g(x) = x_1 f_B(e_1) + \cdots + x_m f_B(e_m) = f_B(x_1 e_1 + \cdots + x_m e_m) = f_B(x)$$

using the linearity of $f_B$. Since $x$ is arbitrary, we conclude that $g = f_B$. □

Proof of Proposition 2.3.11. (1) First assume that $f_A$ is bijective. Since it is linear, the inverse map is linear, so that (by the lemma) there exists a matrix $B \in M_{n,m}(\mathbf{K})$ such that $f_A^{-1} = f_B$.

We then have

$$f_{AB} = f_A \circ f_B = f_A \circ f_A^{-1} = \mathrm{Id}_{\mathbf{K}^m} = f_{1_m},$$

which implies by Proposition 2.2.5 that $AB = 1_m$, and similarly

$$f_{BA} = f_B \circ f_A = f_A^{-1} \circ f_A = \mathrm{Id}_{\mathbf{K}^n} = f_{1_n},$$

which implies by Proposition 2.2.5 that $BA = 1_n$.

(2) Conversely, assume that a matrix $B$ with the stated properties exists. Then Proposition 2.2.5 (2) shows that

$$f_B \circ f_A = f_{BA} = f_{1_n} = \mathrm{Id}_{\mathbf{K}^n}$$

and

$$f_A \circ f_B = f_{AB} = f_{1_m} = \mathrm{Id}_{\mathbf{K}^m}$$

This implies that $f_A$ is bijective and that the inverse map is $f_B$.

(3) Finally, we check the uniqueness of $B$: if $B'A = BA = 1_n$ and $AB' = AB = 1_m$, then we get

$$B' = B'1_m = B'AB = (B'A)B = 1_nB = B.$$

□

For $n = m = 2$, a direct computation shows that a matrix

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

is invertible if and only if $ad - bc \neq 0$, and in that case that the inverse is

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

## 2.4. Subspaces

Definition 2.4.1 (Subspace). Let $V$ be a $\mathbf{K}$-vector space. A subset $W \subset V$ is called a **vector subspace** (or just **subspace**) of $V$ if $0_V \in W$ and if for all $s_1$, $s_2 \in \mathbf{K}$ and $v_1$, $v_2 \in W$, we have

$$s_1v_1 + s_2v_2 \in W.$$

If this is the case, then $W$ with the zero vector $0_V$ and the restriction to $W$ of the operations of $V$, is a $\mathbf{K}$-vector space.

In particular, we get that $-v \in W$ for all $v \in W$ (take $v_1 = v$, $s_1 = -1$ and $s_2 = 0$) and $tv \in W$ for all $t \in \mathbf{K}$ (take $v_1 = v$, $s_1 = t$ and $s_2 = 0$).

By induction, if $W$ is a subspace of $V$, then $W$ contains any sum of the type

$$t_1v_1 + \cdots + t_nv_n,$$

where $t_i \in \mathbf{K}$ and $v_i \in W$. (For instance, if $n = 3$, then $t_1v_1 + t_2v_2 + t_3v_3 = t_1v_1 + 1 \cdot (t_2v_2 + t_3v_3)$, and since $t_2v_2 + t_3v_3 \in W$, and $v_1 \in W$, we see that $t_1v_1 + t_2v_2 + t_3v_3 \in W$).

The last statement concerning $W$ can be checked easily: it is simply because all identities required of the addition and multiplication already hold in $V$ (which is a vector space), and therefore still hold when applied to elements of $W$. For instance, we check (2.8): if $t_1$ and $t_2$ are in $\mathbf{K}$ and $v \in W$, then

$$(t_1 + t_2) \cdot_W v = (t_1 + t_2) \cdot_V v = t_1 \cdot_V v +_V t_2 \cdot_V v = t_1 \cdot_W v +_W t_2 \cdot_W v,$$

using twice the fact that the addition and multiplication for $W$ are the same as for $V$.

EXAMPLE 2.4.2. (1) For any vector space $V$, the subspace $\{0_V\}$ is a subspace.

(2) Let $V_1$ and $V_2$ be vector spaces. Consider the vector space $W$ of all possible maps $f : V_1 \longrightarrow V_2$ (see Example 2.3.6 (3) with $V_1$ in place of $X$ and $V_2$ in place of $V$). Consider the subset

$$\mathrm{Hom}_{\mathbf{K}}(V_1, V_2) = \{f \in W \mid f \text{ is } \mathbf{K}\text{-linear}\} \subset W.$$

Then $\mathrm{Hom}_{\mathbf{K}}(V_1, V_2)$ is a subspace of $W$. To check this, we first note that the zero map is clearly linear. We must therefore check that if $f_1$ and $f_2$ are linear maps from $V_1$ to $V_2$, and if $s_1, s_2 \in \mathbf{K}$, then the map $f = s_1 f_1 + s_2 f_2$ (defined using the addition and multiplication of $W$) is also a linear map. But for any $v \in V_1$, we have

$$f(v) = s_1 f_1(v) + s_2 f_2(v)$$

by definition of the operations on $W$. In particular, for $t_1$ and $t_2$ in $\mathbf{K}$ and $v_1, v_2 \in V_1$, we have

$$\begin{aligned} f(t_1 v_1 + t_2 v_2) &= s_1 f_1(t_1 v_1 + t_2 v_2) + s_2 f_2(t_1 v_1 + t_2 v_2) \\ &= s_1\big(t_1 f_1(v_1) + t_2 f_1(v_2)\big) + s_2\big(t_1 f_2(v_1) + t_2 f_2(v_2)\big) \\ &= t_1(s_1 f_1(v_1) + s_2 f_2(v_1)) + t_2(s_1 f_1(v_2) + s_2 f_2(v_2)) \end{aligned}$$

since $f_1$ and $f_2$ are linear. We recognize that this is $t_1 f(v_1) + t_2 f(v_2)$ (again by definition of the operations on $W$), and this proves that $f$ is linear.

The space $\mathrm{Hom}_{\mathbf{K}}(V_1, V_2)$ is called the space of linear maps from $V_1$ to $V_2$. If $V_1 = V_2$, an element of $\mathrm{Hom}_{\mathbf{K}}(V_1, V_1)$ is called an *endomorphism* of $V_1$. One writes then also $\mathrm{Hom}_{\mathbf{K}}(V_1, V_2) = \mathrm{End}_{\mathbf{K}}(V_1)$.

(3) We now will determine all subspaces of the $\mathbf{R}$-vector space $\mathbf{R}^2$. Let $W \subset \mathbf{R}^2$ be a subspace.

Case 1. If $W = \{(0, 0)\}$, then it is a subspace.

Case 2. If $W$ contains one non-zero element at least, for instance $\begin{pmatrix} a \\ b \end{pmatrix} \in W$ with $a$ and $b$ not both zero, then the definition of vector subspaces shows that, for all $t \in \mathbf{R}$, the element $\begin{pmatrix} ta \\ tb \end{pmatrix}$ belongs to $W$.

The set $W_1$ of all elements of this form is a line in the plane through the origin. It is a subspace in $\mathbf{R}^2$ (exercise), and is contained in $W$ from what we just saw. If $W = W_1$, then $W$ is therefore a line through the origin.

Case 3. If $W \neq W_1$, there is some element $\begin{pmatrix} c \\ d \end{pmatrix} \in W$ that does not belong to $W_1$. In that case, we claim that $W = \mathbf{R}^2$. This means that we have to check that for any $\begin{pmatrix} x \\ y \end{pmatrix} \in \mathbf{R}^2$, there exist two real numbers $t_1$ and $t_2$ with the property that

$$t_1 \begin{pmatrix} a \\ b \end{pmatrix} + t_2 \begin{pmatrix} c \\ d \end{pmatrix} = \begin{pmatrix} x \\ y \end{pmatrix} \tag{2.9}$$

These conditions mean that $f_A(\begin{pmatrix} t_1 \\ t_2 \end{pmatrix}) = A \begin{pmatrix} t_1 \\ t_2 \end{pmatrix} = \begin{pmatrix} x \\ y \end{pmatrix}$, where $A$ is the matrix

$$A = \begin{pmatrix} a & c \\ b & d \end{pmatrix}.$$

We will check in a few seconds that $ad - bc \neq 0$. Then, as shown at the end of Example 2.3.10, the matrix $A$ is invertible with inverse

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

Then $\begin{pmatrix} t_1 \\ t_2 \end{pmatrix} = A^{-1}\begin{pmatrix} x \\ y \end{pmatrix}$ satisfies $A\begin{pmatrix} t_1 \\ t_2 \end{pmatrix} = AA^{-1}\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x \\ y \end{pmatrix}$, which is (2.9).

To show that $ad - bc \neq 0$, suppose that this is not the case. Then we get

$$d\begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} ad \\ bd \end{pmatrix} = \begin{pmatrix} bc \\ bd \end{pmatrix} = b\begin{pmatrix} c \\ d \end{pmatrix}.$$

If $b \neq 0$, this means that $\begin{pmatrix} c \\ d \end{pmatrix} = (d/b)\begin{pmatrix} a \\ b \end{pmatrix} \in W_1$, which contradicts the assumption that $\begin{pmatrix} c \\ d \end{pmatrix} \notin W_1$.

If $b = 0$, then the condition $ad = bc$ means that $a = 0$ or $d = 0$. The first is not possible when $b = 0$, because we also assumed that $\begin{pmatrix} a \\ b \end{pmatrix} \neq \begin{pmatrix} 0 \\ 0 \end{pmatrix}$. So we would get $d = 0$. But then

$$\begin{pmatrix} c \\ d \end{pmatrix} = \begin{pmatrix} c \\ 0 \end{pmatrix} = \frac{c}{a}\begin{pmatrix} a \\ 0 \end{pmatrix} = \frac{c}{a}\begin{pmatrix} a \\ b \end{pmatrix}.$$

This also implies that $\begin{pmatrix} c \\ d \end{pmatrix} \in W_1$, and therefore is also a contradiction. This means that we must have $ad - bc \neq 0$.

Further important examples of subspaces are related to linear maps:

Definition 2.4.3 (Kernel and image). Let $f : V_1 \longrightarrow V_2$ be a linear map.

The **kernel** of $f$ is the subset $\mathrm{Ker}(f) = f^{-1}(\{0_{V_2}\})$ of $V_1$; the **image** of $f$ is the subset $\mathrm{Im}(f) = f(V_1)$ of $V_2$.

Proposition 2.4.4. *Let $f : V_1 \longrightarrow V_2$ be a linear map.*

(1) *The subset $\mathrm{Ker}(f)$ is a subspace of $V_1$, and the subset $\mathrm{Im}(f)$ is a subspace of $V_2$.*

(2) *The linear map $f$ is injective if and only if $\mathrm{Ker}(f) = \{0_{V_1}\}$.*

(3) *The linear map $f$ is surjective if and only if $\mathrm{Im}(f) = V_2$.*

(4) *If $w \in \mathrm{Im}(f)$, then the set of solutions of the equation $f(v) = w$ is*

$$\{v = v_0 + v'\}$$

*where $v_0$ is any fixed element such that $f(v_0) = w$, and $v'$ belongs to the kernel of $f$.*

Proof. (1) We begin with the kernel. If $t_1$, $t_2$ are in $\mathbf{K}$ and $v_1$, $v_2$ in $\mathrm{Ker}(f)$, then

$$f(t_1 v_1 + t_2 v_2) = t_1 f(v_1) + t_2 f(v_2) = t_1 \cdot 0_V + t_2 \cdot 0_V = 0_V$$

so that $t_1 v_1 + t_2 v_2 \in \mathrm{Ker}(f)$.

For the image, again for $t_1$ and $t_2 \in \mathbf{K}$ and $w_1$, $w_2 \in \mathrm{Im}(f)$, there exist $v_1$ and $v_2$ such that $f(v_i) = w_i$. Then, since $f$ is linear, we get

$$f(t_1 v_1 + t_2 v_2) = t_1 w_1 + t_2 w_2$$

which implies that $t_1 w_1 + t_2 w_2 \in \mathrm{Im}(f)$.

(2) If $f$ is injective, then there is at most one element $x \in V_1$ such that $f(x) = 0_{V_2}$. Since $f(0_{V_1}) = 0_{V_2}$, this means that $x = 0_{V_1}$ is the unique element with this property, which means that $\mathrm{Ker}(f) = \{0_{V_1}\}$.

Conversely, assume that the kernel of $f$ is $\{0_{V_1}\}$. To show that $f$ is injective, we consider elements $v_1$ and $v_2$ such that $f(v_1) = f(v_2)$. We then deduce (because $f$ is linear) that $f(v_1 - v_2) = 0$. So $v_1 - v_2 \in \mathrm{Ker}(f)$, hence $v_1 - v_2 = 0_{V_1}$ since the kernel contains only $0_{V_1}$. This means that $v_1 = v_2$. Therefore $f$ is injective.

(3) It is a general fact that a map $f : X \to Y$ is surjective if and only if the image $f(X)$ is equal to $Y$. Therefore the property here is not particular to linear maps.

(4) Suppose $w \in \mathrm{Im}(f)$, and fix $v_0 \in V_1$ such that $f(v_0) = w$. Then for any $v \in V_1$, write $v' = v - v_0$. We have $f(v) = w$ if and only if $f(v) = f(v_0)$, which is equivalent to $f(v') = f(v - v_0) = 0$, or in other words to $v' \in \mathrm{Ker}(f)$. So the solutions of $f(v) = w$ are the elements $v = v_0 + v'$ with $v' \in \mathrm{Ker}(f)$. ☐

Another construction of subspaces is given by intersection of subspaces:

PROPOSITION 2.4.5. *Let $V$ be a $\mathbf{K}$-vector space. For any set $I$ and any collection $V_i$ of subspaces of $V$ for $i \in I$, the intersection*

$$\bigcap_{i\in I} V_i = \{v \in V \mid v \in V_i \text{ for all } i \in I\} \subset V$$

*is a subspace of $V$. In particular, if $V_1$ and $V_2$ are subspaces of $V$, then $V_1 \cap V_2$ is also a subspace of $V$.*

PROOF. Let $W$ be the intersection of the subspaces $V_i$. Let $v_1$, $v_2$ be elements of $W$ and $t_1$, $t_2$ elements of $\mathbf{K}$. Then, for any $i \in I$, the vector $t_1v_1 + t_2v_2$ belongs to $V_i$, since $V_i$ is a subspace of $V$. This is true for all $i \in I$, and therefore $t_1v_1 + t_2v_2 \in W$. ☐

REMARK 2.4.6. In general, if $V_1$ and $V_2$ are subspaces, the union $V_1 \cup V_2$ is not a subspace.

EXAMPLE 2.4.7. Let $V$ be the space of all sequences $(a_n)_{n\geqslant 1}$ of real numbers. Define for $k \geqslant 1$ the subspace

$$F_k = \{(a_n)_{n\geqslant 1} \mid a_{k+2} - a_{k+1} - a_k = 0\}.$$

This is a subspace, for instance because for each $k$, the map $f_k : V \to \mathbf{R}$ such that $f_k((a_n)) = a_{k+2} - a_{k+1} - a_k$ is linear (exercise), and $F_k = \mathrm{Ker}(f_k)$. Then

$$\bigcap_{k\geqslant 1} F_k = \{(a_n)_{n\geqslant 1} \in V \mid a_{n+2} = a_{n+1} + a_n \text{ for all } n \geqslant 1\}.$$

Generalizing the kernel and image, we have the following constructions:

PROPOSITION 2.4.8. *Let $V_1$ and $V_2$ be $\mathbf{K}$-vector spaces and $f \colon V_1 \to V_2$ a linear map.*

(1) *If $W_2 \subset V_2$ is a subspace, then*

$$f^{-1}(W_2) = \{v \in V_1 \mid f(v) \in W\}$$

*is a subspace of $V_1$.*

(2) *If $W_1 \subset V_1$ is a subspace, then*

$$f(W_1) = \{v \in V_2 \mid \text{there exists } w \in W \text{ such that } f(w) = v\}$$

*is a subspace of $V_2$.*

PROOF. This is exactly similar to the proof of Proposition 2.4.4 (1); for instance, if $W_2 \subset V_2$, and $v_1$, $v_2$ are elements of $f^{-1}(W_2)$, while $s$ and $t$ are elements of $\mathbf{K}$, then we get

$$f(tv_1 + sv_2) = tf(v_1) + sf(v_2) \in W_2$$

since $f(v_i) \in W_2$ and $W_2$ is a subspace. ☐

## 2.5. Generating sets

Definition 2.5.1 (Linear combination). Let $V$ be a $\mathbf{K}$-vector space and $S \subset V$ a subset (not necessarily a vector subspace). A **linear combination** of elements of $S$ is a vector $v \in V$ of the form

$$v = t_1 v_1 + \cdots + t_k v_k$$

for some $k \geqslant 0$, where $t_i \in \mathbf{K}$ and $v_i \in S$ for all $i$.

Example 2.5.2. (1) If $S = \varnothing$, then $0_V$ is the only linear combination of elements of $S$ (because an empty sum

$$\sum_{v \in \varnothing} a_v$$

is the zero vector).

(2) If $S = \{v_1\}$ has only one element, then the linear combinations of elements of $S$ are the vectors $tv_1$ where $t \in \mathbf{K}$.

(3) More generally, if $S$ is finite, with $S = \{v_1, \ldots, v_n\}$ where the $v_i$'s are different, then a linear combination of $S$ is a vector of the form

$$t_1 v_1 + \cdots + t_n v_n$$

where all $t_i \in \mathbf{K}$. The point is that if we take a combination of fewer vectors than all of $v_1$, …, $v_n$, we can insert the missing vectors by adding them with coefficient 0; for instance, if $n \geqslant 6$ and

$$v = xv_3 + yv_5$$

we can write

$$v = 0 \cdot v_1 + 0 \cdot v_2 + xv_3 + 0 \cdot v_4 + yv_5 + 0 \cdot v_6 + \cdots + 0 \cdot v_n.$$

Definition 2.5.3 (Subspace generated by a set). Let $V$ be a $\mathbf{K}$-vector space and $S \subset V$ a subset. The **subspace generated by** $S$ is the subset of $V$ whose elements are the linear combinations of elements of $S$. It is a vector subspace of $V$, and is denoted $\langle S \rangle$.

Proof that $\langle S \rangle$ is a subspace. Consider two linear combinations

$$v = t_1 v_1 + \cdots + t_k v_k, \qquad w = s_1 w_1 + \cdots + s_l w_l$$

of elements of $S$ (the vectors $v_i$ and $w_j$ are not necessarily the same). Then for any $x$ and $y \in \mathbf{K}$, we have

$$xv + yw = (xt_1)v_1 + \cdots + (xt_k)v_k + (ys_1)w_1 + \cdots + (ys_l)w_l,$$

which is also a linear combination of elements of $S$. $\square$

Remark 2.5.4. It may be that some of the vectors $v_i$ and $w_j$ are the same. Then the coefficients add up: for instance,

$$x(t_1 v_1 + t_2 v_2) + y(s_1 v_1 + s_2 v_2) = (xt_1 + ys_1)v_1 + (xt_2 + ys_2)v_2.$$

Example 2.5.5. (1) Let $W = \{f : \mathbf{R} \to \mathbf{R}\}$ be the $\mathbf{R}$-vector space of all possible maps from $\mathbf{R}$ to $\mathbf{R}$ (Example 2.3.6 (3), with $\mathbf{K} = \mathbf{R}$, $X = \mathbf{R}$ and $V = \mathbf{R}$). For $i$ integer $\geqslant 0$, let $f_i$ be the element of $W$ defined by

$$f_i(x) = x^i$$

for all $x \in \mathbf{R}$. Let $S = \{f_i \mid i \geqslant 0\}$ be the set of all these functions.

A linear combination of elements of $S$ is a function of the form

$$f = t_1 f_{i_1} + \cdots + t_k f_{i_k} \tag{2.10}$$

where $t_i \in \mathbf{R}$ and $\{i_1, \ldots, i_k\}$ is some subset of integers $\geqslant 0$. If we define $d$ to be the largest of the numbers $\{i_1, \ldots, i_k\}$, and define coefficients $a_i$ for $0 \leqslant i \leqslant d$ so that $a_i$ is the coefficient of $f_i$ in the linear combination (2.10) if $i \in \{i_1, \ldots, i_k\}$, and otherwise $a_i = 0$, then we can write

$$f(x) = a_0 + a_1 x + \cdots + a_d x^d$$

for all $x \in \mathbf{R}$. So the linear combinations of elements of $S$ are precisely the functions of the type

$$f = a_0 + a_1 f_1 + \cdots + a_d f_d$$

for some integer $d \geqslant 0$ and some coefficients $a_i$.

The space $\langle S \rangle$ is called the space of polynomials (or polynomial functions) on $\mathbf{R}$. It is often denoted $\mathbf{R}[x]$.

(2) Let $S = W$, a vector subspace of $V$. Then $\langle W \rangle = W$, since the definition of a subspace implies that any linear combination of elements of $W$ belongs to $W$.

Definition 2.5.6 (Generating set; finite-dimensional space). Let $V$ be a $\mathbf{K}$-vector space

(1) Let $S \subset V$ be a subset. We say that $S$ is a **generating set** of $V$ if $\langle S \rangle = V$, that is, if every element of $V$ can be written as a linear combination of elements of $S$.

(2) If $V$ has a **finite** generating set, then we say that $V$ is **finite-dimensional**.

Lemma 2.5.7. *Let $S_1 \subset S_2$ be two subsets of $V$. Then we have $\langle S_1 \rangle \subset \langle S_2 \rangle$. In particular, if $S_1$ is a generating set of $V$, then any subset that contains $S_1$ is also a generating set.*

Proof. By definition, any linear combination of elements of $S_1$ is also a linear combination of elements of $S_2$, so that $\langle S_1 \rangle \subset \langle S_2 \rangle$. ☐

Example 2.5.8. (1) The empty set is a generating set of the zero-space $\{0\}$.

(2) Let $n \geqslant 1$ and consider $V = \mathbf{K}^n$. For $1 \leqslant i \leqslant n$, let $e_i$ be the column vector with all coefficients equal to 0 except that the $i$-th row has coefficient 1 (see the proof of Proposition 2.2.5). Let $S = \{e_1, \ldots, e_n\} \subset V$. Then for any $x = (x_i)$ in $V$, we have

$$x = \begin{pmatrix} x_1 \\ \cdots \\ x_n \end{pmatrix} = x_1 e_1 + \cdots + x_n e_n,$$

which shows that $x \in \langle S \rangle$. Therefore $S$ is a generating set of $\mathbf{K}^n$. In particular, $\mathbf{K}^n$ is finite-dimensional.

(3) Consider $V = M_{m,n}(\mathbf{K})$. For $1 \leqslant i \leqslant m$ and $1 \leqslant j \leqslant n$, let $E_{i,j} \in V$ be the matrix with all coefficients 0 except the $(i,j)$-th coefficient that is equal to 1. For instance, for $m = n = 2$, we have

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

Then the finite set $S = \{E_{i,j} \mid 1 \leqslant i \leqslant m,\ 1 \leqslant j \leqslant n\}$ is a generating set of $M_{m,n}(\mathbf{K})$, so that in particular $M_{m,n}(\mathbf{K})$ is finite-dimensional. Indeed, for any matrix $A = (a_{i,j})$, we can write

$$A = \sum_{1 \leqslant i \leqslant m} \sum_{1 \leqslant j \leqslant n} a_{i,j} E_{i,j},$$

which shows that $A \in \langle S \rangle$.

(4) Consider the subset

$$P = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_{2,2}(\mathbf{C}) \mid a + d = 0 \right\} ;$$

this is in fact a subspace of $M_{2,2}(\mathbf{C})$, because the map

$$\begin{cases} M_{2,2}(\mathbf{C}) \longrightarrow \mathbf{C} \\ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto a + d \end{cases}$$

is a linear map, and $P$ is its kernel.

We define the *Pauli matrices*:

$$A_1 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad A_2 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad A_3 = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix},$$

and $S = \{A_1, A_2, A_3\}$, which is a subset of $P$. Then $S$ generates $P$: indeed, an element of $P$ is a matrix

$$\begin{pmatrix} a & b \\ c & -a \end{pmatrix}$$

for some complex numbers $a$, $b$, $c$. Then we check that

$$\begin{pmatrix} a & b \\ c & -a \end{pmatrix} = aA_1 + \frac{b+c}{2} A_2 + \frac{c-b}{2i} A_3,$$

which shows that the matrix belongs to $\langle S \rangle$.

(5) Let $V = \mathbf{R}[x]$ be the space of real polynomials of Example 2.5.2 (4), and $S = \{f_i\}$ the set defined there such that $\langle S \rangle = V$. So $S$ generates $V$ by definition. The set $S$ is infinite, and in fact $V$ *is not finite-dimensional*.

To prove this, consider an arbitrary finite set $T \subset V$ (not necessarily a subset of $S$!); we must show that we cannot have $\langle T \rangle = V$. But indeed, if we look at all the functions $f_i$ that appear in an expression of some element $f$ of $T$, there is a largest value of $i$, say $d$, that appears (it is the maximum of a finite set of integers; for instance, for $T = \{1+x+x^3, -x^{10}+\pi x^{100}, \frac{1}{3}x^{107}\}$, this would be $d = 107$). Then any linear combination of elements of $T$ will only involve functions $f_i$ with $0 \leqslant i \leqslant d$, and therefore is not equal to $V$ (for instance, the function $f_{d+1}$ is not in $\langle T \rangle$).

LEMMA 2.5.9. *Let $V_1$ and $V_2$ be $\mathbf{K}$-vector spaces. Let $f : V_1 \longrightarrow V_2$ be a linear map. If $f$ is surjective, and $S$ is a generating set of $V_1$, then $f(S)$ is a generating set of $V_2$. In particular, if $f$ is bijective, then $V_1$ is finite-dimensional if and only if $V_2$ is.*

PROOF. Consider a vector $v \in V_2$. Since $f$ is surjective, we can write $v = f(w)$ for some vector $w \in V_1$. Since $\langle S \rangle = V_1$, we can express $w$ as a linear combination of elements of $S$, of the form

$$w = t_1 w_1 + \cdots + t_n w_n$$

for some $n \geqslant 0$ and some $t_i \in \mathbf{K}$. Then, using the linearity of $f$, we get

$$v = f(w) = t_1 f(w_1) + \cdots + t_n f(w_n),$$

which is a linear combination of elements of $f(S)$. Hence $\langle f(S) \rangle = V_2$.

If $f$ is bijective, then applying this fact to $f^{-1}$ (which is also linear and surjective), we deduce that $S$ generates $V_1$ if and only if $f(S)$ generates $V_2$. In particular, $V_1$ is then finite-dimensional if and only if $V_2$ is, since if $S$ is finite, then so is $f(S)$, and conversely. ☐

## 2.6. Linear independence and bases

Definition 2.6.1 (Linear independence). Let $V$ be a $\mathbf{K}$-vector space and $S \subset V$ a subset.

(1) If $S$ is finite, with $S = \{v_1, \ldots, v_k\}$, with $k \geqslant 0$, where the $v_i$ are the distinct elements of $S$, we say that $S$ is **linearly independent** if and only if, for any coefficients $t_1, \ldots, t_k$ in $\mathbf{K}$, we have

$$t_1 v_1 + \cdots + t_k v_k = 0_V$$

if and only if $t_1 = \cdots = t_k = 0$.

(2) In general, we say that $S$ is linearly independent if and only if *every* finite subset $T$ of $S$ is linearly independent.

Remark 2.6.2. (1) It is always the case that if $t_i = 0$ for all $i$, we have

$$t_1 v_1 + \cdots + t_k v_k = 0_V.$$

So the content of the definition is that, in a linearly-independent set, the only linear combination that *can* be $0_V$ is the "obvious" one.

(2) If $S$ is linearly independent, this is usually used as follows: we have a finite subset $T = \{v_1, \ldots, v_n\} \subset S$, with the $v_i$ distinct, and coefficients $(t_1, \ldots, t_n)$ and $(s_1, \ldots, s_n)$, such that the corresponding linear combinations

$$v = t_1 v_1 + \cdots + t_n v_n, \qquad w = s_1 v_1 + \cdots + s_n v_n,$$

are known to be equal: $v = w$. Then it follows that $t_i = s_i$ for all $i$: two equal linear combinations *must have* the same coefficients. Indeed, by subtracting $w$ from $v = w$ on both sides, we get

$$(t_1 - s_1)v_1 + \cdots + (t_n - s_n)v_n = 0_V,$$

and therefore $t_i = s_i$ by linear independence.

Lemma 2.6.3. (1) *If $S \subset V$ is linearly independent and $T \subset S$ is a subset of $S$, then $T$ is linearly independent.*

(2) *Let $f : V_1 \longrightarrow V_2$ be a linear map between vector spaces over* $\mathbf{K}$. *If $S \subset V_1$ is linearly independent and if $f$ is injective, then $f(S) \subset V_2$ is also linearly independent.*

Proof. (1) Any finite subset of $T$ is a finite subset of $S$, and any linear combination of such a subset which is zero is a linear combination of elements of $S$ which is zero, and therefore if $S$ is linearly independent, the same holds for $T$.

(2) Let $T \subset f(S)$ be a finite subset. If we write $T = \{w_1, \ldots, w_k\}$ where the vectors $w_i \in V_2$ are distinct, then since $T \subset f(S)$, there exist $v_1, \ldots, v_k$ in $S \subset V_1$ such that $f(v_i) = w_i$. Moreover, $v_i$ is unique, since $f$ is injective.

Now assume that $t_1, \ldots, t_k$ in $\mathbf{K}$ are such that

$$t_1 w_1 + \cdots + t_k w_k = 0_{V_2}.$$

This means that

$$f(t_1 v_1 + \cdots + t_k v_k) = 0_{V_2},$$

since $f$ is linear, or in other words that $t_1 v_1 + \cdots + t_k v_k$ belongs to the kernel of $f$. Since $f$ is injective, Proposition 2.4.4 shows that $\mathrm{Ker}(f) = \{0_{V_1}\}$, and therefore we have

$$t_1 v_1 + \cdots + t_k v_k = 0_{V_1}.$$

But since $\{v_1, \ldots, v_k\} \subset S$, this implies that $t_1 = \cdots = t_k = 0$ since $S$ is linearly independent. ☐

Definition 2.6.4 (Basis). Let $V$ be a $\mathbf{K}$-vector space. A subset $S \subset V$ which is a generating set of $V$ and which is also linearly independent is called a **basis** of $V$.

Example 2.6.5. (1) The emptyset is linearly independent in any vector space; if this seems unclear from the definition, it can be taken as a convention (but it is indeed a consequence of the definitions, when properly phrased). Combining this with Example 2.5.8 (1), we see that $\varnothing$ is a basis of the zero space $\{0\}$.

(2) If $S = \{v\}$ has a single element, then $S$ is linearly independent if and only if $v \neq 0_V$. Indeed, if $v = 0_V$, then the linear combination $1 \cdot 0_V = 0_V$ with non-zero coefficient 1 shows that $\{0_V\}$ is not linearly independent. If $v \neq 0_V$, on the other hand, the linear combinations to consider are of the form $tv$ for $t \in \mathbf{K}$, and if $tv = 0_V$, then $t = 0$ follows by Lemma 2.3.3.

(3) In $\mathbf{K}^n$, the set $S$ containing the vectors $e_i$ defined for $1 \leqslant i \leqslant n$ in Example 2.5.8 (2) are linearly independent: indeed, for any $t_1, \ldots, t_n$ in $\mathbf{K}$, we have

$$t_1 e_1 + \cdots + t_n e_n = \begin{pmatrix} t_1 \\ \vdots \\ t_n \end{pmatrix}$$

and this is equal to 0 (in $\mathbf{K}^n$) if and only if $t_1 = \cdots = t_n = 0$.

In combination with Example 2.5.8 (2), this means that $\{e_1, \ldots, e_n\}$ is a basis of $\mathbf{K}^n$. This basis is called the *standard* or *canonical* basis of $\mathbf{K}^n$.

(4) Similarly, the matrices $E_{i,j}$ in $M_{m,n}(\mathbf{K})$ in Example 2.5.8 (3) are linearly independent: for any coefficients $t_{i,j}$ for $1 \leqslant i \leqslant m$ and $1 \leqslant j \leqslant n$, we have

$$\sum_{1 \leqslant i \leqslant m} \sum_{1 \leqslant j \leqslant n} t_{i,j} E_{i,j} = \begin{pmatrix} t_{11} & \cdots & t_{1n} \\ \cdots & \cdots & \cdots \\ t_{m1} & \cdots & t_{mn} \end{pmatrix},$$

which is the zero matrix $0_{m,n}$ only if all coefficients are zero. In combination with Example 2.5.8 (3), this shows that $\{E_{i,j}\}$ is a basis of $M_{m,n}(\mathbf{K})$.

(5) We consider the space $V = \mathbf{R}[x]$ of polynomials of Example 2.5.2 (4). Let $S = \{f_i\}$ be the set of functions $f_i(x) = x^i$ for $i \geqslant 0$ integer considered in that example. By definition, $S$ is a generating set of $V$. We claim that it is also linearly independent, and therefore is a basis of $V$.

Let $T$ be a finite subset of $S$, and $d$ the largest integer such that $f_d$ belongs to $T$. Then $T \subset \{f_0, \ldots, f_d\}$, and using Lemma 2.6.3, it suffices to prove that $\{f_0, \ldots, f_d\}$ is linearly independent to deduce that $T$ is also linearly independent. We will prove this by induction on $d$.

For $d = 0$, the set is $\{f_0\}$, and since $f_0 \neq 0_V$, this is a linearly independent set.

Assume now that $d \geqslant 1$ and that $\{f_0, \ldots, f_{d-1}\}$ is linearly independent. We will prove the same for $\{f_0, \ldots, f_d\}$. Consider real numbers $t_0, \ldots, t_d$ such that

$$t_0 f_0 + \cdots + t_d f_d = 0_V. \tag{2.11}$$

This means that for all real numbers $x$, we have

$$t_0 + t_1 x + \cdots + t_d x^d = 0.$$

The left-hand side is a function of $x$ that is indefinitely differentiable, and so is the right-hand side (which is constant). Differentiating $d$ times on both sides, we get $d! t_d = 0$, which implies that $t_d = 0$. Then the relation (2.11) becomes

$$t_0 f_0 + \cdots + t_{d-1} f_{d-1} = 0_V.$$

Since, by induction, we assumed that $\{f_0, \ldots, f_{d-1}\}$ is linearly independent, the coefficients $t_0$, ..., $t_{d-1}$ must all be zero. Therefore, in (2.11), all coefficients are zero. This means that $\{f_0, \ldots, f_d\}$ is linearly independent.

PROPOSITION 2.6.6. *Let $V$ be a $\mathbf{K}$-vector space and $S = \{v_1, \ldots, v_n\}$ be a finite subset of $V$, with the $v_i$'s distinct. Define*

$$g_S \begin{cases} \mathbf{K}^n \longrightarrow V \\ \begin{pmatrix} t_1 \\ \vdots \\ t_n \end{pmatrix} \mapsto t_1 v_1 + \cdots + t_n v_n. \end{cases}$$

(1) *The map $g_S$ is linear.*
(2) *The map $g_S$ is surjective if and only if $S$ is a generating set of $V$.*
(3) *The map $g_S$ is injective if and only if $S$ is linearly independent.*
(4) *The map $g_S$ is an isomorphism if and only if $S$ is a basis of $V$.*

PROOF. (1) is left as an exercise.

(2) The image of $g_S$ is the set $\langle S \rangle$ of all linear combinations of elements of $S$; therefore $g_S$ is surjective if and only if $\langle S \rangle = V$, which means if and only if $S$ is a generating set of $V$.

(3) The kernel of $g_S$ is the set of vectors $(t_1, \ldots, t_n)$ such that the linear combination

$$t_1 v_1 + \cdots + t_n v_n$$

is equal to $0_V$. Therefore $\mathrm{Ker}(f) = \{0_{\mathbf{K}^n}\}$ if and only if the only linear combination of elements of $S$ that is zero is the one with all coefficients $t_i$ equal to 0, which means precisely if and only if $S$ is linearly independent.

(4) is the combination of (2) and (3). $\square$

## 2.7. Dimension

THEOREM 2.7.1 (Main theorem). *Let $V$ be a $\mathbf{K}$-vector space.*

(1) *For any subset $S$ of $V$ such that $S$ generates $V$, there exists a subset $T \subset S$ such that $T$ is a basis of $V$.*

(2) *For any subset $S$ of $V$ such that $S$ is linearly independent in $V$, there exists a subset $T \subset V$ such that $S \subset T$, and such that $T$ is a basis of $V$.*

(3) *If $S_1$ and $S_2$ are two bases of $V$, then they have the same cardinality, in the sense that there exists a bijection $f : S_1 \to S_2$. If $V$ is finite-dimensional, then any basis of $V$ is finite, and the number of elements in a basis is independent of the choice of the basis.*

COROLLARY 2.7.2. *Let $V$ be a $\mathbf{K}$-vector space. There exists at least one basis in $V$.*

PROOF. One can either:

– Apply part (1) of Theorem 2.7.1 with $S = V$, which generates $V$, so that (1) states that $V$ contains a subset that is a basis;

– Or apply part (2) of Theorem 2.7.1 with $S = \varnothing$, which is linearly independent in $V$, so that (2) states that there is a subset $T$ of $V$ that is a basis. $\square$

DEFINITION 2.7.3 (Dimension). Let $V$ be a $\mathbf{K}$-vector space. The **dimension** of $V$, denoted either $\dim(V)$ or $\dim_{\mathbf{K}}(V)$, is the cardinality of any basis of $V$. It is an integer or zero if $V$ is finite-dimensional.

EXAMPLE 2.7.4. (1) The zero space $\{0\}$ has dimension zero; its only basis is the empty set (Example 2.6.5 (1)).

(2) For $n \geqslant 1$, the space $\mathbf{K}^n$ has dimension $n$, since $\{e_1, \ldots, e_n\}$ is a basis with $n$ elements (Example 2.6.5 (3)).

(3) For $m$, $n \geqslant 1$, the space $M_{m,n}(\mathbf{K})$ has dimension $mn$ since the matrices $E_{ij}$ for $1 \leqslant i \leqslant m$ and $1 \leqslant j \leqslant n$ form a basis (Example 2.6.5 (4)).

We will prove Theorem 2.7.1 only when $V$ is finite-dimensional. We use three lemmas.

LEMMA 2.7.5. *Let $V$ be a $\mathbf{K}$-vector space, and $S \subset V$ linearly independent. Let $W = \langle S \rangle \subset V$. If $w \in V - W$, then the set $S \cup \{w\}$ is linearly independent.*

PROOF. Let $T$ be a finite subset of $S \cup \{w\}$. If $w \notin T$, then $T \subset S$, and hence is linearly independent since $S$ is.

Assume now that $w \in T$. Write $T = \{w, v_1, \ldots, v_n\}$ with $v_i$'s distinct elements of $S$. Then $T$ has $n+1$ elements (since $w \notin \langle S \rangle$, so $w \notin S$). Assume $t_0$, $t_1$, …, $t_n$ are elements of $\mathbf{K}$ such that

$$t_0 w + t_1 v_1 + \cdots + t_n v_n = 0_V.$$

If $t_0 = 0$, we would get a zero linear combination of vectors in $S$, and deduce that $t_1 = \cdots = t_n = 0$ also by linear independence of $S$.

If $t_0 \neq 0$, on the other hand, we would get

$$w = -\frac{1}{t_0}(t_1 v_1 + \cdots + t_n v_n)$$

but the right-hand side of this expression is an element of $\langle S \rangle$, and this is impossible since $w \notin W$. ∎

LEMMA 2.7.6. *Let $V$ be a $\mathbf{K}$-vector space, and $S \subset V$ a generating set. Let $w$ be a vector in $S$. If $w \in \langle S - \{w\} \rangle$, then $S - \{w\}$ is a generating set.*

PROOF. Let $W$ be $\langle S - \{w\} \rangle$. The assumption means that there exists an integer $n \geqslant 0$, elements $v_1$, …, $v_n$ of $S$, different from $w$, and elements $t_1$, …, $t_n$ in $\mathbf{K}$, such that

$$w = t_1 v_1 + \cdots + t_n v_n.$$

Let $v \in V$ be arbitrary. Since $S$ generates $V$, we can express $v$ as a linear combination

$$v = s_1 w_1 + \cdots + s_k w_k$$

where $w_j \in S$ are distinct and $s_j \in \mathbf{K}$. If $w$ does not appear in $\{w_1, \ldots, w_k\}$, it follows that $v \in W$. Otherwise, we may assume that $w_1 = w$ by permuting the vectors. Then we get

$$v = s_1 t_1 v_1 + \cdots + s_1 t_n v_n + s_2 w_2 + \cdots s_k w_k,$$

and this also belongs to $W$ since none of the $v_i$'s or $w_j$'s are equal to $w$. Therefore we see that $V = W$. ∎

LEMMA 2.7.7. *Let $V$ be a finite-dimensional $\mathbf{K}$-vector space, and $S \subset V$ a finite generating set with $n$ elements. If $T \subset V$ has at least $n+1$ elements, then $T$ is linearly dependent.*

PROOF. It suffices to prove this when $T$ has exactly $n+1$ elements (since $T$ always contains a set with that many elements, and if the subset is linearly dependent, then so is $T$).

We will then proceed by induction on $n \geqslant 0$. The property $P(n)$ to be proved for all $n$ is: "for any vector space $V$ over $\mathbf{K}$, if there exists a generating subset $S$ of $V$ with $n$ elements, then all subsets of $V$ with $n+1$ elements are linearly dependent."

We first check that $P(0)$ is true. A generating set with 0 elements must be $\varnothing$, and in that case $V = \langle \varnothing \rangle = \{0\}$; there is only one subset with 1 element (namely $\{0\}$), and it is indeed linearly dependent. So the property $P(0)$ is true.

Now we assume that $n \geqslant 1$ and that $P(n-1)$ is true. We will then prove $P(n)$. Let $V$ be a vector space with a generating set $S = \{v_1, \ldots, v_n\}$ with $n$ elements. Let $T = \{w_1, \ldots, w_{n+1}\}$ be a subset of $V$ with $n+1$ elements. We must show that $T$ is linearly dependent.

Since $\langle S \rangle = V$, there exist numbers $t_{ij}$ for $1 \leqslant i \leqslant n+1$ and $1 \leqslant j \leqslant n$ such that

$$\begin{aligned} w_1 &= t_{11} v_1 + \cdots + t_{1n} v_n \\ \vdots \quad & \quad \vdots \qquad\qquad \vdots \\ w_{n+1} &= t_{n+1,1} v_1 + \cdots + t_{n+1,n} v_n. \end{aligned}$$

<u>Case 1.</u> If $t_{11} = \cdots = t_{n+1,1} = 0$, then the relations become

$$\begin{aligned} w_1 &= t_{12} v_2 + \cdots + t_{1n} v_n \\ \vdots \quad & \quad \vdots \qquad\qquad \vdots \\ w_{n+1} &= t_{n+1,2} v_2 + \cdots + t_{n+1,n} v_n. \end{aligned}$$

This means that $T \subset \langle V_1 \rangle$ where $V_1$ is the subspace $\langle \{v_2, \ldots, v_n\} \rangle$ generated by the $(n-1)$ vectors $v_2, \ldots, v_n$. By the induction hypothesis, applied to $V_1$, $S_1 = \{v_2, \ldots, v_n\}$ and $T_1 = \{w_1, \ldots, w_n\}$, the subset $T_1$ is linearly dependent, which implies that the larger set $T$ is also linearly dependent.

<u>Case 2.</u> If there is some $i$ such that $t_{i1} \neq 0$, then up to permuting the vectors, we may assume that $t_{11} \neq 0$. For $2 \leqslant i \leqslant n+1$, the relations then imply that

$$\begin{aligned} w_i - \frac{t_{i1}}{t_{11}} w_1 &= \Big(t_{i1} - \frac{t_{i1}}{t_{11}} t_{11}\Big) v_1 + \cdots + \Big(t_{in} - \frac{t_{i1}}{t_{11}} t_{1n}\Big) v_n \\ &= \Big(t_{i2} - \frac{t_{i1}}{t_{11}} t_{12}\Big) v_2 + \cdots + \Big(t_{in} - \frac{t_{i1}}{t_{11}} t_{1n}\Big) v_n. \end{aligned}$$

Let

$$w_i' = w_i - \frac{t_{i1}}{t_{11}} w_1 \in V \tag{2.12}$$

for $2 \leqslant i \leqslant n+1$, and

$$s_{ij} = t_{ij} - \frac{t_{i1}}{t_{11}} t_{1j}$$

for $2 \leqslant i \leqslant n+1$ and $2 \leqslant j \leqslant n$. The new relations are of the form

$$\begin{aligned} w_2' &= s_{22} v_2 + \cdots + s_{2n} v_n \\ \vdots \quad & \quad \vdots \qquad\qquad \vdots \\ w_{n+1}' &= s_{n+1,2} v_2 + \cdots + s_{n+1,n} v_n. \end{aligned}$$

This means that the set

$$T' = \{w_2', \ldots, w_{n+1}'\}$$

with $n$ elements is contained in $V_1$, which is generated by $n-1$ elements. By the induction hypothesis, the set $T'$ is linearly dependent. Therefore there exist $x_2, \ldots, x_{n+1}$ in $\mathbf{K}$, not all equal to 0, such that

$$x_2 w_2' + \cdots + x_{n+1} w_{n+1}' = 0_V.$$

If we replace $w_i'$ by its value (2.12), we get

$$-\Big(\sum_{i=2}^{n+1} \frac{t_{i1}}{t_{11}} x_i\Big) w_1 + x_2 w_2 + \cdots + x_{n+1} w_{n+1} = 0_V.$$

Since not all of $(x_2, \ldots, x_{n+1})$ are zero, this means that $T$ is linearly dependent. ☐

Proof of Theorem 2.7.1 for $V$ finite-dimensional. We denote by $n$ an integer $n \geqslant 0$ such that $V$ has a generating set $S_0$ with $n$ elements. This exists because $V$ is finite-dimensional.

(1) Consider the set $D$ of integers $d \geqslant 0$ such that there is a subset $T$ of $S$ with $d$ elements, such that $d$ is linearly independent. Since $\varnothing$ is linearly independent, the set $D$ is not empty. Moreover, by Lemma 2.7.7, the set $D$ is finite because no integer $\geqslant n+1$ can belong to $D$.

Let $m$ be the largest integer in $D$, and let $T \subset S$ be a linearly independent subset with $m$ elements ("a linearly independent subset with as many elements as possible"). We will show that $T$ is a basis of $V$.

Let $W = \langle T \rangle$. Since $T$ is linearly independent, $T$ is a basis of $V$ if and only if $W = V$. If this were *not* the case, then some element $w$ of $S$ would not be in $W$ (otherwise, $S \subset W$ implies that $V = \langle S \rangle \subset W$). But then Lemma 2.7.5 shows that $T \cup \{w\} \subset S$ is linearly independent in $V$, and since it contains more elements than $T$, this contradicts the definition of $m$. This contradictions means that, in fact, we have $W = V$, and therefore $T$ is a basis of $V$ contained in $S$.

(2) Consider now the set $D'$ of integers $d \geqslant 0$ such that there is a subset $T$ of $V$ containing $S$ which is a generating set of $V$. Since $S \cup S_0$ generates $V$, the set $D'$ is not empty. There exists then a smallest element $m$ of $D'$. Let $T$ be a generating subset of $V$, containing $S$, with cardinality $m$. We will show that $T$ is a basis of $V$.

Since $T$ generates $V$, it is enough to check that $T$ is linearly independent. Suppose this is not the case. Write $T = \{v_1, \ldots, v_m\}$ for distinct elements of $V$, where $S = \{v_1, \ldots, v_k\}$ for some $k \leqslant m$ (which we may assume because $S \subset T$).

The linear dependency means that there exist elements $t_1, \ldots, t_m$ of $\mathbf{K}$, not all zero, such that

$$t_1 v_1 + \cdots + t_m v_m = 0.$$

There exists some $i$ with $i \geqslant k+1$ such that $t_i \neq 0$, since otherwise the relation would imply that $S$ is linearly dependent. Assume for instance that $t_{k+1} \neq 0$ (up to exchanging two vectors, we may assume this). Then we get

$$v_{k+1} = -\frac{1}{t_{k+1}} (t_1 v_1 + \cdots + t_k v_k + t_{k+2} v_{k+2} + \cdots + t_m v_m).$$

Denote $T' = \{v_1, \ldots, v_k, v_{k+2}, \cdots, v_m\}$. Then $S \subset T'$, and this relation shows that $v_{k+1} \in \langle T' \rangle$. Lemma 2.7.6 shows that $T'$ generates $V$. Since $T'$ has $m-1$ elements and contains $S$, this contradicts the definition of $m$.

(3) Let $S_1$ and $S_2$ be two bases of $V$. Since $S_2$ is linearly independent and $S_1$ generates $V$, Lemma 2.7.7 shows that $\mathrm{Card}(S_2) \leqslant \mathrm{Card}(S_1)$. Similarly, we get $\mathrm{Card}(S_1) \leqslant \mathrm{Card}(S_2)$, and conclude that $S_1$ and $S_2$ have the same number of elements. ☐

REMARK 2.7.8. In the case of vector spaces which are not finite-dimensional, the proof of Theorem 2.7.1 requires the *axiom of choice* of set theory. In particular, in general, the bases which are shown to exist in Theorem 2.7.1 *cannot be written down explicitly*. As an example, there is no known explicit basis of $\{f : \mathbf{R} \to \mathbf{R}\}$ as an $\mathbf{R}$-vector space.

## 2.8. Properties of dimension

LEMMA 2.8.1. *Let $f : V_1 \longrightarrow V_2$ be an isomorphism between vector spaces. Then* $\dim(V_1) = \dim(V_2)$.

PROOF. Indeed, if $S \subset V_1$ is a basis of $V_1$, then $f(S) \subset V_2$ is a basis of $V_2$, by combining Lemma 2.5.9 and Lemma 2.6.3 (2). ☐

PROPOSITION 2.8.2. *Let $V$ be a $\mathbf{K}$-vector space with finite dimension.*

*Any subspace $W$ of $V$ has finite dimension; we have*

$$0 \leqslant \dim(W) \leqslant \dim(V),$$

*and* $\dim(W) = 0$ *if and only if* $W = \{0_V\}$, *while* $\dim(W) = \dim(V)$ *if and only if* $W = V$.

PROOF. We first prove that $W$ has finite dimension. We give two proofs, one depending on the general case of Theorem 2.7.1, the other not using possibly infinite bases.

**First proof.** Let $S$ be a basis of $W$. It is linearly independent in $V$, and therefore $\mathrm{Card}(S) \leqslant \dim(V)$ by Lemma 2.7.7.

This argument is fast but the existence of a basis was only fully proved in the finite-dimensional case earlier. If one takes this for granted, one can skip the next proof.

**Second proof.** Let $S = \{v_1, \ldots, v_n\}$ be a basis of $V$. For $1 \leqslant i \leqslant n$, we denote $W_i = W \cap \langle\{v_1, \ldots, v_i\}\rangle$. This is a subspace of $W$, and $W_n = W$ since $S$ generates $V$. We will show by induction on $i$, for $1 \leqslant i \leqslant n$, that $W_i$ is finite-dimensional.

For $i = 1$, the space $W_1$ is a subspace of $\langle\{v_1\}\rangle$. This means that either $W_1 = \{0_V\}$ or $W_1 = \{tv_1 \mid t \in \mathbf{K}\}$. In either case, $W_1$ is finite-dimensional.

Assume that $i \geqslant 2$ and that $W_{i-1}$ is finite-dimensional. Let $T_{i-1}$ be a finite generating set of $W_{i-1}$. Now consider $W_i$. If $W_i = W_{i-1}$, this inductive assumption shows that $W_i$ is finite-dimensional. Otherwise, let $w \in W_i - W_{i-1}$. We can write

$$w = t_1 v_1 + \cdots + t_i v_i$$

for some $t_j \in \mathbf{K}$, since $w \in \langle\{v_1, \ldots, v_i\}\rangle$. We have $t_i \neq 0$ since otherwise we would get $w \in W_{i-1}$, which is not the case.

Now let $v$ be any element of $W_i$. We can write

$$v = x_1 v_1 + \cdots + x_i v_i, \qquad x_j \in \mathbf{K}.$$

Then we get

$$v - \frac{x_i}{t_i} w = \Big(x_1 - \frac{x_i}{t_i} t_1\Big) v_1 + \cdots + \Big(x_{i-1} - \frac{x_i}{t_i} t_{i-1}\Big) v_{i-1} \in W_{i-1}.$$

So, in particular, $v - x_i t_i^{-1}$ is a linear combination of $T_{i=1}$, and hence $v$ is a linear combination of $T_{i-1} \cup \{w\}$. Since $v \in W_i$ was arbitrary, this means that $W_i$ is generated by $T_{i-1} \cup \{w\}$, which is finite. So $W_i$ is also finite-dimensional. This concludes the induction step.

Now we come back to our proof. Since $W$ is finite-dimensional, it has a basis $S$. The set $S$ is linearly independent in $V$, and hence by Theorem 2.7.1 (2), there is a basis $S'$ of $V$ containing $S$. This shows that

$$0 \leqslant \dim(W) = \mathrm{Card}(S) \leqslant \mathrm{Card}(S') = \dim(V).$$

If there is equality $\dim(W) = \dim(V)$, this means that $\mathrm{Card}(S) = \mathrm{Card}(S')$, and hence that $S' = S$ since $S \subset S'$. Then we get $W = \langle S' \rangle = V$. Finally, the equality $\dim(W) = 0$ means that $W$ contains no non-zero element, so $W = \{0_V\}$. ☐

DEFINITION 2.8.3 (Rank). Let $V_1$ and $V_2$ be vector spaces, with $V_2$ finite-dimensional. Let $f : V_1 \longrightarrow V_2$ be a linear map. The **rank** of $f$ is $\mathrm{rank}(f) = \dim \mathrm{Im}(f)$. If $A$ is a matrix, then $\mathrm{rank}(A) = \mathrm{rank}(f_A)$.

THEOREM 2.8.4. *Let $V_1$ and $V_2$ be finite-dimensional vector spaces. Let $f : V_1 \longrightarrow V_2$ be a linear map. We have*

$$\dim(V_1) = \dim \mathrm{Ker}(f) + \dim \mathrm{Im}(f) = \dim \mathrm{Ker}(f) + \mathrm{rank}(f). \tag{2.13}$$

PROOF. Let $d = \dim \mathrm{Ker}(f)$ and $n = \dim(V_1)$, so that $d \leqslant n$. Let $S_1 = \{v_1, \ldots, v_d\}$ be a basis of $\mathrm{Ker}(f)$. By Theorem 2.7.1 (2), there exists $S_2 = \{v_{d+1}, \ldots, v_n\}$ such that $S = S_1 \cup S_2$ is a basis of $V_1$.

Consider $T = \{f(v_{d+1}), \ldots, f(v_n)\} \subset V_2$. We will show that $T$ is a basis of $\mathrm{Im}(f)$ with $n - d$ elements, which will show that

$$\dim \mathrm{Im}(f) = \dim(V_1) - \dim \mathrm{Ker}(f),$$

which is the desired formula (2.13).

To check the property, consider $W = \langle S_2 \rangle$, which is a subspace of $V_1$ with dimension $n - d$ (since $S_2$ is linearly independent and generates it). Consider the linear map

$$g : W \longrightarrow \mathrm{Im}(f)$$

defined by $g(v) = f(v)$ for $v \in W$. It is indeed well-defined, since $f(v) \in \mathrm{Im}(f)$ for all $v \in V$. We claim that $g$ is a bijective linear map, from which $n - d = \dim(W) = \dim \mathrm{Im}(f)$ follows.

First, $g$ is injective: suppose $v \in \mathrm{Ker}(g)$. Since $v \in W$, we have

$$v = x_{d+1}v_{d+1} + \cdots + x_n v_n$$

for some $x_i \in \mathbf{K}$, $d + 1 \leqslant i \leqslant n$. But then $f(v) = g(v) = 0_{V_2}$, so $v \in \mathrm{Ker}(f) = \langle S_1 \rangle$, so we also have

$$v = x_1 v_1 + \cdots + x_d v_d$$

for some $x_i \in \mathbf{K}$, $1 \leqslant i \leqslant d$. Therefore

$$0_V = x_1 v_1 + \cdots + x_d v_d - x_{d+1} v_{d+1} - \cdots - x_n v_n.$$

But $S_1 \cup S_2$ is linearly independent, and so we must have $x_i = 0$ for all $i$, which implies $v = 0$. So $\mathrm{Ker}(g) = \{0_{V_1}\}$.

Second, $g$ is surjective: if $w \in \mathrm{Im}(f)$, we can write $w = f(v)$ for some $v \in V_1$; then we write

$$v = t_1 v_1 + \cdots + t_n v_n$$

for some $t_i \in \mathbf{K}$, and we get

$$w = f(v) = f(t_1 v_1 + \cdots + t_d v_d) + f(t_{d+1} v_{d+1} + \cdots + t_n v_n) = 0_V + f(v') = f(v')$$

(since $t_1 v_1 + \cdots + t_d v_d \in \langle S_1 \rangle = \mathrm{Ker}(f)$), where

$$v' = t_{d+1} v_{d+1} + \cdots + t_n v_n \in W.$$

This means that $w = g(v') \in \mathrm{Im}(g)$, so that $\mathrm{Im}(g) = \mathrm{Im}(f)$, and $g$ is surjective. ☐

COROLLARY 2.8.5. *Let $V_1$ and $V_2$ be finite-dimensional vector spaces with $\dim(V_1) = \dim(V_2)$. Let $f : V_1 \to V_2$ be a linear map. Then $f$ is injective if and only if $f$ is surjective if and only if $f$ is bijective.*

PROOF. This is because $f$ is injective if and only if $\mathrm{Ker}(f) = \{0_{V_1}\}$, which is equivalent with $\dim \mathrm{Ker}(f) = 0$, and in turn (2.13) shows that this is equivalent with $\dim \mathrm{Im}(f) = \dim(V_1)$. Under the assumption that $\dim(V_1) = \dim(V_2)$, this is therefore the same as $\dim(V_2) = \dim \mathrm{Im}(f)$, which means that $\mathrm{Im}(f) = V_2$ (since it is a subspace of $V_2$), and this in turn means that $f$ is surjective.

So injectivity is equivalent to surjectivity, and therefore either is equivalent to bijectivity. ☐

COROLLARY 2.8.6. *Let $V_1$ and $V_2$ be finite-dimensional vector spaces and $f : V_1 \to V_2$ be a linear map. We have*

$$\mathrm{rank}(f) \leqslant \min(\dim(V_1), \dim(V_2)),$$

*and furthermore*

$$\mathrm{rank}(f) = \dim(V_1) \Leftrightarrow f \text{ is injective},$$
$$\mathrm{rank}(f) = \dim(V_2) \Leftrightarrow f \text{ is surjective}.$$

PROOF. Since $\mathrm{rank}(f) = \dim \mathrm{Im}(f)$ and $\mathrm{Im}(f) \subset V_2$, it follows from Proposition 2.8.2 that $\mathrm{rank}(f) \leqslant \dim(V_2)$, with equality if and only if $\mathrm{Im}(f) = V_2$, which is exactly the same as surjectivity of $f$.

For the kernel, by (2.13), we have

$$\dim(V_1) = \mathrm{rank}(f) + \dim \mathrm{Ker}(f),$$

and therefore $\mathrm{rank}(f) = \dim(V_1) - \dim \mathrm{Ker}(f) \leqslant \dim(V_1)$, with equality if and only if $\dim \mathrm{Ker}(f) = 0$, which means if and only if $\mathrm{Ker}(f) = \{0_{V_1}\}$, namely if and only if $f$ is injective (Proposition 2.4.4 (2)). ☐

COROLLARY 2.8.7. *Let $V_1$ and $V_2$ be finite-dimensional vector spaces and $f : V_1 \to V_2$ be a linear map.*

(1) *If $\dim(V_1) < \dim(V_2)$, then $f$ is not surjective.*

(2) *If $\dim(V_1) > \dim(V_2)$, then $f$ is not injective. In particular, if $\dim(V_1) > \dim(V_2)$, then there exists a non-zero vector $v \in V_1$ such that $f(v) = 0_{V_2}$.*

PROOF. If $\dim(V_1) < \dim(V_2)$, then $\mathrm{rank}(f) \leqslant \dim(V_1) < \dim(V_2)$, so $f$ is not surjective by Corollary 2.8.6.

If $\dim(V_1) > \dim(V_2)$, then $\mathrm{rank}(f) \leqslant \dim(V_2) < \dim(V_1)$, so $f$ is not injective by Corollary 2.8.6. ☐

We have seen that isomorphic vector spaces have the same dimension (Lemma 2.8.1). The next result shows that conversely, if two spaces have the same dimension, there *exists* an isomorphism between them.

PROPOSITION 2.8.8. *Let $V_1$ and $V_2$ be $\mathbf{K}$-vector spaces with the same dimension. Then there exists an isomorphism $f : V_1 \longrightarrow V_2$.*

PROOF FOR FINITE-DIMENSIONAL SPACES. Let $n = \dim(V_1) = \dim(V_2)$. We begin with the special case $V_1 = \mathbf{K}^n$. Let $T = \{v_1, \ldots, v_n\}$ be a basis of $V_2$. Define the linear map $g_T : \mathbf{K}^n \longrightarrow V_2$ by

$$g_T\left(\begin{pmatrix} t_1 \\ \vdots \\ t_n \end{pmatrix}\right) = t_1 v_1 + \cdots + t_n v_n,$$

as in Proposition 2.6.6. By Proposition 2.6.6 (3), this map $g_T$ is an isomorphism, since $T$ is a basis of $V_2$.

For the general case, consider bases $S$ and $T$ of $V_1$ and $V_2$ respectively. We have linear maps $g_T : \mathbf{K}^n \longrightarrow V_2$ and $g_S : \mathbf{K}^n \longrightarrow V_1$, constructed as above. Both are isomorphisms, and hence

$$g_T \circ g_S^{-1} : V_1 \longrightarrow V_2$$

is an isomorphism (Proposition 2.3.8). ☐

REMARK 2.8.9. In general, there are *many* isomorphisms $V_1 \longrightarrow V_2$. Also, there exist of course linear maps $f : V_1 \longrightarrow V_2$ which are *not* isomorphisms, for instance $f(x) = 0_{V_2}$ for all $x \in V_1$.

## 2.9. Matrices and linear maps

We will now show how to use matrices and bases to describe arbitrary linear maps between finite-dimensional vector spaces.

DEFINITION 2.9.1 (Ordered basis). Let $V$ be a finite-dimensional $\mathbf{K}$-vector space of dimension $d \geqslant 0$. An **ordered basis** of $V$ is a $d$-tuple $(v_1, \ldots, v_d)$ such that the set $\{v_1, \ldots, v_d\}$ is a basis of $V$. Hence an ordered basis is in particular an element of $V^d$.

REMARK 2.9.2. For instance, the following are two *different* ordered bases of $\mathbf{K}^2$:

$$\left(\begin{pmatrix}1\\0\end{pmatrix}, \begin{pmatrix}0\\1\end{pmatrix}\right), \qquad \left(\begin{pmatrix}0\\1\end{pmatrix}, \begin{pmatrix}1\\0\end{pmatrix}\right).$$

On the other hand, the 3-tuple

$$(v_1, v_2, v_3) = \left(\begin{pmatrix}1\\0\end{pmatrix}, \begin{pmatrix}0\\1\end{pmatrix}, \begin{pmatrix}0\\1\end{pmatrix}\right),$$

is *not* an ordered basis because it has more than 2 components, although $\{v_1, v_2, v_3\} = \{v_1, v_2\}$ *is* a basis of $\mathbf{K}^2$.

DEFINITION 2.9.3 (Matrix with respect to a basis). Let $V_1$ and $V_2$ be two finite-dimensional vector spaces with $\dim(V_1) = n$ and $\dim(V_2) = m$. Let $f : V_1 \to V_2$ be a linear map.

Let $B_1 = (e_1, \ldots, e_n)$ and $B_2 = (f_1, \ldots, f_m)$ be ordered bases of $V_1$ and $V_2$, respectively.

The **matrix of $f$ with respect to $B_1$ and $B_2$**, denoted

$$\mathrm{Mat}(f; B_1, B_2),$$

is the matrix $A \in M_{m,n}(\mathbf{K})$ with coefficients $(a_{ij})_{\substack{1 \leqslant i \leqslant m \\ 1 \leqslant j \leqslant n}}$ such that the $j$-th column of $A$ is the vector

$$\begin{pmatrix} a_{1j} \\ \vdots \\ a_{mj} \end{pmatrix} \in \mathbf{K}^m$$

such that

$$f(e_j) = a_{1j} f_1 + \cdots + a_{mj} f_m, \qquad 1 \leqslant j \leqslant n.$$

EXAMPLE 2.9.4. (1) Let $V_1 = V_2$, $B_1 = B_2$, and $f = \mathrm{Id}_{V_1}$. Then $f$ is linear (Proposition 2.3.8 (1)) and $\mathrm{Mat}(\mathrm{Id}_{V_1}; B_1, B_1) = 1_n$, the identity matrix of size $n$.

(2) Let $V_1 = \mathbf{K}^n$, $V_2 = \mathbf{K}^m$, $A = (a_{ij})$ a matrix in $M_{m,n}(\mathbf{K})$ and $f = f_A : V_1 \longrightarrow V_2$ the associated linear map given by $f_A(x) = Ax$.

Consider the ordered bases

$$B_1 = (e_1, \ldots, e_n), \qquad B_2 = (f_1, \ldots, f_m),$$

where $\{e_i\}$ is the basis of Example 2.6.5 (3), and $\{f_j\}$ is the same basis for $\mathbf{K}^m$, so for instance

$$f_1 = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}.$$

We know that $f_A(e_j)$ is the $j$-th column of $A$ (see (2.1)). In the basis $B_2$, this is simply

$$\sum_{i=1}^{m} a_{ij} f_i,$$

and hence the $j$-th column of $\mathrm{Mat}(f_A; B_1, B_2)$ is the same as the $j$-th column of $A$. In other words, we have

$$\mathrm{Mat}(f_A; B_1, B_2) = A.$$

However, one must be careful that this is only because of the specific choice of bases! For instance, take $m = n = 3$, and consider instead the ordered bases

$$B_1' = (e_1, e_3, e_2), \qquad B_2' = (e_3, e_2, e_1).$$

Let $A$ be the matrix

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

The above shows that

$$\mathrm{Mat}(f_A; B_1, B_2) = A.$$

Now we compute $\mathrm{Mat}(f_A; B_1', B_2')$. We have

$$f_A(e_1) = \begin{pmatrix} 1 \\ 4 \\ 7 \end{pmatrix} = 7e_3 + 4e_2 + e_1, \quad f_A(e_3) = \begin{pmatrix} 3 \\ 6 \\ 9 \end{pmatrix} = 9e_3 + 6e_2 + 3e_1,$$

$$f_A(e_2) = \begin{pmatrix} 2 \\ 5 \\ 8 \end{pmatrix} = 8e_3 + 5e_3 + 2e_1,$$

and therefore

$$\mathrm{Mat}(f_A; B_1', B_2') = \begin{pmatrix} 7 & 9 & 8 \\ 4 & 6 & 5 \\ 1 & 3 & 2 \end{pmatrix} \neq A.$$

The most important facts about the matrix representation of linear maps is that: (1) it respects all important operations on linear maps; (2) it determines the linear map. Precisely:

Theorem 2.9.5. *Let $V_1$, $V_2$, $V_3$ be finite-dimensional vector spaces with $\dim(V_1) = n$, $\dim(V_2) = m$ and $\dim(V_3) = p$. Let $B_i$ be an ordered basis of $V_i$ for $1 \leqslant i \leqslant 3$. For any linear maps*

$$V_1 \xrightarrow{f} V_2 \xrightarrow{g} V_3,$$

*we have*

$$\mathrm{Mat}(g \circ f; B_1, B_3) = \mathrm{Mat}(g; B_2, B_3) \cdot \mathrm{Mat}(f; B_1, B_2).$$

Proof. We write $B_1 = (e_1, \ldots, e_n)$, $B_2 = (f_1, \ldots, f_m)$ and $B_3 = (v_1, \ldots, v_p)$. Let $A = \mathrm{Mat}(f; B_1, B_2)$, $B = \mathrm{Mat}(g; B_2, B_3)$ and $C = \mathrm{Mat}(g \circ f; B_1, B_3)$. Write

$$A = (a_{ij})_{\substack{1 \leqslant i \leqslant m \\ 1 \leqslant j \leqslant n}}, \quad B = (b_{ki})_{\substack{1 \leqslant k \leqslant p \\ 1 \leqslant i \leqslant m}}, \quad C = (c_{kj})_{\substack{1 \leqslant k \leqslant p \\ 1 \leqslant j \leqslant n}}.$$

For $1 \leqslant j \leqslant n$, the $j$-th column of $A$ is determined by

$$f(e_j) = \sum_{i=1}^{m} a_{ij} f_i,$$

and the $j$-th column of $C$ is determined by

$$(g \circ f)(e_j) = \sum_{k=1}^{p} c_{kj} v_k.$$

But

$$\begin{aligned} g(f(e_j)) &= \sum_{i=1}^{m} a_{ij} g(f_i) \\ &= \sum_{i=1}^{m} a_{ij} \sum_{k=1}^{p} b_{ki} v_k = \sum_{k=1}^{p} \Big( \sum_{i=1}^{m} b_{ki} a_{ij} \Big) v_k, \end{aligned}$$

and therefore we have

$$c_{kj} = \sum_{i=1}^{m} b_{ki} a_{ij}.$$

This precisely means that $C = BA$ (see Theorem 2.2.1). $\square$

Theorem 2.9.6. *Let $V_1$ and $V_2$ be two finite-dimensional vector spaces with $\dim(V_1) = n$ and $\dim(V_2) = m$. Let $B_i$ be an ordered basis of $V_i$. The map*

$$T_{B_1,B_2} \begin{cases} \mathrm{Hom}_{\mathbf{K}}(V_1, V_2) & \longrightarrow & M_{m,n}(\mathbf{K}) \\ f & \mapsto & \mathrm{Mat}(f; B_1, B_2) \end{cases}$$

*is an isomorphism of vector spaces.*

*In particular:*

(1) *We have $\dim \mathrm{Hom}_{\mathbf{K}}(V_1, V_2) = mn = \dim(V_1)\dim(V_2)$.*

(2) *If two linear maps $f_1$ and $f_2$ coincide on the basis $B_1$, then they are equal.*

Proof. We write

$$B_1 = (e_1, \ldots, e_n), \qquad B_2 = (f_1, \ldots, f_m).$$

The linearity of the map $T_{B_1,B_2}$ is left as exercise. To check that it is an isomorphism, we prove that it is injective and surjective (one can also directly compute the dimension of $\mathrm{Hom}_{\mathbf{K}}(V_1, V_2)$ to see that it is equal to $mn = \dim M_{m,n}(\mathbf{K})$, and then we would only need to check injectivity).

First, we show that the map is injective. So suppose that $f \in \mathrm{Ker}(T_{B_1,B_2})$, so that $\mathrm{Mat}(f; B_1, B_2) = 0_{m,n}$. This means by definition that $f(e_j) = 0_{V_2}$ for $1 \leqslant j \leqslant n$. But then

$$f(t_1 e_1 + \cdots + t_n e_n) = 0_{V_2}$$

for all $t_i \in \mathbf{K}$, by linearity, and since $B_1$ is a basis of $V_1$, this means that $f(v) = 0$ for all $v \in V_1$, or in other words that $f = 0$ as element of $\mathrm{Hom}_{\mathbf{K}}(V_1, V_2)$. Therefore $\mathrm{Ker}(T_{B_1,B_2}) = \{0\}$ so $T_{B_1,B_2}$ is injective (Proposition 2.4.4 (2)). Note that the injectivity implies the last part of the statement: indeed, to say that $f_1$ and $f_2$ coincide on $B_1$ is to say that $f_1(e_j) = f_2(e_j)$ for $1 \leqslant j \leqslant n$, which means that the matrices of $f_1$ and $f_2$ with respect to $B_1$ and $B_2$ are the same, i.e., that $T_{B_1,B_2}(f_1) = T_{B_1,B_2}(f_2)$, so that injectivity implies $f_1 = f_2$.

Second, we prove surjectivity. Let $A = (a_{ij}) \in M_{m,n}(\mathbf{K})$ be given. We define vectors

$$w_j = \sum_{i=1}^{n} a_{ij} f_i \in V_2. \tag{2.14}$$

We then define a map

$$f : V_1 \longrightarrow V_2$$

by

$$f(t_1 e_1 + \cdots + t_n e_n) = \sum_{j=1}^{n} t_j w_j$$

for all $t_i \in \mathbf{K}$. This is well-defined, since any element of $V_1$ has a unique expression as a linear combination of the $e_j$'s.

For any $v_1$ and $v_2$ in $V_1$, expressed as

$$v_1 = t_1 e_1 + \cdots + t_n e_n, \qquad v_2 = s_1 e_1 + \cdots + s_n e_n$$

with $t_i$ and $s_i$ in $\mathbf{K}$, and for any $x_1$, $x_2 \in \mathbf{K}$, we have

$$x_1 v_1 + x_2 v_2 = (x_1 t_1 + x_2 s_1) e_1 + \cdots + (x_1 t_n + x_2 s_n) e_n.$$

Therefore, we have

$$f(x_1 v_1 + x_2 v_2) = \sum_{j=1}^{n} (x_1 t_j + x_2 s_j) w_j = x_1 \sum_j t_j w_j + x_2 \sum_j s_j w_j = x_1 f(v_1) + x_2 f(v_2).$$

This means that $f$ is linear, so $f \in \mathrm{Hom}_{\mathbf{K}}(V_1, V_2)$.

Now we compute the matrix $T(f) = \mathrm{Mat}(f; B_1, B_2)$. By definition we have $f(e_j) = w_j$ for $1 \leqslant j \leqslant n$, so that (2.14) shows that the $j$-th column of $T(f)$ is the vector

$$\begin{pmatrix} a_{1j} \\ \vdots \\ a_{mj} \end{pmatrix}.$$

This is the $j$-th column of $A$, and hence $T_{B_1,B_2}(f) = A$. So $A \in \mathrm{Im}(T_{B_1,B_2})$. Since this is true for all $A$, this means that $T$ is surjective. ☐

Remark 2.9.7. It is important to remember how the surjectivity is proved, because one is often given a matrix and one has to construct the associated linear map!

Corollary 2.9.8. *Let $V_1$ and $V_2$ be finite-dimensional $\mathbf{K}$-vector spaces and $f : V_1 \longrightarrow V_2$ a linear map. Let $B_1$ and $B_2$ be ordered bases of $V_1$ and $V_2$ respectively.*

*Then $f$ is bijective if and only if $\mathrm{Mat}(f; B_1, B_2)$ is invertible.*

*We then have*

$$\mathrm{Mat}(f^{-1}; B_2, B_1) = \mathrm{Mat}(f; B_1, B_2)^{-1}.$$

Proof. Let $n = \dim(V_1)$, $m = \dim(V_2)$.

(1) Suppose that $f$ is bijective. Then $n = m$ (Lemma 2.8.1), and Theorem 2.9.5 shows that

$$\mathrm{Mat}(f^{-1}; B_2, B_1) \cdot \mathrm{Mat}(f; B_1, B_2) = \mathrm{Mat}(f^{-1} \circ f; B_1, B_1) = \mathrm{Mat}(\mathrm{Id}_{V_1}; B_1, B_1) = 1_n,$$

and

$$\mathrm{Mat}(f; B_1, B_2) \cdot \mathrm{Mat}(f^{-1}; B_2, B_1) = \mathrm{Mat}(f \circ f^{-1}; B_2, B_2) = \mathrm{Mat}(\mathrm{Id}_{V_2}; B_2, B_2) = 1_n,$$

so that $\mathrm{Mat}(f; B_1, B_2)$ is indeed invertible with inverse $\mathrm{Mat}(f^{-1}; B_2, B_1)$.

(2) Suppose that the matrix $A = \mathrm{Mat}(f; B_1, B_2)$ is invertible, and let $B$ be its inverse. Since $f_A : \mathbf{K}^n \longrightarrow \mathbf{K}^m$ is bijective, it is an isomorphism (Proposition 2.3.11) so that $n = m$ (Lemma 2.8.1). By the surjectivity part of Theorem 2.9.6, there exists $g \in \mathrm{Hom}_{\mathbf{K}}(V_2, V_1)$ such that $\mathrm{Mat}(g; B_2, B_1) = B$. We then get by Theorem 2.9.5 the relations

$$\mathrm{Mat}(f \circ g; B_2, B_2) = AB = 1_n = \mathrm{Mat}(\mathrm{Id}_{V_2}; B_2, B_2),$$
$$\mathrm{Mat}(g \circ f; B_1, B_1) = BA = 1_n = \mathrm{Mat}(\mathrm{Id}_{V_1}; B_1, B_1).$$

The injectivity statement of Theorem 2.9.6 implies that $f \circ g = \mathrm{Id}_{V_2}$ and $g \circ f = \mathrm{Id}_{V_1}$, which means that $f$ is a bijection with reciprocal bijection $g$. By construction, we get

$$\mathrm{Mat}(f^{-1}; B_2, B_1) = \mathrm{Mat}(g; B_2, B_1) = B = A^{-1}.$$

□

The following lemma shows how to use matrix computations to compute a linear map, given its representation as a matrix with respect to fixed bases.

LEMMA 2.9.9. *Let $V_1$ and $V_2$ be finite-dimensional $\mathbf{K}$-vector spaces and $f : V_1 \longrightarrow V_2$ a linear map. Let $B_1 = (e_1, \ldots, e_n)$ and $B_2 = (f_1, \ldots, f_m)$ be ordered bases of $V_1$ and $V_2$ respectively and $A = \mathrm{Mat}(f; B_1, B_2)$.*

*For $v \in V_1$ such that*

$$v = t_1 e_1 + \cdots + t_n e_n,$$

*we have*

$$f(v) = s_1 f_1 + \cdots + s_m f_m$$

*where*

$$\begin{pmatrix} s_1 \\ \vdots \\ s_m \end{pmatrix} = A \begin{pmatrix} t_1 \\ \vdots \\ t_n. \end{pmatrix}$$

PROOF. Let $A = (a_{ij})$. Since $f$ is linear, we have

$$f(v) = t_1 f(e_1) + \cdots + t_n f(e_n).$$

Replacing $f(e_j)$ with the linear combination of the basis $B_2$ given by the columns of the matrix $A$, we get

$$f(v) = \sum_{j=1}^{n} t_j \sum_{i=1}^{m} a_{ij} f_i = \sum_{i=1}^{m} \Bigl(\sum_{j=1}^{n} a_{ij} t_j\Bigr) f_i.$$

This means that

$$f(v) = s_1 f_1 + \cdots + s_m f_m$$

where

$$s_i = \sum_{j=1}^{n} a_{ij} t_j.$$

But the vector

$$\begin{pmatrix} s_1 \\ \vdots \\ s_m \end{pmatrix} = \begin{pmatrix} \sum_{j=1}^{n} a_{1j} t_j \\ \vdots \\ \sum_{j=1}^{n} a_{mj} t_j \end{pmatrix} \in \mathbf{K}^m$$

is precisely the vector

$$A\begin{pmatrix} t_1 \\ \vdots \\ t_n \end{pmatrix},$$

(see Example 2.2.4) hence the result. $\square$

DEFINITION 2.9.10 (Change of basis matrix). Let $V$ be a finite-dimensional $\mathbf{K}$-vector space. Let $B$ and $B'$ be ordered bases of $V$. The **change of basis matrix** from $B$ to $B'$ is the matrix $\mathrm{Mat}(\mathrm{Id}_V; B, B')$. We denote it also $\mathrm{M}_{B,B'}$.

EXAMPLE 2.9.11. (1) Let $n = \dim(V)$. We have $\mathrm{M}_{B,B} = 1_n$ for any ordered basis $B$ of $V$ (Example 2.9.4 (1)).

(2) Let $V = \mathbf{K}^n$, and let

$$B = \left(\begin{pmatrix} a_{11} \\ \vdots \\ a_{n1} \end{pmatrix}, \ldots, \begin{pmatrix} a_{1n} \\ \vdots \\ a_{nn} \end{pmatrix}\right)$$

and

$$B' = (e_1, \ldots, e_n),$$

the basis of Example 2.6.5 (3). Then

$$\mathrm{M}_{B,B'} = \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & & \vdots \\ a_{n1} & \cdots & a_{nn} \end{pmatrix}$$

since

$$\begin{pmatrix} a_{1j} \\ \vdots \\ a_{nj} \end{pmatrix} = a_{1j}e_1 + \cdots + a_{nj}e_n$$

for $1 \leqslant j \leqslant n$.

PROPOSITION 2.9.12. *Let $V$ be a finite-dimensional $\mathbf{K}$-vector space.*

(1) *For any ordered bases $B$ and $B'$ of $V$, the change of basis matrix $\mathrm{M}_{B,B'}$ is invertible with inverse*

$$\mathrm{M}_{B,B'}^{-1} = \mathrm{M}_{B',B}\,. \tag{2.15}$$

(2) *For any ordered bases $B$, $B'$, $B''$ of $V$, we have*

$$\mathrm{M}_{B,B''} = \mathrm{M}_{B',B''}\,\mathrm{M}_{B,B'}\,. \tag{2.16}$$

PROOF. (1) The linear map $\mathrm{Id}_V$ is bijective, with its inverse equal to $\mathrm{Id}_V$. Therefore Corollary 2.9.8 shows that $\mathrm{M}_{B,B'} = \mathrm{Mat}(\mathrm{Id}_V; B, B')$ is invertible with inverse the matrix $\mathrm{Mat}(\mathrm{Id}_V; B', B) = \mathrm{M}_{B',B}$.

(2) We apply Theorem 2.9.5 to $V_1 = V_2 = V_3 = V$, with $g = f = \mathrm{Id}_V$ and $B_1 = B$, $B_2 = B'$ and $B_3 = B''$. Then $g \circ f = \mathrm{Id}_V$, and we get

$$\mathrm{Mat}(\mathrm{Id}_V; B, B'') = \mathrm{Mat}(\mathrm{Id}_V; B', B'') \cdot \mathrm{Mat}(\mathrm{Id}_V; B, B'),$$

which is exactly (2.16), by definition of the change of basis matrices. $\square$

Proposition 2.9.13. *Let $V_1$ and $V_2$ be finite-dimensional* $\mathbf{K}$*-vector spaces and* $f : V_1 \longrightarrow V_2$ *a linear map. Let* $B_1$, $B_1'$ *be ordered bases of* $V_1$, *and* $B_2$, $B_2'$ *be ordered bases of* $V_2$. *We have*

$$\mathrm{Mat}(f; B_1', B_2') = \mathrm{M}_{B_2,B_2'}\, \mathrm{Mat}(f; B_1, B_2)\, \mathrm{M}_{B_1',B_1}\,. \tag{2.17}$$

*In particular, if* $f : V_1 \longrightarrow V_1$ *is a linear map, we have*

$$\mathrm{Mat}(f; B_1', B_1') = A\,\mathrm{Mat}(f; B_1, B_1)A^{-1} \tag{2.18}$$

*where* $A = \mathrm{M}_{B_1,B_1'}$.

Proof. We consider the composition

$$\begin{array}{ccccccc} V_1 & \xrightarrow{\mathrm{Id}_{V_1}} & V_1 & \xrightarrow{f} & V_2 & \xrightarrow{\mathrm{Id}_{V_2}} & V_2 \\ B_1' & & B_1 & & B_2 & & B_2' \end{array}$$

and the ordered bases indicated. The composite linear map is $f$. By Theorem 2.9.5, we get the matrix equation

$$\mathrm{Mat}(f; B_1', B_2') = \mathrm{Mat}(\mathrm{Id}_{V_2}; B_2, B_2')\,\mathrm{Mat}(f; B_1, B_2)\,\mathrm{Mat}(\mathrm{Id}_{V_1}; B_1', B_1),$$

which is exactly (2.17).

In the special case $V_2 = V_1$, and $B_1 = B_2$, $B_1' = B_2'$, this becomes

$$\mathrm{Mat}(f; B_1', B_1') = \mathrm{Mat}(\mathrm{Id}_{V_1}; B_1, B_1')\,\mathrm{Mat}(f; B_1, B_1)\,\mathrm{Mat}(\mathrm{Id}_{V_1}; B_1', B_1).$$

By Proposition 2.9.12, the matrix $\mathrm{Mat}(\mathrm{Id}_{V_1}; B_1, B_1') = \mathrm{M}_{B_1,B_1'} = A$ is invertible with inverse $A^{-1} = \mathrm{M}_{B_1',B_1} = \mathrm{Mat}(\mathrm{Id}_{V_1}; B_1', B_1)$, so the formula becomes

$$\mathrm{Mat}(f; B_1', B_1') = A\,\mathrm{Mat}(f; B_1, B_1)A^{-1}.$$

$\square$

Example 2.9.14. Consider a real number $t$ and the matrix

$$M = \begin{pmatrix} \cos(t) & -\sin(t) \\ \sin(t) & \cos(t) \end{pmatrix} \in M_{2,2}(\mathbf{C}).$$

Let $f : \mathbf{C}^2 \longrightarrow \mathbf{C}^2$ be the linear map $f(x) = Mx$. Then $M$ is the matrix of $f$ with respect to the ordered basis

$$B = \left(\begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix}\right)$$

of $\mathbf{C}^2$ (namely, $M = \mathrm{Mat}(f; B, B)$).

Consider the vectors

$$B' = \left(\begin{pmatrix} 1 \\ i \end{pmatrix}, \begin{pmatrix} 1 \\ -i \end{pmatrix}\right).$$

We claim that $B'$ is an ordered basis of $\mathbf{C}^2$. We will check this at the same time as computing the change of basis matrix $A = \mathrm{M}_{B,B'}$ and its inverse $A^{-1} = \mathrm{M}_{B',B}$. To compute $A$, we must express the vectors $v$ in $B$ as linear combinations of elements of $B'$; if this succeeds for all $v$ in $B$, this implies that the elements of $B'$ generate $\mathbf{C}^2$, and since there are two, this means that $B'$ is an ordered basis.

So we must find complex numbers $(a, b, c, d)$ such that

$$\begin{pmatrix} 1 \\ 0 \end{pmatrix} = a\begin{pmatrix} 1 \\ i \end{pmatrix} + b\begin{pmatrix} 1 \\ -i \end{pmatrix}$$
$$\begin{pmatrix} 0 \\ 1 \end{pmatrix} = c\begin{pmatrix} 1 \\ i \end{pmatrix} + d\begin{pmatrix} 1 \\ -i \end{pmatrix}.$$

We see that this is possible with $a = b = 1/2$ and $c = -d = 1/(2i)$. So $B'$ is an ordered basis and

$$A = \mathrm{M}_{B,B'} = \begin{pmatrix} 1/2 & 1/(2i) \\ 1/2 & -1/(2i) \end{pmatrix}.$$

To compute $\mathrm{M}_{B',B}$, we use Example 2.9.11 (2): this implies that

$$\mathrm{M}_{B',B} = \begin{pmatrix} 1 & 1 \\ i & -i \end{pmatrix}.$$

(We can also check by hand that this is the inverse of $A$). We now compute the matrix $N$ representing $f$ with respect to the bases $(B', B')$. By (2.18), we get

$$N = AMA^{-1} = \begin{pmatrix} 1/2 & 1/(2i) \\ 1/2 & -1/(2i) \end{pmatrix} \begin{pmatrix} \cos(t) & -\sin(t) \\ \sin(t) & \cos(t) \end{pmatrix} \begin{pmatrix} 1 & 1 \\ i & -i \end{pmatrix}.$$

The product of the second and third matrices is

$$\begin{pmatrix} \cos(t) - i\sin(t) & \cos(t) + i\sin(t) \\ \sin(t) + i\cos(t) & \sin(t) - i\cos(t) \end{pmatrix} = \begin{pmatrix} e^{-it} & e^{it} \\ ie^{-it} & -ie^{it} \end{pmatrix}.$$

Multiplying by the first matrix we get

$$N = \begin{pmatrix} e^{-it}/2 + e^{-it}/2 & e^{it}/2 - e^{it}/2 \\ e^{-it}/2 - e^{-it}/2 & e^{it}/2 + e^{it}/2 \end{pmatrix} = \begin{pmatrix} e^{-it} & 0 \\ 0 & e^{it} \end{pmatrix}.$$

## 2.10. Solving linear equations

We explain in this section the Gauss Elimination Algorithm that gives a systematic approach to solving systems of linear equations, and interpret the results in terms of the image and kernel of a linear map $f_A : \mathbf{K}^n \longrightarrow \mathbf{K}^m$.

The justification of the algorithm will be quite brief, because from our point of view it is a tool, and in general the results that it gives can be checked in any concrete case. For the purpose of this course, it is more important to know how to handle the computations correctly for small systems than to understand the full details (especially with respect to numerical stability, etc).

In this section, we will denote by $C_i$ and $R_j$ the $i$-th column and $j$-th row of a matrix, which will be clear in context.

Definition 2.10.1 (Extended matrix). For a matrix $A \in M_{m,n}(\mathbf{K})$ and $b \in \mathbf{K}^m$, we denote by $(A, b)$ the **extended matrix** in $M_{m,n+1}(\mathbf{K})$ where $b$ is the $(n+1)$-st column.

Definition 2.10.2 (Leading zeros). For a row vector $v = (t_1, \ldots, t_n) \in \mathbf{K}_n = M_{1,n}(\mathbf{K})$, we denote by $N(v)$ the number of **leading zeros** of $v$: for $0 \leqslant i \leqslant n$, we have $N(v) = i$ if and only if

$$t_1 = \cdots = t_i = 0, \qquad t_{i+1} \neq 0,$$

with the conventions that

$$N(0) = n, \qquad N(v) = 0 \text{ if } t_1 \neq 0.$$

Example 2.10.3. To clarify the meaning, observe the following cases:

$$N((1,2,3,4)) = 0, \quad N((0,1,0,0,0,3,0,4)) = 1$$
$$N((0,0,0,1)) = 3.$$

Moreover $v = 0$ if and only if $N(v) = n$.

DEFINITION 2.10.4 (Row Echelon matrices). (1) A matrix $A \in M_{m,n}(\mathbf{K})$ is in **row echelon form** (abbreviated) REF if, for $1 \leqslant i \leqslant m-1$, we have

$$N(R_{i+1}) \geqslant N(R_i),$$

and $N(R_{i+1}) > N(R_i)$ unless $R_i = 0$, where we recall that $R_i$ denotes the $i$-th row of $A$.

(2) For $0 \leqslant k \leqslant n$, a matrix $A \in M_{m,n}(\mathbf{K})$ is in ***k*-partial row echelon form** (abbreviated) $k$-pREF if the matrix formed with the $k$ first columns of $A$, taken in order, is in REF, with the convention that $A$ is always in 0-pREF.

EXAMPLE 2.10.5. (1) The following matrices are REF:

$$\begin{pmatrix} 0 & 1 & 0 & 2 \\ 0 & 0 & 0 & 3 \\ 0 & 0 & 0 & 0 \end{pmatrix}, \quad \begin{pmatrix} -1 & 3 & 4 \\ 0 & 2 & 0 \\ 0 & 0 & 12 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & -5 & 12 \end{pmatrix}$$

but the following are not:

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

The first matrix is 1-pREF, the others are only 0-pREF.

(2) Let $m = n$, and suppose that $A$ is upper-triangular, with non-zero diagonal coefficients:

$$A = \begin{pmatrix} a_{11} & \cdots & \cdots & \cdots \\ 0 & a_{22} & \cdots & \cdots \\ \vdots & \vdots & \vdots & \vdots \\ 0 & \cdots & 0 & a_{nn} \end{pmatrix}$$

with $a_{ij} = 0$ if $i > j$, and $a_{ii} \neq 0$ for $1 \leqslant i \leqslant n$. Then $A$ is REF.

(3) Suppose $n = 1$; then a column vector is REF if and only if it is of the form

$$\begin{pmatrix} t \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

for some $t \in \mathbf{K}$ (which may be zero or not).

(4) Suppose $n = 2$; then a matrix with 2 columns is REF if and only if

$$A = \begin{pmatrix} t & u \\ 0 & v \\ 0 & 0 \\ \vdots & \vdots \end{pmatrix}$$

with:

- $t \neq 0$,
- or $t = 0$ and $v = 0$.

We now consider two types of elementary operations on an extended matrix $(A, b)$.

DEFINITION 2.10.6 (Elementary operations). (1) **(Row exchange)** For $1 \leqslant i, j \leqslant m$, we define $(A', b') = \mathbf{exch}_{i,j}((A, b))$ to be the extended matrix with $R'_k = R_k$ if $k \notin \{i, j\}$, and $R'_j = R_i$, $R'_i = R_j$ (the $i$-th row and the $j$-th row are exchanged).

(2) **(Row operation)** For $1 \leqslant i \neq j \leqslant m$ and $t \in \mathbf{K}$, we define $(A', b') = \mathbf{row}_{i,j,t}((A, b))$ to be the extended matrix with $R'_k = R_k$ if $k \neq j$, and $R'_j = R_j - tR_i$.

EXAMPLE 2.10.7. (1) For instance

$$\mathbf{exch}_{2,3}\left(\begin{pmatrix} 1 & 2 & 3 & b_1 \\ 4 & 5 & 6 & b_2 \\ 7 & 8 & 9 & b_3 \end{pmatrix}\right) = \begin{pmatrix} 1 & 2 & 3 & b_1 \\ 7 & 8 & 9 & b_3 \\ 4 & 5 & 6 & b_2 \end{pmatrix}$$

(note that the last additional column is also involved in the operation).

(2) For row operations:

$$\mathbf{row}_{2,3,t}\left(\begin{pmatrix} 1 & 2 & 3 & b_1 \\ 4 & 5 & 6 & b_2 \\ 7 & 8 & 9 & b_3 \end{pmatrix}\right) = \begin{pmatrix} 1 & 2 & 3 & b_1 \\ 4 & 5 & 6 & b_2 \\ 7-4t & 8-5t & 9-6t & b_3-b_2t \end{pmatrix}$$
$$\mathbf{row}_{3,1,t}\left(\begin{pmatrix} 1 & 2 & 3 & b_1 \\ 4 & 5 & 6 & b_2 \\ 7 & 8 & 9 & b_3 \end{pmatrix}\right) = \begin{pmatrix} 1-7t & 2-8t & 3-9t & b_1-tb_3 \\ 4 & 5 & 6 & b_2 \\ 7 & 8 & 9 & b_3 \end{pmatrix}$$

LEMMA 2.10.8. *Suppose $(A', b')$ is obtained from $(A, b)$ by a sequence of elementary operations.*

*The solution sets of the equations $Ax = b$ and $A'x = b'$ are the same.*

*There exists a matrix $B \in M_{m,m}(\mathbf{K})$ such that $b' = Bb$.*

PROOF. It suffices to check this for a single elementary operation. For a row exchange, this is easy because we are only permuting the equations.

Now consider $(A', b') = \mathbf{row}_{i,j,t}((A, b))$. Only the $j$-th equation is changed. The "old" pair of $i$-th and $j$-th equations is

$$\begin{aligned} a_{i,1}x_1 + \cdots + a_{i,n}x_n &= b_i \\ a_{j,1}x_1 + \cdots + a_{j,n}x_n &= b_j. \end{aligned}$$

The "new" pair is

$$\begin{aligned} a_{i,1}x_1 + \cdots + a_{i,n}x_n &= b_i \\ (a_{j,1} - ta_{i,1})x_1 + \cdots + (a_{j,n} - ta_{i,n})x_n &= b_j - tb_i. \end{aligned}$$

These two pairs of equations are equivalent.

Finally, we give explicit matrices so that $(A', b') = B(A, b)$ for both operations. We only check the result in a small case, leaving the general one for the reader.

(1) For row exchange, consider the matrix $B$ obtained from $1_m$ by exchanging the $i$ and $j$-columns. Then $B$ works. For instance, for $m = n = 3$, and $i = 1$, $j = 3$, we have

$$\begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}\begin{pmatrix} a & b & c & b_1 \\ d & e & f & b_2 \\ g & h & i & b_3 \end{pmatrix} = \begin{pmatrix} g & h & i & b_3 \\ d & e & f & b_2 \\ a & b & c & b_1 \end{pmatrix}$$

which is what we want.

(2) For the row operation $\mathbf{row}_{i,j,t}(A, b)$, the matrix $B = 1_m - tE_{j,i}$ works (where $E_{j,i}$ is the usual matrix first defined in Example 2.5.8 (3)). For instance, for $\mathbf{row}_{2,3,t}((A, b))$

with $m = n = 3$ as above, we have

$$(1_3 - tE_{3,2}) \begin{pmatrix} a & b & c & b_1 \\ d & e & f & b_2 \\ g & h & i & b_3 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & -t & 1 \end{pmatrix} \begin{pmatrix} a & b & c & b_1 \\ d & e & f & b_2 \\ g & h & i & b_3 \end{pmatrix}$$
$$= \begin{pmatrix} a & b & c & b_1 \\ d & e & f & b_2 \\ g - td & h - te & i - tf & b_3 - tb_2 \end{pmatrix},$$

as we want. ☐

We now explain the basic step of the Gaussian Elimination Algorithm. The input is an extended matrix $(A, b)$ such that $A$ is $k$-pREF for some $k < n$. The output is an extended matrix $(A', b')$, obtained by a finite sequence of elementary operations, such that $A'$ is $(k+1)$-pREF. *We not give full justifications.*

- Let $A^{(k)}$ be the matrix formed from the first $k$ columns of $A$. Let $j \geqslant 0$ be the integer such that $R_j$ is the last non-zero row of $A^{(k)}$.
- Consider the coefficients $a_{i,k+1}$ of $A$ for $i \geqslant j$ (on the $k+1$-st column, on or below the $j$-th row); if all these coefficients are zero, then $A$ is alread a $(k+1)$-pREF matrix, and we take $(A', b') = (A, b)$.
- Let $l \geqslant j$ be such that $a_{l,k+1} \neq 0$; exchange the $i$-th and the $l$-th rows (elementary operation)
- Assume that $a_{i,k+1} \neq 0$ (which is the case after exchanging, but we don't want to complicate the notation). Then perform the row operations

$$R'_{i+1} = R_{i+1} - \frac{a_{i+1,k+1}}{a_{i,k+1}} R_i$$
$$\cdots$$
$$R'_m = R_m - \frac{a_{m,k+1}}{a_{i,k+1}} R_i$$

  to get the new matrix $(A', b')$.

If the algorithm goes to the last step, then $(A', b')$ has the same first $k$-columns as $(A, b)$ and the same first $i$ rows. Moreover, the coefficient $a'_{i,k+1}$ is non-zero, and those below $a'_{l,k+1}$ for $l > i$ are zero. This implies that the first $k+1$ columns of $A'$ are REF.

Example 2.10.9. (1) Let

$$(A, b) = \begin{pmatrix} 1 & 2 & -4 & 5 & b_1 \\ 3 & 7 & 0 & -1 & b_2 \\ 2 & 7 & 1 & 6 & b_3 \end{pmatrix}$$

We start with $k = 0$. There is no need to exchange rows since the coefficient $a_{11}$ is non-zero. We therefore perform the row operations

$$R'_2 = R_2 - 3R_1, \qquad R'_3 = R_3 - 2R_1,$$

which gives the first new extended matrix

$$\begin{pmatrix} 1 & 2 & -4 & 5 & b_1 \\ 0 & 7 - 3 \cdot 2 & -3(-4) & -1 - 3 \cdot 5 & b_2 - 3b_1 \\ 0 & 7 - 2 \cdot 2 & 1 - 2(-4) & 6 - 2 \cdot 5 & b_3 - 2b_1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & -4 & 5 & b_1 \\ 0 & 1 & 12 & -16 & b_2 - 3b_1 \\ 0 & 3 & 9 & -4 & b_3 - 2b_1 \end{pmatrix}$$

which is 1-pREF.

Again there is no need to exchange the rows. We perform the row operation $\mathbf{row}_{2,3,3}$ and get the new matrix

$$\begin{pmatrix} 1 & 2 & -4 & 5 & b_1 \\ 0 & 1 & 12 & -16 & b_2 - 3b_1 \\ 0 & 0 & 9 - 3\cdot 12 & -4 - 3(-16) & b_3 - 2b_1 - 3(b_2 - 3b_1) \end{pmatrix} = \begin{pmatrix} 1 & 2 & -4 & 5 & b_1 \\ 0 & 1 & 12 & -16 & b_2 - 3b_1 \\ 0 & 0 & -27 & 44 & b_3 - 3b_2 + 7b_1 \end{pmatrix}$$

which is REF.

(2) Consider the extended matrix

$$(A, b) = \begin{pmatrix} 0 & 1 & 2 & b_1 \\ 0 & 3 & 7 & b_2 \\ 0 & 2 & 7 & b_3 \\ 0 & 4 & -2 & b_4 \end{pmatrix}$$

It is already 1-REF. We do not need to exchange rows to continue. The row operations give

$$\begin{pmatrix} 0 & 1 & 2 & b_1 \\ 0 & 0 & 7 - 3\cdot 2 & b_2 - 3b_1 \\ 0 & 0 & 7 - 2\cdot 2 & b_3 - 2b_1 \\ 0 & 0 & -2 - 4\cdot 2 & b_4 - 4b_1 \end{pmatrix} = \begin{pmatrix} 0 & 1 & 2 & b_1 \\ 0 & 0 & 1 & b_2 - 3b_1 \\ 0 & 0 & 3 & b_3 - 2b_1 \\ 0 & 0 & -10 & b_4 - 4b_1 \end{pmatrix}$$

which is 2-REF. Again on the third column we do not need to exchange rows, and we get

$$\begin{pmatrix} 0 & 1 & 2 & b_1 \\ 0 & 0 & 1 & b_2 - 3b_1 \\ 0 & 0 & 0 & b_3 - 2b_1 - 3(b_2 - 3b_1) \\ 0 & 0 & 0 & b_4 - 4b_1 + 10(b_2 - 3b_1) \end{pmatrix} = \begin{pmatrix} 0 & 1 & 2 & b_1 \\ 0 & 0 & 1 & b_2 - 3b_1 \\ 0 & 0 & 0 & b_3 - 3b_2 + 7b_1 \\ 0 & 0 & 0 & b_4 + 10b_2 - 34b_1 \end{pmatrix}$$

which is REF.

Note that it is a good idea during these computations to check them sometimes. This is relatively easy: at any intermediate stage $(A'', b'')$, if one takes for $b$ one of the column vectors of the original matrix, the corresponding value of $b''$ must be equal to the corresponding column vector of $A''$.

There remains to solve a system $Ax = b$. We consider the REF system $A'x = b'$ associated and the matrix $B$ with $b' = Bb$. Let $r$ be the integer with $0 \leqslant r \leqslant m$ such that there are $r$ non-zero rows of $A'$ (these will in fact be the first $r$ rows).

Definition 2.10.10 (Free column). Let $A'$ be a matrix in REF. We say that the $j$-th column of $A'$ is **free** if the following holds: either the $j$-th column is 0, or else if we denote

$$k = \max\{i \mid a_{ij} \neq 0\},$$

then there exists an integer $1 \leqslant l < j$ such that $a_{kl} \neq 0$.

For instance, the first column may only be free if it is zero.

Example 2.10.11. (1) Let

$$A = \begin{pmatrix} 0 & 2 & 3 & 4 & 0 & 17 \\ 0 & 0 & 0 & 0 & 7 & 2 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

Here we have $r = 2$; the columns $C_1$, $C_3$, $C_4$ and $C_6$ are free.

(2) Let $m = n$, and let $A$ be upper-triangular, with non-zero diagonal coefficients:

$$A = \begin{pmatrix} a_{11} & \cdots & \cdots & \cdots \\ 0 & a_{22} & \cdots & \cdots \\ \vdots & \vdots & \vdots & \vdots \\ 0 & \cdots & 0 & a_{nn} \end{pmatrix}$$

with $a_{ij} = 0$ if $i > j$, and $a_{ii} \neq 0$ for $1 \leqslant i \leqslant n$. Then none of the columns of $A$ are free.

We come back to a general matrix $A$ and extended matrix $(A, b)$. Let $f = f_A$ be the linear map associated to $A$. Let $(A', b')$ be the outcome of the algorithm with $A'$ in REF. Let $B$ be the matrix such that $(A', b') = B(A, b)$, in particular $b' = Bb$.

THEOREM 2.10.12 (Solving linear systems). (1) *The image of $f$ is of dimension $r$, so the rank of $A$ is $r$. The image of $f$ is the space of all $b \in \mathbf{K}^m$ such that $Cb = 0$, where $C \in M_{m-r,m}(\mathbf{K})$ is the matrix with $m - r$ rows given by the last $m - r$ rows of $B$. A basis of* $\mathrm{Im}(f)$ *is the set of all columns $C_j$ of the original matrix $A$ such that the $j$-th column of $A'$ is* not *free.*

(2) *The kernel of $f$ is of dimension $n - r$, which is also the number of free columns. A basis is obtained as follows: for each free column $C'_j$ of $A'$, there is unique vector $v_j \in \mathrm{Ker}(f_A)$ with $j$-th row equal to $1$, and with $i$-th row equal to $0$ for all $i \neq j$ such that $C'_i$ is free. Then $\{v_j \mid C'_j \text{ free}\}$ is a basis of* $\mathrm{Ker}(f)$.

We give a short proof, without justifying all steps in detail. The result will be illustrated in examples later, and for this lecture, the goal is to be able to exploit it in concrete cases.

PROOF. (1) The image of $f$ is the set of all $b$ such that $Ax = b$ has a solution, or equivalently of those $b$ such that $A'x = b' = Bb$ has a solution. Since the last $m - r$ rows of $A'$ are zero, the last $m - r$ equations of the system $A'x = Bb$ are of the form $0 = Cb$. Therefore, it is necessary that $Cb = 0$ for a solution to exist. Conversely, assume that this condition is satisfied. If we fix all variables $x_j$ to be $0$ when the $j$-th column is free, the system becomes a triangular system with the remaining variables. The $r$-th equation determines the value of the variable $x_j$ where $j$ is the largest index of a non-free column, then the $(r-1)$-st equation determines the value of the previous, one, etc, and we find a solution by going backwards.

Moreover, for the matrix $A'$, this solution shows that the image of $f_{A'}$ has the non-free columns $C'_j$ of $A'$ as a basis. But the restriction of $f_B$ to $\mathrm{Im}(f)$ is an isomorphism from $\mathrm{Im}(f)$ to $\mathrm{Im}(f_{A'})$. Therefore a basis of $\mathrm{Im}(f)$ is

$$\{B^{-1}C'_j \mid C'_j \text{ non free}\} = \{C_j \mid C'_j \text{ non free.}\}.$$

(2) Since $\mathrm{rank}(f) = r$ by (1), Theorem 2.8.4 shows that $\dim \mathrm{Ker}(f_A) = n - r$, the number of free columns.

When solving the equation $Ax = 0$, or equivalently $A'x = 0$ (since $b' = 0$ when $b = 0$), we see that we can fix arbitrarily the unknowns $x_j$ for $j$ such that $C'_j$ is a free column, and that for any such fixed choice, there exists a solution. This means that the linear map

$$g : \mathrm{Ker}(f_A) \longrightarrow \mathbf{K}^{n-r}$$

defined by sending $(x_j)$ to $(x_j)_{C'_j \text{ free}}$ is surjective. Since the two spaces have dimension $n - r$, it is an isomorphism. The vectors $v_j$ described in the statement are precisely those such that $g(v_j)$ has one coefficient equal to $1$, and all others $0$. The set $\{g(v_j)\}$ is therefore a basis of $\mathbf{K}^{n-r}$, and therefore $\{v_j\}$ is a basis of $\mathrm{Ker}(f_A)$. $\square$

The following examples not only illustrate the result (explaining its meaning), but also verify the claims in specific cases.

EXAMPLE 2.10.13. (1) Let

$$(A, b) = \begin{pmatrix} 0 & 2 & 3 & 4 & 1 & 17 & b_1 \\ 0 & 0 & 0 & 0 & 7 & 2 & b_2 \\ 0 & 0 & 0 & 0 & 0 & 0 & b_3 \end{pmatrix}$$

It is already REF, so $B = 1_3$ and $C$ is the third row of $B$, namely

$$C = (0\ 0\ 1).$$

The corresponding system of equations is

$$\begin{array}{cccccl} 2x_2 & +3x_3 & +4x_4 & +x_5 & +17x_6 & = b_1 \\ & & & 7x_5 & +2x_6 & = b_2 \\ & & & & 0 & = b_3 \end{array}$$

A necessary condition for the existence of a solution is that $b_3 = Cb = 0$. Assume that this is the case. Then fix $x_1 = x_3 = x_4 = x_6 = 0$. The conditions for a solution with these values is

$$\begin{array}{ccl} 2x_2 & +x_5 & = b_1 \\ & 7x_5 & = b_2, \end{array}$$

which has the solution

$$x_5 = b_2/7, \qquad x_2 = \tfrac{1}{2}(b_1 - x_5) = b_1/2 - b_2/14,$$

or

$$x = \begin{pmatrix} 0 \\ b_1/2 - b_2/14 \\ 0 \\ 0 \\ b_2/7 \\ 0 \end{pmatrix}.$$

So the image is exactly the space where $b_3 = 0$. A basis of this space is indeed given by the two non-free columns of $A' = A$, namely

$$\left\{ \begin{pmatrix} 2 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 7 \\ 0 \end{pmatrix} \right\}.$$

To compute the kernel, take $b_1 = b_2 = b_3 = 0$. Fix arbitrarily the variables $x_1$, $x_3$, $x_4$, $x_6$. Then we have a solution if and only if

$$\begin{array}{ccl} 2x_2 & +x_5 & = -3x_3 - 4x_4 - 17x_6 \\ & 7x_5 & = -2x_6, \end{array}$$

which has a unique solution

$$x_5 = -\frac{2x_6}{7}, \quad x_2 = \frac{1}{2}(-3x_3 - 4x_4 - 17x_6 - x_5)$$

as before. So the kernel is the set of all vectors $v$ of the form

$$v = \begin{pmatrix} x_1 \\ \frac{1}{2}(-3x_3 - 4x_4 - \frac{117}{7}x_6) \\ x_3 \\ x_4 \\ -\frac{2}{7}x_6 \\ x_6 \end{pmatrix}.$$

A basis is

$$v_1 = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \quad v_2 = \begin{pmatrix} 0 \\ -3/2 \\ 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \quad v_3 = \begin{pmatrix} 0 \\ -2 \\ 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}, \quad v_4 = \begin{pmatrix} 0 \\ -\frac{117}{14} \\ 0 \\ 0 \\ -2/7 \\ 1 \end{pmatrix}$$

Indeed, we have

$$v = x_1 v_1 + x_3 v_2 + x_4 v_3 + x_6 v_4,$$

which shows that $\{v_1, v_2, v_3, v_4\}$ generates the kernel, and if

$$x_1 v_1 + x_3 v_2 + x_4 v_3 + x_6 v_4 = 0,$$

looking at the rows 1, 3, 4 and 6 shows that $x_1 = x_3 = x_4 = x_6 = 0$, so this set is also linearly independent.

(2) Consider $m = n$, and let $A$ be a matrix such that the associated REF matrix $A'$ is upper-triangular with non-zero diagonal coefficients:

$$A' = \begin{pmatrix} a'_{11} & \cdots & \cdots & \cdots \\ 0 & a'_{22} & \cdots & \cdots \\ \vdots & \vdots & \vdots & \vdots \\ 0 & \cdots & 0 & a'_{nn} \end{pmatrix}$$

with $a'_{ij} = 0$ if $i > j$, and $a'_{ii} \neq 0$ for $1 \leqslant i \leqslant n$. The number of non-zero rows is $r = n$, and none of the columns of $A'$ are free. This shows that $f$ is surjective. Since $m = n$, this means that $f$ is an isomorphism (Corollary 2.8.5), or in other words that $A$ is invertible. (In particular the kernel of $f$ is $\{0\}$). Moreover, it shows that the columns of $A$ form a basis of $\mathbf{K}^n$.

We might want to compute the inverse of $A$. This can be done by solving the linear system $A'x = b'$, which will give a unique solution $x = Db' = DBb$ for some matrix $D \in M_{n,n}(\mathbf{K})$, and then $x$ is also the unique solution to $Ax = b$, so that $DB = A^{-1}$.

(3) Let

$$(A, b) = \begin{pmatrix} 1 & 2 & -4 & 5 & b_1 \\ 3 & 7 & 0 & -1 & b_2 \\ 2 & 7 & 1 & 6 & b_3 \end{pmatrix}$$

as in Example 2.10.9 (1). We saw that the associated REF matrix $A'$ is given by

$$(A', b') = \begin{pmatrix} 1 & 2 & -4 & 5 & b_1 \\ 0 & 1 & 12 & -16 & b_2 - 3b_1 \\ 0 & 0 & -27 & 44 & b_3 - 3b_2 + 7b_1 \end{pmatrix}.$$

Here we have $r = 3$, which means that $\mathrm{Im}(f)$ is $\mathbf{K}^3$, or in other words that $f$ is surjective. There is one free column of $A'$, the fourth one. So a basis of $\mathrm{Im}(f)$ is

$$\left\{ \begin{pmatrix} 1 \\ 3 \\ 2 \end{pmatrix}, \begin{pmatrix} 2 \\ 7 \\ 7 \end{pmatrix}, \begin{pmatrix} -4 \\ 0 \\ 1 \end{pmatrix} \right\}.$$

Let $b$ be an arbitrary vector in $\mathbf{K}^3$. To find a vector $x \in \mathbf{K}^4$ with $f(x) = Ax = b$, we solve the equation $A'x = b'$: this gives the system

$$\begin{array}{ccccl} x_1 & +2x_2 & -4x_3 & +5x_4 & = b_1 \\ & x_2 & +12x_3 & -16x_4 & = -3b_1 + b_2 \\ & & -27x_3 & +44x_4 & = 7b_1 - 3b_2 + b_3. \end{array}$$

One sees that we can freely choose $x_4$, and then determine uniquely the values of $x_1$, $x_2$, $x_3$. This corresponds to the fact that the solution set is of the form

$$\{x_0 + x' \mid x' \in \mathrm{Ker}(f)\}$$

for any fixed solution $x_0$ of $Ax_0 = b$ (see Proposition 2.4.4 (4)). Precisely, we get

$$\begin{aligned} x_3 &= -\frac{1}{27}(7b_1 - 3b_2 + b_3 - 44x_4) \\ x_2 &= -3b_1 - b_2 + 16x_4 - 12x_3 = \frac{b_1}{9} - \frac{b_2}{3} + \frac{4b_3}{9} - \frac{32x_4}{9} \\ x_1 &= b_1 - 2x_2 + 4x_3 - 5x_4 = -\frac{7b_1}{27} + \frac{10b_2}{9} - \frac{28b_3}{27} + \frac{233x_4}{27}. \end{aligned}$$

The kernel of $f$ is of dimension 1. To obtain a generator we consider a vector of the form

$$v_4 = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ 1 \end{pmatrix}$$

(since the fourth column is free) and solve the equation $Ax = 0$, or equivalently $A'x = 0$. This can be done using the formula above with $b_1 = b_2 = b_3 = 0$: we find

$$v_4 = \begin{pmatrix} -151/27 \\ 32/9 \\ 44/27 \end{pmatrix}.$$

(4) As an example of the situation of Example 2, take

$$A = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 10 \end{pmatrix}.$$

We will compute the inverse of $A$. We begin by applying the Gaussian Algorithm to obtain the associated REF form of the extended matrix, indicating on the left the row operation that we perform:

$$
\begin{aligned}
(A,b) \rightsquigarrow \begin{array}{c} R_1 \\ R_2-4R_1 \\ R_3-7R_1 \end{array} &\begin{pmatrix} 1 & 2 & 3 & b_1 \\ 0 & -3 & -6 & -4b_1+b_2 \\ 0 & -6 & -11 & -7b_1+b_3 \end{pmatrix} \\
\rightsquigarrow \begin{array}{c} R_1 \\ R_2 \\ R_3-2R_2 \end{array} &\begin{pmatrix} 1 & 2 & 3 & b_1 \\ 0 & -3 & -6 & -4b_1+b_2 \\ 0 & 0 & 1 & b_1-2b_2+b_3 \end{pmatrix}.
\end{aligned}
$$

This REF form is indeed upper-triangular with non-zero coefficients on the diagonal. To find the inverse $A^{-1}$ we solve for $Ax = b$, or equivalently for $A'x = b'$, that is

$$
\begin{array}{cccl}
x_1 & +2x_2 & +3x_3 & = b_1 \\
 & -3x_2 & -6x_3 & = -4b_1 + b_2 \\
 & & x_3 & = b_1 - 2b_2 + b_3,
\end{array}
$$

which gives

$$
\begin{aligned}
x_1 &= -2x_2 - 3x_3 + b_1 = -\frac{2}{3}b_1 - \frac{4}{3}b_2 + b_3 \\
x_2 &= -\frac{1}{3}(-4b_1 + b_2 + 6x_3) = -\frac{2b_1}{3} + \frac{11b_2}{3} - 2b_3 \\
x_3 &= b_1 - 2b_2 + b_3,
\end{aligned}
$$

which means that

$$
A^{-1} = \begin{pmatrix} -2/3 & -4/3 & 1 \\ -2/3 & 11/3 & -2 \\ 1 & -2 & 1 \end{pmatrix}.
$$

A concrete consequence of the Gauss Algorithm is a very useful matrix factorization for “almost all” square matrices.

Definition 2.10.14 (Regular matrix). A matrix $A \in M_{n,n}(\mathbf{K})$ is **regular** if the Gaussian Elimination to the REF form $A'$ described above can be run only with row operations of the type $R'_j = R_j - tR_i$ with $j > i$ (in particular without any exchange of rows).

Remark 2.10.15. Warning! Some people use the adjective “regular” to refer to matrices which are invertible. *This is not our convention!* A matrix can be regular according to the previous definition even if it is not invertible.

The examples we have seen were all of this type, and indeed “random” choices of coefficients will lead to regular matrices.

Definition 2.10.16 (Triangular matrices). Let $A = (a_{ij}) \in M_{n,n}(\mathbf{K})$. The matrix $A$ is **upper-triangular** if $a_{ij} = 0$ if $i > j$, and $A$ is **lower-triangular** if $a_{ij} = 0$ if $j > i$.

Example 2.10.17. (1) Note that there is no condition about the values of the diagonal coefficients, which may be zero or not. The matrices

$$
\begin{pmatrix} 1 & 2 & 3 \\ 0 & 5 & 0 \\ 0 & 0 & 9 \end{pmatrix}, \quad \begin{pmatrix} 0 & 5 \\ 0 & 0 \end{pmatrix}
$$

are upper-triangular, and

$$
\begin{pmatrix} 1 & 0 & 0 \\ 0 & 5 & 0 \\ 1 & -3 & 9 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 \\ -3 & 2 \end{pmatrix}
$$

are lower-triangular.

(2) If a matrix $A = (a_{ij}) \in M_{n,n}(\mathbf{K})$ is both upper-triangular and lower-triangular, then it is a *diagonal* matrix: $a_{ij} = 0$ unless $i = j$.

(3) Let $A$ be a REF matrix in $M_{n,n}(\mathbf{K})$. Then $A$ is upper-triangular: the condition that $i \mapsto N(R_i)$ is strictly increasing unless the row is 0 implies that $N(R_i) \geqslant i - 1$, so $a_{ij} = 0$ if $j \leqslant i - 1$.

Note that the converse is not true: for instance the matrix

$$\begin{pmatrix} 1 & 1 & 1 \\ 0 & 0 & 3 \\ 0 & 0 & 4 \end{pmatrix}$$

is upper-triangular but is not in REF.

Lemma 2.10.18. (1) *The matrix product $BA$ of matrices $B$ and $A$ in $M_{n,n}(\mathbf{K})$ which are both upper-triangular (resp. lower-triangular) is upper-triangular (resp. lower-triangular). Moreover, if $A = (a_{ij})$, $B = (b_{ij})$ and $C = (c_{ij})$, then we have $c_{ii} = b_{ii}a_{ii}$ for all $i$.*

(2) *An upper-triangular (resp. lower-triangular) matrix $A$ is invertible if and only if $a_{ii} \neq 0$ for $1 \leqslant i \leqslant n$. In that case, $A^{-1}$ is upper-triangular (resp. lower-triangular) and the diagonal coefficients of $A^{-1}$ are $a_{ii}^{-1}$.*

Proof. We consider only the upper-triangular case.

(1) We have the formula

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

for all $i$ and $j$. If $i > j$, then for any $k$ between one and $n$, either $i > k$ or $k \geqslant i > j$, so either $b_{ik} = 0$ or $a_{kj} = 0$ since $A$ and $B$ are upper-triangular. So $c_{ij} = 0$ if $i > j$. On the other hand, for $i = j$, then for $1 \leqslant k \leqslant n$, we have $i > k$ or $k > j$ unless $k = i = j$. Therefore

$$c_{ii} = b_{ii}a_{ii}.$$

(2) The matrix $A$ is REF. We know that all columns are non-free if the diagonal coefficients are all non-zero (Example 2.10.13 (2)), and that $A$ is invertible in that case.

Conversely, if there is a $j$ such that $a_{jj} = 0$, and $j$ is the smallest such integer, then the $j$-th column of $A$ is free (because either $j = 1$, and the first column of $A$ is zero, or else $a_{j-1,j-1} \neq 0$). So Theorem 2.10.12 implies that $\mathrm{Ker}(f_A) \neq \{0\}$, so that $A$ is not invertible.

Assume that $a_{ii} \neq 0$ for all $i$. To compute the inverse of $A$, we need solve the system

$$\begin{array}{cccccc} a_{11}x_1 & + \cdots & + \cdots & +a_{1n}x_n & = b_1 \\ & a_{22}x_2 & + \cdots & +a_{2n}x_n & = b_2 \\ & & \vdots & \vdots & \\ & & & a_{nn}x_n & = b_n \end{array}$$

with unknowns $x_j$. We see that we get formulas of the type

$$\begin{aligned} x_1 &= \frac{b_1}{a_{11}} + c_{12}b_2 + \cdots + c_{1n}b_n \\ \vdots & \quad \vdots \\ x_n &= \frac{1}{a_{nn}}b_n \end{aligned}$$

(for some coefficients $c_{ij} \in \mathbf{K}$) which means that the inverse matrix of $A$ that expresses $x$ in terms of $b$ is also upper-triangular, namely it is

$$A^{-1} = \begin{pmatrix} a_{11}^{-1} & c_{12} & \cdots & \cdots \\ 0 & a_{22}^{-1} & \cdots & \cdots \\ \vdots & & & \vdots \\ 0 & \cdots & 0 & a_{nn}^{-1} \end{pmatrix}$$

The diagonal coefficients are indeed $1/a_{ii}$.

This might seem a bit unrigorous, so here is another argument by induction on $n$. The case $n = 1$ is clear. So suppose that $A \in M_{n,n}(\mathbf{K})$ is upper-triangular, and that we know the property for matrices of size $n-1$. The equations

$$Ax = b$$

can be restated as

$$\begin{array}{lllll} a_{11}x_1 & + \cdots & + \cdots & + a_{1n}x_n & = b_1 \\ & & & \tilde{A}\tilde{x} & = \tilde{b} \end{array}$$

where $\tilde{A} \in M_{n-1,n-1}(\mathbf{K})$ is the matrix

$$\begin{pmatrix} a_{22} & \cdots & \cdots & a_{2n} \\ 0 & a_{33} & \cdots & a_{3n} \\ \vdots & & & \vdots \\ 0 & \cdots & 0 & a_{nn} \end{pmatrix}$$

and $\tilde{x} = (x_j)_{2 \leqslant j \leqslant n}$, $\tilde{b} = (b_j)_{2 \leqslant j \leqslant n}$ (this is the translation of the fact that only the first equation in the original system involve the variable $x_1$). Since $\tilde{A}$ is upper-triangular with non-zero diagonal coefficients, by induction, there is a unique solution $\tilde{x} = \tilde{A}^{-1}\tilde{b} = (\tilde{x}_j)_{2 \leqslant j \leqslant n}$, and the diagonal coefficients of the inverse matrix $\tilde{A}^{-1}$ are $1/a_{22}, \ldots, 1/a_{nn}$. But then the unique solution to $Ax = b$ is

$$x = \Big(\frac{1}{a_{11}}(b_1 - a_{12}\tilde{x}_2 - \cdots - a_{1n}\tilde{x}_n), \tilde{x}_2, \ldots, \tilde{x}_n\Big).$$

So $A$ is invertible, and the inverse is upper-triangular: it is

$$A^{-1} = \begin{pmatrix} a_{11}^{-1} & \cdots \\ 0 & \tilde{A} \end{pmatrix}$$

in block form. The first diagonal coefficient is $1/a_{11}$ because $\tilde{x}_j$, $j \geqslant 2$, is a function of $b_j$, $j \geqslant 2$, only. ☐

Proposition 2.10.19 (LR decomposition). *Let $A$ be a* regular *matrix.*

(1) *There exists an upper-triangular matrix $R$ and a lower-triangular matrix $L = (l_{ij})$ with $l_{ii} = 1$ for all $i$, such that $A = LR$.*

(2) *The matrix $A$ is invertible if and only if $R$ is invertible. If that is the case, then $L$ and $R$ are unique.*

Proof. (1) Consider the REF form $A'$ of $A$ and the matrix $B$ such that $BA = A'$. Then $A'$ is upper-triangular, and because no exchanges were made, the matrix $B$ is a product of matrices $1_n - tE_{ji}$ with $j > i$, which are lower-triangular (see the proof of Lemma 2.10.8 and the description of the algorithm: when there is no exchange, we always perform operations $R_j \rightsquigarrow R_j - tR_i$ with $j > i$, in which case $E_{ji}$ is lower-triangular). This means that $B$ is lower-triangular as a product of lower-triangular matrices. Moreover, because all intermediate matrices $1_m - tE_{ji}$ have all diagonal coefficients equal to 1, the same is true for $B$, and then for its inverse $B^{-1}$, which is also lower-triangular by the previous lemma. So we get $A = B^{-1}A'$, and $L = B^{-1}$, $R = A'$ has the claimed properties.

(2) Since $A = LR$ and $L$ is invertible (because the diagonal coefficients of $L$ ar equal to 1 and Lemma 2.10.18 (2)), we see that $A$ is invertible if $R$ is. And since $R = L^{-1}A$, we see that conversely $R$ is invertible if $A$ is.

Assume that $A$ is invertible and regular. To check uniqueness of $L$ and $R$, assume that
$$L_1R_1 = L_2R_2$$
with $L_i$ lower-triangular with diagonal coefficients 1 and $R_i$ upper-triangular (note that here $R_i$ does not refer to a row of a matrix). Since the matrices $L_2$ and $R_1$ are invertible, as we observed, and
$$L_2^{-1}L_1 = R_2R_1^{-1}.$$
The left-hand side is lower-triangular with coefficients 1 on the diagonal. The right-hand side is upper-triangular. By Example 2.10.17 (2), this means that $L_2^{-1}L_1$ is diagonal, and since the coefficients are 1, this means that $L_2^{-1}L_1 = 1_n$, or $L_1 = L_2$. But then $L_1R_1 = L_1R_2$ implies $R_1 = R_2$ also by multiplying by the inverse of $L_1$. ☐

EXAMPLE 2.10.20. (1) Let $A$ be the matrix of Example 2.10.13 (4):
$$A = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 10 \end{pmatrix}.$$
We obtained the REF form
$$(A, b) \rightsquigarrow (A', b') = \begin{pmatrix} 1 & 2 & 3 & b_1 \\ 0 & -3 & -6 & -4b_1 + b_2 \\ 0 & 0 & 1 & b_1 - 2b_2 + b_3 \end{pmatrix}.$$
From the last column of $(A', b')$, we have
$$B = \begin{pmatrix} 1 & 0 & 0 \\ -4 & 1 & 0 \\ 1 & -2 & 1 \end{pmatrix}.$$
We can compute the lower-triangular matrix $B^{-1}$ by solving for $b$ the system $Bb = b'$:
$$\begin{array}{llll} b_1 & & & = b'_1 \\ -4b_1 & +b_2 & & = b'_2 \\ b_1 & -2b_2 & +b_3 & = b'_3 \end{array}$$
This gives
$$\begin{aligned} b_1 &= b'_1 \\ b_2 &= 4b'_1 + b'_2 \\ b_3 &= 7b'_1 + 2b'_2 + b'_3, \end{aligned}$$
so that
$$B^{-1} = \begin{pmatrix} 1 & 0 & 0 \\ 4 & 1 & 0 \\ 7 & 2 & 1 \end{pmatrix}.$$
The LR decomposition of $A$ is then
$$A = \begin{pmatrix} 1 & 0 & 0 \\ 4 & 1 & 0 \\ 7 & 2 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 0 & -3 & -6 \\ 0 & 0 & 1 \end{pmatrix}.$$

(2) Proposition 2.10.19 does not extend to all matrices. For instance, the (non-regular) matrix

$$\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \in M_{2,2}(\mathbf{K})$$

does not have an LR decomposition, because this would mean an identity

$$\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ t & 1 \end{pmatrix} \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} = \begin{pmatrix} a & b \\ at & bt+d \end{pmatrix}$$

for some coefficients $(t, a, b, d) \in \mathbf{K}^4$. But this equality would imply that $a = 0$ and then we would get the contradiction $1 = 0$ from the first coefficient on the second row.

## 2.11. Applications

We next discuss the applications of Gaussian Elimination to the solution of many concrete problems of linear algebra.

Consider the following problems involving finite-dimensional vector spaces $V_1$ and $V_2$ and a linear map $f : V_1 \longrightarrow V_2$:

(1) Determine the kernel of $f$;
(2) Determine the image of $f$;
(3) Determine the rank of $f$;
(4) If $f$ is bijective, find the inverse of $f$;
(5) For a basis or finite generating set $S$ of $V_1$ and a vector $v \in V_1$, express $v$ as a linear combination of elements of $S$;
(6) For a subset $S$ of $V_1$, determine the subspace generated by $S$, in particuler, determine whether $S$ is a generating set;
(7) For a finite subset $S$ of $V_1$, determine whether $S$ is linearly independent;
(8) For a linearly independent subset $T$ of $V_1$, find a basis of $V_1$ containing $T$;
(9) For a generating set $T$ of $V_1$, find a basis of $V_1$ contained in $T$;
(10) For a subspace $W$ of $V_1$, given as the kernel of a linear map, determine a basis of $W$, and in particular, determine the dimension of $W$;
(11) For a subspace $W$ of $V_1$, given by a generating set, determine a linear map $f$ such that $W = \mathrm{Ker}(f)$;
(12) For subspaces $W_1$ and $W_2$ of $V_1$, determine the intersection $W_1 \cap W_2$.

We will show that all of these questions can be reduced to the problem of resolving systems of linear equations, as described in the previous section.

We begin with a discussion of what it means to "determine" a subspace $W$ of a vector space $V$, as is often required in the list of problems. There are actually two equally important ways this might be considered to be solved:

(a) Give a basis $(v_1, \ldots, v_k)$ of $W$. This gives an easy answer to the question: "What are some elements of the subspace $W$?" Indeed, any linear combination of the basis vectors is in $W$, and no other vector.

(b) Find another vector space $V_1$ and a linear map $V \longrightarrow V_1$ such that $W = \mathrm{Ker}(f)$. This is useful because, if the linear map is given with concrete formulas, it will be easy to compute $f(v)$ for $v \in V$, and in particular it will be easy to answer the question: "Does a vector $v \in V$ belong to the subspace $W$ or not?"

Depending on the problem to solve, it might be more important to have a description of the first, or of the second kind. Problems (10) and (11) of the list above can be interpreted as saying: "given a description of one kind, find one of the other kind." If we can solve these, then other problems where one has to "determine" a subspace can be solved by providing either a description of type (a) or of type (b), since we can go back and forth.

We first show how one reduces all problems of the list above to systems of linear equations in the special case where $V_1 = \mathbf{K}^n$ and $V_2 = \mathbf{K}^m$. Then we will quickly explain how bases are used to reduce the general case to that one. (Note that we do not attempt to describe what is the most *efficient* solution...)

(1) *Determine the kernel of $f$*: express $f = f_A$ for some matrix $A = (a_{ij}) \in M_{m,n}(\mathbf{K})$, and apply Theorem 2.10.12 (2).

(2) *Determine the image of $f$*: express $f = f_A$ for some matrix $A = (a_{ij}) \in M_{m,n}(\mathbf{K})$, and apply Theorem 2.10.12 (1).

(3) *Determine the rank of $f$*: express $f = f_A$ for some matrix $A = (a_{ij}) \in M_{m,n}(\mathbf{K})$, and apply Theorem 2.10.12 (1).

(4) *If $f$ is bijective, find the inverse of $f$*: express $f = f_A$ for some matrix $A = (a_{ij}) \in M_{m,n}(\mathbf{K})$, reduce it to REF form and express the solution $x$ of $A'x = b'$ as a linear map of $b$.

(5) *For a basis or finite generating set $S$ of $V_1$ and a vector $v \in V_1$, express $v$ as a linear combination of elements of $S$*: let $S = \{v_1, \ldots, v_k\}$ (with $k \geqslant n$ since this is a generating set); solve the system

$$t_1 v_1 + \cdots + t_k v_k = v,$$

which is a linear system with $n$ equations (corresponding to the coordinates of $v$) and $k$ unknowns.

(6) *For a finite subset $S$ of $V_1$, determine the subspace generated by $S$*: let $S = \{v_1, \ldots, v_k\}$; consider the linear map $g_S : \mathbf{K}^k \longrightarrow \mathbf{K}^n$ such that

$$g_S\left(\begin{pmatrix} t_1 \\ \vdots \\ t_k \end{pmatrix}\right) = t_1 v_1 + \cdots + t_k v_k;$$

then compute the image of $g_S$ (Problem (2)); we have then $\langle S \rangle = \operatorname{Im}(g_S)$. (Alternative: to find a basis of $\langle S \rangle$, check if $S$ is linearly independent (Problem (7) below); if not, remove from $S$ a vector $v \in S$ such that

$$v \in \langle S - \{v\} \rangle,$$

until a linearly independent set is found; it is then a basis of $\langle S \rangle$.)

(7) *For a finite subset $S$ of $V_1$, determine whether $S$ is linearly independent, and if not, find a non-trivial linear relation between elements of $S$*: if $S = \{v_1, \ldots, v_k\}$ with

$$v_i = \begin{pmatrix} a_{1j} \\ \vdots \\ a_{nj} \end{pmatrix}, \qquad 1 \leqslant i \leqslant k$$

solve the linear system of equations

$$\begin{aligned} a_{11}x_1 + \cdots + a_{1k}x_k &= 0 \\ &\cdots \\ a_{n1}x_1 + \cdots + a_{nk}x_k &= 0 \end{aligned}$$

with $n$ equations and $k$ unknowns $x_1, \ldots, x_k$; then $S$ is linearly dependent if and only if there exists a solution $(x_i)$ where not all $x_i$ are equal to 0; a corresponding non-trivial linear relation is

$$x_1v_1 + \cdots + x_kv_k = 0.$$

(8) *For a linearly independent subset $T$ of $V_1$, find a basis of $V_1$ containing $T$*: assume $T = \{v_1, \ldots, v_k\}$; let

$$v_{k+1} = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$$

where the $x_i$ are unknown; find $(x_i)$ such that $(v_1, \ldots, v_{k+1})$ are linearly independent (Problem (7)); then continue until a linearly independent set of $n$ elements is found. (Alternatively, if $k < n$, choose the vector $v_{k+1}$ "at random" and check the linear independence for such a specific choice, and if it fails, pick another random choice, etc).

(9) *For a generating set $T$ of $V_1$, find a basis of $V_1$ contained in $T$*: find a basis of the subspace generated by $T$ (Problem (6)).

(10) *For a subspace $W$ of $V_1$, given as the kernel of a linear map $g : V_1 \longrightarrow \mathbf{K}^k$, determine a basis of $W$*: determine the kernel of the linear map (Problem (1)).

(11) *For a subspace $W$ of $V_1$, given by a finite generating set $S$ of $W$, determine a linear map $f$ such that $W = \mathrm{Ker}(f)$*: write $S = \{v_1, \ldots, v_k\}$ for some vectors

$$v_j = \begin{pmatrix} a_{1j} \\ \vdots \\ a_{nj} \end{pmatrix}$$

and let $A$ be the matrix $(a_{ij}) \in M_{n,k}(\mathbf{K})$. The linear map $f_A$ is simply the map

$$\begin{pmatrix} t_1 \\ \vdots \\ t_k \end{pmatrix} \mapsto t_1v_1 + \cdots + t_kv_k,$$

and has image equal to $W$. Apply Theorem 2.10.12 (1) to compute the image of $f_A$: one finds that $W$ is the set of vectors $b \in \mathbf{K}^n$ such that $Cb = 0$ for some matrix $C$. The linear map $g : b \mapsto Cb$ is then a linear map such that $W = \mathrm{Ker}(g)$.

(12) *For subspaces $W_1$ and $W_2$ of $V_1$, determine the intersection $W_1 \cap W_2$*: express $W_1$ and $W_2$ as the kernels of linear maps $f_1$ and $f_2$ (Problem (11)), with $f_i : V_1 \longrightarrow \mathbf{K}^{d_i}$. Then $W_1 \cap W_2 = \mathrm{Ker}(f)$ where

$$f : V_1 \longrightarrow \mathbf{K}^{d_1+d_2}$$

is given by

$$f(v) = (f_1(v), f_2(v));$$

compute this kernel (Problem (1)).

Example 2.11.1. We illustrate some of these calculations with the following problem: compute, by giving a basis and writing it as the kernel of a linear map, the intersection $W_1 \cap W_2 \subset \mathbf{R}^4$ where

$$W_1 = \left\langle \begin{pmatrix} 1 \\ 0 \\ 3 \\ -1 \end{pmatrix}, \begin{pmatrix} -2 \\ 1 \\ 0 \\ 4 \end{pmatrix} \begin{pmatrix} 1 \\ 1 \\ 5 \\ 5 \end{pmatrix} \right\rangle$$

and

$$W_2 = \left\langle \begin{pmatrix} 1 \\ 3 \\ -2 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ -1 \\ -6 \end{pmatrix} \begin{pmatrix} 2 \\ 5 \\ -3 \\ 4 \end{pmatrix} \right\rangle$$

Let

$$(A_1, b) = \begin{pmatrix} 1 & -2 & 1 & b_1 \\ 0 & 1 & 1 & b_2 \\ 3 & 0 & 5 & b_3 \\ -1 & 4 & 5 & b_4 \end{pmatrix}, \quad (A_2, b) = \begin{pmatrix} 1 & 0 & 2 & b_1 \\ 3 & 1 & 5 & b_2 \\ -2 & -1 & -3 & b_3 \\ 1 & -6 & 4 & b_4 \end{pmatrix}$$

be the corresponding extended matrices, so $W_i$ is the subspace generated by the columns of $A_i$. We reduce $(A_1, b)$ and $(A_2, b)$ to REF. First for $(A_1, b)$:

$$(A_1, b) \rightsquigarrow \begin{array}{c} R_1 \\ R_2 \\ R_3 - 3R_1 \\ R_4 + R_1 \end{array} \begin{pmatrix} 1 & -2 & 1 & b_1 \\ 0 & 1 & 1 & b_2 \\ 0 & 6 & 2 & b_3 - 3b_1 \\ 0 & 2 & 6 & b_4 + b_1 \end{pmatrix} \rightsquigarrow \begin{array}{c} R_1 \\ R_2 \\ R_3 - 6R_2 \\ R_4 - 2R_2 \end{array} \begin{pmatrix} 1 & -2 & 1 & b_1 \\ 0 & 1 & 1 & b_2 \\ 0 & 0 & -4 & -3b_1 - 6b_2 + b_3 \\ 0 & 0 & 4 & b_1 - 2b_2 + b_4 \end{pmatrix}$$

$$\rightsquigarrow \begin{array}{c} R_1 \\ R_2 \\ R_3 \\ R_4 + R_3 \end{array} \begin{pmatrix} 1 & -2 & 1 & b_1 \\ 0 & 1 & 1 & b_2 \\ 0 & 0 & -4 & -3b_1 - 6b_2 + b_3 \\ 0 & 0 & 0 & -2b_1 - 8b_2 + b_3 + b_4 \end{pmatrix}.$$

This means that $W_1$, which is the image of the linear map $f_A : \mathbf{K}^3 \to \mathbf{K}^4$, is also the subspace

$$W_1 = \left\{ \begin{pmatrix} b_1 \\ b_2 \\ b_3 \\ b_4 \end{pmatrix} \mid -2b_1 - 8b_2 + b_3 + b_4 = 0 \right\}.$$

Next for $(A_2, b)$, where we note that we will use an exchange of rows:

$$(A_2, b) \rightsquigarrow \begin{array}{c} R_1 \\ R_2 - 3R_1 \\ R_3 + 2R_1 \\ R_4 - R_1 \end{array} \begin{pmatrix} 1 & 0 & 2 & b_1 \\ 0 & 1 & -1 & -3b_1 + b_2 \\ 0 & -1 & 1 & 2b_1 + b_3 \\ 0 & -6 & 2 & -b_1 + b_4 \end{pmatrix} \rightsquigarrow \begin{array}{c} R_1 \\ R_2 \\ R_3 + R_2 \\ R_4 + 6R_2 \end{array} \begin{pmatrix} 1 & 0 & 2 & b_1 \\ 0 & 1 & -1 & -3b_1 + b_2 \\ 0 & 0 & 0 & -b_1 + b_2 + b_3 \\ 0 & 0 & -4 & -19b_1 + 6b_2 + b_4 \end{pmatrix}$$

$$\rightsquigarrow \begin{array}{c} R_1 \\ R_2 \\ R_4 \\ R_3 \end{array} \begin{pmatrix} 1 & 0 & 2 & b_1 \\ 0 & 1 & -1 & -3b_1 + b_2 \\ 0 & 0 & -4 & -19b_1 + 6b_2 + b_4 \\ 0 & 0 & 0 & -b_1 + b_2 + b_3 \end{pmatrix}.$$

Hence

$$W_2 = \left\{ \begin{pmatrix} b_1 \\ b_2 \\ b_3 \\ b_4 \end{pmatrix} \mid -b_1 + b_2 + b_3 = 0 \right\}$$

We can now describe $W_1 \cap W_2$ as a kernel: it is $\mathrm{Ker}(f)$, where

$$f\left( \begin{pmatrix} b_1 \\ b_2 \\ b_3 \\ b_4 \end{pmatrix} \right) = \begin{pmatrix} -2b_1 - 8b_2 + b_3 + b_4 \\ -b_1 + b_2 + b_3 \end{pmatrix}.$$

To find a basis of $W_1 \cap W_2$ (in particular, to find its dimension), we reduce to REF the matrix

$$A = \begin{pmatrix} -2 & -8 & 1 & 1 \\ -1 & 1 & 1 & 0 \end{pmatrix}$$

such that $f = f_A$. We find

$$(A, b) = \begin{pmatrix} -2 & -8 & 1 & 1 & b_1 \\ -1 & 1 & 1 & 0 & b_2 \end{pmatrix} \rightsquigarrow \begin{matrix} R_1 \\ R_2 - R_1/2 \end{matrix} \begin{pmatrix} -2 & -8 & 1 & 1 & b_1 \\ 0 & 5 & 1/2 & -1/2 & -b_1/2 + b_2 \end{pmatrix}$$

This is in REF form and the free columns are the third and fourth. So by Theorem 2.10.12 (2), there is a basis with two vectors $(v_3, v_4)$ with

$$v_3 = \begin{pmatrix} a \\ b \\ 1 \\ 0 \end{pmatrix}, \qquad v_4 = \begin{pmatrix} c \\ d \\ 0 \\ 1 \end{pmatrix}$$

for some real numbers $(a, b, c, d)$; in particular $\dim(W_1 \cap W_2) = 2$. The corresponding systems of equations for these vectors to belong to $W_1 \cap W_2 = \mathrm{Ker}(f)$ are

$$\begin{matrix} -2a & -8b & +1 & = 0 \\ & 5b & +1/2 & = 0 \end{matrix}, \qquad \begin{matrix} -2c & -8d & +1 & = 0 \\ & 5d & -1/2 & = 0 \end{matrix}$$

which we solve to find

$$v_3 = \begin{pmatrix} 9/10 \\ -1/10 \\ 1 \\ 0 \end{pmatrix} \qquad v_4 = \begin{pmatrix} 1/10 \\ 1/10 \\ 0 \\ 1 \end{pmatrix}.$$

(Note that, *for peace of mind*, it might be useful to check that these vectors do belong to $W_1 \cap W_2$, to detect computational errors.)

Finally, what should one do to solve problems similar to the ones described above for other vector spaces than $\mathbf{K}^n$? The method is always the same: one fixes bases of the vector spaces involved, and then translate the problem to $\mathbf{K}^n$ using the coordinates with respect to the bases. After solving the problem in $\mathbf{K}^n$, one translates the result back to the original vector space, using the following facts:

PROPOSITION 2.11.2. *Let $V_1$ and $V_2$ be finite-dimensional vector spaces and $f : V_1 \to V_2$ a linear map. Let*

$$B_1 = (e_1, \ldots, e_n), \qquad B_2 = (f_1, \ldots, f_m)$$

*be ordered bases of $V_1$ and $V_2$ respectively, and let $A = \mathrm{Mat}(f; B_1, B_2)$.*

(1) *The dimension of $\mathrm{Ker}(f)$ and of $\mathrm{Ker}(f_A)$ are the same; we have*

$$\mathrm{Ker}(f) = \left\{ t_1 e_1 + \cdots + t_n e_n \in V_1 \mid \begin{pmatrix} t_1 \\ \vdots \\ t_n \end{pmatrix} \in \mathrm{Ker}(f_A) \right\}.$$

(2) *The rank of $f$ and of $f_A$, and the rank of $A$, are equal; we have*

$$\mathrm{Im}(f) = \left\{ s_1 f_1 + \cdots + s_m f_n \in V_2 \mid \begin{pmatrix} s_1 \\ \vdots \\ s_m \end{pmatrix} \in \mathrm{Im}(f_A) \right\}.$$

Proof. (1) By Lemma 2.9.9, we get

$$\mathrm{Ker}(f) = \left\{ t_1 e_1 + \cdots + t_n e_n \in V_1 \;\middle|\; \begin{pmatrix} t_1 \\ \vdots \\ t_n \end{pmatrix} \in \mathrm{Ker}(f_a) \right\}$$

and since the right-hand side has dimension $\dim \mathrm{Ker}(f_A)$ (because the linear map

$$\begin{pmatrix} t_1 \\ \vdots \\ t_n \end{pmatrix} \mapsto t_1 e_1 + \cdots + t_n e_n$$

is an isomorphism), the equality of dimensions follow.

(2) Similarly, Lemma 2.9.9 gives the equality

$$\mathrm{Im}(f) = \left\{ s_1 f_1 + \cdots + s_m f_n \in V_2 \;\middle|\; \begin{pmatrix} s_1 \\ \vdots \\ s_m \end{pmatrix} \in \mathrm{Im}(f_A) \right\},$$

and since the right-hand side has dimension $\mathrm{rank}(f_A)$, we get the equality of dimensions. ∎

We illustrate this principle with a simple example.

Example 2.11.3. For $n \geqslant 0$, let

$$V_n = \{ P = a_0 + a_1 x + \cdots + a_n x^n \in \mathbf{R}[X] \mid a_i \in \mathbf{R} \}.$$

This is a finite-dimensional vector space with basis $B_n = (P_0, \ldots, P_n)$ where $P_i(x) = x^i$ (by definition, these functions generate $V_n$ and by Example 2.6.5 (5), they are linearly independent).

Consider the linear map

$$f \begin{cases} V_3 \longrightarrow V_4 \\ P \mapsto (x+2)P. \end{cases}$$

We ask to determine the kernel and image of $f$. To do this we use the bases $B_3$ and $B_4$. The computations

$$f(P_0) = x + 2 = 2P_0 + P_1, \quad f(P_1) = 2P_1 + P_2,$$
$$f(P_2) = 2P_2 + P_3, \quad f(P_3) = 2P_3 + P_4$$

show that the matrix $\mathrm{Mat}(f; B_3, B_4)$ is

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

We transform the matrix to REF:

$$(A,b) \rightsquigarrow \begin{array}{r} R_1 \\ R_2 - \frac{1}{2}R_1 \\ R_3 \\ R_4 \\ R_5 \end{array} \begin{pmatrix} 2 & 0 & 0 & 0 & b_1 \\ 0 & 2 & 0 & 0 & -b_1/2 + b_2 \\ 0 & 1 & 2 & 0 & b_3 \\ 0 & 0 & 1 & 2 & b_4 \\ 0 & 0 & 0 & 1 & b_5 \end{pmatrix} \rightsquigarrow \begin{array}{r} R_1 \\ R_2 \\ R_3 - \frac{1}{2}R_2 \\ R_4 \\ R_5 \end{array} \begin{pmatrix} 2 & 0 & 0 & 0 & b_1 \\ 0 & 2 & 0 & 0 & -b_1/2 + b_2 \\ 0 & 0 & 2 & 0 & b_1/4 - b_2/2 + b_3 \\ 0 & 0 & 1 & 2 & b_4 \\ 0 & 0 & 0 & 1 & b_5 \end{pmatrix}$$

$$\rightsquigarrow \begin{array}{r} R_1 \\ R_2 \\ R_3 \\ R_4 - \frac{1}{2}R_3 \\ R_5 \end{array} \begin{pmatrix} 2 & 0 & 0 & 0 & b_1 \\ 0 & 2 & 0 & 0 & -b_1/2 + b_2 \\ 0 & 0 & 2 & 0 & b_1/4 - b_2/2 + b_3 \\ 0 & 0 & 0 & 2 & -b_1/8 + b_2/4 - b_3/2 + b_4 \\ 0 & 0 & 0 & 1 & b_5 \end{pmatrix}$$

$$\rightsquigarrow \begin{array}{r} R_1 \\ R_2 \\ R_3 \\ R_4 \\ R_5 - \frac{1}{2}R_4 \end{array} \begin{pmatrix} 2 & 0 & 0 & 0 & b_1 \\ 0 & 2 & 0 & 0 & -b_1/2 + b_2 \\ 0 & 0 & 2 & 0 & b_1/4 - b_2/2 + b_3 \\ 0 & 0 & 0 & 2 & -b_1/8 + b_2/4 - b_3/2 + b_4 \\ 0 & 0 & 0 & 0 & b_1/16 - b_2/8 + b_3/4 - b_4/2 + b_5. \end{pmatrix}.$$

This shows that the rank of $f_A$ is 4, and since there are no free columns, that $f_A$ is injective. The same is then true for $f$. Moreover, since the vector $b = (b_i)$ corresponds in the basis $B_4$ to the polynomial

$$Q = b_1 P_0 + \cdots + b_5 P_4 \in V_4,$$

we obtain the characterization

$$\mathrm{Im}(f) = \{Q(x) = a_0 + a_1 x + \cdots + a_4 x^4 \in V_4 \mid a_0/16 - a_1/8 + a_2/4 - a_3/2 + a_4 = 0\}.$$

We could have guessed this result as follows: if $Q = f(P) = (x+2)P$, then we get $Q(-2) = 0$, so the image of $f$ must be contained in the subspace

$$W = \{Q \in V_4 \mid Q(-2) = 0\}.$$

But note that for $Q(x) = a_0 + a_1 x + \cdots + a_4 x^4$, we have

$$Q(-2) = a_0 - 2a_1 + 4a_2 - 8a_3 + 16a_4 = 16(a_0/16 - a_1/8 + a_2/4 - a_3/2 + a_4),$$

so that the space $\mathrm{Im}(f)$ that we computed using the REF form is in fact exactly equal to $W$.

This illustrates another important point: if a linear map is defined "abstractly" on some vector space that is not $\mathbf{K}^n$, it might well be that one can compute its image and kernel "by pure thought", and not by a complicated implementation of the Gauss Algorithm.

CHAPTER 3

# Determinants

## 3.1. Axiomatic characterization

The determinant of a matrix $A \in M_{n,n}(\mathbf{K})$ provides a single number $\det(A) \in \mathbf{K}$ such that $A$ is invertible if and only if $\det(A) \neq 0$. Moreover, there is an explicit formula for $\det(A)$ in terms of the coefficients of $A$. This is quite wonderful at first sight, but in fact it is mostly a theoretical tool: except for very small values of $n$, the computation of $\det(A)$ using this formula is absolutely impossible; for instance, for $n = 70$ (which corresponds to rather small matrices from the point of view of actual numerical analysis), this would require $\geqslant 10^{100}$ operations! There are faster methods (the Gauss Algorithm gives one), but these will usually solve *completely* the linear system $Ax = b$, not only determine whether it is always solvable with a unique solution!

Nevertheless, determinants are important to investigate many theoretical aspects of linear algebra, and their geometric interpretation appears in multi-variable calculus.

We present the determinants, as is customary, in an axiomatic manner: stating a list of properties that completely determine the determinant. Then we will prove the existence and uniqueness statements.

We first have two definitions.

Definition 3.1.1 (Multilinear map). Let $V$ and $W$ be vector spaces over $\mathbf{K}$. Let $n \geqslant 1$ be an integer. A map

$$f : V^n \longrightarrow W$$

is called **multilinear** if, for every $i$ with $1 \leqslant i \leqslant n$, and for every $(v_1, \ldots, v_n) \in V^n$, the map $V \to W$ defined by

$$v \mapsto f(v_1, \ldots, v_{i-1}, v, v_{i+1}, \ldots, v_n)$$

is linear. If $n = 2$, one says that $f$ is **bilinear**, if $n = 3$ that it is **trilinear**.

In other words, to say that $f$ is multilinear means that for any $i$ with $1 \leqslant i \leqslant n$, and for any vectors $v_1, \ldots, v_{i-1}, v_i, v_i', v_{i+1}, \ldots, v_n$ and any elements $t, t' \in \mathbf{K}$, we have

$$f(v_1, \ldots, v_{i-1}, tv_i + t'v_i', v_{i+1}, \cdots, v_n) = tf(v_1, \ldots, v_{i-1}, v_i, v_{i+1}, \cdots, v_n) + t'f(v_1, \ldots, v_{i-1}, v_i', v_{i+1}, \cdots, v_n).$$

In particular, if $f$ is multilinear, we have

$$f(v_1, \ldots, v_n) = 0$$

if there exists some $j$ such that $v_j = 0$, and

$$f(v_1, \ldots, v_{i-1}, tv_i, v_{i+1}, \ldots, v_n) = tf(v_1, \ldots, v_n).$$

Example 3.1.2. Consider $V = W = \mathbf{K}$. The multiplication map $m : \mathbf{R}^2 \to \mathbf{R}$ such that $m(x, y) = xy$ is bilinear: we have

$$m(t_1x_1 + t_2x_2, y) = t_1x_1y + t_2x_2y = t_1m(x_1, y) + t_2m(x_2, y)$$

and similarly $m(x, t_1y_1 + t_2y_2) = t_1m(x, y_1) + t_2m(x, y_2)$. More generally, for $n \geqslant 1$, the map

$$f : \mathbf{K}^n \longrightarrow \mathbf{K}$$

such that $f(x_1, \ldots, x_n) = x_1 \cdots x_n$ is multilinear.

Definition 3.1.3 (Symmetric, alternating multilinear maps). Let $V$ and $W$ be vector spaces over $\mathbf{K}$. Let $n \geqslant 1$ be an integer, and let

$$f : V^n \longrightarrow W$$

be a multilinear map.

(1) The map $f$ is said to be **symmetric**, if $f(v_1, \ldots, v_n)$ is not changed when two arguments $v_i$ and $v_j$ are exchanged:

$$f(v_1, \ldots, v_n) = f(v_1, \ldots, v_{i-1}, v_j, v_{i+1}, \ldots, v_{j-1}, v_i, v_{j+1}, \ldots, v_n)$$

for all $(v_1, \ldots, v_n) \in V^n$.

(2) The map $f$ is said to be **alternating**, if $f(v_1, \ldots, v_n) = 0_W$ whenever two arguments at least are equal, namely, whenever there exists $i \neq j$ such that $v_i = v_j$.

Lemma 3.1.4. *Let $f : V^n \longrightarrow W$ be an alternating multilinear map.*

(1) *The value of $f$ changes sign when two arguments $v_i$ and $v_j$ are exchanged:*

$$f(v_1, \ldots, v_n) = -f(v_1, \ldots, v_{i-1}, v_j, v_{i+1}, \ldots, v_{j-1}, v_i, v_{j+1}, \ldots, v_n)$$

*for all $(v_1, \ldots, v_n) \in V^n$ and all $i \neq j$.*

(2) *If there is a linear relation*

$$t_1v_1 + \cdots + t_nv_n = 0_V$$

*with not all $t_i$ zero, then $f(v_1, \ldots, v_n) = 0_W$.*

(3) *Let $1 \leqslant i \leqslant n$ and let $t_j \in \mathbf{K}$ for $1 \leqslant j \leqslant n$. Denote*

$$w = \sum_{j \neq i} t_jv_j.$$

*Then*

$$f(v_1, \ldots, v_{i-1}, v_i + w, v_{i+1}, \ldots, v_n) = f(v_1, \ldots, v_n),$$

*or in other words: the value of $f$ is unchanged if one of the arguments $v_i$ is replaced by $v_i + w$, where $w$ is a linear combination of the other arguments.*

Proof. (1) Consider

$$f(v_1, \ldots, v_{i-1}, v_i + v_j, v_{i+1}, \ldots, v_{j-1}, v_i + v_j, v_{j+1}, \ldots).$$

Since $f$ is alternating, this is equal to $0_W$. On the other hand, using the linearity with respect to the $i$-th and $j$-th argument, we get

$$\begin{aligned} 0_W = f(v_1, \ldots, v_n) &+ f(v_1, \ldots, v_{i-1}, v_j, v_{i+1}, \ldots, v_{j-1}, v_i, v_{j+1}, \ldots) \\ &+ f(v_1, \ldots, v_{i-1}, v_i, v_{i+1}, \ldots, v_{j-1}, v_i, v_{j+1}, \ldots) \\ &+ f(v_1, \ldots, v_{i-1}, v_j, v_{i+1}, \ldots, v_{j-1}, v_j, v_{j+1}, \ldots), \end{aligned}$$

and the last two terms are also zero by the alternating property.

(2) Suppose that $t_i \neq 0$. Then we get

$$v_i = -\sum_{\substack{1 \leqslant j \leqslant n \\ j \neq i}} \frac{t_j}{t_i} v_j,$$

and by multilinearity

$$f(v_1,\dots,v_n) = -\sum_{\substack{1\leqslant j\leqslant n\\ j\neq i}} \frac{t_j}{t_i} f(v_1,\dots,v_{i-1},v_j,v_{i+1},\dots,v_n) = 0_W$$

by applying the alternating property to each of the values of $f$, where the $j$-th and $i$-th arguments are the same.

(3) By multilinearity, we have

$$\begin{aligned} f(v_1,\dots,v_{i-1},v_i+w,v_{i+1},\dots,v_n) = f(v_1,\dots,v_{i-1},v_i,v_{i+1},\dots,v_n)\\ + f(v_1,\dots,v_{i-1},w,v_{i+1},\dots,v_n). \end{aligned}$$

The element $w$ satisfies

$$1\cdot w - \sum_{j\neq i} t_j v_j = 0,$$

so by (2) the second term is equal to $0_W$. ☐

REMARK 3.1.5. For $\mathbf{K}=\mathbf{Q}$, or $\mathbf{R}$ or $\mathbf{C}$, or most other fields, one can in fact that the property (1) as definition of alternating multilinear maps. Indeed, if (1) holds, then when $v_i = v_j$ with $i\neq j$, we get by exchanging the $i$-th and $j$-th arguments the relation

$$f(v_1,\dots,v_n) = -f(v_1,\dots,v_n),$$

and for such fields, it follows that $f(v_1,\dots,v_n)=0$, so that $f$ is alternating.

However, the general theory of fields (see Chapter 9) allows for the possibility that this relation is always true (this is the case for the field $\mathbf{F}_2$ with two elements, for instance). In full generality, the "correct" definition of an alternating map is that in Definition 3.1.3.

EXAMPLE 3.1.6. (1) The map $f : \mathbf{K}^n \longrightarrow \mathbf{K}$ such that

$$f(x_1,\dots,x_n) = x_1\cdots x_n$$

is multilinear and symmetric.

(2) If $n=1$, then any linear map is both symmetric and alternating.

THEOREM 3.1.7 (Existence and uniqueness of determinants). *Let $\mathbf{K}$ be a field, and let $V$ be a finite-dimensional vector space with $\dim(V)=n\geqslant 1$. Let $B=(e_1,\dots,e_n)$ be a fixed ordered basis of $V$ and let $t_0\in\mathbf{K}$ be a fixed element of $\mathbf{K}$.*

*There exists a unique alternating multilinear map*

$$D_{B,t_0} : V^n \longrightarrow \mathbf{K}$$

*such that $D_{B,t_0}(e_1,\dots,e_n)=t_0$.*

For a specific choice, we obtain the determinant:

COROLLARY 3.1.8. *Let $\mathbf{K}$ be a field, let $n\geqslant 1$ and let $V=\mathbf{K}^n$ be the $n$-dimensional vector space of column vectors of size $n$. There exists a unique alternating multilinear map*

$$\det : V^n \longrightarrow \mathbf{K}$$

*such that, for the standard basis of $\mathbf{K}^n$, we have*

$$\det\left(\begin{pmatrix}1\\0\\\vdots\end{pmatrix},\begin{pmatrix}0\\1\\\vdots\end{pmatrix},\dots,\begin{pmatrix}0\\\vdots\\1\end{pmatrix}\right) = 1.$$

PROOF. It suffices to take for $B$ the standard basis of $\mathbf{K}^n$, and $t_0=1$, so that $\det = D_{B,1}$ where $D$ is the map of Theorem 3.1.7. ☐

DEFINITION 3.1.9 (Determinant of a matrix). Let $\mathbf{K}$ be a field and let $n \geqslant 1$ be an integer. The **determinant** of matrices is the map

$$\det : M_{n,n}(\mathbf{K}) \longrightarrow \mathbf{K}$$

defined by $\det(A) = \det(C_1, \ldots, C_n)$, where the vectors $C_i \in \mathbf{K}^n$ are the columns of the matrix $A$.

In principle, all properties of determinants should be computable from the defining properties of Theorem 3.1.7, since this results shows that there is a unique map with the stated properties. We illustrate this in Section 3.4, which the reader can read now if desired. In the two intermediate sections, we will treat the example of $n = 2$ and then prove the existence and uniqueness in general.

As a matter of notation, one also denotes the determinant of a matrix $A = (a_{ij})$ by writing the matrix between "straight brackets": for instance, we write

$$\det\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}\right) = \begin{vmatrix} a & b \\ c & d \end{vmatrix}.$$

## 3.2. Example

We illustrate and motivate a bit the construction of the next section by working out the formula for $n = 2$ from scratch.

For simplicity, we take $V = \mathbf{K}^2$ and the standard basis $B = (e_1, e_2)$ with

$$e_1 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \quad e_2 = \begin{pmatrix} 0 \\ 1 \end{pmatrix},$$

but we do not fix $t_0$. We can interpret $V^2$ as the space of $2 \times 2$ matrices by looking at columns.

We first assume that a map

$$\det : V^2 \longrightarrow \mathbf{K}$$

has the properties of Theorem 3.1.7, and will find a unique possible formula for it. We will then check that this formula does indeed define an alternating bilinear map with $\det(B) = t_0$.

Consider how to compute

$$\det\left(\begin{pmatrix} a \\ b \end{pmatrix}, \begin{pmatrix} c \\ d \end{pmatrix}\right).$$

We write

$$\begin{pmatrix} a \\ b \end{pmatrix} = ae_1 + be_2, \qquad \begin{pmatrix} c \\ d \end{pmatrix} = ce_1 + de_2,$$

and use linearity with respect to the first argument to get

$$\begin{aligned} \det\left(\begin{pmatrix} a \\ b \end{pmatrix}, \begin{pmatrix} c \\ d \end{pmatrix}\right) &= \det(ae_1 + be_2, ce_1 + de_2) \\ &= a\det(e_1, ce_1 + de_2) + b\det(e_2, ce_1 + de_2). \end{aligned}$$

For each of these two expressions, we use linearity with respect to the second argument to get

$$\det\left(\begin{pmatrix} a \\ b \end{pmatrix}, \begin{pmatrix} c \\ d \end{pmatrix}\right) = a\big(c\det(e_1, e_1) + d\det(e_1, e_2)\big) + b\big(c\det(e_2, e_1) + d\det(e_2, e_2)\big).$$

The only determinants that remain have some basis vectors as arguments! But by assumption we should have $\det(e_1, e_2) = t_0$, and since det is assumed to be alternating, we have $\det(e_1, e_1) = \det(e_2, e_2) = 0$. And again because det is alternating, we have

$\det(e_2, e_1) = -\det(e_1, e_2) = -t_0$ (Lemma 3.1.4 (1)). So the determinant can only be the map given by the formula

$$\det\left(\begin{pmatrix} a \\ b \end{pmatrix}, \begin{pmatrix} c \\ d \end{pmatrix}\right) = (ad - bc)t_0.$$

Now conversely, let's define $f : V^2 \longrightarrow \mathbf{K}$ by this formula. We will check that it is indeed alternating and bilinear, and that $f(B) = t_0$.

The last condition is immediate. For bilinearity with respect to the first argument, we have

$$\begin{aligned} f\left(t_1 \begin{pmatrix} a_1 \\ b_1 \end{pmatrix} + t_2 \begin{pmatrix} a_2 \\ b_2 \end{pmatrix}, \begin{pmatrix} c \\ d \end{pmatrix}\right) &= f\left(\begin{pmatrix} t_1a_1 + t_2a_2 \\ t_1b_1 + t_2b_2 \end{pmatrix}, \begin{pmatrix} c \\ d \end{pmatrix}\right) \\ &= t_0\Big((t_1a_1 + t_2a_2)d - (t_1b_1 + t_2b_2)c\Big) \\ &= t_1t_0(a_1d - b_1c) + t_2t_0(a_2d - b_2c) \\ &= t_1 f\left(\begin{pmatrix} a_1 \\ b_1 \end{pmatrix}, \begin{pmatrix} c \\ d \end{pmatrix}\right) + t_2 f\left(\begin{pmatrix} a_2 \\ b_2 \end{pmatrix}, \begin{pmatrix} c \\ d \end{pmatrix}\right). \end{aligned}$$

Similarly, we check the bilinearity with respect to the second argument.

To check that $f$ is alternating, we just compute

$$f\left(\begin{pmatrix} a \\ b \end{pmatrix}, \begin{pmatrix} a \\ b \end{pmatrix}\right) = t_0(ab - ab) = 0.$$

We conclude:

Proposition 3.2.1. *The determinant for $M_{2,2}(\mathbf{K})$ is given by*

$$\det\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}\right) = \begin{vmatrix} a & b \\ c & d \end{vmatrix} = ad - bc.$$

## 3.3. Uniqueness and existence of the determinant

We will prove Theorem 3.1.7 in this section. Some readers may prefer to first read the next section, which proves the most important properties of the determinants, without referring to any specific construction, but using instead the properties of Theorem 3.1.7 that make it unique.

For the uniqueness of the determinant, we can proceed essentially as in the previous section.

We write $B = (e_1, \ldots, e_n)$. Then we assume that $D : V^n \longrightarrow \mathbf{K}$ has the properties of Theorem 3.1.7.

Let $v_1, \ldots, v_n$ be elements of $V$. We write

$$v_j = a_{1j}e_1 + \cdots + a_{nj}e_n.$$

We want to show that $D(v_1, \ldots, v_n)$ is determined by the multilinearity, the alternating property, and the condition $D(B) = t_0$.

We use linearity with respect to each argument in term; this will lead to a big expression for $D(v_1, \ldots, v_n)$ as a sum of $n^n$ different terms of the type

$$a_{k_1,1}a_{k_2,2}\cdots a_{k_n,n}D(e_{k_1}, \ldots, e_{k_n}), \tag{3.1}$$

where each index $k_j$ is between 1 and $n$. Among these terms, all those where there exist $i \neq j$ with $k_i = k_j$ will be zero because $D$ is alternating, and there would be twice the same argument. So $D(v_1, \ldots, v_n)$ must be the sum of these expressions where the map

$$i \mapsto k_i$$

is injective. Since this maps sends the finite set $\{1, \ldots, n\}$ to itself, this means that it is a bijection of $\{1, \ldots, n\}$ into itself.

The integers $(k_1, \ldots, k_n)$ are not necessarily in order. But each integer from 1 to $n$ appears in the list, since the map $i \mapsto k_i$ is surjective. By exchanging the $k_1$-st argument with that where $k_j = 1$, and repeating, using the consequence of the alternating property from Lemma 3.1.4 (1), we see that for each term (3.1), there is a sign $\varepsilon \in \{-1, 1\}$ such that

$$D(e_{k_1}, \ldots, e_{k_n}) = \varepsilon D(e_1, \ldots, e_n) = \varepsilon t_0.$$

Hence we find that $D(v_1, \ldots, v_n)$ can indeed take only one value if we assume the basic properties of Theorem 3.1.7. This proves the uniqueness.

Now we consider existence. There exist a number of different proofs of the existence of the determinant. One idea is to write down the formula that arises from the previous argument, and to check that it works (as we did for $n = 2$).

We will use a slightly different idea that requires less notation. We proceed by induction on $n$. For $n = 1$, and $B = (e_1)$ a basis of $V$, the function

$$D_{B,t_0}(te_1) = t_0 t$$

satisfies the properties of Theorem 3.1.7. Now assume that the maps of Theorem 3.1.7 exist for vector spaces of dimension $n-1$ and all $t_0 \in \mathbf{K}$. Define a vector space $V_1$ to be the subspace of $V$ with basis $B_1 = (e_k)_{2 \leqslant i \leqslant n}$. So $\dim(V_1) = n - 1$. Let $f : V \longrightarrow V_1$ be the linear map such that

$$f(t_1 e_1 + \cdots + t_n e_n) = t_2 e_2 + \cdots + t_n e_n \in V_1.$$

By assumption, there exists an alternating multilinear map

$$D_1 : V_1^{n-1} \longrightarrow \mathbf{K}$$

with $D_1(B_1) = t_0$. Then, writing as before

$$v_i = a_{1i} e_1 + \cdots + a_{ni} e_n,$$

we define $D : V^n \longrightarrow \mathbf{K}$ by

$$D(v_1, \ldots, v_n) = \sum_{i=1}^{n} (-1)^{i-1} a_{1i} D_1(f(v_1), \ldots, f(v_{i-1}), f(v_{i+1}), \ldots, f(v_n)), \tag{3.2}$$

where the $i$-th term in the sum omits the $i$-th vector $f(v_i)$.

Example 3.3.1. Consider $V = \mathbf{K}^3$. Then $V_1$ is isomorphic to $\mathbf{K}^2$, and the determinant $D_1$ is given by the previous section. This means that (for $t_0 = 1$) we define

$$\begin{aligned} D\left(\begin{pmatrix} a \\ b \\ c \end{pmatrix}, \begin{pmatrix} d \\ e \\ f \end{pmatrix}, \begin{pmatrix} g \\ h \\ i \end{pmatrix}\right) &= aD_1\left(\begin{pmatrix} e \\ f \end{pmatrix}, \begin{pmatrix} h \\ i \end{pmatrix}\right) - dD_1\left(\begin{pmatrix} b \\ c \end{pmatrix}, \begin{pmatrix} h \\ i \end{pmatrix}\right) + gD_1\left(\begin{pmatrix} b \\ c \end{pmatrix}, \begin{pmatrix} e \\ f \end{pmatrix}\right) \\ &= a(ei - fh) - d(bi - ch) + g(bf - ce) \\ &= aei + dhc + gbf - ceg - fha - ibd. \end{aligned}$$

Coming back to the general case, we claim that this map $D$ has all the properties we want. First, we get

$$D(e_1, \ldots, e_n) = 1 \cdot D_1(e_2, \ldots, e_n) = D_1(B_1) = t_0$$

since $a_{11} = 1$ and $a_{1i} = 0$ for $i \geqslant 2$ in that case and $f(v_2) = v_2, \ldots, f(v_n) = v_n$.

Next we check multilinearity, for instance with respect to the first argument (the others are similar). For any

$$v_1' = a_{11}' e_1 + \cdots + a_{n1}' e_n,$$

and any $t_1$, $t_2 \in \mathbf{K}$, we get

$$D(t_1 v_1 + t_2 v_1', v_2, \ldots, v_n) = (t_1 a_{11} + t_2 a_{11}') D_1(f(v_2), \ldots, f(v_n)) + \sum_{i=2}^{n} (-1)^{i-1} a_{1i} D_1(f(t_1 v_1 + t_2 v_1'), \ldots, \widehat{f(v_i)}, \ldots, f(v_n)),$$

(where the hat indicates that $f(v_i)$ is omitted in the argument list in the last sum). Using the linearity of $f$ and the multilinearity of $D_1$ with respect to the first argument, this is equal to

$$t_1 \Big( a_{11} D_1(f(v_2), \ldots, f(v_n)) + \sum_{i=2}^{n} (-1)^{i-1} a_{1i} D_1(f(v_1), \ldots, \widehat{f(v_i)}, \ldots, f(v_n)) \Big)$$
$$+ t_2 \Big( a_{11}' D_1(f(v_2), \ldots, f(v_n)) + \sum_{i=2}^{n} (-1)^{i-1} a_{1i} D_1(f(v_1'), \ldots, \widehat{f(v_i)}, \ldots, f(v_n)) \Big)$$
$$= t_1 D(v_1, v_2, \ldots, v_n) + t_2 D(v_1', v_2, \ldots, v_n).$$

Finally we check that $D$ is alternating, which will complete the induction step and the proof of Theorem 3.1.7. We consider the case where $v_1 = v_1$, the others being similar.

We first consider $i \geqslant 3$ and the $i$-th term in (3.2) for $D(v_1, v_1, v_3, \ldots, v_n)$. This is

$$(-1)^{i-1} a_{1i} D_1(f(v_1), f(v_1), \ldots, f(v_{i-1}), f(v_{i+1}), \ldots, f(v_n)),$$

with $f(v_i)$ omitted. Since $D_1$ is alternating, this is equal to 0.

If $i = 1$, we obtain

$$(-1)^{1-1} a_{11} D_1(f(v_1), f(v_3), \ldots, f(v_n)) = a_{11} D_1(f(v_1), f(v_3), \ldots, f(v_n)).$$

Similarly, for $i = 2$, we get

$$(-1)^{1-2} a_{11} D_1(f(v_1), f(v_3), \ldots, f(v_n)) = -a_{11} D_1(f(v_1), f(v_3), \ldots, f(v_n)).$$

The sum of these two terms is 0, so $D(v_1, v_1, v_3, \ldots, v_n) = 0$.

The basic identity used in the proof is worth stating separately for matrices.

PROPOSITION 3.3.2. *Let $n \geqslant 1$. Let $A$ be a matrix in $M_{n,n}(\mathbf{K})$. For $1 \leqslant k, l \leqslant n$, we denote by $A^{(k,l)}$ the matrix in $M_{n-1,n-1}(\mathbf{K})$ obtained from $A$ by removing the $k$-th row and $l$-th column.*

*For $1 \leqslant k \leqslant n$, we have the formula*

$$\det(A) = \sum_{i=1}^{n} (-1)^{i-k} a_{ki} \det(A^{(k,i)}),$$

*called* expansion of the determinant with respect to the $k$-th row.

PROOF. For $k = 1$, this is (3.2). The general case can be done similarly, taking care of the signs. ☐

EXAMPLE 3.3.3. Let $n = 3$, and consider $k = 2$. Then the formula is

$$\begin{vmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{vmatrix} = -a_{21} \begin{vmatrix} a_{12} & a_{13} \\ a_{32} & a_{33} \end{vmatrix} + a_{22} \begin{vmatrix} a_{11} & a_{13} \\ a_{31} & a_{33} \end{vmatrix} - a_{23} \begin{vmatrix} a_{11} & a_{12} \\ a_{31} & a_{32} \end{vmatrix}.$$

## 3.4. Properties of the determinant

In this section we deduce the fundamental properties of the determinant directly from Theorem 3.1.7, without using any specific features of any construction of the determinants.

THEOREM 3.4.1. *Let* $\mathbf{K}$ *be a field and* $n \geqslant 1$*. The determinant*

$$\det : M_{n,n}(\mathbf{K}) \longrightarrow \mathbf{K}$$

*has the following properties:*

(1) *For any matrices* $A$ *and* $B$*, we have*

$$\det(BA) = \det(B)\det(A) = \det(A)\det(B) = \det(AB).$$

(2) *We have* $\det(A) = 0$ *if and only if* $A$ *is not invertible, if and only if the columns of* $A$ *are linearly dependent, if and only if the columns of* $A$ *do not form a basis of* $\mathbf{K}^n$*. If* $A$ *is invertible, then* $\det(A^{-1}) = \det(A)^{-1}$*.*

PROOF. Let $B_0$ be the standard basis of $\mathbf{K}^n$ with column vectors forming the identity matrix $1_n$.

(1) Fix a matrix $B \in M_{n,n}(\mathbf{K})$. We consider the two maps

$$d_B : M_{n,n}(\mathbf{K}) \longrightarrow \mathbf{K}, \qquad d'_B : M_{n,n}(\mathbf{K}) \longrightarrow \mathbf{K},$$

defined by

$$d_B(A) = \det(BA), \qquad d'_B(A) = \det(B)\det(A).$$

We view these maps as defined on $V^n$, where $V = \mathbf{K}^n$, where we interpret a matrix $A$ as the list of its column vectors.

The map $d'_B$ is multilinear and alternating (it is a constant times the determinant), and $d'_B(1_n) = \det(B)\det(1_n) = \det(B)$, so that $d'_B = D_{B_0,t_0}$ with $t_0 = \det(B)$.

The map $d_B$ is also multilinear: indeed, $d_B = \det \circ m_B$, where $m_B : V^n \longrightarrow V^n$ is the map corresponding to multiplication by $B$ on the left. This map is linear, hence the composite is multilinear.

The map $d_B$ is alternating: indeed, if $A$ has two columns equal, then $m_B(A)$ also does (since the columns of $BA$ are the products of $B$ with the columns of $A$, see Example 2.2.4 (2)). Hence $d_B(A) = \det(m_B(A)) = 0$.

It follows from Theorem 3.1.7 that $d_B = D_{B_0,t_1}$ with $t_1 = d_B(1_n) = \det(B) = t_0$. Therefore the maps $d_B$ and $d'_B$ coincide, which means that

$$\det(BA) = \det(B)\det(A)$$

for all $A \in M_{n,n}(\mathbf{K})$. Since this is valid for all $B$, we get the result.

(2) Assume first that $A$ is not invertible. This means that the linear map $f_A$ is not surjective (Proposition 2.3.11 and Corollary 2.8.5), and therefore that the $n$ column vectors $(C_1, \ldots, C_n)$ of $A$, which generate the image of $f_A$, cannot form an ordered basis of $\mathbf{K}^n$. So they cannot be linearly independent and there exist elements of $\mathbf{K}$, not all 0, such that

$$t_1 C_1 + \cdots + t_n C_n = 0_n.$$

Then Lemma 3.1.4 (2) shows that $\det(A) = 0$.

Now suppose that $\det(A) = 0$. Then $A$ cannot be invertible: if it were, there would exist a matrix $B$ with $BA = 1_n$, and then (1) implies that

$$\det(B)\det(A) = \det(BA) = \det(1_n) = 1,$$

which is a contradiction. So $A$ is not invertible.

Finally, for a matrix $A \in M_{n,n}(\mathbf{K})$, we already know that $A$ is not invertible if and only if the columns of $A$ do not form a basis of $\mathbf{K}^n$, and since there are $n$ elements, this is if and only if the columns of $A$ are not linearly independent.

From $1 = \det(1_n) = \det(AA^{-1}) = \det(A)\det(A^{-1})$, we get $\det(A^{-1}) = \det(A)^{-1}$. ☐

EXAMPLE 3.4.2. For instance, for any invertible matrix $A$ and any matrix $B$, we get

$$\det(ABA^{-1}) = \det(B),$$

and if $A$ and $B$ are invertible, then

$$\det(ABA^{-1}B^{-1}) = 1.$$

COROLLARY 3.4.3. *Let* $\mathbf{K}$ *be a field and* $n \geqslant 1$. *For* $A = (a_{ij})$ *upper-triangular (resp. lower-triangular), we have*

$$\det(A) = a_{11} \cdots a_{nn},$$

*the product of the diagonal coefficients.*

PROOF. We first consider upper-triangular matrices. We then use induction on $n$. For $n = 1$, we have $\det(a) = a$, and there is nothing to prove. Assume now that the statement holds for upper-triangular matrices of size $n-1$.

Let

$$A = \begin{pmatrix} a_{11} & \cdots & \cdots & \cdots \\ 0 & a_{22} & \cdots & \cdots \\ \vdots & \vdots & \vdots & \vdots \\ 0 & \cdots & 0 & a_{nn} \end{pmatrix}$$

be upper-triangular. We denote by $A_1$ the matrix

$$A_1 = \begin{pmatrix} a_{22} & \cdots & \cdots & \cdots \\ 0 & a_{33} & \cdots & \cdots \\ \vdots & \vdots & \vdots & \vdots \\ 0 & \cdots & 0 & a_{nn} \end{pmatrix}$$

which is upper-triangular of size $n-1$. By induction we have

$$\det(A_1) = a_{22} \cdots a_{nn},$$

and it suffices therefore to prove that

$$\det(A) = a_{11}\det(A_1)$$

to conclude.

In fact, we claim that for *any* matrix $B \in M_{n-1,n-1}(\mathbf{K})$, we have

$$\det\left(\begin{pmatrix} a_{11} & a' \\ 0 & B \end{pmatrix}\right) = a_{11}\det(B) \tag{3.3}$$

where $a' = (a_{1i})_{2 \leqslant i \leqslant n}$, and where we write the matrix in block form.

To prove (3.3), we first note that it is true if $a_{11} = 0$, since both sides are then zero. Suppose then that $a_{11} \neq 0$. Write $C_i$ the columns of the matrix $\begin{pmatrix} a_{11} & a' \\ 0 & B \end{pmatrix}$. Then by Lemma 3.1.4 (3), applied successively with $w = -a_{12}/a_{11}C_1$, …, $w = -a_{1n}/a_{11}C_1$, we get

$$\det\left(\begin{pmatrix} a_{11} & a' \\ 0 & B \end{pmatrix}\right) = \det(C_1, C_2 - \tfrac{a_{12}}{a_{11}} C_1, C_3, \ldots, C_n)$$
$$= \det(C_1, C_2 - \tfrac{a_{12}}{a_{11}} C_1, C_3 - \tfrac{a_{13}}{a_{11}} C_1, \ldots, C_n - \tfrac{a_{1n}}{a_{11}} C_1)$$
$$= \det\left(\begin{pmatrix} a_{11} & 0 \\ 0 & B \end{pmatrix}\right).$$

By linearity with respect to the first column, we get

$$\det\left(\begin{pmatrix} a_{11} & a' \\ 0 & B \end{pmatrix}\right) = a_{11} d(B),$$

where $d : M_{n-1,n-1}(\mathbf{K}) \longrightarrow \mathbf{K}$ is the map

$$d(B) = \det\left(\begin{pmatrix} 1 & 0 \\ 0 & B \end{pmatrix}\right).$$

The map $d$ is multilinear (viewing $M_{n-1,n-1}(\mathbf{K})$ as $(\mathbf{K}^{n-1})^{n-1}$ using the columns of a matrix, as usual). It is alternating, since if $B$ has two columns equal, then so does the matrix $\begin{pmatrix} 1 & 0 \\ 0 & B \end{pmatrix}$. Finally, we have $d(1_{n-1}) = \det(1_n) = 1$. We conclude from Theorem 3.1.7 that $d(B) = \det(B)$ for all matrices $B \in M_{n-1,n-1}(\mathbf{K})$. Hence we conclude that

$$\det\left(\begin{pmatrix} a_{11} & a' \\ 0 & B \end{pmatrix}\right) = a_{11} d(B) = a_{11} \det(B),$$

proving (3.3).

Now consider lower-triangular matrices. Again by induction on $n \geqslant 1$, it suffices to prove that

$$\det\left(\begin{pmatrix} a_{11} & 0 \\ a' & B \end{pmatrix}\right) = a_{11} \det(B) \tag{3.4}$$

for any $a_{11} \in \mathbf{K}$ and any matrix $B \in M_{n-1,n-1}(\mathbf{K})$, where $a' = (a_{i1})_{2 \leqslant i \leqslant n}$ denotes an arbitrary (fixed) vector in $\mathbf{K}^{n-1}$.

As a function of $B$, the left-hand side of (3.4) is directly seen to be multilinear and alternating, because the determinant is (it is important that the coefficients on the first row, except maybe for $a_{11}$, are zero, because it means that if two columns of $B$ are equal, then two columns of $\begin{pmatrix} a_{11} & 0 \\ a' & B \end{pmatrix}$ are equal). Finally, we compute for $B = 1_{n-1}$ that

$$\det\left(\begin{pmatrix} a_{11} & 0 \\ a' & 1_{n-1} \end{pmatrix}\right) = a_{11} \det(1_n) + \sum_{i=2}^{n} a_{i1} \det(e_i, e_2, \ldots, e_n)$$
$$= a_{11}$$

by using the multilinearity with respect to the first column and the alternating property. So we must have

$$\det\left(\begin{pmatrix} a_{11} & 0 \\ a' & B \end{pmatrix}\right) = a_{11} \det(B)$$

for any $B \in M_{n-1,n-1}(\mathbf{K})$, by uniqueness in Theorem 3.1.7. □

This corollary provides what is often the quickest way to compute a determinant in practice, using the Gauss Elimination Algorithm.

Corollary 3.4.4. *Let $A \in M_{n,n}(\mathbf{K})$, and let $A' = (a'_{ij})$ be a REF matrix obtained from $A$ by the Gauss Algorithm. Then $\det(A) = (-1)^k \det(A')$ where $k$ is the number of exchange of rows during the reduction of $A$ to $A'$. Since $A'$ is upper-triangular, this means that*

$$\det(A) = (-1)^k a'_{11} \cdots a'_{nn}.$$

Proof. By Lemma 2.10.8, the elementary operations in the steps

$$A = A_0 \rightsquigarrow A_1 \rightsquigarrow \cdots \rightsquigarrow A_k = A'$$

leading to $A'$ can be represented by

$$A_{k+1} = B_k A_k$$

for some matrix $B_k$. Therefore $\det(A_{k+1}) = \det(B_k)\det(A_k)$, and in particular we obtain the formula for $\det(A)$ provided: (1) we have $\det(B_k) = -1$ if the step $A_k \rightsquigarrow A_{k+1}$ is an exchange of rows; (2) we have $\det(B_k) = 1$ if the step $A_k \rightsquigarrow A_{k+1}$ is a row operation $R'_j = R_j - tR_i$.

In the first case, Lemma 2.10.8 shows that $B_k$ is the matrix obtained from $1_n$ by exchanging two columns; but then by the alternating property of Lemma 3.1.4 (1), we have $\det(B_k) = -\det(1_n) = -1$.

In the second case, Lemma 2.10.8 shows that $B_k = 1_n - tE_{ji}$ with $j \neq i$. This matrix is either upper-triangular (if $j > i$) or lower-triangular (if $j < i$), and its diagonal coefficients are equal to 1. Therefore Corollary 3.4.3 shows that $\det(1_n - tE_{ji}) = 1$. ☐

Remark 3.4.5. If there is no exchange of rows in the REF reduction then the LR decomposition (Proposition 2.10.19) gives $A = LR$ with $L$ lower-triangular with coefficients 1 on the diagonal, and $R$ upper-triangular (and is in fact the REF matrix associated to $A$). Then $\det(A) = \det(R)$ by Corollary 3.4.3.

We considered matrices as elements of $V^n$ for $V = \mathbf{K}^n$ the space of column vectors. We might also have viewed $M_{n,n}(\mathbf{K})$ as $W^n$, where $W = \mathbf{K}_n = M_{1,n}(\mathbf{K})$ is the space of row vectors. By Theorem 3.1.7, there exists a unique map

$$\det{}' : M_{n,n}(\mathbf{K}) \longrightarrow \mathbf{K}$$

which is an alternating multilinear map *of the rows* of a matrix $A \in M_{n,n}(\mathbf{K})$, and such that $\det'(1_n) = 1$, where we view $1_n$ as the sequence of $n$ successive row vectors

$$((1, 0, \ldots, 0), (0, 1, 0, \ldots, 0), \ldots, (0, \ldots, 0, 1)).$$

Example 3.4.6. For $n = 1$, we have $\det'(a) = a = \det(a)$. For $n = 2$, we can computer $\det'$ as in Section 3.2 (note that we already know that $\det'$ exists). Write $f_1 = (1, 0)$, and $f_2 = (0, 1)$, so that $(f_1, f_2)$ is a basis of $\mathbf{K}_2$. Then

$$\begin{aligned}
\det{}'\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}\right) &= \det{}'(af_1 + bf_2, cf_1 + df_2) \\
&= ac\det{}'(f_1, f_1) + ad\det{}'(f_1, f_2) + bc\det{}'(f_2, f_1) + bd\det{}'(f_2, f_2) \\
&= ad - bc = \det\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}\right).
\end{aligned}$$

The fact that $\det = \det'$ for $n = 1$ and $n = 2$ extends to the general case. To prove this, it is useful to also consider the *transpose* of a matrix, which reverses the roles of columns and rows.

Definition 3.4.7 (Transpose). Let $n \geqslant 1$ and $m \geqslant 1$ be integers. For $A = (a_{ij}) \in M_{m,n}(\mathbf{K})$, we denote by ${}^tA$ the **transpose** of $A$, which is the matrix in $M_{n,m}(\mathbf{K})$ with ${}^tA = (a_{ji})$.

In other words, the column vectors of $A$ are the row vectors of ${}^tA$.

Example 3.4.8. (1) Let $A = \begin{pmatrix} 2 & 4 & 1 \\ 0 & -8 & 2 \end{pmatrix}$. Then

$$ {}^tA = \begin{pmatrix} 2 & 0 \\ 4 & -8 \\ 1 & 2 \end{pmatrix}. $$

(2) Let $E_{ij} \in M_{m,n}(\mathbf{K})$ be the usual matrix with a single coefficient 1 on the $i$-th row and $j$-th column (see Example 2.6.5 (4)). Then ${}^tE_{ij} = E_{ij} \in M_{n,m}(\mathbf{K})$.

Lemma 3.4.9. *The transpose map $M_{m,n}(\mathbf{K}) \longrightarrow M_{n,m}(\mathbf{K})$ is linear and is an isomorphism.*

Proof. The linearity is easy to check. Moreover we have ${}^t({}^tA) = A$, so that the transpose is a bijection, with reciprocal bijection given by the transpose on $M_{n,m}(\mathbf{K})$. ☐

Proposition 3.4.10. *Let $n \geqslant 1$ be an integer. We have* $\det(A) = \det({}^tA) = \det'(A)$ *for any $A \in M_{n,n}(\mathbf{K})$.*

Proof. We begin by proving that $\det'(A) = \det({}^tA)$ for any matrix $A \in M_{n,n}(\mathbf{K})$. Indeed, because the transpose exchanges rows and columns, the map $d : M_{n,n}(\mathbf{K}) \longrightarrow \mathbf{K}$ defined by $d(A) = \det({}^tA)$ is a multilinear map of the rows, and it is alternating, since if a matrix $A$ has two equal rows, then ${}^tA$ has two equal columns, so that $\det({}^tA) = 0$. Since ${}^t1_n = 1_n$, we have $d(A) = 1$. So by the unicity of $\det'$ from Theorem 3.1.7, we have $d = \det'$.

Now, we check that $\det' = \det$. First of all, arguing as in Theorem 3.4.1 (but using $B \mapsto \det'(BA)$, because multiplication on the right by a fixed matrix corresponds to operations on the rows instead of columns), we obtain the property

$$ \det{}'(AB) = \det{}'(A)\det{}'(B), $$

for any $A$ and $B$ in $M_{n,n}(\mathbf{K})$. Then, proceeding as in Corollary 3.4.3 and Corollary 3.4.4, we get

$$ \det{}'(A) = (-1)^k a'_{11} \cdots a'_{nn} $$

where $A' = (a'_{ij})$ is the REF reduction of $A$, $k$ being the number of exchanges of rows in the reduction. This means that $\det'(A) = \det(A)$. ☐

Further properties of the tranpose (and a "theoretical" interpretation) will be found in Chapter 8.

### 3.5. The Vandermonde determinant

The following determinant, known as the Vandermonde determinant, is both a very good example of computing determinants and an important result for many applications.

Proposition 3.5.1 (Vandermonde determinant). *Let* $n \geqslant 1$, *and let* $t_1, \ldots, t_n$ *be elements of* $\mathbf{K}$. *Let* $A = (t_i^{j-1})_{\substack{1\leqslant i\leqslant n\\ 1\leqslant j\leqslant n}}$. *Then we have*

$$\det(A) = \prod_{1\leqslant i<j\leqslant n} (t_j - t_i),$$

*with the convention that the product, which is empty, is equal to* 1 *if* $n = 1$. *In particular, we have* $\det(A) = 0$ *if and only if two or more of the elements* $t_i$ *are equal.*

For instance, in the cases $n = 2$ and $n = 3$, this corresponds to the following determinants:

$$\begin{vmatrix} 1 & t_1 \\ 1 & t_2 \end{vmatrix} = t_2 - t_1, \qquad \begin{vmatrix} 1 & t_1 & t_1^2 \\ 1 & t_2 & t_2^2 \\ 1 & t_3 & t_3^2 \end{vmatrix} = (t_3 - t_2)(t_3 - t_1)(t_2 - t_1).$$

Proof. We proceed by induction on $n$. For $n = 1$ or $n = 2$, the result is clear. Now suppose the formula holds for Vandermonde determinants of size $n - 1$. Let $A = (t_i^{j-1}) \in M_{n,n}(\mathbf{K})$.

We subtract the first row from the second row; this leaves unchanged the determinant (Lemma 3.1.4, (3), and Proposition 3.4.10, since we apply a transformation of the rows) so

$$\det(A) = \begin{vmatrix} 1 & t_1 & \cdots & t_1^{n-1} \\ 0 & t_2 - t_1 & \cdots & t_2^{n-1} - t_1^{n-1} \\ 1 & t_3 & \cdots & t_3^{n-1} \\ \vdots & & \vdots & \\ 1 & t_n & \cdots & t_n^{n-1} \end{vmatrix}.$$

We repeat with the third row, replaced by $R_3 - R_1$, and so on, up to the $n$-th row, and obtain

$$\det(A) = \begin{vmatrix} 1 & t_1 & \cdots & t_1^{n-1} \\ 0 & t_2 - t_1 & \cdots & t_2^{n-1} - t_1^{n-1} \\ \vdots & & \vdots & \\ 0 & t_n - t_1 & \cdots & t_n^{n-1} - t_1^{n-1} \end{vmatrix}.$$

Note that for $i \geqslant 2$ and $j \geqslant 1$, we have

$$t_i^j - t_1^j = (t_i - t_1)(t_i^{j-1} + t_i^{j-2}t_1 + \cdots + t_i t_1^{j-2} + t_1^{j-1})$$

(with the convention that the second factor is just 1 for $j = 1$). Hence by the multilinearity with respect to the rows, applied to the second, third, etc, up to the $n$-th row, we get

$$\det(A) = (t_2 - t_1)\cdots(t_n - 1) \begin{vmatrix} 1 & t_1 & \cdots & \cdots & t_1^{n-1} \\ 0 & 1 & t_2 + t_1 & \cdots & t_2^{n-2} + \cdots + t_1^{n-2} \\ \vdots & & & \vdots & \\ 0 & 1 & t_n + t_1 & \cdots & t_n^{n-2} + \cdots + t_1^{n-2} \end{vmatrix}.$$

By the formula (3.3) used in the proof of Corollary 3.4.3, this is the same as

$$\det(A) = (t_2 - t_1)\cdots(t_n - 1) \begin{vmatrix} 1 & t_2 + t_1 & \cdots & t_2^{n-2} + \cdots + t_1^{n-2} \\ \vdots & & & \vdots \\ 1 & t_n + t_1 & \cdots & t_n^{n-2} + \cdots + t_1^{n-2} \end{vmatrix}.$$

The second column here is

$$\begin{pmatrix} t_2 + t_1 \\ \vdots \\ t_n + t_1 \end{pmatrix} = \begin{pmatrix} t_2 \\ \vdots \\ t_n \end{pmatrix} + t_1 \begin{pmatrix} 1 \\ \vdots \\ 1 \end{pmatrix}$$

So, by Lemma 3.1.4 (3), we get

$$\det(A) = (t_2 - t_1) \cdots (t_n - 1) \begin{vmatrix} 1 & t_2 & t_2^2 + t_1 t_2 + t_1^2 & \cdots & t_2^{n-2} + \cdots + t_1^{n-2} \\ \vdots & & & & \vdots \\ 1 & t_n & t_n^2 + t_1 t_n + t_1^2 & \cdots & t_n^{n-2} + \cdots + t_1^{n-2} \end{vmatrix}.$$

Then the columns $C_j$ of this new matrix satisfy the relation

$$C_3 - t_1^2 C_1 - t_1 C_2 = \begin{pmatrix} t_2^2 \\ \vdots \\ t_n^2 \end{pmatrix}$$

so that (Lemma 3.1.4 again) we have

$$\det(A) = (t_2 - t_1) \cdots (t_n - 1) \begin{vmatrix} 1 & t_2 & t_2^2 & \cdots & t_2^{n-2} + \cdots + t_1^{n-2} \\ \vdots & & & & \vdots \\ 1 & t_n & t_n^2 & \cdots & t_n^{n-2} + \cdots + t_1^{n-2} \end{vmatrix}.$$

Repeating with each successive column, we get

$$\det(A) = (t_2 - t_1) \cdots (t_n - 1) \begin{vmatrix} 1 & t_2 & t_2^2 & \cdots & t_2^{n-2} \\ \vdots & & & & \vdots \\ 1 & t_n & t_n^2 & \cdots & t_n^{n-2} \end{vmatrix}.$$

The last determinant is the Vandermonde determinant of size $n-1$ associated to $(t_2, \ldots, t_n)$. By induction we get

$$\det(A) = (t_2 - t_1) \cdots (t_n - 1) \prod_{2 \leqslant i < j \leqslant n} (t_j - t_i) = \prod_{1 \leqslant i < j \leqslant n} (t_j - t_i),$$

which concludes the induction. ☐

### 3.6. Permutations

Definition 3.6.1 (Permutation). Let $n \geqslant 1$ be an integer. A **permutation** of $n$ elements is a bijection

$$\sigma : \{1, \ldots, n\} \longrightarrow \{1, \ldots, n\}.$$

We denote by $\mathrm{S}_n$ the set of all permutations of $n$ elements. We also denote by $\sigma\tau$ or $\sigma \cdot \tau$ the composition $\sigma \circ \tau$ of two permutations, and often call it the *product* of $\sigma$ and $\tau$, and by 1 the identity map on $\{1, \ldots, n\}$, which is a permutation of $n$ elements. We say that the inverse permutation $\sigma^{-1}$ is the inverse of $\sigma$ in $\mathrm{S}_n$. We also write

$$\tau^2 = \tau\tau, \qquad \tau^n = \tau \cdots \tau \text{ (for } n \geqslant 1,\ n \text{ times)}, \qquad \tau^{-n} = (\tau^{-1})^n.$$

The following proposition summarizes known properties of composition, and of the number of bijections of a set with $n$ elements.

PROPOSITION 3.6.2. *Let $n \geqslant 1$ be an integer.*
(1) *The product on $\mathrm{S}_n$ and the inverse satisfy the rules:*

$$\sigma_1(\sigma_2\sigma_3) = (\sigma_1\sigma_2)\sigma_3, \qquad \sigma\sigma^{-1} = 1 = \sigma^{-1}\sigma, \qquad \sigma \cdot 1 = 1 \cdot \sigma = \sigma$$

*for all permutations $\sigma$, $\sigma_1$, $\sigma_2$, $\sigma_3$ in $\mathrm{S}_n$.*
(2) *The set $\mathrm{S}_n$ is finite and* $\mathrm{Card}(\mathrm{S}_n) = n!$.

EXAMPLE 3.6.3. It is often useful to represent a permutation $\sigma$ by a matrix with two rows, where the columns are $\begin{pmatrix} i \\ \sigma(i) \end{pmatrix}$ for $1 \leqslant i \leqslant n$. Consider for instance the permutation

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

(i.e., $\sigma(1) = 3$, ..., $\sigma(5) = 2$). Then $P_\sigma$ is the matrix

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

We can associate a matrix in $M_{n,n}(\mathbf{K})$ to a permutation of $n$ elements.

DEFINITION 3.6.4 (Permutation matrix). Let $n \geqslant 1$ be an integer and $\sigma$ a permutation of $n$ elements. Let $B = (e_1, \ldots, e_n)$ be the standard basis of $\mathbf{K}^n$ *(*see Example 2.6.5 (3)*)*. The **permutation matrix** $P_\sigma$ associated to $\sigma$ is the matrix with column vectors

$$e_{\sigma(1)}, \ldots, e_{\sigma(n)},$$

or in other words the matrix of the linear map $\mathbf{K}^n \longrightarrow \mathbf{K}^n$ that maps $e_i$ to $e_{\sigma(i)}$ for $1 \leqslant i \leqslant n$.

PROPOSITION 3.6.5. *Let $n \geqslant 1$ be an integer. We have $P_1 = 1_n$. Moreover we have*

$$P_{\sigma\tau} = P_\sigma P_\tau$$

*for all $\sigma$ and $\tau$ in $\mathrm{S}_n$, and any permutation matrix is invertible with $P_\sigma^{-1} = P_{\sigma^{-1}}$.*

PROOF OF PROPOSITION 3.6.5. It is clear that $P_1 = 1_n$. We next show that $P_{\sigma\tau} = P_\sigma P_\tau$. The $i$-th column of $P_{\sigma\tau}$ is $e_{\sigma\tau(i)}$. The $i$-th column of $P_\sigma P_\tau$ is $P_\sigma P_\tau e_i = P_\sigma e_{\tau(i)} = e_{\sigma(\tau(i))} = e_{\sigma\tau(i)}$. So the two matrices are the same.

It follows that

$$P_\sigma P_{\sigma^{-1}} = P_{\sigma\sigma^{-1}} = P_1 = 1_n,$$

and similarly $P_{\sigma^{-1}} P_\sigma = 1$, so that $P_\sigma$ is invertible and its inverse if $P_{\sigma^{-1}}$. ☐

DEFINITION 3.6.6 (Signature). Let $\sigma$ be a permutation of $n$ elements. The **signature** $\mathrm{sgn}(\sigma)$ is the determinant of $P_\sigma$. It is a non-zero element of $\mathbf{K}$ and satisfies

$$\mathrm{sgn}(1) = 1, \qquad \mathrm{sgn}(\sigma\tau) = \mathrm{sgn}(\sigma)\mathrm{sgn}(\tau), \qquad \mathrm{sgn}(\sigma^{-1}) = \mathrm{sgn}(\sigma)^{-1}.$$

The properties stated in the definition follow from Proposition 3.6.5 and from the fact that $\det(AB) = \det(A)\det(B)$.

DEFINITION 3.6.7 (Transposition). Let $n \geqslant 1$ and let $i \neq j$ be two integers such that $1 \leqslant i, j \leqslant n$. The **transposition** $\tau_{i,j} \in \mathrm{S}_n$ exchanging $i$ and $j$ is the bijection defined by

$$\tau_{i,j}(i) = j, \quad \tau_{i,j}(j) = i, \quad \tau_{i,j}(k) = k \text{ if } k \notin \{i, j\}.$$

The inverse of $\tau_{i,j}$ is $\tau_{i,j}$ itself.

The permutation matrix $P_{\tau_{i,j}}$ is obtained from $1_n$ by exchanging the $i$-th and $j$-th columns, or by exchanging the $i$-th and $j$-th rows. In particular, since the determinant is an alternating function of the columns of a matrix, we have

$$\operatorname{sgn}(\tau_{i,j}) = \det(P_{\tau_{i,j}}) = -\det(1_n) = -1. \tag{3.5}$$

It turns out that transpositions, although they are very simple, can lead to information about *all* permutations, because of the following lemma:

LEMMA 3.6.8. *Let $n \geqslant 1$ and $\sigma \in \mathrm{S}_n$. There exists $m \geqslant 0$ and transpositions*

$$\tau_1, \ldots, \tau_m$$

*such that*

$$\sigma = \tau_1 \cdots \tau_m,$$

*with the convention that for $m = 0$, the product of transpositions is* 1.

PROOF. We prove this by induction on $n$. For $n = 1$, $\sigma = 1$ is the only element of $\mathrm{S}_n$, and is the case $m = 0$. Assume the statement holds for $\mathrm{S}_{n-1}$.

Let $\sigma \in \mathrm{S}_n$. Consider $k = \sigma(n)$. Let $\tau = \tau_{n,k}$. Then the permutation $\sigma_1 = \tau\sigma$ satisfies $\tau\sigma(n) = \tau(k) = n$. Therefore the restriction of $\sigma_1$ to $\{1, \ldots, n-1\}$ is an element of $\mathrm{S}_{n-1}$. By induction, we find $m \geqslant 0$ and transpositions $\tau_1, \ldots, \tau_m$ (exchanging elements of $\{1, \ldots, n-1\}$) such that

$$\tau\sigma = \tau_1 \cdots \tau_m.$$

Multiplying on the left with $\tau$, and using $\tau^2 = 1$, we get

$$\sigma = \tau\tau_1 \cdots \tau_m.$$

□

EXAMPLE 3.6.9. Intuitively, this just says that we can re-order a list of $n$ numbers by a finite sequence of exchanges involving only two numbers.

For instance, consider the permutation $\sigma$ of 7 elements given by

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 6 & 2 & 5 & 1 & 7 & 4 \end{pmatrix}.$$

To express it as a product of transpositions, we can proceed as follows:

$$\begin{array}{ccccccc c} 1 & 2 & 3 & 4 & 5 & 6 & 7 & \text{(start)} \\ 3 & 2 & 1 & 4 & 5 & 6 & 7 & \tau_{1,3} \\ 3 & 6 & 1 & 4 & 5 & 2 & 7 & \tau_{2,6} \\ 3 & 6 & 2 & 4 & 5 & 1 & 7 & \tau_{3,6} \\ 3 & 6 & 2 & 5 & 4 & 1 & 7 & \tau_{4,5} \\ 3 & 6 & 2 & 5 & 1 & 4 & 7 & \tau_{5,6} \\ 3 & 6 & 2 & 5 & 1 & 7 & 4 & \tau_{6,7} \end{array}$$

i.e., we have

$$\sigma = \tau_{1,3}\tau_{2,6}\tau_{3,6}\tau_{4,5}\tau_{5,6}\tau_{6,7}.$$

(For instance, by composition, we get indeed $7 \mapsto 6 \mapsto 5 \mapsto 4$, etc).

Here is an example of using transpositions to deduce information about all permutations.

Proposition 3.6.10. *Let $n \geqslant 1$ be an integer and $\sigma \in \mathrm{S}_n$.*

(1) *The signature of $\sigma$ is either 1 or $-1$; precisely, if $\sigma$ is a product of $m \geqslant 0$ transpositions, then $\operatorname{sgn}(\sigma) = \det(P_\sigma) = (-1)^m$.*

(2) *The REF of the permutation matrix $P_\sigma$ is $1_n$, and can be obtained by row exchanges only. We have $\det(P_\sigma) = (-1)^m$, where $m \geqslant 0$ is the number of row exchanges involved.*

Proof. (1) If $\sigma = \tau_{i,j}$ is a transposition, we already saw in (3.5) that $\operatorname{sgn}(\tau_{i,j}) = -1$. Let then $m \geqslant 0$ and $\tau_1, \ldots, \tau_m$ be transpositions such that

$$\sigma = \tau_1 \cdots \tau_m$$

(Lemma 3.6.8). Then the multiplicativity of the determinant shows that $\operatorname{sgn}(\sigma) = \det(P_\sigma) = (-1)^m$.

(2) Write again $\sigma = \tau_1 \cdots \tau_m$. Then $P_\sigma$ is obtained from $1_n$ by $m$ exchanges of rows, so the REF matrix is $1_n$. We get

$$P_\sigma = P_{\tau_1} \cdots P_{\tau_m}$$

and therefore $\det(P_\sigma) = (-1)^m$. ☐

Permutations and their signatures provide a "formula" for the determinant:

Proposition 3.6.11 (Leibniz formula). *Let $n \geqslant 1$ be an integer and let $A = (a_{ij}) \in M_{n,n}(\mathbf{K})$. Then we have*

$$\det(A) = \sum_{\sigma \in \mathrm{S}_n} \operatorname{sgn}(\sigma) a_{1\sigma(1)} \cdots a_{n\sigma(n)}. \tag{3.6}$$

Proof. Let $d : M_{n,n}(\mathbf{K}) \longrightarrow \mathbf{K}$ be the map determined by the right-hand side of (3.6). We will show that this satisfies the conditions of Theorem 3.1.7.

First we compute $d(1_n)$. The coefficients $a_{ij}$ of $1_n$ are zero unless $i = j$, so that in the sum, we will get

$$a_{1\sigma(1)} \cdots a_{n\sigma(n)} = 0$$

unless $\sigma(1) = 1, \ldots, \sigma(n) = n$, which means unless $\sigma = 1$. Then $\operatorname{sgn}(1) = 1$, so we get $d(1_n) = 1$.

For multilinearity, consider the $k$-th argument, and let $A'$ be the matrix with coefficients $a'_{ij}$ where the $k$-th column is given by

$$a'_{ik} = t_1 a_{ik} + t_2 b_{ik},$$

and $a'_{ij} = a_{ij}$ if $j \neq k$ (this corresponds to linearity with respect to the $k$-th column). Then

$$\begin{aligned}
d(A') &= \sum_{\sigma \in \mathrm{S}_n} \operatorname{sgn}(\sigma) a_{1\sigma(1)} \cdots a_{i-1,\sigma(i-1)} \big(t_1 a_{i\sigma(i)} + t_2 b_{i\sigma(i)}\big) a_{i+1,\sigma(i+1)} \cdots a_{n\sigma(n)} \\
&= t_1 \sum_{\sigma \in \mathrm{S}_n} \operatorname{sgn}(\sigma) a_{1\sigma(1)} \cdots a_{i-1,\sigma(i-1)} a_{i\sigma(i)} a_{i+1,\sigma(i+1)} \cdots a_{n\sigma(n)} \\
&\qquad + t_2 \sum_{\sigma \in \mathrm{S}_n} \operatorname{sgn}(\sigma) a_{1\sigma(1)} \cdots a_{i-1,\sigma(i-1)} a_{b\sigma(i)} a_{i+1,\sigma(i+1)} \cdots a_{n\sigma(n)} \\
&= t_1 d(A) + t_2 d(B)
\end{aligned}$$

where $B$ is the matrix with the same columns as $A$, except that the $k$-th is $(b_{ik})$. This proves the multilinearity of $d$ with respect to columns.

Now suppose that the $k$-th and $l$-th columns of $A$ are equal with $k < l$. This means that for $1 \leqslant i \leqslant n$, we have

$$a_{ik} = a_{il}. \tag{3.7}$$

In the definition of $d(A)$, we separate those $\sigma \in \mathrm{S}_n$ with $\mathrm{sgn}(\sigma) = 1$ and the others, so that

$$d(A) = \sum_{\substack{\sigma \in \mathrm{S}_n \\ \mathrm{sgn}(\sigma)=1}} a_{1\sigma(1)} \cdots a_{n\sigma(n)} - \sum_{\substack{\sigma \in \mathrm{S}_n \\ \mathrm{sgn}(\sigma)=-1}} a_{1\sigma(1)} \cdots a_{n\sigma(n)}.$$

Let $\tau$ be the transposition exchanging $k$ and $l$. If $\sigma$ satisfies $\mathrm{sgn}(\sigma) = 1$, then $\mathrm{sgn}(\tau\sigma) = -1$. Moreover, since $\tau^2 = \tau\tau = 1$, any $\sigma$ with $\mathrm{sgn}(\sigma) = -1$ can be expressed as $\sigma = \tau\sigma_1$ with $\sigma_1 = \tau\sigma$ such that $\mathrm{sgn}(\sigma_1) = 1$. This means that we can in fact write

$$d(A) = \sum_{\sigma \in \mathrm{S}_n \mathrm{sgn}(\sigma)=1} \Big( a_{1\sigma(1)} \cdots a_{n\sigma(n)} - a_{1,\tau\sigma(1)} \cdots a_{n,\tau\sigma(n)} \Big).$$

But for $i$ such that $\sigma(i) \notin \{k, l\}$, we have

$$a_{i,\sigma(i)} = a_{i,\tau\sigma(i)},$$

while, according to (3.7), for $i = \sigma^{-1}(k)$, so that $\sigma(i) = k$, we have

$$a_{i,\sigma(i)} = a_{\sigma^{-1}(k),k} = a_{\sigma^{-1}(k),l} = a_{\sigma^{-1}(k),\tau(k)} = a_{i,\tau\sigma(i)},$$

and for $i = \sigma^{-1}(l)$, we get

$$a_{i,\sigma(i)} = a_{\sigma^{-1}(l),l} = a_{\sigma^{-1}(l),k} = a_{\sigma^{-1}(l),\tau(l)} = a_{i,\tau\sigma(i)}.$$

So for each $\sigma \in \mathrm{S}_n$ with $\mathrm{sgn}(\sigma) = 1$, we deduce that

$$a_{1\sigma(1)} \cdots a_{n\sigma(n)} = a_{1,g\sigma(1)} \cdots a_{n,g\sigma(n)},$$

and hence finally that $d(A) = 0$.

$\square$

Exercise 3.6.12. Using the formula (3.6), try to prove all properties of Section 3.4, using only the properties of the signature in Definition 3.6.6.

CHAPTER 4

# Endomorphisms

## 4.1. Sums and direct sums of vector spaces

DEFINITION 4.1.1 (Sums of subspaces). Let $V$ be a $\mathbf{K}$-vector space, and let $(V_i)_{i\in I}$ be any vector subspaces of $V$. The **sum of the subspaces** $V_i$, denoted $\sum V_i$, is the vector space generated by the union of the subspaces $V_i$. If $I = \{1, \ldots, n\}$, we also write

$$\sum V_i = V_1 + \cdots + V_n.$$

LEMMA 4.1.2. *The space $\sum V_i$ is the space of all vectors $v \in V$ that one can express in the form*

$$v = \sum_{i\in I} v_i, \tag{4.1}$$

*where $v_i \in V_i$ for each $i$ and $v_i = 0$ except for $i$ in a finite subset $J \subset I$, that may depends on $v$.*

PROOF. Let $S$ be the union of the subspaces $V_i$, so that $\sum V_i = \langle S\rangle$, and let $W$ be the set of all vectors of the form (4.1). All vectors in $W$ are expressed as linear combinations of the vectors $v_i$, which belong to $S$, so that they belong to $\langle S\rangle$. Hence $W \subset \langle S\rangle$.

Conversely, let $v$ be an element of $\sum V_i$. By definition, we have

$$v = t_1 w_1 + \cdots + t_m w_m$$

for some $m \geqslant 0$, with $t_k \in \mathbf{K}$ and $w_k \in S$ for all $k$. For each $k$, since $w_k \in S$, there exists an index $i(k)$ such that $w_k \in V_{i(k)}$, and hence $t_k w_k \in V_{i(k)}$ also (since each $V_i$ is a subspace of $V$). For each $i$, let $v_i$ be the sum of $t_k w_k$ for all those $k$ such that $i(k) = i$. Then $v_i \in V_i$, and what we observed shows that $v$ is the sum of the vectors $v_i$, so that $v$ belongs to $W$. Hence $\langle S\rangle \subset W$, and we conclude that there is equality. ☐

If $I = \{1, \ldots, n\}$ for some $n \geqslant 1$ (as will very often be the case), this means that the elements of $V_1 + \cdots + V_n$ are all vectors of the type

$$v_1 + \cdots + v_n$$

where $v_i \in V_i$.

EXAMPLE 4.1.3. (1) Let $S \subset V$ be a generating set of $V$, and for $v \in S$, let $W_v$ be the space generated by $v$ (the set of all $tv$ where $t \in \mathbf{K}$). Then the sum of the subspaces $W_v$ is equal to $V$, by the very definition of a generating set.

(2) Let $n \geqslant 1$ be an integer and let $V = \mathbf{C}^n$. Consider the subspaces of $V$ given by

$$W_1 = \left\{ \begin{pmatrix} t_1 \\ \vdots \\ t_n \end{pmatrix} \mid t_1 + \cdots + t_n = 0 \right\},$$

and

$$W_2 = \langle v_0 \rangle, \qquad \text{where} \quad v_0 = \begin{pmatrix} 1 \\ \vdots \\ 1 \end{pmatrix}.$$

Then $W_1 + W_2 = V$. Indeed, by the lemma, it suffices to show that if $v \in \mathbf{C}^n$, we can write $v = v_1 + v_2$, where $v_1 \in W_1$ and $v_2 \in W_2$. To do this, let $v = (t_i)_{1 \leqslant i \leqslant n}$. Define

$$t = \frac{1}{n}(t_1 + \cdots + t_n) \in \mathbf{C},$$

and $v_1 = v - tv_0$. Then the coordinates of $v_1$ are $(t_1 - t, \ldots, t_n - t)$, with sum equal to

$$t_1 + \cdots + t_n - nt = 0.$$

Hence $v_1 \in W_1$. Since $tv_0 \in W_2$, the decomposition $v = v_1 + tv_0$ shows that $v \in W_1 + W_2$.

(3) The following simple facts (left as exercises) show in particular that the notation $V_1 + \cdots + V_n$ must be taken with some care: it does not always behave like a sum of numbers:

- We have $V_1 + V_2 = V_2 + V_1$ for all subspaces $V_1$ and $V_2$, and $(V_1 + V_2) + V_3 = V_1 + (V_2 + V_3)$ for all subspaces $V_1$, $V_2$ and $V_3$;
- We have $V_1 + V_1 = V_1$ for all $V_1 \subset V$; more generally, if $V_2 \subset V_1$, then $V_2 + V_1 = V_1$;
- We have $V + V_1 = V$ and $V_1 + \{0\} = V_1$ for any subspace $V_1$;
- If $V_1 + V_2 = V_1 + V_3$, then *it does not follow* that $V_2 = V_3$ (see Example 4.1.14 (2) below)!

Remark 4.1.4. Using the Gauss Algorithm, one can compute the sum of finitely many subspaces $V_1$, ..., $V_m$ of a finite-dimensional vector space $V$ as follows:

- Find ordered bases $B_i$ of $V_i$;
- Compute the subset generated by the union of the $B_i$, as described in Application 6 of the Gauss Elimination algorithm.

Definition 4.1.5 (Direct sum). Let $V$ be a $\mathbf{K}$-vector space, and let $(V_i)_{i \in I}$ be any vector subspaces of $V$. We say that the sum of the subspaces $V_i$ is **direct**, or that the subspaces are **linearly independent** if any relation

$$\sum_{i \in I} v_i = 0$$

for some $v_i \in V_i$, where only finitely many $v_i$ are non-zero, implies that $v_i = 0$ for all $i$. In this case, we denote by

$$\bigoplus_{i \in I} V_i,$$

the sum of the spaces $V_i$. If $I = \{1, \ldots, n\}$, we write also

$$V_1 \oplus \cdots \oplus V_n.$$

Proposition 4.1.6. *Let $V$ be a $\mathbf{K}$-vector space, and let $(V_i)_{i\in I}$ be any vector subspaces of $V$. Let $W$ be the sum of the $V_i$'s.*

(1) *The subspaces $V_i$ are in direct sum if and only if, for any $i \in I$, there is no non-zero vector $v \in V_i$ that belongs to the sum of the other spaces $(V_j)_{j\neq i}$. In particular, if $I = \{1, 2\}$, two subspaces $V_1$ and $V_2$ are in direct sum if and only if $V_1 \cap V_2 = \{0\}$.*

(2) *If the subspaces $V_i$ are in direct sum, then any $v \in W$ is in a unique way the sum of vectors $v_i \in V_i$, in the sense that if*

$$v = \sum_{i\in I} v_i = \sum_{i\in I} w_i,$$

*with $v_i$ and $w_i$ in $V_i$, and only finitely many are non-zero, then $v_i = w_i$ for all $i$.*

(3) *If the subspaces $V_i$ are in direct sum, and if $v_i \in V_i$ are non-zero vectors, then the subset $\{v_i\}$ of $V$ is linearly independent.*

Proof. (1) Suppose the spaces are in direct sum, and fix $i_0 \in I$. If a vector $v \in V_i$ belongs to the sum of the spaces $V_j$ with $j \neq i_0$, we get

$$v = \sum_{j\neq i_0} v_j$$

for some vectors $v_j \in V_j$. But then, putting $v_{i_0} = -v$, we get

$$\sum_{i\in I} v_i = 0,$$

hence by definition of the direct sum, it follows that $-v = v_{i_0} = 0$, so $v$ is zero. Conversely, assume the condition in (1), and let $v_i \in V_i$ be vectors, all zero except finitely many, such that

$$\sum_{i\in I} v_i = 0.$$

For each $i_0$, we deduce

$$-v_{i_0} = \sum_{j\neq i_0} v_j \in \sum_{j\neq i_0} V_j,$$

so that the assumption implies that $v_{i_0} = 0$. Hence all $v_i$ are zero.

(2) We suppose that the spaces are in direct sum. If

$$\sum_{i\in I} v_i = \sum_{i\in I} w_i,$$

then we have

$$\sum_{i\in I} (v_i - w_i) = 0,$$

hence $v_i = w_i$ for all $i$.

(3) To prove that $\{v_i\}$ are linearly independent, let $t_i$, for $i \in I$, be elements of $\mathbf{K}$, with $t_i = 0$ for all but finitely many $i$, such that

$$\sum_i t_i v_i = 0.$$

Then $t_i v_i \in V_i$ and since the spaces are in direct sum, this means that $t_i v_i = 0$ for all $i$. This implies $t_i = 0$ since we assumed that the vectors are non-zero. ∎

Example 4.1.7. (1) Let $V$ be finite-dimensional and let $B$ be a basis of $V$. If $B_1, \ldots,$ $B_n$ are disjoint subsets of $B$ with union equal to $B$, and if $V_i$ is the subspace generated by $B_i$, then the spaces $V_i$ are in direct sum and

$$\bigoplus_{1 \leqslant i \leqslant n} V_i = V.$$

Indeed, suppose that $v_i \in V_i$ are such that

$$v_1 + \cdots + v_n = 0.$$

Each $v_i$ is a linear combination of the vectors $w \in B_i$; expressing them in this way, the equation becomes a linear combination of vectors of $B$ that is zero; then each coefficient is zero, which means that $v_i = 0$ for all $i$.

(2) Let $n \geqslant 1$ and let $V = \mathbf{K}^n$ and $W_1$ and $W_2$ be the subspaces in Example 4.1.3. Then $W_1$ and $W_2$ are in direct sum. Indeed, if $v \in W_1 \cap W_2$ then $v = (t_1, \ldots, t_n)$ with $t_1 + \cdots + t_n = 0$, and all $t_i$ are equal, which means that $t_i = 0$ for all $i$.

(3) Let $V = M_{n,n}(\mathbf{K})$ and let $W_+$ (resp. $W_-$) be the space of upper-triangular (resp. lower-triangular) matrices. Then $V = W_1 + W_2$, because any matrix $A = (a_{ij})$ can be writen $A = B + C$ where $B = (b_{ij})$ and $C = (c_{ij})$ with

$$\begin{aligned} b_{ij} &= a_{ij} \text{ if } i \leqslant j, \quad & b_{ij} &= 0 \text{ if } i > j \\ c_{ij} &= a_{ij} \text{ if } i < j, \quad & c_{ij} &= 0 \text{ if } i \leqslant j, \end{aligned}$$

and $B$ is then upper-triangular while $C$ is lower-triangular.

However, the sum $W_1 + W_2$ is *not* direct, since the intersection $W_1 \cap W_2$ is the space of diagonal matrices.

Definition 4.1.8 (External direct sum). Let $(V_i)_{i \in I}$ be $\mathbf{K}$-vector spaces. The space

$$V = \{(v_i)_{i \in I} \mid v_i = 0 \text{ for all } i \text{ except finitely many}\}$$

with the zero element $0 = (0_{V_i})_{i \in I}$ and the operations

$$t \cdot (v_i)_i = (tv_i)_i, \qquad (v_i)_i + (w_i)_i = (v_i + w_i)_i$$

is a vector space, called the **external direct sum** of the spaces $V_i$. It is also denoted

$$\bigoplus_{i \in I} V_i \text{ or } \boxplus_{i \in I} V_i$$

If $I$ is finite, one also writes

$$\bigoplus_{i \in I} V_i = \boxplus_{i \in I} V_i = prod_{i \in I} V_i.$$

Remark 4.1.9. One must be careful that the notation $\bigoplus V_i$ is ambiguous if all the spaces $V_i$ are subspaces of a given vector space $V$! We will carefully distinguish between the sum as subspaces and the "external" direct sum, but not all books do so...

It is left as an exercise to check that this space is a vector space.

Lemma 4.1.10. *If $V_i$ are finite-dimensional vector spaces for $1 \leqslant i \leqslant n$, then the external direct sum*

$$V = \boxplus_{1 \leqslant i \leqslant n} V_i$$

*is finite-dimensional and has dimension*

$$\dim(V_1) + \cdots + \dim(V_n).$$

Proof. For each $i$, let $B_i = \{v_{i,j} \mid 1 \leqslant j \leqslant \dim(V_i)\}$ be a basis of $V_i$. Let $\varphi_i \colon V_i \to V$ be the map

$$\varphi_i(v) = (0, \ldots, 0, v, 0, \ldots, 0) \in V_1 \times \cdots \times V_i \times \cdots \times V_n.$$

This map is linear (exercise) and injective, since its kernel is immediately seen to be $\{0\}$.

Let $B \subset V$ be the set of all vectors $\varphi_i(v_{i,j})$ where $1 \leqslant i \leqslant n$ and $1 \leqslant j \leqslant \dim(V_i)$. We claim that it a basis of $V$. Indeed, for any $(v_i)_{1 \leqslant i \leqslant n} \in V$, we can write

$$v = (v_1, 0, \ldots, 0) + (0, v_2, 0, \ldots) + \cdots + (0, 0, \ldots, 0, v_n) = \varphi_1(v_1) + \cdots + \varphi_n(v_n)$$

in $V$, and then since $v_i$ is a linear combination of the elements of $B_i$, we obtain a linear combination of vectors in $B$ representing $v$. Therefore $B$ is a generating set for $V$. Moreover, it is linearly independent since $(v_1, \ldots, v_n) = 0$ in $V$ if and only if $v_i = 0$ for all $i$, and since $B_i$ is a basis. Precisely, assume that

$$\sum_{i=1}^{n} \sum_{j=1}^{\dim(V_i)} t_{i,j} \varphi_i(v_{i,j}) = 0$$

in $V$; looking at the $i$-th component of this equality, we get

$$\sum_{j=1}^{\dim(V_i)} t_{i,j} v_{i,j} = 0,$$

which implies $t_{i,j} = 0$ for all $j$, since $B_i$ is a basis of $V_i$; this holds for all $i$, and therefore the elements of $B$ are linearly independent.

Finally, the cardinality of $B$ is $\dim(V_1) + \cdots + \dim(V_n)$, since $\varphi_i(v_{i,k}) = \varphi_j(v_{j,l})$, for $1 \leqslant i \leqslant n$ and $1 \leqslant j \leqslant \dim(V_i)$, $1 \leqslant l \leqslant \dim(V_j)$ imply that implies that $i = j$ (otherwise the vectors "live" in different factors of the product) and then that $v_{i,k} = v_{i,l}$ because $\varphi_i$ is injective. ☐

Proposition 4.1.11. *Let $V_1$ and $V_2$ be subspaces of a vector space $V$. We have*

$$\dim(V_1 + V_2) + \dim(V_1 \cap V_2) = \dim(V_1) + \dim(V_2),$$

*and $V_1$ and $V_2$ are in direct sum if and only if $V_1 \cap V_2 = \{0\}$, if and only if* $\dim(V_1 + V_2) = \dim(V_1) + \dim(V_2)$.

Proof. We prove this only when $V_1$ and $V_2$ are finite-dimensional, although the statement – properly interpreted – is valid in all cases.

Consider the external direct sum

$$W = V_1 \boxplus V_2 = V_1 \times V_2.$$

Define a map $f \colon W \to V$ by

$$f(v_1, v_2) = v_1 + v_2.$$

It is linear. Therefore we have

$$\dim \operatorname{Im}(f) = \dim(W) - \dim \operatorname{Ker}(f)$$

(Theorem 2.8.4). However, the image of $f$ is the set of sums $v_1 + v_2$ where $v_i \in V_i$, and is therefore the sum $V_1 + V_2$. The previous lemma also shows that $\dim(W) = \dim(V_1) + \dim(V_2)$. It remains to prove that $\dim \operatorname{Ker}(f) = \dim(V_1 \cap V_2)$ to conclude. But indeed, if $f(v_1, v_2) = 0$, we get $v_1 = -v_2$, so that $v_1 \in V_2 \cap V_1$ and $v_2 \in V_1 \cap V_2$; conversely, if $v \in V_1 \cap V_2$, then $(v, -v) \in \operatorname{Ker}(f)$. The linear map $g \colon V_1 \cap V_2 \to \operatorname{Ker}(f)$ such that $g(v) = (v, -v)$ is therefore well-defined, and it is an isomorphism since $(v_1, v_2) \mapsto v_1$ is an inverse. Hence $\dim \operatorname{Ker}(f) = \dim(V_1 \cap V_2)$, as expected. ☐

Definition 4.1.12 (Complement). Let $V$ be a vector space and $W$ a subspace of $V$. A **complement** $W'$ of $W$ in $V$, or **complementary subspace** of $W$ in $V$, is a subspace of $V$ such that the sum of $W$ and $W'$ is direct and $W \oplus W' = V$.

In particular, if $V$ is finite-dimensional, then a complement of $W$ must have dimension $\dim(V) - \dim(W)$ by Proposition 4.1.11.

Lemma 4.1.13. *Let $V$ be a vector space and $W$ a subspace of $V$. There always exists a complement of $W$. In fact, if $S$ is a basis of $W$, there exists a subset $S'$ of $V$ such that $S \cup S'$ is a basis of $V$, and the subspace $W'$ generated by $S'$ is a complement of $W$.*

Proof. Let $S$ be a basis of $W$. Then $S$ is linearly independent in $V$, so there exists, as claimed, a subset $S'$ of $V$ such that $S \cup S'$ is a basis of $V$ (Theorem 2.7.1 (2)). We now check that the subspace $W'$ generated by $S'$ is indeed a complement of $W$.

First, $W$ and $W'$ are in direct sum, since if we have

$$w + w' = 0$$

with $w \in W$ and $w' \in W'$, writing these as linear combinations of $S$ and $S'$ will imply that each coefficient is zero, hence also $w = 0$ and $w' = 0$. So $W + W' = W \oplus W'$. But since $S \cup S'$ is a basis of $V$, we have $W + W' = V$, hence $W \oplus W' = V$, as claimed. □

Example 4.1.14. (1) For a subspace $W$ of $V$, a complement of $W$ is equal to $\{0\}$ if and only if $W = V$.

(2) One should be careful that in general there are many complements of a given subspace! In other words, one cannot "simplify" in a direct sum: the equation $V = V_1 \oplus V_2 = V_1 \oplus V_3$ does *not* imply that $V_2 = V_3$. For instance, let $V = \mathbf{K}^2$, and let $V_1$ be the space generated by the vector $e_1 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$. A complement of $V_1$ has dimension 1, so it is generated by a vector $v = \begin{pmatrix} a \\ b \end{pmatrix}$. Because of Proposition 4.1.11, we have $V_1 \oplus V_2 = \mathbf{K}^2$ if and only if $V_1 \cap V_2 = \{0\}$, and this happens if and only if $b \neq 0$. So *all* vectors $\begin{pmatrix} a \\ b \end{pmatrix}$ with $b \neq 0$ generate a complement of $V_1$.

(3) Let $V_1 \subset V$ be a subspace such that $\dim(V_1) = \dim(V) - 1$. Then a complement $V_2$ of $V_1$ has dimension 1. It is generated by a single non-zero vector $v_2 \in V$, and the necessary and sufficient condition for the one-dimensional space $V_2 = \langle v_2 \rangle$ to be a complement of $V_1$ is that $v_2 \notin V_1$. Indeed, if $v_2 \notin V_1$, the space $V_1 + V_2$ contains $V_1$ and a vector not in $V_1$, so its dimension is strictly larger than that of $V_1$, and this means that $\dim(V_1 + V_2) = \dim(V_1) + 1 = \dim(V)$, which by Proposition 4.1.11 means that $V_1$ and $V_2$ are in direct sum, so that $V_2$ is a complement of $V_1$. Conversely, if $V_1 + V_2 = V$, then $v_2$ cannot be an element of $V_1$.

## 4.2. Endomorphisms

As already mentioned in Example 2.4.2 (2), an endomorphism of a vector space $V$ is a linear map from $V$ to $V$. The space of all endomorphisms of $V$ is a vector space denoted $\mathrm{End}_{\mathbf{K}}(V)$. If $V$ is finite-dimensional, then $\dim(\mathrm{End}_{\mathbf{K}}(V)) = \dim(V)^2$.

Endomorphisms are important for many reasons in applications. In physics, for instance, they are crucial to quantum mechanics, because observable quantities (e.g., energy, momentum) are represented by endomorphisms of certain vector spaces. Mathematically, the essential feature is that composing endomorphisms leads to other endomorphisms (similar to the composition of permutations being another permutation): if $V$ is a $\mathbf{K}$-vector space and $f$, $g$ are elements of $\mathrm{End}_{\mathbf{K}}(V)$, then $f \circ g$ is also an element of $\mathrm{End}_{\mathbf{K}}(V)$. We often call $f \circ g$ the *product* of $f$ and $g$, and write simply $fg = f \circ g$. We have $f(gh) = (fg)h$ for any endomorphisms of $V$. We write

$$f^2 = ff, \qquad f^n = f \circ \cdots \circ f \text{ (for } n \geqslant 1, n \text{ times).}$$

We will often write simply 1 for the identity map $\mathrm{Id}_V$, which is an element of $\mathrm{End}_{\mathbf{K}}(V)$. So we get $1 \cdot f = f \cdot 1 = f$ for any $f \in \mathrm{End}_{\mathbf{K}}(V)$.

PROPOSITION 4.2.1. *Let $V$ be a $\mathbf{K}$-vector space. For any $f$, $g$, $h \in \mathrm{End}_{\mathbf{K}}(V)$, we have*

$$f(g+h) = fg + fh, \qquad (f+g)h = fh + gh,$$

*where the + refers to the addition of endomorphisms.*

PROOF. Let $f_1 = f(g+h)$ and $f_2 = fg + fh$. For any vector $v \in V$, we have by definition

$$f_1(v) = f((g+h)(v)) = f(g(v) + h(v)) = f(g(v)) + f(h(v)) = fg(v) + fh(v) = f_2(v),$$

since $f$ is linear. Therefore $f_1 = f_2$. Similarly one checks that $(f+g)h = fh + gh$. ☐

REMARK 4.2.2. In contrast with permutations, there is in general no inverse for an endomorphism!

DEFINITION 4.2.3 (Commuting endomorphisms; stable subspaces). Let $V$ be a $\mathbf{K}$-vector space.

(1) Let $f$ and $g$ be endomorphisms of $V$. One says that $f$ and $g$ **commute** if $fg = gf$.

(2) Let $f$ be an endomorphism of $V$ and $W$ a subspace of $V$. One says that $W$ is **stable under** $f$, or a **stable subspace** for $f$, if $f(W) \subset W$, i.e., if $f(w)$ belongs to $W$ for any $w \in W$. In that case, the restriction of $f$ to $W$ is an endomorphism of $W$, that we will often denote $f|W$, and call the **endomorphism of the stable subspace** $W$ **induced by** $f$.

REMARK 4.2.4. Be careful that in general the restriction of an endomorphism to a subspace $W$ is not an endomorphism of $W$, because the image of a vector $w \in W$ might not belong to $W$!

In terms of matrices, it is relatively easy to "see" that a subspace is a stable subspace.

LEMMA 4.2.5. *Let $V$ be a finite-dimensional vector space and $f$ an endomorphism of $V$. Let $W$ be a subspace of $V$ and let $B_0$ be an ordered basis of $W$ and $B = (B_0, B_1)$ an ordered basis of $V$. Then $W$ is stable under $f$ if and only if the matrix $A = \mathrm{Mat}(f; B, B)$ has the form*

$$A = \begin{pmatrix} A_0 & X \\ 0 & D_1 \end{pmatrix}$$

*where 0 is the zero matrix with $\dim(W)$ columns and $\dim(V) - \dim(W)$ rows. Then $A_0$ is the matrix of the endomorphism $f|W$ of $W$.*

PROOF. A matrix $A$ is of the stated form if and only if, for the basis vectors $v$ in $B_0$, we have $f(v) \in B_0$. By linearity, this condition is equivalent with asking that $f(v) \in W$ for all $v \in W$, namely with the condition that $W$ is stable for $f$.

If that is the case, the definition of matrices representing a linear map shows that $A_0 = \mathrm{Mat}(f|W; B_0, B_0)$. ☐

Now we define important invariants related to endomorphisms. The first is the *rank*, which is the dimension of the image. Other invariants are specific to endomorphisms. First we have a definition:

Definition 4.2.6 (Trace of a matrix). Let $n \geqslant 1$ be an integer and $A = (a_{ij})_{1\leqslant i,j\leqslant n} \in M_{n,n}(\mathbf{K})$. The sum

$$\sum_{i=1}^{n} a_{i,i}$$

of the diagonal coefficients of $A$ is called the **trace** of $A$, and denoted $\mathrm{Tr}(A)$.

The map $A \mapsto \mathrm{Tr}(A)$ is a linear map from $M_{n,n}(\mathbf{K})$ to $\mathbf{K}$.

Lemma 4.2.7. *For $A$ and $B$ in $M_{n,n}(\mathbf{K})$, we have $\mathrm{Tr}(AB) = \mathrm{Tr}(BA)$.*

Proof. If we write $A = (a_{ij})$ and $B = (b_{ij})$, then $AB$ is the matrix with coefficients

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

while $BA$ is the matrix with coefficients

$$d_{ij} = \sum_{k=1}^{n} b_{ik}a_{kj}.$$

Therefore we have

$$\mathrm{Tr}(AB) = \sum_{i=1}^{n} c_{ii} = \sum_{i=1}^{n}\sum_{k=1}^{n} a_{ik}b_{ki} = \sum_{k=1}^{n}\sum_{i=1}^{n} b_{ki}a_{ik} = \sum_{k=1}^{n} d_{kk} = \mathrm{Tr}(BA).$$

□

Proposition 4.2.8. *Let $V$ be a finite-dimensional vector space over $\mathbf{K}$. Let $f : V \to V$ be an endomorphism of $V$.*

(1) *For any ordered basis $B$ of $V$, the determinant of the matrix $\mathrm{Mat}(f; B, B)$ is the same.*

(2) *For any ordered basis $B$ of $V$, the trace of the matrix $\mathrm{Mat}(f; B, B)$ is the same.*

Be careful that in these statements, we consider the matrices representing $f$ *with respect to the same bases!*

Proof. Let $B'$ be another ordered basis of $V$. Let $X$ be the change of basis matrix $\mathrm{M}_{B,B'}$. Denote $A = \mathrm{Mat}(f; B, B)$ and $A' = \mathrm{Mat}(f; B', B')$. We then have $A' = XAX^{-1}$ by Proposition 2.9.13. Then (1) follows because $\det(XAX^{-1}) = \det(X)\det(A)\det(X)^{-1} = \det(A)$ by Theorem 3.4.1. And (2) follows from the previous lemma by writing

$$\mathrm{Tr}(A') = \mathrm{Tr}(X(AX^{-1})) = \mathrm{Tr}((AX^{-1})X) = \mathrm{Tr}(A).$$

□

Definition 4.2.9 (Trace and determinant of an endomorphism). For a finite-dimensional vector space $V$ and $f \in \mathrm{End}_{\mathbf{K}}(V)$, the **trace** $\mathrm{Tr}(f)$ of $f$ is the trace of the matrix representing $f$ with respect to an arbitrary ordered basis of $V$, and the **determinant** $\det(f)$ of $f$ is the determinant of the matrix representing $f$ with respect to an arbitrary ordered basis of $V$.

PROPOSITION 4.2.10. *Let $V$ be a finite-dimensional vector space.*

(1) *The map $f \mapsto \mathrm{Tr}(f)$ is a linear map from $\mathrm{End}_{\mathbf{K}}(V)$ to $\mathbf{K}$. It satisfies $\mathrm{Tr}(1) = \dim(V)$ and $\mathrm{Tr}(fg) = \mathrm{Tr}(gf)$ for all $f, g \in \mathrm{End}_{\mathbf{K}}(V)$.*

(2) *The determinant map $f \mapsto \det(f)$ from $\mathrm{End}_{\mathbf{K}}(V)$ to $\mathbf{K}$ satisfies*

$$\det(fg) = \det(f)\det(g),$$

*and $\det(f) \neq 0$ if and only if $f$ is bijective, if and only if $f$ is injective, if and only if $f$ is surjective, in which case we have*

$$\det(f^{-1}) = \frac{1}{\det(f)}.$$

PROOF. We fix an ordered basis $B$ of $V$.

(1) To avoid ambiguity, denote by $\mathrm{Tr}' \colon M_{n,n}(\mathbf{K}) \to \mathbf{K}$ the trace map for matrices. The previous proposition implies that $\mathrm{Tr}(f) = \mathrm{Tr}'(\mathrm{Mat}(f; B, B))$ for all $f$, or in other words we have

$$\mathrm{Tr} = \mathrm{Tr}' \circ T_{B,B}$$

with the notation of Theorem 2.9.6. Since the trace of matrices $\mathrm{Tr}'$ is linear and the map $T_{B,B} \colon f \mapsto \mathrm{Mat}(f; B, B)$ is linear (Theorem 2.9.6), the trace is linear on $\mathrm{End}_{\mathbf{K}}(V)$ by composition.

We have $\mathrm{Tr}(1) = \mathrm{Tr}(\mathrm{Id}_V) = \mathrm{Tr}(1_n) = n$ (see Example 2.9.4 (1)). Moreover, by the previous lemma, Theorem 2.9.5 and Lemma 4.2.7, we get

$$\begin{aligned}\mathrm{Tr}(fg) &= \mathrm{Tr}(\mathrm{Mat}(fg; B, B)) = \mathrm{Tr}(\mathrm{Mat}(f; B, B)\,\mathrm{Mat}(g; B, B)) \\ &= \mathrm{Tr}(\mathrm{Mat}(g; B, B)\,\mathrm{Mat}(f; B, B)) = \mathrm{Tr}(\mathrm{Mat}(gf; B, B)) = \mathrm{Tr}(gf).\end{aligned}$$

(2) Similarly, we have $\det(f) = \det(\mathrm{Mat}(f; B, B))$ for all $f$, and therefore

$$\det(fg) = \det(\mathrm{Mat}(f \circ g; B, B)) = \det(\mathrm{Mat}(f; B, B)\,\mathrm{Mat}(g; B, B)) = \det(f)\det(g)$$

by Theorem 2.9.5 and Theorem 3.4.1. The last part follows then from Corollary 2.9.8, Corollary 2.8.5 (that shows that for endomorphisms, injectivity, surjectivity and bijectivity are equivalent) and the formula $\det(X^{-1}) = \det(X)^{-1}$ for $X$ invertible. ☐

Endomorphisms can be represented by a matrix by choosing an ordered basis of $V$. A fundamental observation is that these matrices usually depend on the basis, whereas we saw that certain properties (e.g., the value of the determinant) do not. This dependency means that *it makes sense to try to find a basis such that the matrix representing $f$ is as simple as possible.*

EXAMPLE 4.2.11. Let $t \in \mathbf{R}$. Consider the space $V = \mathbf{C}^2$ and the endomorphism $f(v) = Mv$ where

$$M = \begin{pmatrix} \cos(t) & -\sin(t) \\ \sin(t) & \cos(t) \end{pmatrix} \in M_{2,2}(\mathbf{C})$$

as in Example 2.9.14. The matrix of $f$ with respect to the standard basis of $M$ is simply $M$. It is not a particularly simple matrix (e.g., for computing $M^n$ if $n$ is large by just computing the products). But we saw in Example 2.9.14 that, with respect to the basis

$$B' = \left(\begin{pmatrix} 1 \\ i \end{pmatrix}, \begin{pmatrix} 1 \\ -i \end{pmatrix}\right)$$

of $V$, the matrix representing $f$ is

$$N = \begin{pmatrix} e^{-it} & 0 \\ 0 & e^{it} \end{pmatrix}.$$

This is a much simpler matrix! In particular, it is very simple to deduce that

$$N^n = \begin{pmatrix} e^{-int} & 0 \\ 0 & e^{int} \end{pmatrix}.$$

for any $n \in \mathbf{Z}$.

DEFINITION 4.2.12 (Similarity). Let $A$ and $B$ be matrices in $M_{n,n}(\mathbf{K})$. One says that $A$ is **similar to** $B$ **over** $\mathbf{K}$ , or that $A$ is **conjugate to** $B$ **over** $\mathbf{K}$, if there exists an invertible matrix $X \in M_{n,n}(\mathbf{K})$ such that $B = XAX^{-1}$.

REMARK 4.2.13. We will often just say "$A$ is similar to $B$", when $\mathbf{K}$ is clear, but it is important to note that (for instance) two matrices may be similar over $\mathbf{C}$, but not over $\mathbf{Q}$.

By Proposition 2.9.13, if $f$ is an endomorphism of a vector space $V$ of dimension $n$, then the matrices representing $f$ with respect to various ordered bases of $V$ are all similar. In general, similar matrices share many important properties – for instance, they have the same determinant and traces, as above.

LEMMA 4.2.14. *The following properties are true:*
(1) *A matrix is similar to itself;*
(2) *If $A$ is similar to $B$, then $B$ is similar to $A$;*
(3) *If $A$ is similar to $B$ and $B$ is similar to $C$, then $A$ is similar to $C$.*

PROOF. (1) is clear. For (2), note that if $B$ is similar to $A$, we have $B = XAX^{-1}$, and then $A = X^{-1}BX$, so that $A$ is similar to $B$, and for (3), if $B = XAX^{-1}$ and $C = YBY^{-1}$, then we get $C = (YX)AX^{-1}Y^{-1} = (YX)A(YX)^{-1}$. ☐

REMARK 4.2.15. One summarizes these facts by saying that the relation "$A$ is similar to $B$ over $\mathbf{K}$" is an *equivalence relation* on the set $M_{n,n}(\mathbf{K})$. For any $A \in M_{n,n}(\mathbf{K})$, the set of matrices similar to $A$ is called the *conjugacy class* of $A$ over $\mathbf{K}$. Note that any matrix belongs to a single conjugacy class.

Because of (2) in particular, one can say that two matrices $A$ and $B$ are similar without ambiguity. Then we see from Proposition 2.9.13 that $A$ and $B$ are similar if and only if there exists an endomorphism $f$ of $\mathbf{K}^n$ such that $A$ and $B$ represent $f$ with respect to two ordered bases of $\mathbf{K}^n$.

## 4.3. Eigenvalues and eigenvectors

We will study how to understand how endomorphisms "work" by trying to find "nice" representations of them. This will mean that we search for a basis of the underlying vector space for which the matrix of $f$ is as simple as possible. If $f$ is the endomorphism $f_A$ of $\mathbf{K}^n$, this means finding a matrix $B$ similar to $A$ that is as simple as possible.

DEFINITION 4.3.1 (Eigenvector, eigenspace, eigenvalue). Let $V$ be a vector space over $\mathbf{K}$ and $t \in \mathbf{K}$. An **eigenvector** of $f$ with **eigenvalue** $t$ is a *non-zero* vector $v \in V$ such that $f(v) = tv$.

If $t$ is an eigenvalue of $f$, then the **$t$-eigenspace** $\mathrm{Eig}_{t,f}$ of $f$ is the set of all vectors $v$ such that $f(v) = tv$. It is a vector subspace of $V$. The dimension of the eigenspace is called the **geometric multiplicity**, or sometimes simply multiplicity, of $t$ as an eigenvalue of $f$.

The set of all eigenvalues of $f$ is called the **spectrum** of $f$.

If $n \geqslant 1$ and $A \in M_{n,n}(\mathbf{K})$, we speak of eigenvalues, eigenvectors, eigenspaces and spectrum of $A$ to mean those of the endomorphism $f_A\colon v \mapsto Av$ of $\mathbf{K}^n$.

Warning. An eigenvector *must* be non-zero! It is not enough to check $f(v) = tv$ to deduce that $t$ is an eigenvalue. On the other hand, 0 always belongs to the $t$-eigenspace of $f$.

One point of an eigenvector is that if $v$ is one, then it becomes extremely easy to compute not only $f(v) = tv$, but also $f^k(v) = t^k v$, and so on...

By definition, if $v$ belongs to the $t$-eigenspace of $f$, we have $f(v) = tv$, which also belongs to this eigenspace. So the $t$-eigenspace $\mathrm{Eig}_{t,f}$ is a stable subspace for $f$. By definition, the endomorphism of $\mathrm{Eig}_{t,f}$ induced by $f$ on the $t$-eigenspace is the multiplication by $t$ on this space.

Remark 4.3.2. In quantum mechanics, eigenvalues are especially important: when making an experiment on a quantum system, the measurement of some observable quantity (energy, momentum, spin, etc), which is represented by an endomorphism $f$, is always an eigenvalue of $f$. Hence, for instance, the observable energy levels of an hydrogen atom are among the possible eigenvalues of the corresponding endomorphism.

Example 4.3.3. (1) The number $t = 0$ is an eigenvalue of $f$ if and only if the kernel of $f$ is not $\{0\}$, or in other words, if and only if $f$ is not injective (equivalently, if $V$ is finite-dimensional, if and only if $f$ is not an isomorphism); the corresponding eigenvectors are the non-zero elements of the kernel of $f$.

(2) Let $V = \mathbf{R}[X]$ be the vector space of polynomials with real coefficients. Consider the endomorphism $f(P) = P'$, where $P'$ is the derivative of $P$. Then the kernel of $f$ is the space of constant polynomials, so 0 is an eigenvalue for $f$ with eigenspace the space of constant polynomials. This is in fact the only eigenvalue: if $t \neq 0$ and $P' = tP$, then we must have $P$ constant because otherwise the degree of $P'$ is the degree of $P$ minus 1, whereas the degree of $tP$ is the same as that of $P$.

Consider on the other hand the endomorphism $g(P) = XP$. Then $g$ has *no* eigenvalue, since if $P \neq 0$, the degree of $XP$ is $\deg(P) + 1$, and either $tP = 0$ (if $t = 0$) or $\deg(tP) = \deg(P)$ for $t \in \mathbf{R}$.

(3) The eigenvalues depend on the choice of the field! A matrix in $M_{n,n}(\mathbf{Q})$ might have no eigenvalues, whereas the same does have some when viewed as a matrix with real of complex coefficients (see Example 4.3.18 (4) below, for instance).

Remark 4.3.4. Using the Gauss Algorithm, one can compute the eigenvalues and eigenspaces of an endomorphism $f$ of a finite-dimensional vector space $V$ of dimension $n$ as follows:

- Fix an ordered basis $B$ of $V$ and compute the matrix $A = \mathrm{Mat}(f; B, B)$;
- Consider an arbitrary element $t \in \mathbf{K}$, and solve the linear system $Ax = tx$ for $x \in \mathbf{K}^n$;
- The result will be a condition on $t$ for the existence of a non-zero solution $x \in \mathbf{K}^n$; those $t$ which satisfy this condition are the eigenvalues of $A$ and of $f$;
- For each eigenvalue $t$ (we will see below that, in this setting, there are only finitely many), find the (non-zero) subspace $W \subset \mathbf{K}^n$ of solutions of $Ax = tx$; then use the basis $B$ and Proposition 2.11.2 to “transport” the solution space $W$ of this equation to a subspace $W'$ of $V$.

Proposition 4.3.5. *Let $V$ be a vector space and $f$ an endomorphism of $V$. The eigenspaces $\mathrm{Eig}_{t,f}$ of $f$ for the eigenvalues $t$ of $f$ are in direct sum.*

*In particular, if $v_1, \ldots, v_m$ are eigenvectors of $f$ corresponding to* different *eigenvalues $t_1, \ldots, t_m$, then the vectors $\{v_1, \ldots, v_m\}$ are linearly independent in $V$.*

Proof. Let $S \subset \mathbf{K}$ be the spectrum of $f$. To check that the eigenspaces $\mathrm{Eig}_{t,f}$ for $t \in S$ are in direct sum, let $v_t \in \mathrm{Eig}_{t,f}$, for $t \in S$, be vectors such that $v_t = 0$ for all but finitely many $t$ and

$$\sum_{t \in S} v_t = 0.$$

We must show that $v_t = 0$ for all $t$. If this is not the case, there exists a smallest integer $m \geqslant 1$ for which there is a relation of this type with exactly $m$ non-zero vectors $v_t$. Let $t_1$, $\ldots$, $t_m$ be corresponding (distinct) eigenvalues. So $v_{t_i} \neq 0$. Applying $f$ to the equation

$$v_{t_1} + \cdots + v_{t_m} = 0,$$

we get by definition

$$t_1 v_{t_1} + \cdots + t_m v_{t_m} = 0.$$

We multiply the first equation by $t_1$ and subtract the result from this relation. It follows that

$$0 \cdot v_{t_1} + (t_2 - t_1) v_{t_2} + \cdots + (t_m - t_1) v_{t_m} = 0.$$

Writing $w_{t_i} = (t_i - t_1) v_{t_i}$ for $2 \leqslant i \leqslant m$, we obtain $m - 1$ *non-zero* vectors (since $t_i \neq t_1$) in $\mathrm{Eig}_{t_i,f}$ with

$$w_{t_2} + \cdots + w_{t_m} = 0.$$

This contradicts the choice of $m$ as the smallest integer for which such a relation exists. So we must indeed have $v_t = 0$ for all $t$.

The final statement follows then from Proposition 4.1.11. $\square$

Lemma 4.3.6. *Let $V$ be a finite-dimensional vector space and $f \in \mathrm{End}_{\mathbf{K}}(V)$.*

(1) *Suppose $t_1$, $\ldots$, $t_m$ are distinct eigenvalues of $f$ with eigenspaces $V_1$, $\ldots$, $V_m$ of dimensions $n_1$, $\ldots$, $n_m$. Then the spaces $V_i$ are in direct sum, and if $B_1$, $\ldots$, $B_m$ are ordered bases of $V_1$, $\ldots$, $V_m$, and $B'$ is an ordered basis of a complement $W$ of $V_1 \oplus \cdots \oplus V_m$, then $(B_1, \ldots, B_m, B')$ is an ordered basis of $V$ and the matrix representing $f$ in this basis has the block-form*

$$\begin{pmatrix} t_1 1_{n_1} & 0 & 0 & \cdots & 0 & \star \\ 0 & t_2 1_{n_2} & 0 & \cdots & 0 & \star \\ \vdots & & & & \vdots & \\ 0 & 0 & 0 & \cdots & t_m 1_{n_m} & \star \\ 0 & 0 & 0 & \cdots & 0 & A \end{pmatrix}$$

*for some matrix $A$ in $M_{d,d}(\mathbf{K})$, where $d$ is the dimension of $W$.*

(2) *Conversely, if there exists a basis $B$ of $V$ such that the matrix of $f$ in the basis $B$ is*

$$\begin{pmatrix} t_1 1_{n_1} & 0 & 0 & \cdots & 0 & \star \\ 0 & t_2 1_{n_2} & 0 & \cdots & 0 & \star \\ \vdots & & & & \vdots & \\ 0 & 0 & 0 & \cdots & t_m 1_{n_m} & \star \\ 0 & 0 & 0 & \cdots & 0 & A \end{pmatrix}$$

*for some $t_i \in \mathbf{K}$ and positive integers $n_i \geqslant 1$, then $t_i$ is an eigenvalue of $f$ with geometric multiplicity at least $n_i$.*

Proof. (1) By the previous proposition, the eigenspaces are in direct sum. By Lemma 4.1.13, there exists a complement $W$ in $V$ of $V_1 \oplus \cdots \oplus V_m$, and hence an ordered basis $B'$ of $W$. It is elementary and left as an exercise that $(B_1, \ldots, B_m, B')$ is an ordered basis of $V$. Let $A = \mathrm{Mat}(f; B, B)$. For the vectors in $B_1$, we have $f(v) = t_1 v$, so the corresponding columns have coefficients $t_1$ on the diagonal, and 0 everywhere else. Similarly for $B_2, \ldots, B_m$. This gives the stated form.

(2) For the converse, if $B$ is a basis where the matrix of $f$ has the form indicated, let $B_i$ be the vectors in $B$ corresponding to the columns where the diagonal $t_i 1_{n_i}$ appears. For any vector $v \in B_i$, we have $f(v) = t_i v$, so $t_i$ is an eigenvalue of $f$, and the space generated by $B_i$, which has dimension $n_i$, is contained in the $t_i$-eigenspace. ☐

Example 4.3.7. (1) For instance, if $\mathbf{K} = \mathbf{R}$, $\dim(V) = 7$ and $t_1 = -2$ is an eigenvalue with geometric multiplicity 3 and $t_2 = \pi$ is an eigenvalue with geometric multiplicity 2, the matrix representing $f$ with respect to a basis of the type described in this lemma has the form

$$\begin{pmatrix} -2 & 0 & 0 & 0 & 0 & a_{16} & a_{17} \\ 0 & -2 & 0 & 0 & 0 & a_{26} & a_{27} \\ 0 & 0 & -2 & 0 & 0 & a_{36} & a_{37} \\ 0 & 0 & 0 & \pi & 0 & a_{46} & a_{47} \\ 0 & 0 & 0 & 0 & \pi & a_{56} & a_{57} \\ 0 & 0 & 0 & 0 & 0 & a_{66} & a_{67} \\ 0 & 0 & 0 & 0 & 0 & a_{76} & a_{77} \end{pmatrix}$$

for some coefficients $a_{ij}$ in $\mathbf{R}$.

(2) In the converse statement, note that without knowing more about the "remaining columns", one can not be sure that the geometric multiplicity of the eigenvalue $t_i$ is not larger than $n_i$.

Definition 4.3.8 (Diagonalizable matrix and endomorphism). Let $V$ be a vector space and $f$ an endomorphism of $V$. One says that $f$ is **diagonalizable** if there exists an ordered basis $B$ of $V$ such that the elements of $B$ are eigenvectors of $f$.

If $n \geqslant 1$ and $A \in M_{n.n}(\mathbf{K})$ is basis, one says that $A$ is diagonalizable (over $\mathbf{K}$) if the endomorphism $f_A$ of $\mathbf{K}^n$ is diagonalizable.

Example 4.3.9. Diagonalizability is *not* restricted to finite-dimensional spaces! Consider the space $V = \mathbf{R}[X]$ and the endomorphism

$$f(P(X)) = P(2X)$$

for all polynomials $P$, so that for instance $f(X^2 - 3X + \pi) = 4X^2 - 6X + \pi$. Then $f$ is diagonalizable: indeed, if we consider the ordered basis $(P_i)_{i\geqslant 0}$ of $V$ where $P_i = X^i$, we have $f(P_i) = 2^i X^i = 2^i P_i$, so that $P_i$ is an eigenvector for the eigenvalue $2^i$. So there exists a basis of eigenvectors.

On the other hand, the endomorphisms $P \mapsto P'$ and $P \mapsto XP$ are not diagonalizable, since the former has only 0 has eigenvalue, and the corresponding eigenspace has dimension 1, and the second has no eigenvalue at all.

Proposition 4.3.10. *Let $V$ be a finite-dimensional vector space and $f$ an endomorphism of $V$. Then $f$ is diagonalizable if and only if there exists an ordered basis of $B$ of $V$ such that* $\mathrm{Mat}(f; B, B)$ *is diagonal.*

*If $A \in M_{n,n}(\mathbf{K})$, then $A$ is diagonalizable if and only if $A$ is similar over $\mathbf{K}$ to a diagonal matrix, namely to a matrix $B = (b_{ij})$ with $b_{ij} = 0$ if $i \neq j$.*

Proof. If $f$ is diagonalizable, then the matrix representing $f$ in an ordered basis of eigenvectors is diagonal, since $f(v)$ is a multiple of $v$ for any basis vector. Conversely, if the matrix $A = (a_{ij})$ representing $f$ in an ordered basis $B$ is diagonal, then for any $v \in B$, we get $f(v) = a_{ii} v$, so that each vector $v$ of the basis is an eigenvector.

For the second, recall that the matrix representing $f_A$ in a basis $B$ of $\mathbf{K}^n$ is $XAX^{-1}$, where $X$ is the change of basis matrix from the standard basis to $B$. So the first part shows that $f_A$ is diagonalizable if and only if there exists $X$ invertible with $XAX^{-1}$ diagonal. ☐

PROPOSITION 4.3.11. *Let $V$ be a finite-dimensional vector space and $f$ an endomorphism of $V$. Then $t \in \mathbf{K}$ is an eigenvalue of $f$ if and only if* $\det(t \cdot \mathrm{Id}_V - f) = 0$. *The $t$-eigenspace of $f$ is the kernel of $t \cdot \mathrm{Id}_V - f$.*

PROOF. By definition, $v$ satisfies $f(v) = tv$ if and only if $(t \cdot \mathrm{Id}_V - f)(v) = 0$, or equivalently if $v \in \mathrm{Ker}(t \cdot \mathrm{Id}_V - f)$. This shows that $t$ is an eigenvalue of $f$ if and only if the kernel of $t \cdot \mathrm{Id}_V - f$ is not $\{0\}$, and that the eigenspace is then this kernel. Finally, since an endomorphism $g$ is injective if and only if $\det(g) \neq 0$ (Proposition 4.2.10), it follows that $t$ is an eigenvalue if and only if $\det(t \cdot \mathrm{Id}_V - f) = 0$. ☐

DEFINITION 4.3.12 (Characteristic polynomial). The function $t \mapsto \det(t \cdot \mathrm{Id}_V - f)$ is called the **characteristic polynomial** of the endomorphism $f$. It is denoted $\mathrm{char}_f$, so that $\mathrm{char}_f(t) = \det(t \cdot \mathrm{Id}_V - f)$.

For any eigenvalue $t_0$ of $f$, the **algebraic multiplicity** of $f$ is the multiplicity of $t_0$ as a zero of $\mathrm{char}_f$, i.e., the largest integer $k \geqslant 1$ such that there exists a polynomial $g$ with

$$\mathrm{char}_f(t) = (t - t_0)^k g(t)$$

for all $t \in \mathbf{K}$, or equivalently the integer $k \geqslant 1$ such that

$$\mathrm{char}_f(t_0) = \cdots = \mathrm{char}_f^{(k-1)}(t_0) = 0, \qquad \mathrm{char}_f^{(k)}(t_0) \neq 0.$$

In practice, one can compute the characteristic polynomial of $f$ by fixing an ordered basis $B$ of $V$, computing the matrix $A$ representing $f$ with respect to $B$, and then we have

$$\mathrm{char}_f(t) = \det(t1_n - A).$$

For a matrix $A$, the function $t \mapsto \det(t1_n - A)$, which is the characteristic polynomial of the linear map $f_A$, is also called the characteristic polynomial of $A$.

LEMMA 4.3.13. *The characteristic polynomial is indeed a polynomial; it has degree* $n = \dim(V)$. *More precisely, there are elements $c_0, \ldots, c_{n-1}$ in $\mathbf{K}$ such that*

$$\mathrm{char}_f(t) = t^n + c_{n-1}t^{n-1} + \cdots + c_1 t + c_0 \tag{4.2}$$

*for all $t \in \mathbf{K}$. We have in particular*

$$c_0 = (-1)^n \det(f), \qquad c_{n-1} = -\mathrm{Tr}(f).$$

PROOF. Let $B$ be an ordered basis of $V$, and $A = \mathrm{Mat}(f; B, B)$ so that, as explained, we have $\mathrm{char}_f(t) = \det(t1_n - A)$ for all $t \in \mathbf{K}$. Write $A = (a_{ij})_{1 \leqslant i,j \leqslant n}$. Then the matrix $t1_n - A$ has coefficients $b_{ij}$ where

$$b_{ii} = t - a_{ii}, \qquad b_{ij} = -a_{ij} \text{ if } i \neq j.$$

Using (3.6), we have

$$\mathrm{char}_f(t) = \det(B) = \sum_{\sigma \in \mathrm{S}_n} \mathrm{sgn}(\sigma) b_{1\sigma(1)} \cdots b_{n\sigma(n)}.$$

This is a finite sum where each term is a product of either an element of $\mathbf{K}$ (if $\sigma(i) \neq i$) or a polynomial $t - a_{ii}$ (if $\sigma(i) = i$). So each term is a polynomial of degree at most $n$, and therefore the sum is also a polynomial of degree at most $n$.

To compute the precise degree, note that

$$\operatorname{sgn}(\sigma) b_{1\sigma(1)} \cdots b_{n\sigma(n)} \tag{4.3}$$

is a polynomial of degree at most equal to the number $F(\sigma)$ of integers $i$ such that $\sigma(i) = i$ (since these correspond to factors $b_{i\sigma(i)}$ of degree 1. So the terms of degree $n$ correspond to permutations with $\sigma(i) = i$ for all $i$, which means that this is only the case of the permutation $\sigma = 1$.

Moreover. we claim that if $\sigma \neq 1$, then the degree of (4.3) is at most $n-2$. Indeed, if the degree is $\geqslant n-1$, this would mean that there exist $n-1$ integers $1 \leqslant i \leqslant n$ with $\sigma(i) = i$. Let $j$ be remaining integer between 1 and $n$. Since $\sigma$ is injective, for any $i \neq j$, we have $i = \sigma(i) \neq \sigma(j)$. So $\sigma(j)$ must also be equal to $j$, which means that $\sigma = 1$.

Since the term (4.3) for $\sigma = 1$ is

$$(t - a_{11}) \cdots (t - a_{nn})$$

the conclusion is that

$$\operatorname{char}_f(t) = (t - a_{11}) \cdots (t - a_{nn}) + P(t)$$

where $P$ has degree at most $n-2$. So the characteristic polynomial has the form (4.2).

We compute the coefficient $c_0$ by noting that $c_0 = \operatorname{char}_f(0) = \det(-A) = (-1)^n \det(A)$ (because of multilinearity applied to the $n$ columns of $-A$). To compute $c_{n-1}$, we compute the coefficient of $t^{n-1}$ in $(t - a_{11}) \cdots (t - a_{nn})$, and this is $-a_{11} - \cdots - a_{nn}$, which means that $c_{n-1} = -\operatorname{Tr}(f)$. ☐

Theorem 4.3.14 (Existence of eigenvalues). *Let* $\mathbf{K} = \mathbf{C}$ *and* $n \geqslant 1$. *Any endomorphism* $f$ *of a vector space* $V$ *over* $\mathbf{C}$ *of dimension* $\dim(V) = n$ *has at least one eigenvalue. In addition, the sum of the* algebraic *multiplicities of the eigenvalues of* $f$ *is equal to* $n$.

*In particular, if* $A \in M_{n,n}(\mathbf{C})$ *is a matrix, then there is at least one eigenvalue of* $A$.

Proof. Because of Proposition 4.3.11 and Lemma 4.3.13, an eigenvalue of $f$ is a root of the characteristic polynomial $\operatorname{char}_f$; this polynomial is of degree $n \geqslant 1$, and by the fundamental theorem of algebra, there exists at least one $t \in \mathbf{C}$ such that $\operatorname{char}_f(t) = 0$. ☐

Remark 4.3.15. This property is very special and is *not true* for $\mathbf{K} = \mathbf{Q}$ or $\mathbf{K} = \mathbf{R}$, or when $V$ has infinite dimension. In fact, it is *equivalent* to the fundamental theorem of algebra because any polynomial $P \in \mathbf{C}[X]$ with degree $n \geqslant 1$ is the characteristic polynomial of some matrix $A \in M_{n,n}(\mathbf{C})$, so that eigenvalues of $A$ correspond exactly to zeros of $P$.

Proposition 4.3.16. *Let* $V$ *be a finite-dimensional* $\mathbf{K}$*-vector space of dimension* $n \geqslant 1$ *and* $f$ *an endomorphism of* $V$. *If the characteristic polynomial has* $n$ distinct *roots in* $\mathbf{K}$, *or in other words, if the algebraic multiplicity of any eigenvalue is equal to* 1, *then* $f$ *is diagonalizable.*

Proof. This is because there will then be $n$ eigenvectors corresponding to the $n$ distinct eigenvalues; these are linearly independent (by Lemma 4.3.6 (1)), and the space they generate has dimension $n$, and is therefore equal to $V$ (Proposition 2.8.2), so there is a basis of eigenvectors of $f$. ☐

Note that this sufficient condition is *not* necessary. For instance, the identity endomorphism is obviously diagonalizable, and its characteristic polynomial is $(t-1)^n$, which has one eigenvalue with algebraic multiplicity equal to $n$.

Remark 4.3.17. If $\mathbf{K} = \mathbf{C}$, then for "random" examples of matrices or endomorphisms, the condition indicated will be true. So, in some sense, "almost" all matrices are diagonalizable.

However, this is certainly not the case of all matrices (if the dimension is $\geqslant 2$). We will discuss later in Chapter 7 how to find a good replacement (the "Jordan form") for diagonalization. that applies to all matrices.

Example 4.3.18. (1) For $V$ of dimension 2, the characteristic polynomial of $f \in \mathrm{End}_{\mathbf{K}}(V)$ is

$$\mathrm{char}_f(t) = t^2 - \mathrm{Tr}(f)t + \det(f).$$

If $\mathbf{K} = \mathbf{C}$, we see that $f$ is diagonalizable if $\mathrm{Tr}(f)^2 - 4\det(f) \neq 0$. If $\mathbf{K} = \mathbf{R}$, we see that $f$ has at least one eigenvalue if and only if $\mathrm{Tr}(f)^2 - 4\det(f) \geqslant 0$, and is diagonalizable if $\mathrm{Tr}(f)^2 - 4\det(f) > 0$.

(2) For $A = 1_n$ (or $f = \mathrm{Id}_V$), the characteristic polynomial is $(t-1)^n$.

(3) For an upper-triangular matrix

$$A = \begin{pmatrix} a_{11} & a_{12} & \cdots & \cdots \\ 0 & a_{22} & \cdots & \cdots \\ \vdots & \vdots & \vdots & \vdots \\ 0 & \cdots & 0 & a_{nn} \end{pmatrix},$$

we have

$$\mathrm{char}_A(t) = \begin{vmatrix} t-a_{11} & -a_{12} & \cdots & \cdots \\ 0 & t-a_{22} & \cdots & \cdots \\ \vdots & \vdots & \vdots & \vdots \\ 0 & \cdots & 0 & t-a_{nn} \end{vmatrix} = (t-a_{11})\cdots(t-a_{nn})$$

so that $t$ is an eigenvalue of $A$ if and only if $t$ is one of the diagonal coefficients $a_{ii}$. If the diagonal coefficients $a_{ii}$ are all different, then $A$ is diagonalizable. The converse is however again not true.

The geometric multiplicity of an eigenvalue $t$ is in general *not* equal to the algebraic multiplicity, which is the number of indices such that $a_{ii} = t$. For instance, let $t_0 \in \mathbf{K}$ and consider

$$A = \begin{pmatrix} t_0 & 1 \\ 0 & t_0 \end{pmatrix} \in M_{2,2}(\mathbf{K}).$$

The only eigenvalue of $A$ is $t = t_0$, with algebraic multiplicity equal to 2, and the characteristic polynomial is $(t-t_0)^2$. However, if we solve the linear system $A\begin{pmatrix} x \\ y \end{pmatrix} = t_0\begin{pmatrix} x \\ y \end{pmatrix}$ to find the $t_0$-eigenspace of $f_A$, we obtain

$$\begin{cases} t_0x + y = t_0x \\ t_0y = t_0y \end{cases},$$

which is equivalent to $y = 0$. This means that the 1-eigenspace is the space of vectors $\begin{pmatrix} x \\ 0 \end{pmatrix}$, which is one-dimensional. In particular, there is no basis of eigenvectors, so $A$ is *not* diagonalizable.

(4) Here is a very classical example of using eigenvalues to solve a problem a priori unrelated to linear algebra. Consider the Fibonacci sequence $(F_n)_{n\geqslant 1}$ where $F_0 = 0$, $F_1 = 1$ and $F_{n+2} = F_{n+1} + F_n$ for all $n \geqslant 0$. In particular, $F_2 = 1$, $F_3 = 2$, etc. The goal

is to find a formula for $F_n$ (from which one can, in particular, easily answer questions such as: how many digits does $F_n$ have when $n$ is large?).

We first find a matrix representation of $F_n$. Let

$$A = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} F_0 & F_1 \\ F_1 & F_2 \end{pmatrix} \in M_{2,2}(\mathbf{C}).$$

A simple induction shows that for $n \geqslant 1$, we have the formula

$$A^n = \begin{pmatrix} F_{n-1} & F_n \\ F_n & F_{n+1} \end{pmatrix}.$$

So we are led to the problem of computing the coefficients of $A^n$. The idea is to diagonalize $A$ (if possible), because it is easy to compute the powers of a diagonal matrix. The characteristic polynomial of $A$ is

$$P(t) = t^2 - \mathrm{Tr}(A)t + \det(A) = t^2 - t - 1.$$

It has discriminant 5 and two real roots

$$\omega_1 = \frac{1+\sqrt{5}}{2}, \qquad \omega_2 = \frac{1-\sqrt{5}}{2}.$$

(note that if we view $A$ as an element of $M_{2,2}(\mathbf{Q})$, then the spectrum is empty, since $\omega_1$ and $\omega_2$ are not in $\mathbf{Q}$). Therefore $A$ is diagonalizable. We find eigenvectors of $A$ by solving the equations $Av_1 = \omega_1 v_1$ and $Av_2 = \omega_2 v_2$, and find easily that

$$v_1 = \begin{pmatrix} 1 \\ \omega_1 \end{pmatrix} \in \mathrm{Eig}_{\omega_1,A}, \qquad v_2 = \begin{pmatrix} 1 \\ \omega_2 \end{pmatrix} \in \mathrm{Eig}_{\omega_2,A}$$

(this can be checked:

$$f(v_1) = \begin{pmatrix} \omega_1 \\ 1+\omega_1 \end{pmatrix} = \begin{pmatrix} \omega_1 \\ \omega_1^2 \end{pmatrix} = \omega_1 v_1,$$

because $\omega_1^2 = \omega_1 + 1$, etc.)

In the basis $B = (v_1, v_2)$, the matrix representing $f_A$ is the diagonal matrix

$$D = \begin{pmatrix} \omega_1 & 0 \\ 0 & \omega_2 \end{pmatrix}.$$

Note that

$$D^n = \begin{pmatrix} \omega_1^n & 0 \\ 0 & \omega_2^n \end{pmatrix}$$

for any $n \geqslant 1$. The change of basis matrix $X$ from the standard basis to $B$ is computed by expressing the standard basis vectors in terms of $v_1$ and $v_2$; we find

$$X = \begin{pmatrix} \frac{\omega_2}{\omega_2-\omega_1} & \frac{1}{\omega_1-\omega_2} \\ -\frac{\omega_1}{\omega_2-\omega_1} & -\frac{1}{\omega_1-\omega_2} \end{pmatrix}$$

e.g., we have

$$\frac{\omega_2}{\omega_2-\omega_1}v_1 - \frac{\omega_1}{\omega_2-\omega_1}v_2 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}.$$

So this means that

$$A = XDX^{-1},$$

and then by induction we get

$$A^n = XD^nX^{-1}$$

for all $n \geqslant 1$ (for instance, $A^2 = XDX^{-1} \cdot XDX^{-1} = XD^2X^{-1}$, and so on). Computing the product and using

$$A^n = \begin{pmatrix} F_{n-1} & F_n \\ F_n & F_{n+1} \end{pmatrix}$$

leads to the formula

$$F_n = \frac{\omega_1^n - \omega_2^n}{\omega_1 - \omega_2}.$$

In general, we have seen that the geometric and algebraic multiplicities are not equal, but there are nevertheless some relations.

PROPOSITION 4.3.19. *Let $V$ be a finite-dimensional vector space of dimension $n \geqslant 1$ and let $f \in \mathrm{End}_{\mathbf{K}}(V)$.*

(1) *Let $t_0$ be an eigenvalue of $f$. Then the algebraic multiplicity of $t_0$ is at least the geometric multiplicity of $t_0$.*

(2) *If $\mathbf{K} = \mathbf{C}$, then the endomorphism $f$ is diagonalizable if and only if, for all eigenvalues $t_0$ of $f$, the algebraic and geometric multiplicities are equal.*

PROOF. (1) Let $m = \dim(\mathrm{Eig}_{t_0,f})$ be the geometric multiplicity of $t$ as an eigenvalue of $f$, and let $B_0 = (v_1, \ldots, v_m)$ be an ordered basis of the $t$-eigenspace. Let $B = (B_0, B_1)$ be an ordered basis of $V$. The matrix representing $f$ with respect to $B$ is partially diagonal:

$$\mathrm{Mat}(f; B, B) = \begin{pmatrix} t_0 & 0 & 0 & \cdots & 0 & \star \\ 0 & t_0 & 0 & \cdots & 0 & \star \\ \vdots & & & & \vdots & \\ 0 & 0 & 0 & \cdots & t_0 & \star \\ 0 & 0 & 0 & \cdots & 0 & A \end{pmatrix}$$

where $A$ is some matrix of size $\mathrm{Card}(B_1) = \dim(V) - m = n - m$. Then

$$\mathrm{Mat}(t\mathrm{Id}_V - f; B, B) = \begin{pmatrix} t - t_0 & 0 & 0 & \cdots & 0 & \star \\ 0 & t - t_0 & 0 & \cdots & 0 & \star \\ \vdots & & & & \vdots & \\ 0 & 0 & 0 & \cdots & t - t_0 & \star \\ 0 & 0 & 0 & \cdots & 0 & t1_{n-m} - A \end{pmatrix}$$

is also partially diagonal. Using $m$ times the formula (3.3), it follows that

$$\mathrm{char}_f(t) = (t - t_0)^m \mathrm{char}_A(t).$$

So the algebraic multiplicity of $t_0$ is at least $m$.

(2) Assume $\mathbf{K} = \mathbf{C}$. If $f$ is diagonalizable, then we obtain

$$\mathrm{char}_f(t) = \prod_{i=1}^{n} (t - t_i)$$

where $(t_1, \ldots, t_n)$ are the diagonal coefficients in a diagonal matrix representing $f$ in a basis $(v_1, \ldots, v_n)$ of eigenvectors. It follows that, for any eigenvalue $t_j$, the algebraic multiplicity is the number of indices $i$ with $t_i = t_j$, and the corresponding eigenspace is generated by the $v_i$'s for the same indices $i$. In particular, the algebraic and geometric multiplicities are the same.

Conversely, assume that the algebraic and geometric multiplicities are the same. Since $\mathbf{K} = \mathbf{C}$, the sum of the algebraic multiplicities is $n$ (Theorem 4.3.14); therefore the sum of the dimensions of the different eigenspaces is also equal to $n$, and since these are linearly independent, this means that putting together thebases of the eigenspaces of $f$, we obtain a basis of $V$. Hence $f$ is diagonalizable. □

## 4.4. Some special endomorphisms

We consider some extremely special but important classes of endomorphisms.

Definition 4.4.1 (Projection, involution, nilpotent endomorphism). (1) Let $X$ be any set and $f\colon X \to X$ any map. One says that $f$ is an **involution** if $f \circ f = \mathrm{Id}_X$. If $X$ is a $\mathbf{K}$-vector space and $f$ is linear, we say that $f$ is a **linear involution**.

(2) Let $V$ be a $\mathbf{K}$-vector space. A **projection** of $V$ is an endomorphism $p$ of $V$ such that $p \circ p = p$.

(3) Let $V$ be a $\mathbf{K}$-vector space and $f$ an endomorphism of $V$. One says that $f$ is **nilpotent** if there exists an integer $k \geqslant 0$ such that $f^k = f \circ f \circ \cdots \circ f = 0$. If $A$ is a matrix, we say that $A$ is nilpotent if there exists $k \geqslant 0$ such that $A^k = 0$, or equivalently if the endomorphism $f_A$ of $\mathbf{K}^n$ is nilpotent.

Example 4.4.2. (1) The identity map is an involution on any set $X$; on $X = \{1, \ldots, n\}$, any transposition is an involution. The linear map associated to the permutation matrix of a transposition is a linear involution.

(2) Let $V = M_{n,n}(\mathbf{K})$. The transpose map $A \mapsto {}^tA$ on $V = M_{n,n}(\mathbf{K})$ is a linear involution. Let $X$ be the set of invertible matrices in $V$; the map $A \mapsto A^{-1}$ is an involution on $X$, but it is not linear (the set $X$ is not a vector space anyway).

(3) Let $X = \mathbf{C}$; the complex conjugate map $c\colon z \mapsto \bar{z}$ is an involution. If $X$ is viewed as a real vector space, then $c$ is a linear involution, but if $X$ is viewed as a complex vector space, it is not (since $c(iz) = -iz$).

(4) Let $V$ be the space of all functions from $[-1, 1]$ to $\mathbf{C}$. For $f \in V$, define $j(f)$ to be the function $x \mapsto f(-x)$. Then $j\colon V \to V$ is a linear involution.

(5) Let $V$ be a $\mathbf{K}$-vector space and let $W_1$ and $W_2$ be subspaces such that $V = W_1 \oplus W_2$. For any $v \in V$, we can then write $v = w_1 + w_2$ for some unique vectors $w_1 \in W_1$ and $w_2 \in W_2$. Therefore we can define a map $p\colon V \to V$ by $p(v) = w_1$. This map is linear, because of the uniqueness: for $v$ and $v'$ in $V$ and $t$, $t' \in \mathbf{K}$, if we have $v = w_1 + w_2$ and $v' = w_1' + w_2'$, then $tv + t'v' = (tw_1 + t'w_1') + (tw_2 + t'w_2')$, with $tw_1 + t'w_1' \in W_1$ and $tw_2 + t'w_2' \in W_2$, so that $p(tv + t'v') = tw_1 + t'w_1' = tp(v) + t'p(v')$.

The map $p$ is a projection of $V$: indeed, since $p(v) \in W_1$, the decomposition of $p(v)$ in terms of $W_1$ and $W_2$ is $p(v) = p(v) + 0$, and get $p(p(v)) = p(v)$. We say that $p$ is the *projection of $V$ on $W_1$ parallel to $W_2$*, or the *projection with image $W_1$ and kernel $W_2$* (see below for the justification of this terminology).

(6) Suppose that $V = \mathbf{K}^n$ and $f = f_A$ where $A = (a_{ij})$ is upper-triangular with diagonal coefficients equal to 0:

$$A = \begin{pmatrix} 0 & a_{12} & \cdots & \cdots \\ 0 & 0 & a_{23} & \vdots \\ \vdots & \vdots & \vdots & \vdots \\ 0 & \cdots & 0 & a_{n-1,n} \\ 0 & \cdots & 0 & 0 \end{pmatrix}.$$

(in other words, we have $a_{ij} = 0$ if $i \geqslant j$). Then $f_A$ is nilpotent, and more precisely, we have $f_A^n = f_{A^n} = 0$.

To prove, we claim that for $1 \leqslant k \leqslant n-1$, the image of $f_A^k$ is contained in the subspace $W_k$ of $\mathbf{K}^n$ generated by the first $n-k$ basis vectors of the standard basis of $\mathbf{K}^n$. Indeed, the point is that the form of the matrix shows that for $1 \leqslant i \leqslant n$, the vector $f_A(e_i)$ is a linear combination of $e_1, \ldots, e_{i-1}$, so belongs to $W_{i-1}$. Then we get $\mathrm{Im}(f_A) \subset W_1$ since $W_i \subset W_1$ for $i \geqslant 1$. Then the image of $f_A^2$ is contained in the image of the first $n-1$ basis vectors under $f_A$, which is contained in $W_2$, etc. This gives the stated claim by induction. Now the image of $f_A^{n-1}$ is contained in $W_{n-1}$, which is the space generated by $e_1$. But the matrix shows that $f_A(e_1) = 0$, and hence the image of $f_A^n$ is $\{0\}$.

The next proposition deals with involutions.

Proposition 4.4.3. *Let* $\mathbf{K}$ *be a field* of characteristic different from 2, *for instance* $\mathbf{Q}$, $\mathbf{R}$ *or* $\mathbf{C}$.

*Let $V$ be a $\mathbf{K}$-vector space and $j$ a linear involution of $V$. Then the spectrum of $j$ is contained in $\{-1, 1\}$ and $V$ is the direct sum of the 1-eigenspace of $j$ and the $-1$-eigenspace of $j$. In particular, $j$ is diagonalizable.*

Proof. If $t$ is an eigenvalue of $j$ and $v$ a $t$-eigenvector, then from applying $j$ to the relation $j(v) = tv$, we get $v = (j \circ j)(v) = tj(v) = t^2 v$, so that $(1-t^2)v = 0$. Since $v \neq 0$, we have $t^2 = 1$ so $t$ is either 1 or $-1$.

The 1-eigenspace is $V_1 = \{v \in V \mid j(v) = v\}$ and the $(-1)$-eigenspace is $V_{-1} = \{v \in V \mid j(v) = -v\}$. They are in direct sum (as explained in the first part of Lemma 4.3.6). To check that $V_1 \oplus V_{-1} = V$, we simply write

$$v = \frac{1}{2}(v + j(v)) + \frac{1}{2}(v - j(v)), \tag{4.4}$$

and observe that since $j$ is an involution, we have

$$\begin{aligned} j\Big(\frac{1}{2}(v + j(v))\Big) &= \frac{1}{2}(j(v) + j^2(v)) = \frac{1}{2}(j(v) + v), \\ j\Big(\frac{1}{2}(v - j(v))\Big) &= \frac{1}{2}(j(v) - j^2(v)) = -\frac{1}{2}(v - j(v)), \end{aligned}$$

so $v \in V_1 + V_{-1}$.

Taking an ordered basis $B_1$ of $V_1$ and an ordered basis $B_{-1}$ of $V_{-1}$, we see that $(B_1, B_{-1})$ is an ordered basis of $V$ formed of eigenvectors of $j$, so $j$ is diagonalizable. ☐

The following proposition gives a "geometric" description of the set of all projections on a vector space $V$.

Proposition 4.4.4. *Let $V$ be a vector space. Let $X_1$ be the set of all projections $p \in \mathrm{End}_{\mathbf{K}}(V)$ and let $X_2$ be the set of all pairs $(W_1, W_2)$ of subspaces of $V$ such that $W_1 \oplus W_2 = V$, i.e., such that $W_1$ and $W_2$ are in direct sum and their sum is $V$.*

*The maps*

$$F_1 \begin{cases} X_1 \to X_2 \\ p \mapsto (\mathrm{Im}(p), \mathrm{Ker}(p)) \end{cases}$$

*and (cf. Example 4.4.2 (5))*

$$F_2 \begin{cases} X_2 \to X_1 \\ (W_1, W_2) \mapsto \textit{the projection on } W_1 \textit{ parallel to } W_2 \end{cases}$$

*are well-defined and are reciprocal bijections. Moreover* $\mathrm{Im}(p) = \mathrm{Ker}(\mathrm{Id}_V - p)$.

Proof. We first check that $\mathrm{Im}(p) = \mathrm{Ker}(\mathrm{Id}_V - p)$. Indeed, if $v \in V$ and $w = p(v)$, then we get $p(w) = p^2(v) = p(v) = w$, so that the image of $p$ is contained in $\mathrm{Ker}(\mathrm{Id}_V - p)$. Conversely, if $p(v) = v$, then $v$ belongs to the image of $p$.

Now we check first that $F_1$ is well-defined, which means that $(\mathrm{Im}(p), \mathrm{Ker}(p))$ belongs to $X_2$. Since $\mathrm{Im}(p) = \mathrm{Ker}(\mathrm{Id}_V - P)$, the sum of $\mathrm{Im}(p)$ and $\mathrm{Ker}(p)$ is the sum of eigenspaces corresponding to different eigenvalue of $p$, and therefore it is a direct sum (Proposition 4.3.5). Moreover $\mathrm{Im}(p) + \mathrm{Ker}(p) = V$ because we can write any $v \in V$ as

$$v = p(v) + (v - p(v))$$

where the first term belongs to $\mathrm{Im}(p)$ and the second satisfies $p(v-p(v)) = p(v)-p^2(v) = 0$, so that it belongs to $\mathrm{Ker}(p)$.

It remains to check that the compositions $F_1 \circ F_2$ and $F_2 \circ F_1$ are the respective identity maps.

First, if $p \in X_1$, then $q = F_2(F_1(p))$ is the projection to $\mathrm{Im}(p)$ parallel to $\mathrm{Ker}(p)$; this means that for $v \in V$, we have $q(v) = w_1$ where

$$v = w_1 + w_2$$

with $w_1 \in \mathrm{Im}(p)$ and $w_2 \in \mathrm{Ker}(p)$. But then $p(v) = p(w_1) = w_1$, so we have $q = p$. This means that $F_2 \circ F_1 = \mathrm{Id}_{X_1}$.

Finally, for $(W_1, W_2) \in X_2$, we have $F_1(F_2(W_1, W_2)) = (\mathrm{Im}(p), \mathrm{Ker}(p))$ where $p$ is the projection on $W_1$ parallel to $W_2$. By definition, the image of $p$ is contained in $W_1$, and in fact is equal to $W_1$, since $p(w_1) = w_1$ for all $w_1 \in W_1$, which shows the converse inclusion. And by construction, we have $p(v) = 0$ if and only if $v = 0 + w_2$ with $w_2 \in W_2$, which means that $\mathrm{Ker}(p) = W_2$. So $F_1(F_2(W_1, W_2)) = (W_1, W_2)$, which means that $F_1 \circ F_2 = \mathrm{Id}_{X_2}$. ☐

PROPOSITION 4.4.5. *Let $V$ be a $\mathbf{K}$-vector space and $p$ a projection of $V$.*

(1) *The spectrum of $j$ is contained in $\{0, 1\}$ and $V$ is the direct sum of the kernel $V_0$ of $p$ and the 1-eigenspace of $p$. In particular, $p$ is diagonalizable. Moreover, the 1-eigenspace $V_1$ of $p$ is the image of $p$.*

(2) *The linear map $q = \mathrm{Id}_V - p$ is a projection with kernel equal to the image of $p$ and image equal to the kernel of $p$.*

PROOF. (1) If $t$ is an eigenvalue of $p$ and $v$ a $t$-eigenvector, then from $p(v) = tv$ we deduce that $p^2(v) = t^2 v$, so that $(t - t^2)v = 0$, and hence $t(1-t) = 0$. So the spectrum is contained in $\{0, 1\}$. The 0-eigenspace is of course the kernel of $p$. The previous proposition shows that $\mathrm{Ker}(\mathrm{Id}_V - p) = \mathrm{Im}(p)$, so that the 1-eigenspace (if non-zero) is the image of $p$. Since $\mathrm{Im}(p) \oplus \mathrm{Ker}(p) = V$, this means that $p$ is diagonalizable: if $B_0$ is a basis of $\mathrm{Im}(p) = \mathrm{Ker}(\mathrm{Id}_V - p)$ and $B_1$ is a basis of $\mathrm{Ker}(p)$, then $B_0 \cup B_1$ is a basis of $V$ made of eigenvectors of $p$.

(2) We can compute

$$q^2 = (\mathrm{Id}_V - p) \circ (\mathrm{Id}_V - p) = (\mathrm{Id}_V - p) - p \circ (\mathrm{Id}_V - p) = \mathrm{Id}_V - p - p + p^2 = \mathrm{Id}_V - p = q,$$

so that $q$ is a projection. We see immediately that the kernel of $q$ is the 1-eigenspace of $p$, hence is the image of $p$, and that the image of $q$, which is its 1-eigenspace, is the kernel of $p$. ☐

PROPOSITION 4.4.6. *Let $V$ be a finite-dimensional $\mathbf{K}$-vector space and let $f$ be a nilpotent endomorphism of $V$. Let $n = \dim(V)$. Then $f^n = 0$. More precisely, for any vector $v \neq 0$ in $V$, and $k \geqslant 0$ such that $f^k(v) = 0$ but $f^{k-1}(v) = 0$, the vectors*

$$(v, f(v), \ldots, f^{k-1}(v))$$

*are linearly independent.*

In Proposition 7.2.3 below, we will obtain a much more precise description of nilpotent endomorphisms, and this will be a key ot the Jordan Normal Form.

Proof. First, the second statement is indeed more precise than the first: let $k \geqslant 1$ be such that $f^k = 0$ but $f^{k-1} \neq 0$; there exists $v \neq 0$ such that $f^{k-1}(v) \neq 0$, and we obtain $k \leqslant n$ by applying the second result to this vector $v$.

We now prove the second claim. Assume therefore that $v \neq 0$ and that $f^k(v) = 0$ but $f^{k-1}(v) \neq 0$. Let $t_0, \ldots, t_{k-1}$ be elements of $\mathbf{K}$ such that

$$t_1 v + \cdots + t_{k-1} f^{k-1}(v) = 0.$$

Apply $f^{k-1}$ to this relation; since $f^k(v) = \cdots = f^{2k-2}(v) = 0$, we get

$$t_1 f^{k-1}(v) = t_1 f^{k-1}(v) + t_2 f^k(v) + \cdots + t_{k-1} f^{2k-2}(v) = 0,$$

and therefore $t_1 f^{k-1}(v) = 0$. Since $f^{k-1}(v)$ was assumed to be non-zero, it follows that $t_1 = 0$. Now repeating this argument, but applying $f^{k-2}$ to the linear relation (and using the fact that $t_1 = 0$), we get $t_2 = 0$. Then similarly we derive by induction that $t_i = 0$ for all $i$, proving the linear independence stated. $\square$

CHAPTER 5

# Euclidean spaces

## 5.1. Properties of the transpose

The following properties of the transpose of matrices will be reviewed and understood more conceptually in the chapter on duality, but they can be checked here quickly.

Proposition 5.1.1. *Let* $\mathbf{K}$ *be a field.*
(1) *For* $A \in M_{m,n}(\mathbf{K})$, $B \in M_{p,m}(\mathbf{K})$, *we have*

$$^t(BA) = {}^tA^tB \in M_{p,n}(\mathbf{K}).$$

(2) *A matrix* $A \in M_{n,n}(\mathbf{K})$ *is invertible if and only if* $^tA$ *is invertible, and we have* $(^tA)^{-1} = {}^t(A^{-1})$.

Proof. (1) is a direct computation from the definition.
(2) We know that $\det(A) = \det(^tA)$, so $A$ is invertible if and only if $^tA$ is. Moreover from

$$^tA^t(A^{-1}) = {}^tA^{-1}A = {}^t1_n = 1_n,$$

we see that the inverse of $^tA$ is the transpose of $A^{-1}$. ☐

## 5.2. Bilinear forms

Definition 5.2.1 (Bilinear form). Let $V$ be a $\mathbf{K}$-vector space. A **linear form** on $V$ is a linear map $V \to \mathbf{K}$. A **bilinear form** $b$ on $V$ is a bilinear map $V \times V \to \mathbf{K}$.
As in Definition 3.1.3, a bilinear form $b$ is **symmetric** if $b(v_1, v_2) = b(v_2, v_1)$ for $v_1$ and $v_2$ in $V$, and it is **alternating** if $b(v, v) = 0$ for all $v \in V$.

In other words, a bilinear form is a map with values in $\mathbf{K}$ such that

$$b(sv_1 + tv_2, w) = sb(v_1, w) + tb(v_2, w), \qquad b(v, sw_1 + tw_2) = sb(v, w_1) + tb(v, w_2)$$

for all $s$ and $t \in \mathbf{K}$, and all $v_1$, $v_2$, $v$, $w$, $w_1$, $w_2$ in $V$.
If $b$ is alternating then from $b(x + y, x + y) = 0$, we deduce that $b(x, y) = -b(y, x)$.

Example 5.2.2. (1) For any linear forms $\lambda_1$ and $\lambda_2$, the product

$$b(v_1, v_2) = \lambda_1(v_1)\lambda_2(v_2)$$

is a bilinear form. It is symmetric if $\lambda_1 = \lambda_2$ (but only alternating if $\lambda_1 = 0$ or $\lambda_2 = 0$).
(2) The set $\mathrm{Bil}(V)$ of all bilinear forms on $V$ is a subset of the space of all functions $V \times V \to \mathbf{K}$; it is in fact a vector subspace: the sum of two bilinear forms is bilinear and the product of a bilinear form with an element of $\mathbf{K}$ is bilinear. Moreover, the sets $\mathrm{Bil}^s(V)$ and $\mathrm{Bil}^a(V)$ of symmetric and alternating bilinear forms are subspaces of $\mathrm{Bil}(V)$.
(3) Let $V$ be the vector space over $\mathbf{C}$ of all complex-valued continuous functions on $[0, 1]$. Let

$$b_1(f_1, f_2) = f_1(0)f_2(0)$$

and

$$b_2(f_1, f_2) = \int_0^1 f_1(x)f_2(x)dx$$

for $f_1$ and $f_2$ in $V$. Then $b_1$ and $b_2$ are symmetric bilinear forms on $V$. On the other hand, the bilinear form $b_3(f_1, f_2) = f_1(0)f_2(1)$ is not symmetric.

(4) Let $V = \mathbf{K}^2$. Define

$$b\left(\begin{pmatrix} x \\ z \end{pmatrix}, \begin{pmatrix} y \\ t \end{pmatrix}\right) = xt - yz.$$

Then $b$ is an alternating bilinear form on $V$.

(5) Let $n \geqslant 1$ be an integer and let $V = \mathbf{K}^{2n}$. For $v = (t_i)_{1\leqslant i\leqslant 2n}$ and $w = (s_i)_{1\leqslant i\leqslant 2n}$, define

$$b(v, w) = t_1 s_2 - t_2 s_1 + \cdots + t_{2n-1}s_{2n} - t_{2n}s_{2n-1}.$$

Then $b$ is a bilinear form (because each map $v \mapsto t_i$ or $w \mapsto s_i$ is a linear form, and $b$ is a sum of products of two linear forms, so that Examples (1) and (2) imply that it is bilinear). It is moreover alternating, as one sees immediately.

(6) Let $f_1$, $f_2 \colon V_1 \to V_2$ be linear maps. For any $b \in \mathrm{Bil}(V_2)$, define

$$b_{f_1,f_2}(v, w) = b(f_1(v), f_2(w)).$$

Then $b_{f_1,f_2}$ is a bilinear form on $V_1$, and the map

$$\mathrm{Bil}(f_1, f_2) \colon b \mapsto b_{f_1,f_2}$$

is a linear map from $\mathrm{Bil}(V_2)$ to $\mathrm{Bil}(V_1)$.

(7) Let $V = \mathbf{K}^n$ and let $A \in M_{n,n}(\mathbf{K})$. For $x \in V$, the transpose ${}^t x$ is a row vector in $\mathbf{K}_n$; we define

$$b(x, y) = {}^t x A y$$

for $x$ and $y \in \mathbf{K}^n$. Then $b$ is a bilinear form. Indeed, this product is a matrix in $M_{1,1}(\mathbf{K})$, hence an element of $\mathbf{K}$. We have

$$b(x, ty_1 + sy_2) = {}^t x A(ty_1 + sy_2) = {}^t x(tAy_1 + sAy_2) = tb(x, y_1) + sb(x, y_2)$$

and similarly $b(tx_1 + sx_2, y) = tb(x_1, y) + sb(x_2, y)$. In terms of the coefficients $a_{ij}$ of $A$, one checks (see the proof of Proposition 5.2.3 below) that for $x = (x_i)_{1\leqslant i\leqslant n}$ and $y = (y_j)_{1\leqslant j\leqslant n}$ in $\mathbf{K}^n$, we have

$$b(x, y) = \sum_{i,j} a_{ij} x_i y_j.$$

In particular, if $A = 1_n$ is the identity matrix, we obtain

$$b(x, y) = \sum_{i=1}^{n} x_i y_i.$$

Proposition 5.2.3. *Let $V$ be a finite-dimensional space.*

(1) *For any ordered basis $B = (v_1, \ldots, v_n)$ of $V$, the application*

$$\beta_B \begin{cases} \mathrm{Bil}(V) & \to M_{n,n}(\mathbf{K}) \\ b & \mapsto (b(v_i, v_j))_{1 \leqslant i,j \leqslant n} \end{cases}$$

*is an isomorphism. In particular, $\dim \mathrm{Bil}(V) = \dim(V)^2$. The bilinear form $b$ is symmetric if and only if ${}^t\beta_B(b) = \beta_B(b)$.*

(2) *For any $x = (t_i) \in \mathbf{K}^n$ and $y = (s_j) \in \mathbf{K}^n$, we have*

$$b\Big(\sum_i t_i v_i, \sum_j s_j v_j\Big) = \sum_{i,j} b(v_i, v_j) t_i s_j = {}^t x A y$$

*where $A = \beta_B(b)$.*

(3) *If $B$ and $B'$ are ordered bases of $V$ and $X = \mathrm{M}_{B',B}$ is the change of basis matrix, then for all $b \in \mathrm{Bil}(V)$ we have*

$$\beta_{B'}(b) = {}^t X \beta_B(b) X.$$

Proof. (1) The linearity of $\beta_B$ is easy to check. We next check that this map is injective. If $\beta_B(b) = 0$, then $b(v_i, v_j) = 0$ for all $i$ and $j$. Then, using bilinearity, for any vectors

$$v = t_1 v_1 + \cdots + t_n v_n, \qquad w = s_1 v_1 + \cdots + s_n v_n, \tag{5.1}$$

we get

$$\begin{aligned} b(v, w) = b(t_1 v_1 + \cdots + t_n v_n, w) &= \sum_{i=1}^n t_i b(v_i, w) \\ &= \sum_{i=1}^n t_i b(v_i, s_1 v_1 + \cdots + s_n v_n) \\ &= \sum_{i,j} t_i s_j b(v_i, v_j) = 0, \end{aligned}$$

so that $b = 0$. Finally, given a matrix $A = (a_{ij}) \in M_{n,n}(\mathbf{K})$, define

$$b(v, w) = \sum_{i,j} a_{ij} t_i s_j$$

for $v$ and $w$ as in (5.1). This is a well-defined map from $V \times V$ to $\mathbf{K}$. For each $i$ and $j$, $(v, w) \mapsto a_{ij} t_i s_j$ is bilinear (product of two linear forms and a number), so the sum $b$ is in $\mathrm{Bil}(V)$. For $v = v_{i_0}$ and $w = v_{j_0}$, the coefficients $t_i$ and $s_j$ are zero except that $t_{i_0} = 1$ and $s_{j_0} = 1$. Therefore $b(v_i, v_j) = a_{ij}$. This means that $\beta_B(b) = A$, which means that any $A$ is in the image of $\beta_B$, and hence we conclude that $\beta_B$ is surjective.

By bilinearity, a bilinear form $b$ is symmetric if and only if $b(v_i, v_j) = b(v_j, v_i)$ for all $i$ and $j$, and this condition is equivalent to saying that the transpose of the matrix $\beta_B(b)$ is equal to itself.

(2) The first formula has already been deduced during the proof of (1), so we need to check that for $A = \beta_B(b)$, we have

$$\sum_{i,j} b(v_i, v_j) t_i s_j = {}^t x A y.$$

Indeed, we have
$$Ay = \Big(\sum_j b(v_i, v_j)s_j\Big)_{1\leqslant i\leqslant n},$$
and therefore
$$^t x A y = (t_1 \ \cdots \ t_n) \cdot Ay = \sum_i t_i \Big(\sum_j b(v_i, v_j)s_j\Big) = \sum_{1\leqslant i,j\leqslant n} t_i s_j b(v_i, v_j).$$

(3) Let $B' = (w_1, \ldots, w_n)$. If $X = \mathrm{M}_{B',B} = (a_{ij})$ is the change of basis matrix, and $x_j = (a_{ij})_{1\leqslant i\leqslant n}$ denotes the $j$-th column of $X$, then we have by definition
$$w_j = \sum_{i=1}^{n} a_{ij} v_i$$
for $1 \leqslant j \leqslant n$. So by (2) we get
$$b(w_i, w_j) = {}^t x_i \beta_B(b) x_j$$
for all $i$ and $j$. Now consider the matrix ${}^t X \beta_B(b) X$ and denote its coefficients $(c_{ij})$. Then $c_{ij}$ is the product of the $i$-th row of ${}^t X$ with the $j$-th column of $\beta_B(b)X$, which is the product of $\beta_B(b)$ and the $j$-th column of $X$. This means that
$$c_{ij} = {}^t x_i \beta_B(b) x_j = b(w_i, w_j),$$
and hence $\beta_{B'}(b) = {}^t X \beta_B(b) X$. ☐

Definition 5.2.4 (Left and right kernels). Let $b$ be a bilinear form on $V$. The **left-kernel** of $b$ is the set of vectors $v \in V$ such that
$$b(v, w) = 0 \text{ for all } w \in V,$$
and the **right-kernel** of $b$ is the set of vectors $w \in V$ such that
$$b(v, w) = 0 \text{ for all } v \in V.$$

A bilinear form $b$ on $V$ is **non-degenerate** if the right and the left kernels are both equal to $\{0\}$.

If $b$ is symmetric, then the left and right kernels are equal.

Proposition 5.2.5. *Let $V$ be a finite-dimensional vector space and $B = (v_i)$ an ordered basis of $V$. Then a bilinear form $b$ on $V$ is non-degenerate if and only if* $\det(\beta_B(b)) \neq 0$.

Proof. Suppose first that the left-kernel of $b$ contains a non-zero vector $v$. There is an ordered basis $B'$ of $V$ such that $v$ is the first vector of $B'$ (Theorem 2.7.1 (2)). We have
$$\beta_B(b) = {}^t X \beta_{B'}(b) X$$
where $X = \mathrm{M}_{B,B'}$ (Proposition 5.2.3 (3)). Since the coefficients $b(v, v')$ of the first row of $\beta_{B'}(b)$ are zero, we get $\det(\beta_{B'}(b)) = 0$, hence $\det(\beta_B(b)) = 0$. Similarly, if the right-kernel of $b$ is non-zero, we deduce that $\det(\beta_B(b)) = 0$.

We now consider the converse and assume that $\det(\beta_B(b)) = 0$. Then the columns $C_j$ of the matrix $\beta_B(b)$ are not linearly independent. Let then $t_1, \ldots, t_n$ be elements of $\mathbf{K}$, not all equal to 0, such that
$$t_1 C_1 + \cdots + t_n C_n = 0_n \in \mathbf{K}^n.$$
Since $C_j = (b(v_i, v_j))_{1\leqslant i\leqslant n}$, this means that for $1 \leqslant i \leqslant n$, we have
$$t_1 b(v_i, v_1) + \cdots + t_n b(v_i, v_n) = 0.$$

By bilinearity, this means that

$$b(v_i, t_1v_1 + \cdots + t_nv_n) = 0$$

for all $i$. But then (by bilinearity again) the vector $t_1v_1 + \cdots + t_nv_n$ belongs to the right-kernel of $b$. Similarly, using the fact that the rows of $\beta_B(b)$ are not linearly independent, we deduce that the left-kernel of $b$ is non-zero. $\square$

Proposition 5.2.6. *Let $V$ be finite-dimensional and let $b \in \mathrm{Bil}(V)$ be a non-degenerate bilinear form. For $w \in V$, denote by $\lambda_w$ the linear form*

$$\lambda_w(v) = b(v, w).$$

*Then the map*

$$\begin{cases} V & \to \mathrm{Hom}_{\mathbf{K}}(V, \mathbf{K}) \\ w & \mapsto \lambda_w \end{cases}$$

*is an isomorphism.*

Proof. Since both spaces have the same dimension, it suffices to check that this map is injective. But if $\lambda_w = 0$, we obtain $b(v, w) = 0$ for all $v$, which means that $w$ belongs to the right-kernel of $b$, which is zero since $b$ is non-degenerate. $\square$

Example 5.2.7. (1) We describe more precisely $\mathrm{Bil}(\mathbf{K}^n)$ for $n = 1$ and 2. For $n = 1$, a bilinear form on $\mathbf{K}$ is of the form $b(x, y) = axy$ for some $a \in \mathbf{K}$. It is always symmetric and non-degenerate if and only if $a \neq 0$.

For $n = 2$, the bilinear form associated to the matrix

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

is

$$b\left(\begin{pmatrix} x_1 \\ y_1 \end{pmatrix}, \begin{pmatrix} x_2 \\ y_2 \end{pmatrix}\right) = a_{11}x_1x_2 + a_{12}x_1y_2 + a_{21}x_2y_1 + a_{22}x_2y_2.$$

This bilinear form is non-degenerate if and only if $a_{11}a_{22} - a_{12}a_{21} \neq 0$. It is symmetric if and only if $a_{12} = a_{21}$, and alternating if and only if $a_{11} = a_{22} = 0$ and $a_{12} = -a_{21}$. (This corresponds to the fact that the determinant is, up to multiplication with a fixed number, the only alternating bilinear form on $\mathbf{K}^2$).

(2) Let $b$ be the alternating bilinear form on $\mathbf{K}^{2n}$ of Example 5.2.2 (5):

$$b(v, w) = t_1s_2 - t_2s_1 + \cdots + t_{2n-1}s_{2n} - t_{2n}s_{2n-1}$$

for $v = (t_i)$ and $w = (s_j)$. This bilinear form is *non-degenerate*. Indeed, the alternating property (in the form $b(v, w) = -b(w, v)$) shows that it suffices to prove that the left-kernel of $b$ is non-zero. Let $v = (t_i)$ be such that $b(v, w) = 0$ for all $w \in \mathbf{K}^{2n}$. Taking for $w$ the elements $e_1, \ldots, e_{2n}$ of the standard basis, we obtain

$$0 = b(v, e_{2i}) = t_{2i-1}, \qquad 0 = b(v, e_{2i-1}) = -t_{2i}$$

for $1 \leqslant i \leqslant n$, so $t_i = 0$ for all $i$.

## 5.3. Euclidean scalar products

We now consider exclusively the case $\mathbf{K} = \mathbf{R}$. In this case there is an extra structure available: the ordering between real numbers.

Definition 5.3.1 (Positive bilinear form, scalar product). Let $V$ be an $\mathbf{R}$-vector space. A bilinear form $b \in \mathrm{Bil}(V)$ is called **positive** if $b$ is symmetric and

$$b(v, v) \geqslant 0$$

for all $v \in V$; it is called **positive definite**, or a **scalar product** if it is positive and if $b(v, v) = 0$ if and only if $v = 0$.

If $b$ is positive, then two vectors $v$ and $w$ are said to be **orthogonal** if and only if $b(v, w) = 0$. This is denoted $v \perp w$, or $v \perp_b w$ if we wish to specify wichi bilinear form $b$ is considered.

If $v$ and $w$ are orthogonal, note that we obtain

$$b(v + w, v + w) = b(v, v) + b(w, w) + b(v, w) + b(w, v) = b(v, v) + b(w, w).$$

Example 5.3.2. Let $V = \mathbf{R}^n$. The bilinear form

$$b(x, y) = \sum_{i=1}^{n} x_i y_i$$

is a scalar product on $\mathbf{R}^n$: indeed, it is clearly symmetric, and since

$$b(x, x) = \sum_{i=1}^{n} x_i^2,$$

it follows that $b(x, x) \geqslant 0$ for all $x \in \mathbf{R}^n$, with equality only if each $x_i$ is zero, that is only if $x = 0$.

This scalar product on $\mathbf{R}^n$ is called the **standard scalar product**.

Proposition 5.3.3 (Cauchy-Schwarz inequality). *Let $b$ be a positive bilinear form on $V$. Then for all $v$ and $w \in V$, we have*

$$|b(v, w)|^2 \leqslant b(v, v) b(w, w).$$

*Moreover, if $b$ is positive definite, there is equality if and only if $v$ and $w$ are linearly dependent.*

Proof. We consider first the case of a positive definite bilinear form. We may then assume that $v \neq 0$, since otherwise the inequality takes the form $0 = 0$ (and $0$ and $w$ are linearly dependent). Then observe the decomposition $w = w_1 + w_2$ where

$$w_1 = \frac{b(v, w)}{b(v, v)} v, \qquad w_2 = w - \frac{b(v, w)}{b(v, v)} v.$$

Note that

$$b(w_1, w_2) = \frac{b(v, w)}{b(v, v)} b(v, w) - \frac{b(v, w)}{b(v, v)} b(v, w) = 0.$$

Hence we get, as observed above, the relation

$$b(w, w) = b(w_1, w_1) + b(w_2, w_2) = \frac{|b(v, w)|^2}{b(v, v)^2} b(v, v) + b(w_2, w_2) \geqslant \frac{|b(v, w)|^2}{b(v, v)}.$$

This leads to the Cauchy-Schwarz inequality. Moreover, we have equality if and only if $b(w_2, w_2) = 0$. If $b$ is positive definite, this means that $w_2 = 0$, which by definition of $w_2$ means that $v$ and $w$ are linearly dependent.

In the general case, we use a different argument that is more classical. Consider the function $f\colon \mathbf{R} \to \mathbf{R}$ defined by

$$f(t) = b(v + tw, v + tw).$$

By expanding, we obtain

$$f(t) = b(v,v) + 2tb(v,w) + t^2 b(w,w),$$

so that $f$ is a polynomial of degree at most 2. Since $b$ is positive, we have $f(t) \geqslant 0$ for all $t \in \mathbf{R}$. If $b(w,w) = 0$, so that the polynomial has degree at most 1, this is only possible if furthermore $b(v,w) = 0$, in which case the inequality holds. Otherwise, the polynomial $f$ can not have two distinct real zeros, as it would then take negative values. So the discriminant is $\leqslant 0$, namely:

$$4b(v,w)^2 - 4b(v,v)b(w,w) \leqslant 0.$$

□

Example 5.3.4. (1) For $V = \mathbf{R}^n$ with the standard scalar product, the inequality translates to

$$\Big|\sum_{i=1}^n x_i y_i\Big| \leqslant \Big(\sum_{i=1}^n x_i^2\Big)^{1/2} \Big(\sum_{i=1}^n y_i^2\Big)^{1/2}$$

for all real numbers $x_1, \ldots, x_n$ and $y_1, \ldots, y_n$. Moreover, there is equality if and only if there exist two real numbers $a$ and $b$, not both zero, such that

$$ax_i + by_i = 0$$

for $1 \leqslant i \leqslant n$.

(2) For any continuous real-valued functions $f_1$ and $f_2$ on an interval $[a,b]$, we have

$$\Big|\int_a^b f_1(x)f_2(x)dx\Big|^2 \leqslant \Big(\int_a^b f_1(x)^2 dx\Big) \times \Big(\int_a^b f_2(x)^2 dx\Big).$$

Indeed, the map

$$b(f_1, f_2) = \int_a^b f_1(x) f_2(x) dx$$

is a positive bilinear form on the $\mathbf{R}$-vector space $V$ of real-valued continuous functions from $[a,b]$ to $\mathbf{R}$. Note how simple the proof is, although this might look like a complicated result in analysis.

Lemma 5.3.5. *A symmetric bilinear form $b \in \mathrm{Bil}(V)$ is a scalar product if and only if it is positive and non-degenerate.*

Proof. If $b$ is a scalar product and $v$ is in the left (or right) kernel of $b$, then we get $0 = b(v,v)$ hence $v = 0$, so $b$ is non-degenerate. Conversely, assume that $b$ is positive and non-degenerate. Let $v \in V$ be such that $b(v,v) = 0$. By Proposition 5.3.3, we see that $b(v,w) = 0$ for any $w \in V$, so that $v = 0$ since $b$ is non-degenerate. □

Definition 5.3.6 (Euclidean space). A **euclidean space** is the data of an $\mathbf{R}$-vector space $V$ and a scalar product $b$ on $V$. One often denotes

$$\langle v|w\rangle = b(v,w).$$

For $v \in V$, one denotes $\|v\| = \sqrt{\langle v|v\rangle}$. The function $v \mapsto \|v\|$ is called the **norm** on $V$. For $v$, $w \in V$, the norm $\|v - w\|$ is called the **distance** between $v$ and $w$, and is sometimes denoted $d(v,w)$.

Note that for any symmetric bilinear form $b$, we have

$$b(v+w, v+w) = b(v,v) + b(w,w) + b(v,w) + b(w,v) = b(v,v) + b(w,w) + 2b(v,w),$$

and in particular for a scalar product we deduce that

$$\langle v|w\rangle = \frac{1}{2}(\|v+w\|^2 - \|v\|^2 - \|w\|^2). \tag{5.2}$$

This means that the norm *determines* the scalar product.

LEMMA 5.3.7. *Let $V$ be a euclidean space. If $W \subset V$ is a vector subspace, then the restriction of the scalar product to $W \times W$ makes $W$ a euclidean space.*

PROOF. It is immediate that the restriction of a bilinear form on $V$ to $W \times W$ is a bilinear form on $W$. For a scalar product, the restriction is a positive bilinear form since $b(w, w) \geqslant 0$ for all $w \in W$, and it satisfies $b(w, w) = 0$ if and only if $w = 0$, so it is a scalar product. ☐

REMARK 5.3.8. It is not true, in general, that the restriction of a *non-degenerate* bilinear form to a subspace is non-degenerate. For instance, if $V = \mathbf{R}^{2n}$ and $b$ is the non-degenerate alternating bilinear form of Example 5.2.2 (5), so that

$$b((t_i)_{1\leqslant i\leqslant 2n}, (s_i)_{1\leqslant i\leqslant 2n}) = t_1s_2 - t_2s_1 + \cdots + t_{2n-1}s_{2n} - t_{2n}s_{2n-1},$$

and if $W$ denotes the subspace

$$W = \{(t_1, 0, t_2, 0, \ldots, t_n, 0) \in \mathbf{R}^{2n}\},$$

then we get $b(v, w) = 0$ for *all* $v$ and $w$ in $W$. Hence the restriction of $b$ to $W \times W$ is the zero bilinear form, and it isn't non-degenerate.

In terms of the scalar product and the norm, the Cauchy-Schwarz inequality translates to

$$|\langle v|w\rangle| \leqslant \|v\|\|w\|$$

for $v$ and $w$ in $V$.

LEMMA 5.3.9. *Let $V$ be a euclidean space.*

(1) *The norm satisfies $\|v\| \geqslant 0$, with $\|v\| = 0$ if and only if $v = 0$, it satisfies $\|tv\| = |t|\|v\|$ for all $t \in \mathbf{R}$ and $v \in V$, and the triangle inequality*

$$\|v + w\| \leqslant \|v\| + \|w\|.$$

(2) *The distance satisfies $d(v, w) \geqslant 0$, with equality if and only if $v = w$, it satisfies $d(v, w) = d(w, v)$ and the triangle inequality*

$$d(v, w) \leqslant d(v, u) + d(u, w)$$

*for any $u$, $v$, $w$ in $V$.*

PROOF. (1) Only the triangle inequality is not a direct consequence of the definition of scalar products. For that, we have

$$\|v + w\|^2 = b(v + w, v + w) = b(v, v) + b(w, w) + 2b(v, w) = \|v\|^2 + \|w\|^2 + 2\langle v|w\rangle.$$

Using the Cauchy-Schwarz inequality, we derive

$$\|v + w\|^2 \leqslant \|v\|^2 + \|w\|^2 + 2\|v\|\|w\| = (\|v\| + \|w\|)^2,$$

hence the result since the norm is $\geqslant 0$.

(2) is a translation in terms of distance of some of these properties, and left as exercise. ☐

Example 5.3.10. The most important example is $V = \mathbf{R}^n$ with the "standard" euclidean scalar product

$$\langle v|w\rangle = x_1y_1 + \cdots + x_ny_n,$$

for $v = (x_i)$ and $w = (y_i)$, where the norm is the standard euclidean norm

$$\|v\| = \sqrt{x_1^2 + \cdots + x_n^2}.$$

If $n = 2$ or $3$, then the distance $d(v, w)$ is the usual distance of classical geometry between two points in the plane, or in space.

Definition 5.3.11 (Angle). Let $V$ be a euclidean space. The **(unoriented) angle** between two non-zero vectors $v$ and $w$ is the unique real number $t \in [0, \pi]$ such that

$$\cos(t) = \frac{\langle v|w\rangle}{\|v\|\|w\|}.$$

This is well-defined because the Cauchy-Schwarz inequality shows that the quantity on the right is a real number between $-1$ and $1$, and we know that cosine is a bijection between $[0, \pi]$ and $[-1, 1]$.

Note that the angle is $\pi/2$ if and only if $\langle v|w\rangle = 0$, i.e., if and only if $v$ and $w$ are orthogonal.

## 5.4. Orthogonal bases, I

Definition 5.4.1 (Orthogonal, orthonormal sets). Let $V$ be a euclidean space. A subset $S$ of $V$ such that $\langle v|w\rangle = 0$ for all $v \neq w$ in $S$ is said to be an **orthogonal subset** of $V$. If, in addition, $\|v\| = 1$ for all $v \in S$, then $S$ is said to be an **orthonormal subset** of $V$.

An **orthogonal** (resp. **orthonormal**) basis of $V$ is an orthogonal subset (resp. an orthonormal subset) which is a basis of $V$.

If $V$ is finite-dimensional of dimension $d$, then an ordered orthogonal (resp. orthonormal) basis is a $d$-tuple $(v_1, \ldots, v_d)$ such that $\{v_1, \ldots, v_d\}$ is an orthogonal (resp. orthonormal) basis.

Example 5.4.2. Let $V$ be the space of real-valued continuous functions on $[0, 2\pi]$ with the scalar product

$$\langle f_1|f_2\rangle = \frac{1}{2\pi}\int_0^{2\pi} f_1(x)f_2(x)dx.$$

Then the set $\{c_0, c_n, s_n \mid n \geqslant 1\}$, where $c_0(x) = 1$ and

$$c_n(x) = \sqrt{2}\cos(nx), \qquad s_n(x) = \sqrt{2}\sin(nx)$$

for $n \geqslant 1$, is an orthonormal subset.

Proposition 5.4.3. *Let $V$ be a real vector space. If $S$ is an orthogonal subset in $V$ such that $0 \notin S$, then $S$ is linearly independent. Moreover, if $w \in \langle S \rangle$, then the decomposition of $w$ as a linear combination of vectors in $S$ is*

$$w = \sum_{v \in S} \frac{\langle w|v \rangle}{\|v\|^2} v.$$

*In particular, if $(v_1, \ldots, v_d)$ is an ordered orthonormal basis of $V$, then we have the decomposition*

$$w = \sum_{i=1}^{d} \langle w|v_i \rangle v_i$$

*for all $w \in V$. Further, we then have*

$$\|w\|^2 = \sum_{i=1}^{d} |\langle w|v_i \rangle|^2, \qquad \langle v|w \rangle = \sum_{i=1}^{d} \langle v|v_i \rangle \langle w|v_i \rangle$$

*for all $v$ and $w$ in $V$.*

This proposition means that if $\dim(V) = d$, then a tuple $(v_1, \ldots, v_d)$ is an ordered orthogonal basis if and only if

$$v_i \neq 0 \text{ for all } i, \qquad \langle v_i|v_j \rangle = 0 \text{ for } i \neq j,$$

and it is an ordered orthonormal basis if and only if we have

$$\langle v_i|v_i \rangle = 1, \text{ for all } i, \qquad \langle v_i|v_j \rangle = 0 \text{ for } i \neq j,$$

since the proposition shows that these vectors are then linearly independent.

It is often convenient to group the two cases together using the *Kronecker symbol* $\delta_{x,y}$ or $\delta(x, y) \in \mathbf{R}$, defined to be either 1 if $x = y$ and 0 otherwise. Then an ordered orthonormal basis is a tuple $(v_1, \ldots, v_d)$ such that

$$\langle v_i|v_j \rangle = \delta(i, j)$$

for all $i$ and $j$.

Proof. Let $(t_v)_{v \in S}$ be real numbers, all but finitely many of which are zero, such that

$$\sum_{v \in S} t_v v = 0.$$

Fix $v_0 \in S$. Computing the scalar product with $v_0$, we get

$$0 = \langle \sum_{v \in S} t_v v | v_0 \rangle = \sum_{v \in S} t_v \langle v|v_0 \rangle$$

which by orthogonality means that $0 = t_{v_0} \langle v_0|v_0 \rangle$. Since $v_0 \neq 0$, we deduce that $t_{v_0} = 0$. This holds for all $v_0 \in S$, which means that $S$ is linearly independent.

Now let

$$w = \sum_{v \in S} t_v v$$

be an element of $\langle S \rangle$. Taking the scalar product with $v \in S$, we get similarly

$$\langle w|v \rangle = t_v \langle v|v \rangle.$$

Finally, we compute the scalar product for any $v$ and $w$ in $V$:

$$\langle v|w \rangle = \sum_i \sum_j \langle v|v_i \rangle \, \langle w|v_j \rangle \, \langle v_i|v_j \rangle = \sum_i \langle v|v_i \rangle \langle w|v_i \rangle$$

since $\langle v_i | v_j \rangle$ is zero unless $i = j$. The case of $\|w\|^2$ follows by taking $v = w$. $\square$

THEOREM 5.4.4 (Gram-Schmidt orthonormalization). *Let $V$ be a finite-dimensional euclidean space. Let $B = (v_1, \ldots, v_n)$ be an ordered basis of $V$. There exists a unique ordered* orthonormal *basis $(w_1, \ldots, w_n)$ of $V$ such that for $1 \leqslant i \leqslant n$, we have*

$$w_i \in \langle v_1, \ldots, v_i \rangle,$$

*and such that the coefficient of $v_i$ in the linear combination representing $w_i$ is $> 0$. In particular, this shows that orthonormal bases of $V$ exist.*

PROOF. We use induction on $n$. For $n = 1$, the vector $w_1$ is of the form $cv_1$, and $c$ must satisfy

$$1 = \|w_1\|^2 = \langle cv_1 | cv_1 \rangle = c_1^2 \|v_1\|^2,$$

so that $c_1^2 = \|v_1\|^{-2}$; since the last requirement is that $c_1 > 0$, the unique choice is $c_1 = \|v_1\|^{-1}$.

Now assume that $n \geqslant 2$ and that the result is known for spaces of dimension $n - 1$. Applying it to $\langle v_1, \ldots, v_{n-1} \rangle$, we deduce that there exist unique orthonormal vectors $(w_1, \ldots, w_{n-1})$ such that $w_i$ is a linear combination of $(v_1, \ldots, v_i)$ for $1 \leqslant i \leqslant n - 1$ and such that the coefficient of $v_i$ in $w_i$ is $> 0$.

We search for $w$ as a linear combination

$$w = t_1 w_1 + \cdots + t_{n-1} w_{n-1} + t_n v_n$$

for some $t_i \in \mathbf{R}$, with $t_n > 0$. The conditions to be satisfied are that $\langle w | w_i \rangle = 0$ for $1 \leqslant i \leqslant n - 1$ and that $\langle w | w \rangle = 1$. The first $n - 1$ equalities translate to

$$0 = \langle w | w_i \rangle = t_i + t_n \langle v_n | w_i \rangle,$$

which holds provided $t_i = -t_n \langle v_n | w_i \rangle$ for $1 \leqslant i \leqslant n - 1$. We assume this condition, so that

$$w = t_n \Big( v_n - \sum_{i=1}^{n-1} \langle v_n | w_i \rangle w_i \Big).$$

Then $t_n$ is the only remaining parameter and can only take the positive value such that

$$\frac{1}{t_n} = \Big\| v_n - \sum_{i=1}^{n-1} \langle v_n | w_i \rangle w_i \Big\|.$$

This concludes the proof, provided the vector

$$x = v_n - \sum_{i=1}^{n-1} \langle v_n | w_i \rangle w_i$$

is non-zero. But by construction, this is a linear combination of $v_1, \ldots, v_n$ where the coefficient of $v_n$ is 1, hence non-zero. Since the vectors $v_i$ for $1 \leqslant i \leqslant n$ are linearly independent, it follows that $x \neq 0$. $\square$

REMARK 5.4.5. In practice, one may proceed as follows to find the vectors $(w_1, \ldots, w_n)$: one computes

$$w_1 = \frac{v_1}{\|v_1\|}$$

$$w_2' = v_2 - \langle v_2 | w_1 \rangle w_1, \qquad w_2 = \frac{w_2'}{\|w_2'\|}$$

and so on

$$w'_n = v_n - \langle v_n | w_1 \rangle w_1 - \cdots - \langle v_n | w_{n-1} \rangle w_{n-1}, \qquad w_n = \frac{w'_n}{\|w'_n\|}.$$

Indeed, these vectors satisfy the required conditions: first, the vectors are of norm 1, then the coefficient of $v_n$ in $w_n$ is $1/\|w'_n\| > 0$ (once one knows it is defined!) and finally, we have orthogonality because, for instance for $i < n$, we get

$$\langle w_n | w_i \rangle = \langle v_n | w_i \rangle - \langle v_n | w_i \rangle \langle w_i | w_i \rangle = 0.$$

Note that what these formulas do not show (which explains why we had to prove the theorem!) is that the vectors $w'_i$ are non-zero, which is needed to normalize them, and that they are the unique vectors with the desired property.

COROLLARY 5.4.6. *Let $V$ be a finite-dimensional euclidean space. Let $W \subset V$ be a subspace of $V$, and let $B$ be an orthonormal ordered basis of $W$. Then there is an orthonormal ordered basis of $V$ containing $B$.*

PROOF. Write $B = (w_1, \ldots, w_m)$. Let $B'$ be such that $(B_0, B')$ is an ordered basis of $V$, and let $\tilde{B} = (v_1, \ldots, v_n)$ be the ordered orthonormal basis given by Theorem 5.4.4. Because of the uniqueness property, we have in fact $v_i = w_i$ for $1 \leqslant i \leqslant m$: indeed, if we consider $(w_1, \ldots, w_m, v_{m+1}, \ldots, v_n)$, the vectors also satisfy the conditions of Theorem 5.4.4 for the basis $B_0$. ☐

EXAMPLE 5.4.7. Let $n \geqslant 1$ be an integer and consider the space $V_n$ of real polynomials of degree at most $n$ with the scalar product

$$\langle P_1 | P_2 \rangle = \int_{-1}^{1} P_1(x) P_2(x) dx$$

(it is indeed easy to see that this is a scalar product).

For the basis vectors $e_i = X^i$ for $0 \leqslant i \leqslant n$, we have

$$\langle e_i | e_j \rangle = \int_{-1}^{1} x^{i+j} dx = \frac{1 - (-1)^{i+j+1}}{i + j + 1}.$$

If we apply the Gram-Schmidt process, we deduce that there exist unique polynomials $P_0, \ldots, P_n$, such that $(P_0, \ldots, P_n)$ is an ordered orthonormal basis of $V_n$ and such that

$$P_i = \sum_{j=0}^{i} c_j e_j$$

with $c_j \in \mathbf{R}$ and $c_i > 0$, or in other words, such that $P_i$ is a polynomial of degree exactly $i$ with the coefficient of $x^i$ strictly positive.

*A priori*, the polynomials $P_i$ should depend on $n$. But if we consider $V_n$ as a subspace of $V_{n+1}$, the uniqueness property shows that this is not the case: indeed, writing temporarily $P_{n+1,i}$ for the polynomials arising from $V_{n+1}$, we see that $(P_{n+1,0}, \ldots, P_{n+1,n})$ satisfy the properties required of $(P_{n,0}, \ldots, P_{n,n})$, hence must be equal.

There is therefore an infinite sequence $(P_n)_{n \geqslant 0}$ of polynomials such that (1) for any $n$ and $m$, we have

$$\int_{-1}^{1} P_n(x) P_m(x) dx = \delta(n, m),$$

and (2) the polynomial $P_n$ is of degree $n$ with leading term $> 0$. These (or multiples of them, depending on normalization) are called *Legendre polynomials*.

We can easily compute the polynomials for small values of $n$ using Remark 5.4.5, but the normalization factors tend to make these complicated to write down. It is therefore usual in practice to relax the orthonormality condition.

COROLLARY 5.4.8 (Cholesky decomposition). *Let $n \geqslant 1$ and let $A \in M_{n,n}(\mathbf{R})$ be a symmetric matrix such that the bilinear form $b(x,y) = {}^t x A y$ is a scalar product on $\mathbf{R}^n$. Then there exists a unique upper-triangular matrix $R \in M_{n,n}(\mathbf{R})$ with diagonal coefficients $> 0$ such that $A = {}^t R R$.*

*Conversely, for any invertible matrix $R \in M_{n.n}(\mathbf{R})$, the bilinear form on $\mathbf{R}^n$ defined by $b(x,y) = {}^t x({}^t R R)y$ is a scalar product.*

PROOF. We consider the euclidean space $V = \mathbf{R}^n$ with the scalar product

$$\langle x|y\rangle = {}^t x A y.$$

We then consider the standard basis $E = (e_1, \ldots, e_n)$ of $\mathbf{R}^n$. Let $B = (v_1, \ldots, v_n)$ be the ordered orthonormal basis obtained from the standard basis by Gram-Schmidt orthonormalization (Theorem 5.4.4). Let $R = \mathrm{M}_{E,B}$ be the change of basis matrix from $E$ to $B$. Because $v_i \in \langle e_1, \ldots, e_i\rangle$, the matrix $R^{-1} = \mathrm{M}_{B,E}$ is upper-triangular, and since the coefficient of $e_i$ in $v_i$ is $> 0$, the diagonal coefficients of $R^{-1}$ are $> 0$. Then by Lemma 2.10.18 (2), the matrix $R$ is also upper-triangular with $> 0$ diagonal entries.

We now check that $A = {}^t R R$. The point is that since $B$ is an orthonormal basis, we have

$$\langle x|y\rangle = \sum_i t_i s_i = {}^t t s$$

if we denote by $t = (t_i)$ and $s = (s_j)$ the vectors such that

$$x = \sum_i t_i v_i, \qquad y = \sum_j s_j v_j.$$

We have also $t = Rx$ and $s = Ry$ by definition of the change of basis. It follows therefore that

$${}^t x A y = {}^t (Rx) R y = {}^t x {}^t R R y.$$

Because this is true for *all* $x$ and $y$, it follows that $A = {}^t R R$.

Conversely, let $b(x,y) = {}^t x({}^t R R)y$ for $R \in M_{n,n}(\mathbf{R})$. Since ${}^t({}^t R R) = {}^t R R$, the matrix $A = {}^t R R$ is symmetric, and therefore $b$ is symmetric. Moreover, we can write $b(x,y) = {}^t(Rx)Ry$, and hence $b(x,x) = \langle Rx|Rx\rangle$, where the scalar product is the standard euclidean scalar product on $\mathbf{R}^n$. This implies that $b(x,x) \geqslant 0$ and that $b(x,x) = 0$ if and only if $Rx = 0$. If $R$ is invertible, it follows that $R$ is a scalar product. ☐

## 5.5. Orthogonal complement

DEFINITION 5.5.1 (Orthogonal of a subspace). Let $V$ be a euclidean space. The **orthogonal** $W^\perp$ of a subspace $W$ of $V$ is the set made of vectors in $V$ that are orthogonal to all elements of $W$:

$$W^\perp = \{v \in V \mid \langle v|w\rangle = 0 \text{ for all } w \in W\}.$$

The bilinearity shows that $W^\perp$ is a vector subspace of $V$.

Proposition 5.5.2. *Let $V$ be a euclidean space.*

(1) *We have $\{0\}^{\perp} = V$ and $V^{\perp} = \{0\}$.*

(2) *For any subspaces $W_1$ and $W_2$ of $V$ such that $W_1 \subset W_2$, we have $W_2^{\perp} \subset W_1^{\perp}$; if $V$ is finite-dimensional, then $W_1 \subset W_2$ if and only if $W_2^{\perp} \subset W_1^{\perp}$.*

(3) *If $V$ is finite-dimensional then $(W^{\perp})^{\perp} = W$; in particular, $W_1 = W_2$ if and only if $W_2^{\perp} = W_1^{\perp}$.*

(4) *If $V$ is finite-dimensional then $V = W \oplus W^{\perp}$ for any subspace $W$ of $V$. In particular, we have then $\dim(W^{\perp}) = \dim(V) - \dim(W)$.*

Proof. (1) By definition, all vectors are orthogonal to 0; because the scalar product is non-degenerate, only 0 is orthogonal to all of $V$.

(2) If $W_1 \subset W_2$, all vectors orthogonal to $W_2$ are orthogonal to $W_1$, so $W_2^{\perp} \subset W_1^{\perp}$. The converse follows from (3).

(3) Let $(v_1, \ldots, v_m, v_{m+1}, \ldots, v_n)$ be an orthonormal ordered basis of $V$ such that $(v_1, \ldots, v_m)$ is an orthonormal ordered basis of $W$ (Corollary 5.4.6). By linearity, a vector $v \in W$ belongs to $W^{\perp}$ if and only if $v$ is orthogonal to the basis vectors $v_1, \ldots, v_m$, of $W$. But since $B$ is an orthonormal basis of $V$, we can write

$$v = \sum_{i=1}^{n} \langle v|v_i\rangle v_i$$

and this shows that $v \in W^{\perp}$ if and only if

$$v = \sum_{i=m+1}^{n} \langle v|v_i\rangle v_i.$$

This means that $(v_{m+1}, \ldots, v_n)$ generate $W^{\perp}$; since they are orthonormal vectors, they form an ordered orthonormal basis of $W^{\perp}$.

Similarly, by linearity, a vector $v$ belongs to $(W^{\perp})^{\perp}$ if and only if $\langle v|v_i\rangle = 0$ for $m + 1 \leqslant i \leqslant n$, if and only if

$$v = \sum_{i=1}^{m} \langle v|v_i\rangle v_i,$$

which means if and only if $v \in W$.

(4) We first see that $W$ and $W^{\perp}$ are in direct sum: indeed, an element $v \in W \cap W^{\perp}$ satisfies $\langle v|v\rangle = 0$, so $v = 0$. Then we have $W + W^{\perp} = V$ by the argument in (3): using the notation introduced in that argument, we can write

$$v = \sum_{i=1}^{m} \langle v|v_i\rangle v_i + \sum_{i=m+1}^{n} \langle v|v_i\rangle v_i$$

where the first term belongs to $W$ and the second to $W^{\perp}$. ☐

Because of (3), one also says that $W^{\perp}$ is the *orthogonal complement* of $W$ in $V$.

Definition 5.5.3 (Orthogonal direct sum). Let $V$ be a euclidean space and $I$ an arbitrary set. If $(W_i)_{i \in I}$ are subspaces of $V$, we say that they are in **orthogonal direct sum** if for all $i \neq j$ and $w \in W_i$, $w' \in W_j$, we have $\langle w|w'\rangle = 0$, or equivalently if $W_i \subset W_j^{\perp}$ for all $i \neq j$.

Lemma 5.5.4. *If $(W_i)_{i \in I}$ are subspaces of $V$ in orthogonal direct sum, then they are linearly independent, i.e., they are in direct sum.*

Proof. This is because of Proposition 5.4.3, since any choice of vectors $w_i$ in $W_i$ will form an orthogonal subset of $V$. ☐

Definition 5.5.5 (Orthogonal projection). Let $V$ be a finite-dimensional euclidean space and let $W$ be a subspace of $V$. The projection $p_W$ on $W$ with kernel $W^\perp$ is called the **orthogonal projection** on $W$.

The orthogonal projection $p_W$ on $W$ is therefore characterized as the unique map $p_W$ from $V$ to $V$ such that $p_W(v) \in W$ and $v - p_W(v) \perp w$ for all $w \in W$.

Lemma 5.5.6. *Let $V$ be a finite-dimensional euclidean space and let $W$ be a subspace of $V$. If $(v_1, \ldots, v_m)$ is an orthonormal ordered basis of $W$, then the orthogonal projection on $W$ is given by*

$$p_W(v) = \sum_{i=1}^{m} \langle v|v_i\rangle v_i$$

*for all $v \in V$.*

Proof. Indeed, since $p_W(v)$ belongs to $W$, Proposition 5.4.3, applied to $W$ and the basis $(v_1, \ldots, v_m)$, shows that

$$p_W(v) = \sum_{i=1}^{m} \langle p_W(v)|v_i\rangle v_i.$$

But since $v = p_W(v) + v'$ where $v' \in W^\perp$, we have

$$\langle v|v_i\rangle = \langle p_W(v)|v_i\rangle + \langle v'|v_i\rangle = \langle v|v_i\rangle$$

for $1 \leqslant i \leqslant m$. ☐

## 5.6. Adjoint, I

In this section, we consider only finite-dimensional euclidean spaces.

Let $f\colon V_1 \to V_2$ be a linear map between euclidean spaces. For any $v \in V_2$, we can define a linear map $\lambda_v\colon V_1 \to \mathbf{R}$ by

$$\lambda_v(w) = \langle f(w)|v\rangle,$$

where the scalar product is the one on $V_2$. According to Proposition 5.2.6, there exists a unique vector $f^*(v) \in V_1$ such that

$$\langle f(w)|v\rangle = \lambda_v(w) = \langle w|f^*(v)\rangle.$$

for all $w \in V_1$. Because of the uniqueness, we can see that the map $v \mapsto f^*(v)$ is a linear map from $V_2$ to $V_1$.

Definition 5.6.1 (Adjoint). The linear map $f^*$ is called the **adjoint** of $f$.

If $V$ is a euclidean space, then $f \in \mathrm{End}_{\mathbf{R}}(V)$ is called **normal** if and only if $f^*f = ff^*$, and it is called **self-adjoint** if $f^* = f$.

So the adjoint of $f\colon V_1 \to V_2$ is characterized by the equation

$$\langle f(w)|v\rangle = \langle w|f^*(v)\rangle \tag{5.3}$$

for all $w \in V_1$ and $v \in V_2$.

Example 5.6.2. Let $A \in M_{m,n}(\mathbf{R})$ and let $f = f_A\colon \mathbf{R}^n \to \mathbf{R}^m$, where $\mathbf{R}^n$ and $\mathbf{R}^m$ are viewed as euclidean spaces with the standard scalar product. Then for $x \in \mathbf{R}^n$ and $y \in \mathbf{R}^m$, we have

$$\langle f(x)|y\rangle = {}^t(f(x))y = {}^t(Ax)y = {}^tx{}^tAy = \langle x|{}^tAy\rangle.$$

This means that $f^*(y) = {}^tAy$, or in other words, that the adjoint of $f_A$ is $f_{{}^tA}$.

LEMMA 5.6.3. (1) *The map* $f \mapsto f^*$ *is an isomorphism*

$$\mathrm{Hom}_{\mathbf{R}}(V_1, V_2) \to \mathrm{Hom}_{\mathbf{R}}(V_2, V_1),$$

*with inverse also given by the adjoint, i.e., for any* $f \in \mathrm{Hom}_{\mathbf{R}}(V_1, V_2)$*, we have* $(f^*)^* = f$*.*

(2) *The adjoint of the identity* $\mathrm{Id}_V$ *is* $\mathrm{Id}_V$*.*

(3) *For* $V_1$*,* $V_2$*,* $V_3$ *finite-dimensional euclidean spaces and* $f \in \mathrm{Hom}_{\mathbf{R}}(V_1, V_2)$*,* $g \in \mathrm{Hom}_{\mathbf{R}}(V_2, V_3)$*, we have*

$$(g \circ f)^* = f^* \circ g^*.$$

PROOF. (1) The linearity follows easily from the characterization (5.3) and is left as an exercise. To prove the second part, it is enough to check that $(f^*)^* = f$. Indeed, for $w \in V_2$ and $v \in V_1$, we have

$$\langle f^*(w)|v\rangle = \langle w|f(v)\rangle$$

(by definition of $f^*$ and symmetry). By definition, this means that $f = (f^*)^*$.

(2) It is immediate from the definition that $\mathrm{Id}_V^* = \mathrm{Id}_V$.

(3) The composition $g \circ f$ is a linear map from $V_1$ to $V_3$. For any $v \in V_3$ and $w \in V_1$, we have

$$\langle g(f(w))|v\rangle = \langle f(w)|g^*(v)\rangle = \langle w|f^*(g^*(v))\rangle,$$

which shows that $(g \circ f)^*(v) = f^*(g^*(v))$. ☐

PROPOSITION 5.6.4. *Let* $f\colon V_1 \to V_2$ *be a linear map between finite-dimensional euclidean spaces.*

(1) *We have*

$$\mathrm{Ker}(f^*) = \mathrm{Im}(f)^{\perp}, \qquad \mathrm{Im}(f^*) = \mathrm{Ker}(f)^{\perp},$$

*and in particular* $f^*$ *is surjective if and only if* $f$ *is injective, and* $f^*$ *is injective if and only if* $f$ *is surjective.*

(2) *We have* $\mathrm{rank}(f) = \mathrm{rank}(f^*)$*.*

Note in particular that because of Example 5.6.2, it follows that $\mathrm{rank}({}^tA) = \mathrm{rank}(A)$ for any matrix $A \in M_{m,n}(\mathbf{R})$. We will see in Chapter 8 that this is in fact true over any field.

PROOF. (1) To say that an element $v \in V_2$ belongs to $\mathrm{Ker}(f^*)$ is to say that $f^*(v)$ is orthogonal to all $w \in V_1$. So $v \in \mathrm{Ker}(f^*)$ if and only if

$$\langle w|f^*(v)\rangle = \langle f(w)|v\rangle = 0$$

for all $w \in V_1$. This is equivalent to saying that $v$ is orthogonal (in $V_2$) to all vectors $f(w)$, i.e., that $v \in \mathrm{Im}(f)^{\perp}$.

If we then apply this property to $f^*\colon V_2 \to V_1$, we obtain $\mathrm{Ker}((f^*)^*) = \mathrm{Im}(f^*)^{\perp}$, or in other words that $\mathrm{Ker}(f) = \mathrm{Im}(f^*)^{\perp}$. Computing the orthogonal and using Proposition 5.5.2 (3), we get $\mathrm{Ker}(f)^{\perp} = \mathrm{Im}(f^*)$.

From this we see that $f^*$ is injective if and only if $\mathrm{Im}(f)^{\perp} = 0$, which means (Proposition 5.5.2) if and only if $\mathrm{Im}(f) = V_2$, i.e., if $f$ is surjective. Similarly, $f^*$ is surjective if and only if $f$ is injective.

(2) We compute, using (1) and Proposition 5.5.2 (4), that

$$\begin{aligned}\mathrm{rank}(f^*) &= \dim(V_1) - \dim\mathrm{Ker}(f^*)\\ &= \dim(V_1) - \dim(\mathrm{Im}(f)^{\perp}) = \dim\mathrm{Im}(f) = \mathrm{rank}(f).\end{aligned}$$

☐

PROPOSITION 5.6.5. *Let $V_1$ and $V_2$ be finite-dimensional euclidean spaces of dimension $n$ and $m$ respectively. Let $f\colon V_1 \to V_2$ be a linear map. Let $B_1 = (v_1, \ldots, v_n)$ be an ordered orthonormal basis of $V_1$ and $B_2 = (w_1, \ldots, w_m)$ an ordered orthonormal basis of $V_2$. We then have*

$$\mathrm{Mat}(f; B_1, B_2) = (\langle f(v_j)|w_i\rangle)_{\substack{1\leqslant i\leqslant m\\ 1\leqslant j\leqslant n}}.$$

*In particular, we have*

$$\mathrm{Mat}(f^*; B_2, B_1) = {}^t\mathrm{Mat}(f; B_1, B_2)$$

*and if $V_1 = V_2$, the endomorphism $f$ is self-adjoint if and only if* $\mathrm{Mat}(f; B_1, B_1)$ *is symmetric.*

Note that this proposition *only* applies to orthornomal bases!

PROOF. Write $\mathrm{Mat}(f; B_1, B_2) = (a_{ij})_{\substack{1\leqslant i\leqslant m\\ 1\leqslant j\leqslant n}}$. Then for $1 \leqslant j \leqslant n$, we have

$$f(v_j) = \sum_{i=1}^{m} a_{ij} w_i.$$

Since the basis $B_2$ is orthornomal, the coefficients $a_{ij}$ are therefore given by

$$a_{ij} = \langle f(v_j)|w_i\rangle.$$

Similarly, the matrix $\mathrm{Mat}(f^*; B_2, B_1) = (b_{ji})_{\substack{1\leqslant j\leqslant n\\ 1\leqslant i\leqslant m}}$ has coefficients

$$b_{ji} = \langle f^*(w_i)|v_j\rangle = \langle w_i|f(v_j)\rangle = a_{ij}.$$

This means that $\mathrm{Mat}(f^*; B_2, B_1) = {}^tA$. $\square$

COROLLARY 5.6.6. *Let $V$ be a finite-dimensional euclidean space and $f \in \mathrm{End}_{\mathbf{R}}(V)$. We have then* $\det(f) = \det(f^*)$.

PROOF. This follows from the proposition and the fact that $\det({}^tA) = \det(A)$. $\square$

## 5.7. Self-adjoint endomorphisms

PROPOSITION 5.7.1. *Let $V$ be a finite-dimensional euclidean space and $f \in \mathrm{End}_{\mathbf{R}}(V)$. If $f$ is self-adjoint, then the eigenspaces of $f$ are orthogonal to each other. In other words, if $t_1 \neq t_2$ are eigenvalues of $f$, and $v_i \in \mathrm{Eig}_{t_i,f}$, then we have $\langle v_1|v_2\rangle = 0$.*

PROOF. We have

$$t_1\langle v_1|v_2\rangle = \langle f(v_1)|v_2\rangle = \langle v_1|f(v_2)\rangle = t_2\langle v_1|v_2\rangle,$$

so the scalar product $\langle v_1|v_2\rangle$ is zero since $t_1 \neq t_2$. $\square$

THEOREM 5.7.2 (Spectral theorem for self-adjoint endomorphisms). *Let $V$ be a finite-dimensional euclidean space and $f \in \mathrm{End}_{\mathbf{R}}(V)$.*

*If $f$ is self-adjoint, then there exists an* orthonormal *basis $B$ of $V$ such that the elements of $B$ are eigenvectors of $f$. In particular, the endomorphism $f$ is diagonalizable.*

The key steps are the following lemmas.

LEMMA 5.7.3. *Let $V$ be a finite-dimensional euclidean space and $f \in \mathrm{End}_{\mathbf{R}}(V)$. If $f$ is normal, $t \in \mathbf{R}$ is an eigenvalue of $f$ and $W \subset V$ is the $t$-eigenspace of $f$, then $W$ is stable for $f^*$ and $W^\perp$ is stable for $f$.*

Proof. For $v \in W$ we have

$$f(f^*(v)) = f^*(f(v)) = tf^*(v),$$

so that $f^*(v) \in W$.

Now let $w \in W^\perp$. In order to check that $f(w) \in W^\perp$, we compute for $v \in W$ that

$$\langle f(w)|v\rangle = \langle w|f^*(v)\rangle.$$

Since $f^*(v) \in W$ and $w \in W^\perp$, we get $\langle f(w)|v\rangle = 0$ for all $v \in W$, i.e., $f(w) \in W^\perp$. ☐

Lemma 5.7.4. *Let $V$ be a finite-dimensional euclidean space of dimension $n \geqslant 1$ and $f \in \mathrm{End}_{\mathbf{R}}(V)$. If $f$ is self-adjoint, then there exists an eigenvalue $t \in \mathbf{R}$ of $f$.*

Proof. Let $B$ be an orthonormal basis of $V$ and $A = \mathrm{Mat}(f; B, B)$. We then have ${}^tA = A \in M_{n,n}(\mathbf{R})$. We view $A$ as a matrix with coefficients in $\mathbf{C}$. We claim that all eigenvalues of $A$ are real numbers. Since $A$ has an eigenvalue as complex matrix (Theorem 4.3.14), this will show that there exists $t \in \mathbf{R}$ such that $\det(t1_n - A) = 0$, hence $t$ is an eigenvalue of $A$, hence also of $f$.

By Theorem 4.3.14, there exists $t \in \mathbf{C}$ and $x \neq 0$ in $\mathbf{C}^n$ such that $Ax = tx$. We write $x = x_1 + ix_2$, where $x_i \in \mathbf{R}^n$ and $t = t_1 + it_2$ where $t_i \in \mathbf{R}$. Expanding the equation $Ax = tx$, we obtain the two relations

$$\begin{cases} Ax_1 = t_1x_1 - t_2x_2 \\ Ax_2 = t_2x_1 + t_1x_2. \end{cases}$$

Since $A$ is symmetric, we have the relation $\langle Ax_1|x_2\rangle = \langle x_1|Ax_2\rangle$ (for the standard scalar product). Hence

$$t_1\langle x_1|x_2\rangle - t_2\|x_2\|^2 = t_2\|x_1\|^2 + t_1\langle x_2|x_1\rangle,$$

hence

$$t_2(\|x_1\|^2 + \|x_2\|^2) = 0.$$

Since $x \neq 0$, one of the vectors $x_1$ or $x_2$ is non-zero, so this relation means that $t_2 = 0$, or in other words that $t = t_1$ is real. ☐

Proof of Theorem 5.7.2. We use induction on $n = \dim(V) \geqslant 1$. If $n = 1$, all linear maps are diagonal. Suppose now that $n \geqslant 2$ and that the result holds for self-adjoint linear maps of euclidean vector spaces of dimension $\leqslant n-1$. Let $V$ be a euclidean space of dimension $n$ and $f \in \mathrm{End}_{\mathbf{R}}(V)$ a self-adjoint endomorphism.

By the previous lemma, there exists an eigenvalue $t \in \mathbf{R}$ of $f$. Let $W \subset V$ be the $t$-eigenspace of $f$. We then have

$$V = W \oplus W^\perp$$

(Proposition 5.5.2 (4)) and $W^\perp$ is stable for $f^* = f$ (Lemma 5.7.3). Let $g\colon W^\perp \to W^\perp$ be the endomorphism induced by $f$ on $W^\perp$. This is still a self-adjoint endomorphism of the euclidean space $W^\perp$, because the scalar products of vectors in $W^\perp$ is the same as the scalar product computed in $V$. By induction, there is an orthonormal basis $B_1$ of eigenvectors of $g$ on $W^\perp$. Then if $B_0$ is an orthonormal basis of $W$, the basis $(B_0, B_1)$ is an orthonormal basis of $V$, and its elements are eigenvectors of $f$. ☐

Corollary 5.7.5 (Principal Axes Theorem). *Let $A \in M_{n,n}(\mathbf{R})$ be a symmetric matrix with real coefficients. Then $A$ is diagonalizable, and there is a basis of eigenvectors which is an orthonormal basis of $\mathbf{R}^n$ for the standard euclidean scalar product.*

Proof. This is Theorem 5.7.2 for the self-adjoint endomorphism $f = f_A$ of $\mathbf{R}^n$ with the standard scalar product. ☐

Remark 5.7.6. One can compute an orthonormal basis where a symmetric matrix is diagonal by first diagonalizing the matrix using the determination of eigenspaces and eigenvalues (knowing that the matrix will be diagonalizable with real eigenvalues may help detecting mistakes); in any basis of eigenvectors, the vectors corresponding to distinct eigenvalues are already orthogonal, and one need only perform the Schmidt orthonormalisation for each eigenspace separately. For instance, if the eigenspace is one-dimensional (which often happens), then one need only replace an eigenvector $v$ by $v/\|v\|$.

## 5.8. Orthogonal endomorphisms

Definition 5.8.1 (Orthogonal transformation). Let $V_1$ and $V_2$ be euclidean spaces. A linear map $f\colon V_1 \to V_2$ is an **orthogonal transformation** if $f$ is an isomorphism and

$$\langle f(v)|f(w)\rangle = \langle v|w\rangle$$

for all $v$ and $w \in V$.

If $V$ is a euclidean space, then the set of all orthogonal transformations from $V$ to $V$ is denoted $\mathrm{O}(V)$ and called the **orthogonal group of** $V$. Note that *it depends on the scalar product!*

For $n \geqslant 1$, we denote $\mathrm{O}_n(\mathbf{R})$ the set of all matrices $A \in M_{n,n}(\mathbf{R})$ such that $f_A$ is an orthogonal transformation of $\mathbf{R}^n$ with respect to the standard scalar product; these are called **orthogonal matrices**.

Lemma 5.8.2. *Let $V$ be a finite-dimensional euclidean space.*

(1) *An endomorphism $f$ of $V$ is an orthogonal transformation if and only if it is invertible and $f^{-1} = f^*$, if and only if $f^*f = \mathrm{Id}_V$. In particular, if $f \in \mathrm{O}(V)$, then we have* $\det(f) = 1$ *or* $\det(f) = -1$.

(2) *An endomorphism $f$ of $V$ is an orthogonal transformation if and only $\langle f(v)|f(w)\rangle = \langle v|w\rangle$ for all $v$ and $w \in V$.*

(3) *A matrix $A \in M_{n,n}(\mathbf{R})$ is orthogonal if and only if it is invertible and $A^{-1} = {}^tA$, if and only if $A^tA = {}^tAA = 1_n$. We then have* $\det(A) = 1$ *or* $\det(A) = -1$.

Proof. (1) If $f$ is invertible, then it is an orthogonal transformation if and only if

$$\langle v|f^*f(w)\rangle = \langle v|w\rangle$$

for all $v$, $w \in V$. This condition is equivalent to $f^*f = \mathrm{Id}_V$. This is also equivalent with $f$ invertible with inverse $f^*$ (since $V$ is finite-dimensional).

Since $\det(f^{-1}) = \det(f)^{-1}$ and $\det(f^*) = \det(f)$, it follows that if $f \in \mathrm{O}(V)$, we have $\det(f)^{-1} = \det(f)$, hence $\det(f)^2 = 1$, which implies that $\det(f)$ is either 1 or $-1$.

(2) It suffices to show that the condition $\langle f(v)|f(w)\rangle = \langle v|w\rangle$ implies that $f$ is invertible if $V$ is finite-dimensional. It implies in particular that $\|f(v)\|^2 = \|v\|^2$ for all $v \in V$. In particular, $f(v) = 0$ if and only if $v = 0$, so that $f$ is injective, and hence invertible since $V$ is finite-dimensional.

(3) The statement follows from (1) using Proposition 5.6.5. ☐

Proposition 5.8.3. *Let $V$ be a euclidean space.*

(1) *The identity 1 belongs to $\mathrm{O}(V)$; if $f$ and $g$ are elements of $\mathrm{O}(V)$, then the product $fg$ is also one. Moreover, the inverse $f^{-1}$ of $f$ belongs to $\mathrm{O}(V)$.*

(2) *If $f \in \mathrm{O}(V)$, then $d(f(v), f(w)) = d(v, w)$ for all $v$ and $w$ in $V$, and the angle between $f(v)$ and $f(w)$ is equal to the angle between $v$ and $w$.*

Proof. (1) It is elementary that $1 \in \mathrm{O}(V)$; if $f$ and $g$ are orthogonal transformations, then

$$\langle fg(v)|fg(w)\rangle = \langle f(g(v))|f(g(w))\rangle = \langle g(v)|g(w)\rangle = \langle v|w\rangle$$

for all $v$ and $w$ in $V$, so that $fg$ is orthogonal. Let $g = f^{-1}$. We have $g^* = (f^*)^* = f = (f^{-1})^{-1} = g^{-1}$, so that $f^{-1}$ is orthogonal.

(2) is elementary from the definitions. □

Example 5.8.4. Let $V$ be a euclidean space of dimension $n \geqslant 1$. Fix a non-zero vector $v_0 \in V$. We define a linear map $r_{v_0}$ by

$$r_{v_0}(v) = v - 2\frac{\langle v|v_0\rangle}{\langle v_0|v_0\rangle}v_0$$

for all $v \in V$. This is the *orthogonal reflection along* $v_0$. It is indeed an orthogonal transformation: we have

$$\begin{aligned}\langle r_{v_0}(v)|r_{v_0}(w)\rangle &= \langle v - 2\frac{\langle v|v_0\rangle}{\langle v_0|v_0\rangle}v_0|w - 2\frac{\langle w|v_0\rangle}{\langle v_0|v_0\rangle}v_0\rangle\\ &= \langle v|w\rangle - 2\frac{\langle v|v_0\rangle}{\langle v_0|v_0\rangle}\langle v_0|w\rangle - 2\frac{\langle w|v_0\rangle}{\langle v_0|v_0\rangle}\langle v|v_0\rangle + 4\frac{\langle v|v_0\rangle\langle w|v_0\rangle}{\langle v_0|v_0\rangle^2}\langle v_0|v_0\rangle\\ &= \langle v|w\rangle\end{aligned}$$

since the scalar product is symmetric.

Moreover, $r_{v_0}$ is an involution: indeed, observe first that

$$r_{v_0}(v_0) = v_0 - 2v_0 = -v_0,$$

and then

$$r_{v_0}^2(v) = r_{v_0}\Bigl(v - 2\frac{\langle v|v_0\rangle}{\langle v_0|v_0\rangle}v_0\Bigr) = v - 2\frac{\langle v|v_0\rangle}{\langle v_0|v_0\rangle}v_0 + 2\frac{\langle v|v_0\rangle}{\langle v_0|v_0\rangle}v_0 = v$$

for all $v$. It follows from Proposition 4.4.3 that $r_{v_0}$ is diagonalizable, and more precisely that $V$ is the direct sum of the 1-eigenspace of $r_{v_0}$ and of the $(-1)$-eigenspace.

We can easily determine these spaces: first, we have $r_{v_0}(v) = -v$ if and only if

$$v - 2\frac{\langle v|v_0\rangle}{\langle v_0|v_0\rangle}v_0 = -v,$$

which means

$$v = \frac{\langle v|v_0\rangle}{\langle v_0|v_0\rangle}v_0.$$

In other words, $v_0$ generates the $(-1)$-eigenspace of $r_{v_0}$, which is one-dimensional.

Now the 1-eigenspace is the space of vectors $v$ such that

$$v - 2\frac{\langle v|v_0\rangle}{\langle v_0|v_0\rangle}v_0 = v,$$

or in other words the space of vectors orthogonal to $v_0$. This is the orthogonal complement $\langle v_0\rangle^\perp$ of the $(-1)$-eigenspace.

In particular, if $V$ is finite-dimensional, then the 1-eigenspace of $V$ has dimension $\dim(V) - 1$. If $B = (v_0, v_1, \ldots, v_n)$ is an ordered basis of $V$ such that $(v_1, \ldots, v_n)$ is a basis of $\langle v_0\rangle^\perp$, then the matrix representing $r_{v_0}$ with respect to $B$ is

$$\begin{pmatrix} -1 & 0 & 0 & \cdots & 0\\ 0 & 1 & 0 & \cdots & 0\\ 0 & 0 & 1 & \cdots & 0\\ \vdots & & & & \vdots\\ 0 & 0 & \cdots & 0 & 1 \end{pmatrix}.$$

In particular, the determinant of $r_{v_0}$ is $-1$.

LEMMA 5.8.5. *Let $n \geqslant 1$. A matrix $A \in M_{n,n}(\mathbf{R})$ is orthogonal if and only if ${}^tAA = 1_n$, if and only if the column vectors of $A$ form an orthonormal basis of the euclidean space $\mathbf{R}^n$ with the standard scalar product.*

PROOF. We have already seen the first point. If $A$ is orthogonal, the column vectors $C_i$ of $A$ satisfy

$$\langle C_i|C_j\rangle = \langle Ae_i|Ae_j\rangle = \langle e_i|e_j\rangle = \delta(i,j)$$

where $(e_1,\ldots,e_n)$ is the standard basis of $\mathbf{R}^n$. So these vectors form an orthonormal basis of $\mathbf{R}^n$.

Conversely, the condition $\langle C_i|C_j\rangle = \delta(i,j)$ means that $\langle Ae_i|Ae_j\rangle = \langle e_i|e_j\rangle$ for all $i$ and $j$, and using bilinearity we deduce that

$$\langle A\begin{pmatrix} t_1\\ \vdots\\ t_n\end{pmatrix}|A\begin{pmatrix} s_1\\ \vdots\\ s_n\end{pmatrix}\rangle = \sum_i\sum_j t_is_j\langle Ae_i|Ae_j\rangle = \sum_i t_is_i = \langle\begin{pmatrix} t_1\\ \vdots\\ t_n\end{pmatrix}|\begin{pmatrix} s_1\\ \vdots\\ s_n\end{pmatrix}\rangle,$$

and hence that $f_A$ is an orthogonal transformation. ☐

DEFINITION 5.8.6 (Special orthogonal group). Let $V$ be a finite-dimensional euclidean space. The set of all orthogonal endomorphisms $f \in \mathrm{O}(V)$ such that $\det(f) = 1$ is called the **special orthogonal group** of $V$, and denoted $\mathrm{SO}(V)$. If $V = \mathbf{R}^n$ with the standard euclidean product, we denote it $\mathrm{SO}_n(\mathbf{R})$.

EXAMPLE 5.8.7. (1) Let $V = \mathbf{R}^2$ with the standard scalar product. For $t \in \mathbf{R}$, the matrix

$$R_t = \begin{pmatrix} \cos(t) & -\sin(t)\\ \sin(t) & \cos(t)\end{pmatrix}$$

is orthogonal, and has determinant 1. Indeed, the two column vectors are orthogonal and $\cos(t)^2 + \sin(t)^2 = 1$ shows that their norms is 1. Geometrically, the corresponding linear map $\begin{pmatrix} x\\ y\end{pmatrix} \mapsto R_t\begin{pmatrix} x\\ y\end{pmatrix}$ is a rotation by the angle $t$ in the clockwise direction.

Conversely, let $A \in M_{2,2}(\mathbf{R})$ be an orthogonal matrix. Assume first that $\det(A) = 1$. Then we claim that there exists $t \in \mathbf{R}$ such that $A = R_t$. Indeed, if

$$A = \begin{pmatrix} a & b\\ c & d\end{pmatrix}$$

then the conditions for $A \in \mathrm{SO}_2(\mathbf{R})$ are that

$$\begin{cases} a^2 + c^2 = 1\\ b^2 + d^2 = 1\\ ab + cd = 0\\ ad - bc = 1.\end{cases}$$

The first implies that there exists $t \in \mathbf{R}$ such that $a = \cos(t)$, $c = \sin(t)$. Similarly, there exists $s \in \mathbf{R}$ such that $b = \cos(s)$ and $d = \sin(s)$. The last equation becomes

$$1 = \cos(t)\sin(s) - \sin(t)\cos(s) = \sin(s-t).$$

Hence there exists $k \in \mathbf{Z}$ such that $s-t = \pi/2+2k\pi$. Therefore $b = \cos(s) = \cos(t+\pi/2) = -\sin(t)$ and $d = \sin(s) = \sin(t+\pi/2) = \cos(t)$. This means that

$$A = \begin{pmatrix} \cos(t) & -\sin(t) \\ \sin(t) & \cos(t) \end{pmatrix} = R_t.$$

If $\det(A) = -1$, then $\det(BA) = 1$, where

$$B = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \in O_2(\mathbf{R})$$

($f_B$ is the orthogonal reflection along the vector $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$). Hence there exists $t \in \mathbf{R}$ such that

$$A = B^{-1}R_t = BR_t = \begin{pmatrix} -\cos(t) & \sin(t) \\ \sin(t) & \cos(t) \end{pmatrix}.$$

(2) Let $V = \mathbf{R}^n$ and let $\sigma \in \mathrm{S}_n$. The permutation matrix $P_\sigma$ is orthogonal: indeed, its column vectors are just a permutation of the column vectors of the standard orthonormal basis of $\mathbf{R}^n$.

Proposition 5.8.8 (Principal Axes Theorem, 2). *Let $A \in M_{n,n}(\mathbf{R})$ be a symmetric matrix with real coefficients. There exists an orthogonal matrix $X$ such that $XAX^{-1} = XA^tX$ is diagonal.*

Proof. This a translation of Corollary 5.7.5: let $B$ be the standard basis of $\mathbf{R}^n$ and $B'$ an ordered orthonormal basis of $\mathbf{R}^n$ for which $\mathrm{Mat}(f_A; B', B')$ is diagonal. Since $B'$ is orthonormal, the change of basis matrix $X = \mathrm{M}_{B,B'}$ is orthogonal, and $XAX^{-1} = \mathrm{Mat}(f_A; B', B')$ is diagonal (see Proposition 2.9.13). ☐

Proposition 5.8.9 (QR or Iwasawa decomposition). *Let $A \in M_{n,n}(\mathbf{R})$ be any matrix. There exists an orthogonal matrix $Q \in \mathrm{O}_n(\mathbf{R})$ and an upper-triangular matrix $R$ such that $A = QR$.*

Proof. We prove this only in the case where $A$ is invertible. Consider the matrix $T = {}^tAA$. By the Cholesky Decomposition (Corollary 5.4.8), there exists an upper-triangular matrix $R$ with positive diagonal coefficients such that $T = {}^tRR$. This means that ${}^tRR = {}^tAA$. Since $R$ and ${}^tR$ are invertible, with $({}^tR)^{-1} = {}^t(R^{-1})$, we get

$$1_n = {}^t(AR^{-1})AR^{-1}.$$

This means that $Q = AR^{-1}$ is an orthogonal matrix. Consequently, we have $A = QR$. ☐

Corollary 5.8.10. *Let $A = (a_{ij}) \in M_{n,n}(\mathbf{R})$ be a symmetric matrix. Then the bilinear form $b(x,y) = {}^txAy$ is a scalar product if and only if, for $1 \leqslant k \leqslant n$, we have $\det(A_k) > 0$, where $A_k \in M_{k,k}(\mathbf{R})$ is the matrix defined by $A_k = (a_{ij})_{\substack{1\leqslant i\leqslant k \\ 1\leqslant j\leqslant k}}$.*

The matrices $A_k$ are called the "principal minors" of $A$.

Proof. Let $B = (v_1, \ldots, v_n)$ be a basis of $\mathbf{R}^n$ formed of eigenvectors of $A$, with $Av_i = \lambda_i v_i$. Using the standard scalar product, we have

$$b(x,y) = \langle x | Ay \rangle$$

and therefore

$$b(v_i, v_j) = \lambda_i \delta(i, j).$$

It follows that $b$ is a scalar product if (and only if) the eigenvalues $\lambda_i$ are all $> 0$.

We now prove the "if" direction by induction with respect to $n$. For $n = 1$, the result is clear. Assume now that $n \geqslant 2$, and that the result holds for matrices of size $\leqslant n - 1$. Let $A$ be such that $\det(A_k) > 0$ for $1 \leqslant k \leqslant n$. By induction, the bilinear form defined by $A_{n-1}$ on $\mathbf{R}^{n-1}$ is a scalar product. The product of the eigenvectors is equal to the determinant of $A$, which is $\det(A_n) > 0$. Hence, all eigenvalues are non-zero, and if there is one eigenvalue $< 0$, then there is at least another one. Assume for instance that $\lambda_1 \neq \lambda_2$ are two eigenvalues $< 0$. The vectors $v_1$ and $v_2$ are linearly independent, so there exist $a$ and $b$ in $\mathbf{R}$, not both zero, such that $w = av_1 + bv_2 \in \mathbf{R}^n$ is a non-zero vector where the last coordinate is 0. Hence we can write

$$w = \begin{pmatrix} \tilde{w} \\ 0 \end{pmatrix}$$

where $\tilde{w}$ is a non-zero element of $\mathbf{R}^{n-1}$. But then we have

$${}^t\tilde{w}A_{n-1}\tilde{w} = {}^twAw = a^2 b(v_1, v_1) + b^2 b(v_2, v_2) = -a^2 - b^2 < 0,$$

and this contradicts the fact that $A_{n-1}$ defines a scalar product on $\mathbf{R}^{n-1}$. Therefore $A$ has only positive eigenvalues, and $b$ is a scalar product.

Conversely, assume that $b$ is a scalar product on $\mathbf{R}^n$. Then its restriction $b_k$ to the subspace $W_k$ generated by the first $k$ basis vectors of the standard basis is a scalar product. If we identify $W_k$ with $\mathbf{R}^k$, then we get

$$b_k(x, y) = {}^txA_ky$$

for all $x$, $y \in \mathbf{R}^k$. From the remarks at the beginning, we therefore have $\det(A_k) > 0$. ☐

## 5.9. Quadratic forms

The Principal Axes Theorem has another interpretation in terms of quadratic forms.

Definition 5.9.1 (Quadratic form). Let $n \geqslant 1$. A map $Q\colon \mathbf{R}^n \to \mathbf{R}$ is called a **quadratic form** if there exists a symmetric matrix $A \in M_{n,n}(\mathbf{R})$ such that

$$Q(x) = {}^txAx$$

for all $x \in \mathbf{R}^n$.

By "polarization", one sees that the matrix $A = (a_{ij})$ associated to a quadratic form $Q$ is uniquely determined by $Q$: if we denote $b(x, y) = {}^txAy$, then we have

$$Q(x + y) = Q(x) + Q(y) + 2b(x, y),$$

and $b(e_i, e_j) = a_{ij}$ for the standard basis vectors $(e_i)$.

Example 5.9.2. (1) For $A = 1_n$, we get $Q(x) = \|x\|^2$.

(2) Let $A$ be a diagonal matrix with diagonal coefficients $a_1, \ldots, a_n$. Then for $x = (x_i) \in \mathbf{R}^n$, we have

$$Q(x) = a_1 x_1^2 + \cdots + a_n x_n^2.$$

(3) Let

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

for some $a \in \mathbf{R}$. Then we have

$$Q(x_1, x_2, x_3) = 2ax_1x_2 - x_3^2.$$

THEOREM 5.9.3 (Principal Axes Theorem). *Let $n \geqslant 1$ and let $Q$ be a quadratic form on $\mathbf{R}^n$.*

(1) *There exists an orthonormal basis $B = (w_1, \ldots, w_n)$ of $\mathbf{R}^n$, for the standard euclidean scalar product, integers $p \geqslant 0$, $q \geqslant 0$, with $p + q \leqslant n$, and real numbers $\lambda_i > 0$ for $1 \leqslant i \leqslant p + q$ such that*

$$Q(x) = \lambda_1 y_1^2 + \cdots + \lambda_p y_p^2 - \lambda_{p+1} y_{p+1}^2 - \cdots - \lambda_{p+q} y_{p+q}^2$$

*for all $x \in \mathbf{R}^n$, where $(y_i)$ are the coefficients of $x$ with respect to the basis $B$:*

$$x = y_1 w_1 + \cdots + y_n w_n.$$

(2) *There exists an* orthogonal *basis $B' = (v_1, \ldots, v_n)$ of $\mathbf{R}^n$, for the standard euclidean scalar product, integers $p \geqslant 0$, $q \geqslant 0$, with $p + q \leqslant n$, such that*

$$Q(x) = y_1^2 + \cdots + y_p^2 - y_{p+1}^2 - \cdots - y_{p+q}^2$$

*for all $x \in \mathbf{R}^n$, where $(y_i)$ are the coefficients of $x$ with respect to the basis $B'$.*

The lines generated by the vectors $(w_i)$ of a basis given by this theorem are called *principal axes* of the quadratic form. The number $p-q$ is called the *index* of the quadratic form. Especially when $n = p + q$, one often says that $Q$ is of type $(p, q)$.

DEFINITION 5.9.4 (Positive, negative, quadratic forms). A symmetric bilinear form $b$ on $\mathbf{R}^n$, or the quadratic form $Q(x) = b(x, x)$, or the symmetric matrix $A \in M_{n,n}(\mathbf{R})$ such that $b(x, y) = {}^t x A y$ is called

(1) **Positive or positive semi-definite** if $Q(x) \geqslant 0$ for all $x \in \mathbf{R}^n$;
(2) **Positive-definite** if it positive and $Q(x) = 0$ if and only if $x = 0$, or in other words if $b$ is a scalar product;
(3) **Negative or negative semi-definite** if $Q(x) \leqslant 0$ for all $x \in \mathbf{R}^n$;
(4) **Negative-definite** if it negative and $Q(x) = 0$ if and only if $x = 0$, or in other words if $-b$ is a scalar product.

PROOF. Let $A$ be the symmetric matrix such that $Q(x) = {}^t x A x$ for all $x \in \mathbf{R}^n$ and $b$ the associated bilinear form. Since $A$ is symmetric, it is diagonalizable in an orthonormal basis $B = (w_1, \ldots, w_n)$ of $\mathbf{R}^n$ (Corollary 5.7.5), say $Aw_i = t_i w_i$ for $1 \leqslant i \leqslant n$. We define $p$ and $q$, and we order the basis vectors of $B$ so that $t_i > 0$ for $1 \leqslant i \leqslant p$, $t_i < 0$ for $p + 1 \leqslant i \leqslant p + q$, and $t_i = 0$ for $i > p + q$ (it may be that $p$, or $q$ or both are zero). We then put $\lambda_i = t_i$ if $1 \leqslant i \leqslant p$ and $\lambda_i = -t_i$ if $p + 1 \leqslant i \leqslant p + q$. So we get real numbers $\lambda_i > 0$ for $1 \leqslant i \leqslant p + q$.

If

$$x = y_1 w_1 + \cdots + y_n w_n,$$

then we compute

$$Q(x) = b(x, x) = b\Big(\sum_i y_i w_i, \sum_j y_j w_j\Big) = \sum_{i,j} y_i y_j b(w_i, w_j)$$

by bilinearity. But

$$b(w_i, w_j) = {}^t w_i A w_j = t_j \langle w_i | v_j \rangle = 2 t_j \delta(i, j)$$

since $(w_1, \ldots, w_n)$ is orthonormal. Therefore we get

$$Q(x) = \lambda_1 y_1^2 + \cdots + \lambda_p y_p^2 - \lambda_{p+1} y_{p+1}^2 - \cdots - \lambda_{p+q} y_{p+q}^2.$$

We then define $v_i = |\lambda_i|^{-1/2} w_i$ for $1 \leqslant i \leqslant p+q$, and $v_i = w_i$ for $i > p+q$. Then $(v_1, \ldots, v_n)$ is an orthogonal basis of $\mathbf{R}^n$ (but not necessarily orthonormal anymore), and we have

$$Q(x) = y_1^2 + \cdots + y_p^2 - y_{p+1}^2 - \cdots - y_{p+q}^2$$

for all $x \in \mathbf{R}^n$. ☐

In terms of the type $(p, q)$, we see that:

(1) $Q$ is positive if and only if $q = 0$;
(2) $Q$ is positive-definite if and only if $p = n$;
(3) $Q$ is negative if and only if $p = 0$;
(4) $Q$ is negative-definite if and only if $q = n$.

To check the first one, for instance (the others are similar or easier), note first that if $q = 0$, then we get

$$Q(x) = \sum_{i=1}^{p} a_i y_i^2 \geqslant 0$$

for all $x = y_1 v_1 + \cdots + y_n v_n \in \mathbf{R}^n$, so that $q = 0$ implies that $Q$ is positive. Conversely, if $q \geqslant 1$, note that

$$Q(v_{p+1}) = -a_{p+1} < 0$$

so that $Q$ is then *not* positive.

It is often useful to visualize the properties of quadratic forms in terms of the solutions to the equations $Q(x) = a$ for some $a \in \mathbf{R}$.

Definition 5.9.5 (Quadric). Let $n \geqslant 1$. A **(homogeneous) quadric** in $\mathbf{R}^n$ is a subset of the type

$$X_{Q,a} = \{x \in \mathbf{R}^n \mid Q(x) = a\}$$

where $Q$ is a quadratic form and $a \in \mathbf{R}$.

Example 5.9.6. (1) Consider $n = 2$. We see that there are five types of quadratic forms, in terms of the representation with respect to principal axes:

- $p = q = 0$: this is the zero quadratic form; the quadric is either empty (if $a \neq 0$) or equal to $\mathbf{R}^2$ (if $a = 0$);
- $p = 2$, $q = 0$: this is the norm associated to a scalar product; the quadric $Q(x) = a$ is an ellipse in the plane if $a > 0$, a point if $a = 0$ and empty if $a < 0$;
- $p = 0$, $q = 2$: then $-Q$ is the norm associated to a scalar product; the quadric $Q(x) = a$ is empty if $a > 0$, a point if $a = 0$ and an ellipse if $a < 0$;
- $p = q = 1$: in the orthonormal basis of principal axes, we have $Q(x) = y_1^2 - y_2^2$. The quadric is a hyperbola in the plane if $a \neq 0$, and the union of two orthogonal lines if $a = 0$.
- $p = 1$, $q = 0$: in the orthonormal basis of principal axes, we have $Q(x) = y_1^2$. The quadric is a single line if $a \geqslant 0$, and empty if $a < 0$.
- $q = 1$, $p = 0$: in the orthonormal basis of principal axes, we have $Q(x) = -y_2^2$. The quadric is a single line if $a \leqslant 0$, and empty if $a > 0$.

(2) Consider $n = 3$. Then we have the following types of quadratic forms and quadrics (where we simplify the description by using the symmetry between $p$ and $q$ corresponding to replacing $Q$ with $-Q$):

- $p = q = 0$: this is the zero quadratic form; the quadric is either empty (if $a \neq 0$) or equal to $\mathbf{R}^3$ (if $a = 0$);
- $p = 3$, $q = 0$: this is the norm associated to a scalar product; the quadric $Q(x) = a$ is an ellipsoid in $\mathbf{R}^3$ if $a > 0$, a point if $a = 0$ and empty if $a < 0$;

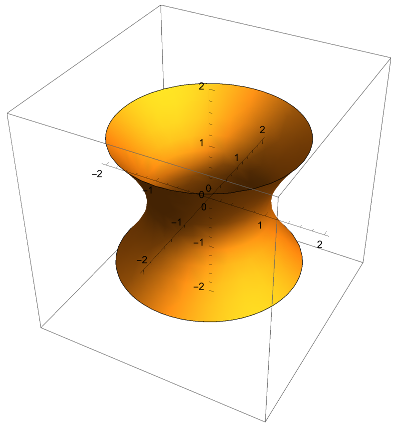

FIGURE 5.1. A hyperboloid with one sheet

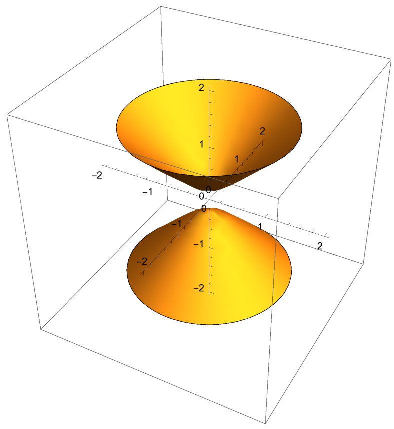

FIGURE 5.2. A hyperboloid with two sheets

- $p = 2$, $q = 1$: in the orthonormal basis of principal axes, we have $Q(x) = y_1^2 + y_2^2 - y_3^2$. The quadric $Q(x) = a$ is a hyperboloid with one sheet if $a > 0$ (the intersection with a plane where $y_3$ is fixed is a circle of radius $\sqrt{a + y_3^2}$), it is a cone with vertex at the origin if $a = 0$ (the intersection with a plane where $y_3$ is fixed is a circle of radius $|y_3|$, or a point if $y_3 = 0$), and it is a hyperboloid with two sheets if $a < 0$ (the intersection with a plane where $y_3$ is fixed is empty if $|y_3| < \sqrt{|a|}$ and is a circle of radius $\sqrt{a + y_3^2}$ if $|y_3| \geqslant \sqrt{|a|}$).
- $p = 2$, $q = 0$: in the orthonormal basis of principal axes, we have $Q(x) = y_1^2 + y_2^2$.
- $p = q = 1$: in the orthonormal basis of principal axes, we have $Q(x) = y_1^2 - y_2^2$.

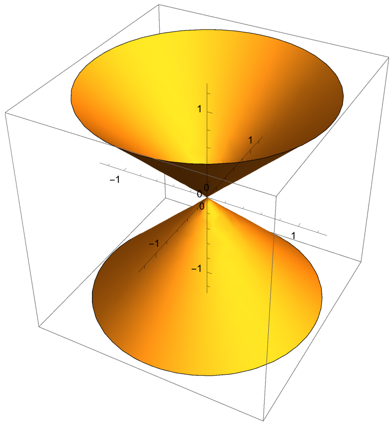


FIGURE 5.3. The cone

### 5.10. Singular values decomposition

THEOREM 5.10.1 (Singular value or Cartan decomposition). *Let $V$ be a finite-dimensional euclidean space and $f \in \mathrm{End}_{\mathbf{R}}(V)$. Let $n = \dim(V)$ and $r = \mathrm{rank}(f)$. There exist orthonormal bases*

$$B_1 = (v_1, \ldots, v_n)$$
$$B_2 = (w_1, \ldots, w_n)$$

*of $V$, possibly different, and $r$ strictly positive real numbers $\sigma_1, \ldots, \sigma_r$ such that for all $v \in V$, we have*

$$f(v) = \sum_{i=1}^{r} \sigma_i \langle v | v_i \rangle w_i.$$

*Equivalently, we have $f(v_i) = \sigma_i w_i$ for $1 \leqslant i \leqslant r$ and $f(v_i) = 0$ for $i > r$, so that the matrix $\mathrm{Mat}(f; B_1, B_2)$ is diagonal with diagonal coefficients*

$$(\sigma_1, \ldots, \sigma_r, 0, \ldots, 0).$$

The numbers $\sigma_1, \ldots, \sigma_r$ are called the *singular values* of $f$. Up to ordering, they are uniquely defined.

PROOF. Consider the endomorphism $g = f^* f$ of $V$. Then $g^* = f^*(f^*)^* = f^* f$, so that $g$ is self-adjoint. Let $B_1 = (v_1, \ldots, v_n)$ be an orthonormal basis of $V$ of eigenvectors of $g$, say $g(v_i) = \lambda_i v_i$ for $1 \leqslant i \leqslant n$. Because

$$\lambda_i \|v_i\|^2 = \langle g(v_i) | v_i \rangle = \langle f^*(f(v_i)) | v_i \rangle = \|f(v_i)\|^2,$$

the eigenvalues are $\geqslant 0$. We can order them so that the first $s$ eigenvalues are $> 0$, and the eigenvalues $\lambda_{s+1}, \ldots, \lambda_n$ are zero. We then see from the equation above that $f(v_i) = 0$ for $i > s$.

Let $v \in V$. We have

$$v = \sum_{i=1}^{n} \langle v | v_i \rangle v_i,$$

since the basis $B_1$ is orthonormal, hence

$$f(v) = \sum_{i=1}^{n} \langle v | v_i \rangle f(v_i).$$

For $1 \leqslant i \leqslant s$ and $1 \leqslant j \leqslant s$, we have

$$\langle f(v_i)|f(v_j)\rangle = \langle g(v_i)|v_j\rangle = \lambda_i\langle v_i|v_j\rangle = \lambda_i\delta(i,j),$$

again because $B_1$ is an orthonormal basis. This means that if we define

$$w_i = \frac{1}{\sqrt{\lambda_i}}f(v_i),$$

for $1 \leqslant i \leqslant s$ (which is possible since $\lambda_i > 0$), then we have

$$\langle w_i|w_j\rangle = \delta(i,j).$$

Now we can write the formula for $f(v)$ in the form

$$f(v) = \sum_{i=1}^{s}\sqrt{\lambda_i}\langle v|v_i\rangle w_i.$$

This gives the desired result with $\sigma_i = \sqrt{\lambda_i}$ (completing the orthonormal set $(w_1,\ldots,w_s)$ to an orthonormal basis $B_2$ of $V$).

Finally, the description shows that $\mathrm{Im}(f) \subset \langle\{w_1,\ldots,w_s\}\rangle$, and since $f(v_i) = \sigma_i w_i$ with $\sigma_i > 0$ for $1 \leqslant i \leqslant s$, we have in fact equality. Since $(w_1,\ldots,w_s)$ are linearly independent (as they are orthonormal), it follows that $s = \dim(\mathrm{Im}(f)) = r$. $\square$

Remark 5.10.2. Although it can be useful to remember the construction of the singular values and of the bases $B_1$ and $B_2$, one should not that it is not difficult to recover the fact that $B_1$ is a basis of eigenvectors of $f^*f$ from the stated result. Indeed, if we consider each linear map

$$\ell_i\colon v \mapsto \langle v|v_i\rangle w_i$$

for $1 \leqslant i \leqslant r$, then we compute easily the adjoint of $\ell_i$: we have

$$\langle \ell_i(v)|w\rangle = \langle v|v_i\rangle\langle w_i|w\rangle = \langle v|\ell_i^*(w)\rangle$$

where $\ell_i^*(w) = \langle w_i|w\rangle v_i$. Since

$$f = \sum_{i=1}^{r}\sigma_i\ell_i,$$

we have

$$f^* = \sum_{i=1}^{r}\sigma_i\ell_i^*.$$

Hence

$$f^*f = \sum_{i=1}^{r}\sum_{j=1}^{r}\sigma_i\sigma_j\ell_i^*\ell_j.$$

But

$$(\ell_i^*\ell_j)(v) = \langle v|v_j\rangle\ell_i^*(w_j) = \langle v|v_j\rangle\langle w_i|w_j\rangle v_i = \delta(i,j)\langle v|v_i\rangle v_i,$$

so that

$$f^*f(v) = \sum_{i=1}^{r}\sigma_i^2\langle v|v_i\rangle v_i.$$

This implies in particular that $f^*f(v_i) = \sigma_i^2 v_i$ for $1 \leqslant i \leqslant r$ and $f^*f(v_i) = 0$ for $i > r$.

Corollary 5.10.3 (Singular values decomposition for matrices). *Let $n \geqslant 1$ and let $A \in M_{n,n}(\mathbf{R})$. There exist orthogonal matrices $X_1$ and $X_2$ and a diagonal matrix $D \in M_{n,n}(\mathbf{R})$ with diagonal entries*

$$(\sigma_1, \ldots, \sigma_r, 0, \ldots, 0)$$

*where $\sigma_i > 0$ for $1 \leqslant i \leqslant r$, such that $A = X_1 D X_2$.*

Proof. This is the theorem applied to $f = f_A$ on $\mathbf{R}^n$ with the standard scalar product: let $B$ be the standard basis of $\mathbf{R}^n$, and denote $X_1 = \mathrm{M}_{B_2,B}$, $X_2 = \mathrm{M}_{B,B_1}$. Then we have

$$A = \mathrm{Mat}(f_A; B, B) = X_1 \,\mathrm{Mat}(f_A; B_1, B_2) X_2 = X_1 D X_2$$

by Proposition 2.9.13, and the matrices $X_1$ and $X_2$ are orthogonal because $B_1$ and $B_2$ are orthonormal bases (Lemma 5.8.5). ☐

Example 5.10.4. Consider $V = \mathbf{R}^2$ and $f = f_A$ where

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

so that

$$f\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x+y \\ y \end{pmatrix}.$$

We then have

$$A^t A = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}$$

which has characteristic polynomial $t^2 - 3t + 1$, with positive roots

$$t_1 = \frac{3+\sqrt{5}}{2} = 2.618033\ldots, \qquad t_2 = \frac{3-\sqrt{5}}{2} = 0.381966\ldots.$$

Therefore

$$\sigma_1 = \sqrt{t_1} = \frac{1+\sqrt{5}}{2}, \qquad \sigma_2 = \sqrt{t_2} = \frac{-1+\sqrt{5}}{2},$$

and the matrix $D$ is

$$\begin{pmatrix} \sigma_1 & 0 \\ 0 & \sigma_2 \end{pmatrix}.$$

To find eigenvectors of $A^t A$ with eigenvalues $t_1$ and $t_2$, we write the linear systems

$$\begin{cases} x + y = t_1 x \\ 2x + y = t_1 y \end{cases}, \qquad \begin{cases} x + y = t_2 x \\ 2x + y = t_2 y \end{cases}.$$

We know that there exist non-zero solutions, so any non-zero solution of the first equation (for instance) must also be a solution of the second (otherwise, the solution set would be reduced to 0). So the vectors

$$\tilde{v}_1 = \begin{pmatrix} 1 \\ t_1 - 1 \end{pmatrix} = \begin{pmatrix} 1 \\ (1+\sqrt{5})/2 \end{pmatrix}, \qquad \tilde{v}_2 = \begin{pmatrix} 1 \\ t_2 - 1 \end{pmatrix} = \begin{pmatrix} 1 \\ (1-\sqrt{5})/2 \end{pmatrix}$$

are eigenvectors for $t_1$ and $t_2$ respectively. We have $\|\tilde{v}_1\|^2 = (5+\sqrt{5})/2$, $\|\tilde{v}_2\|^2 = (5-\sqrt{5})/2$ and $\langle \tilde{v}_1 | \tilde{v}_2 \rangle = 0$ so an orthonormal basis of eigenvectors is

$$(v_1, v_2) = \Big( \frac{\tilde{v}_1}{\|\tilde{v}_1\|}, \frac{\tilde{v}_2}{\|\tilde{v}_2\|} \Big).$$

The singular decomposition formula for $f$ is therefore

$$f(v) = \langle v | v_1 \rangle f(v_1) + \langle v | v_2 \rangle f(v_2).$$

CHAPTER 6

# Unitary spaces

## 6.1. Hermitian forms

The next few sections will be very close to the discussion of euclidean vector spaces. They concern the analogue, for the field of complex numbers, of the notions related to euclidean spaces and scalar product. The key feature of $\mathbf{C}$ is that, for any $z \in \mathbf{C}$, the complex number $|z|^2 = z\bar{z}$ is a non-negative real number.

Definition 6.1.1 (Sesquilinear form). Let $V$ be a $\mathbf{C}$-vector space. A **sesquilinear form** $b$ on $V$ is a map $V \times V \to \mathbf{C}$ such that

$$\begin{cases} b(v, w_1 + w_1) & = b(v, w_1) + b(v, w_2) \\ b(v_1 + v_2, w) & = b(v_1, w) + b(v_2, w) \\ b(v, tw) & = tb(v, w) \\ b(tv, w) & = \bar{t}b(v, w) \end{cases}$$

for all $v$, $v_1$, $v_2$, $w$, $w_1$, $w_2$ in $V$ and $t \in \mathbf{C}$.

A sesquilinear form $b$ on $V$ is called **hermitian** if and only if we have

$$b(v, w) = \overline{b(w, v)}$$

for all $v$ and $w$ in $V$.

The difference with a bilinear form is that, with respect to the first argument, a sesquilinear form is not linear, but "conjugate-linear", while it is linear with respect to the second argument. On the other hand, hermitian forms are the analogues of symmetric forms – note that if $b$ is a sesquilinear form, then $(v, w) \mapsto b(w, v)$ is *not* sesquilinear, since it is linear with respect to the first argument, and not the second. But $(v, w) \mapsto \overline{b(w, v)}$ is a sesquilinear form.

It should be noted that it is a *convention* that the first argument is conjugate-linear, and the second linear; different authors might use the opposite convention, and one must be careful to check which definition is used before translating formulas.

Sometimes, it is simpler to work with bilinear forms, and there is a trick for this.

Definition 6.1.2 (Conjugate space). Let $V$ be a $\mathbf{C}$-vector space. The **conjugate space** $\bar{V}$ is the $\mathbf{C}$-vector space with the same underlying set as $V$, and with

$$0_{\bar{V}} = 0_V$$

$$v_1 +_{\bar{V}} v_2 = v_1 + v_2$$

$$t \cdot_{\bar{V}} v = \bar{t}v$$

for $v$, $v_1$, $v_2$ in $V$ and $t \in \mathbf{C}$.

It is elementary to check that this is a vector space. For instance, for $t \in \mathbf{C}$ and $v_1$, $v_2 \in \bar{V} = V$, we have

$$t \cdot_{\bar{V}} (v_1 + v_2) = \bar{t}(v_1 + v_2) = \bar{t}v_1 + \bar{t}v_2 = t \cdot_{\bar{V}} v_1 + t \cdot_{\bar{V}} v_2.$$

The point of the definition is the following lemma.

LEMMA 6.1.3. *Let $V$ and $W$ be $\mathbf{C}$-vector spaces. A map $f\colon V \to W$ is a linear map from $V$ to $\bar{W}$ if and only if we have*

$$f(v_1 + v_2) = f(v_1) + f(v_2) \text{ for } v_1,\ v_2 \in V$$
$$f(tv) = \bar{t} f(v) \text{ for } t \in \mathbf{C},\ v \in V.$$

We will see a number of maps having both of the properties; these are not linear from $V$ to $W$, but we can interpret them as linear from $V$ to $\bar{W}$; in particular, we can speak of their kernel, range, of the dimensions of these, and (for instance) say that $f$ is injective if and only if the kernel is $\{0\}$.

PROOF. By definition of $\bar{W}$, the second condition is equivalent to $f(tv) = t \cdot_{\bar{W}} f(v)$. Using the additivity of the first condition, this means that $f$ is linear from $V$ to $\bar{W}$. ☐

LEMMA 6.1.4. *Let $V$ be a $\mathbf{C}$-vector space. For any subset $S$ of $V$, the subspace generated by $S$ in $V$ and $\bar{V}$ is the same subset of $V$, and $S$ is linearly independent in $V$ if and only if it is linearly independent in $\bar{V}$. In particular $V$ and $\bar{V}$ have the same dimension.*

PROOF. To say that $w$ is a linear combination of $v_1, \ldots, v_n$ in $V$ means that there exist $t_1, \ldots, t_n$ in $\mathbf{C}$ with

$$w = t_1 v_1 + \cdots + t_n v_n,$$

or equivalently that

$$w = \bar{t}_1 \cdot_{\bar{V}} v_1 +_{\bar{V}} \cdots +_{\bar{V}} \bar{t}_n \cdot_{\bar{V}} v_n.$$

So the linear combinations of elements of $S$ are the same in $V$ as in $\bar{V}$, and a linear combination equal to 0 in $V$ corresponds to a linear combination equal to 0 in $\bar{V}$. The result follows. ☐

EXAMPLE 6.1.5. (1) For any linear forms $\lambda_1$ and $\lambda_2$ on the $\mathbf{C}$-vector space $V$, the product

$$b(v_1, v_2) = \overline{\lambda_1(v_1)} \lambda_2(v_2)$$

is sesquilinear. It is hermitian if $\lambda_1 = \lambda_2$.

(2) The set $\mathrm{Ses}(V)$ of all sesquilinear forms on $V$ is a subset of the space of all functions $V \times V \to \mathbf{C}$. It is a vector subspace. The set of all hermitian forms is *not* a subspace of $\mathrm{Ses}(V)$, only a real-vector subspace: if $b$ is hermitian, then $ib$ satisfies

$$\overline{(ib)(v, w)} = -i\overline{b(v, w)} = -(ib)(w, v)$$

so that it is not hermitian (unless $b = 0$).

(3) Let $V$ be the vector space over $\mathbf{C}$ of all complex-valued continuous functions on $[0, 1]$. Let

$$b_1(f_1, f_2) = \overline{f_1(0)} f_2(0)$$

and

$$b_2(f_1, f_2) = \int_0^1 \overline{f_1(x)} f_2(x) dx$$

for $f_1$ and $f_2$ in $V$. Then $b_1$ and $b_2$ are sesquilinear forms on $V$, and they are hermitian.

(4) Let $V = \mathbf{C}^n$ and let $A \in M_{n,n}(\mathbf{C})$. For $x = (x_i) \in V$, the transpose ${}^t x$ is a row vector, and the conjugate

$${}^t\bar{x} = (\bar{x}_1, \ldots, \bar{x}_n)$$

is also a row vector. Let

$$b(x, y) = {}^t\bar{x} A y$$

for $x$ and $y \in \mathbf{C}^n$. Then $b$ is a sesquilinear form. In particular, if $A = 1_n$ is the identity matrix, we obtain

$$b(x, y) = \sum_i \bar{x}_i y_i.$$

Definition 6.1.6 (Conjugate of a matrix). If $n$, $m \geqslant 1$ and if $A = (a_{i,j}) \in M_{m,n}(\mathbf{C})$, we denote by $\bar{A}$ the matrix $(\overline{a_{ij}})$ of $M_{m,n}(\mathbf{C})$, and call $\bar{A}$ the **conjugate** of $A$.

Lemma 6.1.7. (1) *The application $A \mapsto \bar{A}$ satisfies*

$$\bar{\bar{A}} = A, \quad \overline{tA + sB} = \bar{t}\bar{A} + \bar{s}\bar{B},$$

*for any $A$, $B \in M_{m,n}(\mathbf{C})$ and $s$, $t \in \mathbf{C}$. In particular, it is $\mathbf{R}$-linear, and more precisely it is a linear involution from $M_{m,n}(\mathbf{C})$ to the conjugate space $\bar{M}_{n,m}(\mathbf{C})$.*

(2) *For $m$, $n$, $p \geqslant 1$, and for $A \in M_{m,n}(\mathbf{C})$ and $B \in M_{p,m}(\mathbf{C})$, we have*

$$\overline{BA} = \bar{B}\bar{A}.$$

*In particular, $A$ is invertible if and only if $\bar{A}$ is invertible, and $(\bar{A})^{-1} = \overline{A^{-1}}$.*

(3) *For $n \geqslant 1$ and $A \in M_{n,n}(\mathbf{C})$, we have* $\det(\bar{A}) = \overline{\det(A)}$.

Proof. (1) is elementary, and (2) follows from the definition of the product and the fact that $\overline{st} = \bar{s}\bar{t}$ for any complex numbers $s$ and $t$.

(3) can be derived from the Leibniz formula, or by checking that

$$A \mapsto \overline{\det(\bar{A})}$$

is an alternating multilinear map of the columns of $A$ that takes value 1 for the identity matrix. $\square$

Definition 6.1.8 (Hermitian matrix). A matrix $A \in M_{n,n}(\mathbf{C})$ is **hermitian** if and only if ${}^t\bar{A} = A$, or equivalently if ${}^tA = \bar{A}$: the conjugate of $A$ is equal to its transpose.

Proposition 6.1.9. *Let $V$ be a finite-dimensional complex vector space.*

(1) *For any ordered basis $B = (v_1, \ldots, v_n)$ of $V$, the application*

$$\beta_B \begin{cases} \mathrm{Ses}(V) & \to M_{n,n}(\mathbf{C}) \\ b & \mapsto (b(v_i, v_j))_{1 \leqslant i,j \leqslant n} \end{cases}$$

*is an isomorphism of vector spaces. In particular,* $\dim \mathrm{Ses}(V) = \dim_{\mathbf{C}}(V)^2$. *The sesquilinear form $b$ is hermitian if and only if $\beta_B(b)$ is hermitian.*

(2) *For any $x = (t_i) \in \mathbf{C}^n$ and $y = (s_j) \in \mathbf{C}^n$, we have*

$$b\Big(\sum_i t_i v_i, \sum_j s_j v_j\Big) = \sum_{i,j} b(v_i, v_j)\bar{t}_i s_j = {}^t\bar{x}Ay$$

*where $A = \beta_B(b)$.*

(3) *If $B$ and $B'$ are ordered bases of $V$ and $X = \mathrm{M}_{B',B}$ is the change of basis matrix, then for all $b \in \mathrm{Ses}(V)$ we have*

$$\beta_{B'}(b) = {}^t\bar{X}\beta_B(b)X.$$

Proof. (1) The linearity of $\beta_B$ is easy to check. We next check that this map is injective. If $\beta_B(b) = 0$, then $b(v_i, v_j) = 0$ for all $i$ and $j$. Then, using bilinearity, for any vectors

$$v = t_1 v_1 + \cdots + t_n v_n, \qquad w = s_1 v_1 + \cdots + s_n v_n, \tag{6.1}$$

we get

$$\begin{aligned}
b(v,w) = b(t_1v_1 + \cdots + t_nv_n, w) &= \sum_{i=1}^n \bar{t}_i b(v_i, w) \\
&= \sum_{i=1}^n \bar{t}_i b(v_i, s_1v_1 + \cdots + s_nv_n) \\
&= \sum_{i,j} \bar{t}_i s_j b(v_i, v_j) = 0,
\end{aligned}$$

so that $b = 0$. Finally, given a matrix $A = (a_{ij}) \in M_{n,n}(\mathbf{C})$, define

$$b(v,w) = \sum_{i,j} a_{ij}\bar{t}_i s_j$$

for $v$ and $w$ as in (6.1). This is a well-defined map from $V \times V$ to $\mathbf{C}$. For each $i$ and $j$, the map $(v,w) \mapsto a_{ij}\bar{t}_i s_j$ is sesquilinear (Example 6.1.5 (1)), so the sum $b$ is in $\mathrm{Ses}(V)$. For $v = v_{i_0}$ and $w = v_{j_0}$, the coefficients $t_i$ and $s_j$ are zero, except that $t_{i_0} = s_{j_0} = 1$, which shows that $b(v_i, v_j) = a_{ij}$. This means that $\beta_B(b) = A$, and hence we conclude that $\beta_B$ is also surjective.

A sesquilinear form $b$ is hermitian if and only if $b(v_i, v_j) = \overline{b(v_j, v_i)}$ for all $i$ and $j$, and this means that the transpose of the matrix $\beta_B(b)$ is equal to its conjugate.

(2) The first formula has already been deduced during the proof of (1), so we need to check that

$$\sum_{i,j} b(v_i, v_j) t_i s_j = {}^t\bar{x}Ay.$$

Indeed, we have

$$Ay = \Bigl(\sum_j b(v_i, v_j)s_j\Bigr)_{1 \leqslant i \leqslant n},$$

and therefore

$${}^t\bar{x}Ay = (\bar{t}_1 \ \cdots \ \bar{t}_n) \cdot Ay = \sum_i \bar{t}_i \sum_j b(v_i, v_j)s_j = \sum_{1 \leqslant i,j \leqslant n} \bar{t}_i s_j b(v_i, v_j).$$

(3) Let $B' = (w_1, \ldots, w_n)$. If $X = (a_{ij}) = \mathrm{M}_{B',B}$ is the change of basis matrix, and $x_j = (a_{ij})_{1 \leqslant i \leqslant n}$ denote the $j$-th column of $X$, then we have by definition

$$w_j = \sum_{i=1}^n a_{ij} v_i$$

for $1 \leqslant j \leqslant n$. So by (2) we get

$$b(w_i, w_j) = {}^t\bar{x}_i \beta_B(b) x_j$$

for all $i$ and $j$. Now consider the matrix ${}^t\bar{X}\beta_B(b)X$ and denote its coefficients $(c_{ij})$. Then $c_{ij}$ is the product of the $i$-th row of ${}^t\bar{X}$ with the $j$-th column of $\beta_B(b)X$, which is the product of $\beta_B(b)$ and the $j$-th column of $X$. This means that

$$c_{ij} = {}^t\bar{x}_i \beta_B(b) x_j = b(w_i, w_j)$$

and hence $\beta_{B'}(b) = {}^t\bar{X}\beta_B(b)X$. ☐

Definition 6.1.10 (Left and right kernels of a sesquilinear form). Let $b$ be a sesquilinear form on $V$. The **left-kernel** of $b$ is the set of vectors $v \in V$ such that

$$b(v, w) = 0 \text{ for all } w \in V,$$

and the **right-kernel** of $b$ is the set of vectors $w \in V$ such that

$$b(v, w) = 0 \text{ for all } v \in V.$$

A sesquilinear form $b$ on $V$ is **non-degenerate** if the right and the left kernels are both equal to $\{0\}$.

If $b$ is hermitian, then the left and right kernels are equal.

Proposition 6.1.11. *Let $V$ be a finite-dimensional vector space and $B = (v_i)$ an ordered basis of $V$. Then a sesquilinear form $b$ on $V$ is non-degenerate if and only if* $\det(\beta_B(b)) \neq 0$.

Proof. Suppose first that the left-kernel of $b$ contains a non-zero vector $v$. Then there is an ordered basis $B'$ of $V$ such that $v$ is the first vector of $B'$ (Theorem 2.7.1 (2)). We have

$$\beta_B(b) = {}^t\bar{X}\beta_{B'}(b)X$$

where $X = \mathrm{M}_{B',B}$ (Proposition 6.1.9 (3)). Since the coefficients $b(v, v')$ of the first row of $\beta_{B'}(b)$ are zero, we get $\det(\beta_{B'}(b)) = 0$, hence $\det(\beta_B(b)) = 0$. Similarly, if the right-kernel of $b$ is non-zero, we deduce that $\det(\beta_B(b)) = 0$.

We now consider the converse and assume that $\det(\beta_B(b)) = 0$. Then the columns $C_j$ of the matrix $\beta_B(b)$ are not linearly independent. Let then $t_1, \ldots, t_n$ be elements of $\mathbf{K}$, not all equal to 0, such that

$$t_1C_1 + \cdots + t_nC_n = 0_n \in \mathbf{C}^n.$$

Since $C_j = (b(v_i, v_j))_{1 \leqslant i \leqslant n}$, this means that for $1 \leqslant i \leqslant n$, we have

$$t_1b(v_i, v_1) + \cdots + t_nb(v_i, v_n) = 0.$$

By linearity with respect to the second argument, this means that

$$b(v_i, t_1v_1 + \cdots + t_nv_n) = 0$$

for all $i$. But then (by sesquilinearity) the vector $t_1v_1 + \cdots + t_nv_n$ belongs to the right-kernel of $b$. Similarly, using the fact that the rows of $\beta_B(b)$ are not linearly independent, we deduce that the left-kernel of $b$ is non-zero. ☐

Proposition 6.1.12. *Let $V$ be a finite-dimensional $\mathbf{C}$-vector space and let $b \in \mathrm{Ses}(V)$ be a non-degenerate sesquilinear form. For $v \in V$, denote by $\lambda_v$ the linear form*

$$\lambda_v(w) = b(v, w)$$

*on $V$. Then the map*

$$\begin{cases} \bar{V} & \to \mathrm{Hom}_{\mathbf{C}}(V, \mathbf{C}) \\ v & \mapsto \lambda_v \end{cases}$$

*is an isomorphism.*

Proof. We first check that the map is linear. It is elementary that $\lambda_{v_1+v_2} = \lambda_{v_1} + \lambda_{v_2}$. Let $v \in V$ and $t \in \mathbf{C}$.

Then, denoting by $tv$ the product in $V$, we have

$$\lambda_{tv}(w) = b(tv, w) = \bar{t}b(v, w) = \bar{t}\lambda_v(w)$$

which means that $\lambda_{tv} = \bar{t}\lambda_v$. Translating in terms of $\bar{V}$, this means that

$$\lambda_{t \cdot_{\bar{V}} v} = \lambda_{\bar{t}v} = t\lambda_v,$$

so that $\lambda$ is linear from $\bar{V}$ to $\mathrm{Hom}_{\mathbf{C}}(V, \mathbf{C})$.

Now that we know that the map is linear, we observe that both spaces have the same dimension (Lemma 6.1.4), so it suffices to check that this map is injective. But if $\lambda_v = 0$, we obtain $b(v, w) = 0$ for all $w \in V$, which means that $w$ belongs to the right-kernel of $b$, which is zero since $b$ is non-degenerate. □

Example 6.1.13. We describe more precisely $\mathrm{Ses}(\mathbf{C}^n)$ for $n = 1$ and 2. For $n = 1$, a sesquilinear form on $\mathbf{C}$ is of the form $b(x, y) = a\bar{x}y$ for some $a \in \mathbf{C}$. This form is hermitian if and only if $a \in \mathbf{R}$, and non-degenerate if and only if $a \neq 0$.

For $n = 2$, the sesquilinear form associated to the matrix

$$A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \in M_{2,2}(\mathbf{C})$$

is

$$b\left(\begin{pmatrix} x_1 \\ y_1 \end{pmatrix}, \begin{pmatrix} x_2 \\ y_2 \end{pmatrix}\right) = a_{11}\bar{x}_1 x_2 + a_{12}\bar{x}_1 y_2 + a_{21}\bar{x}_2 y_1 + a_{22}\bar{x}_2 y_2.$$

This sesquilinear form is non-degenerate if and only if $a_{11}a_{22} - a_{12}a_{21} \neq 0$. It is hermitian if and only if $a_{11}$ and $a_{22}$ are real and if $a_{12} = \bar{a}_{21}$.

Definition 6.1.14 (Positive, positive-definite hermitian forms). Let $V$ be a $\mathbf{C}$-vector space. A sesquilinear form $b \in \mathrm{Ses}(V)$ is called **positive** if $b$ is hermitian and

$$b(v, v) \geqslant 0$$

for all $v \in V$; it is called **positive definite**, or a **(complex) scalar product** if it is positive and if $b(v, v) = 0$ if and only if $v = 0$.

If $b$ is positive, then two vectors $v$ and $w$ are said to be **orthogonal** if and only if $b(v, w) = 0$. This is denoted $v \perp w$, or $v \perp_b w$ if we wish to specify which sesquilinear form $b$ is considered.

Remark 6.1.15. If $v$ and $w$ are orthogonal, note that we obtain

$$b(v + w, v + w) = b(v, v) + b(w, w) + b(v, w) + b(w, v) = b(v, v) + b(w, w).$$

As for euclidean spaces (see (5.2)), a positive (in fact, hermitian) form $b$ is determined by the map $q \colon v \mapsto b(v, v)$. To see this, note that

$$q(v + w) - q(v) - q(w) = b(v, w) + b(w, v) = 2\,\mathrm{Re}(b(v, w))$$

so the real part of $b(v, w)$ is determined for all $v$ and $w$ by the map $q$. But moreover

$$\mathrm{Im}(b(v, w)) = -\,\mathrm{Re}(ib(v, w)) = \mathrm{Re}(b(iv, w))$$

is then also determined by $q$.

Proposition 6.1.16 (Cauchy-Schwarz inequality). *Let $V$ be a complex vector space and let $b$ be a scalar product on $V$. Then for all $v$ and $w \in V$, we have*

$$|b(v, w)|^2 \leqslant b(v, v)b(w, w).$$

*Moreover there is equality if and only if $v$ and $w$ are linearly dependent.*

Proof. We may then assume that $v \neq 0$, since otherwise the inequality takes the form $0 = 0$ (and $0$ and $w$ are linearly dependent). Then observe the decomposition $w = w_1 + w_2$ where

$$w_1 = \frac{b(v,w)}{b(v,v)}v, \qquad w_2 = w - \frac{b(v,w)}{b(v,v)}v.$$

Note that

$$b(w_1, w_2) = \frac{b(v,w)}{b(v,v)}b(v,w) - \frac{b(v,w)}{b(v,v)}b(v,w) = 0.$$

Hence we get, as observed above, the relation

$$b(w,w) = b(w_1,w_1) + b(w_2,w_2) = \frac{|b(v,w)|^2}{b(v,v)^2}b(v,v) + b(w_2,w_2) \geqslant \frac{|b(v,w)|^2}{b(v,v)}.$$

This leads to the Cauchy-Schwarz inequality. Moreover, we have equality if and only if $b(w_2, w_2) = 0$. If $b$ is positive definite, this means that $w_2 = 0$, which by definition of $w_2$ means that $v$ and $w$ are linearly dependent. ☐

Example 6.1.17. For any continuous complex-valued functions $f_1$ and $f_2$ on an interval $[a,b]$, we have

$$\Big|\int_a^b \overline{f_1(x)} f_2(x)dx\Big|^2 \leqslant \Big(\int_a^b |f_1(x)|^2dx\Big) \times \Big(\int_a^b |f_2(x)|^2dx\Big).$$

Indeed, the map

$$b(f_1, f_2) = \int_a^b \overline{f_1(x)} f_2(x)dx$$

is a positive-definite sesquilinear form on the $\mathbf{C}$-vector space $V$ of complex-valued continuous functions from $[a,b]$ to $\mathbf{C}$.

Definition 6.1.18 (Unitary space). A **unitary space** or **pre-Hilbert space** is the data of a $\mathbf{C}$-vector space $V$ and a scalar product $b$ on $V$. One often denotes

$$\langle v|w\rangle = b(v,w).$$

For $v \in V$, one denotes $\|v\| = \sqrt{\langle v|v\rangle}$. The function $v \mapsto \|v\|$ is called the **norm** on $V$. For $v, w \in V$, the norm $\|v-w\|$ is called the **distance** between $v$ and $w$, and is sometimes denoted $d(v,w)$.

Example 6.1.19. Let $V = \mathbf{C}^n$. The sesquilinear form

$$b(x,y) = \sum_{i=1}^n \bar{x}_i y_i$$

is a scalar product on $\mathbf{C}^n$: indeed, it is clearly symmetric, and since

$$b(x,x) = \sum_{i=1}^n |x_i|^2,$$

it follows that $b(x,x) \geqslant 0$ for all $x \in \mathbf{C}^n$, with equality only if each $x_i$ is zero, that is only if $x = 0$.

This scalar product on $\mathbf{C}^n$ is called the **standard (unitary) scalar product**.

Lemma 6.1.20. *Let $V$ be a unitary space. If $W \subset V$ is a vector subspace, then the restriction of the scalar product to $W \times W$ makes $W$ a unitary space.*

PROOF. It is immediate that the restriction of a hermitian form on $V$ to $W \times W$ is a hermitian form on $W$. For a scalar product, the restriction is a positive hermitian form since $b(w, w) \geqslant 0$ for all $w \in W$, and it satisfies $b(w, w) = 0$ if and only if $w = 0$, so it is a scalar product. ☐

In terms of the scalar product and the norm, the Cauchy-Schwarz inequality translates to

$$|\langle v|w\rangle| \leqslant \|v\|\|w\|$$

for $v$ and $w$ in $V$.

LEMMA 6.1.21. *Let $V$ be a unitary space.*

(1) *The norm satisfies $\|v\| \geqslant 0$, with $\|v\| = 0$ if and only if $v = 0$, it satisfies $\|tv\| = |t|\|v\|$ for all $t \in \mathbf{C}$ and $v \in V$, and the triangle inequality*

$$\|v + w\| \leqslant \|v\| + \|w\|.$$

(2) *The distance satisfies $d(v, w) \geqslant 0$, with equality if and only if $v = w$, it satisfies $d(v, w) = d(w, v)$ and the triangle inequality*

$$d(v, w) \leqslant d(v, u) + d(u, w)$$

*for any $u$, $v$, $w$ in $V$.*

PROOF. (1) Only the triangle inequality is not a direct consequence of the definition of scalar products. For that, we have

$$\|v+w\|^2 = b(v+w, v+w) = b(v, v)+b(w, w)+b(v, w)+b(w, v) = \|v\|^2+\|w\|^2+2\,\mathrm{Re}(\langle v|w\rangle).$$

Using the bound $|\mathrm{Re}(z)| \leqslant |z|$ and the Cauchy-Schwarz inequality, we derive

$$\|v + w\|^2 \leqslant \|v\|^2 + \|w\|^2 + 2\|v\|\|w\| = (\|v\| + \|w\|)^2,$$

hence the result since the norm is $\geqslant 0$.

(2) is a translation in terms of distance of some of these properties, and left as exercise. ☐

EXAMPLE 6.1.22. The most important example is $V = \mathbf{C}^n$ with the "standard" scalar product

$$\langle v|w\rangle = \bar{x}_1 y_1 + \cdots + \bar{x}_n y_n = {}^t\bar{v}w,$$

for $v = (x_i)$ and $w = (y_i)$. The norm is the standard hermitian norm

$$\|v\| = \sqrt{|x_1|^2 + \cdots + |x_n|^2}.$$

DEFINITION 6.1.23 (Angle). Let $V$ be a unitary space. The **(unoriented) angle** between two non-zero vectors $v$ and $w$ is the unique real number $t \in [0, \pi/2]$ such that

$$\cos(t) = \frac{|\langle v|w\rangle|}{\|v\|\|w\|}.$$

This is well-defined because the Cauchy-Schwarz inequality shows that the quantity on the right is a real number between 0 and 1, and we know that cosine is a bijection between $[0, \pi/2]$ and $[0, 1]$.

Note that the angle is $\pi/2$ if and only if $\langle v|w\rangle = 0$, i.e., if and only if $v$ and $w$ are orthogonal.

## 6.2. Orthogonal bases, II

DEFINITION 6.2.1 (Orthogonal and orthonormal subsets). Let $V$ be a unitary space. A subset $S$ of $V$ such that $\langle v|w\rangle = 0$ for all $v \neq w$ in $S$ is said to be an **orthogonal subset** of $V$. If, in addition, $\|v\| = 1$ for all $v \in S$, then $S$ is said to be an **orthonormal subset** of $V$.

An **orthogonal** (resp. **orthonormal**) basis of $V$ is an orthogonal subset (resp. an orthonormal subset) which is a basis of $V$.

If $V$ is finite-dimensional of dimension $d$, then an ordered orthogonal (resp. orthonormal) basis is a $d$-tuple $(v_1, \ldots, v_d)$ such that $\{v_1, \ldots, v_d\}$ is an orthogonal (resp. orthonormal) basis.

EXAMPLE 6.2.2. Let $V$ be the space of complex-valued continuous functions on $[0, 2\pi]$ with the scalar product

$$\langle f_1|f_2\rangle = \frac{1}{2\pi}\int_0^{2\pi} \overline{f_1(x)} f_2(x)dx.$$

Then the set $\{e_n \mid n \in \mathbf{Z}\}$ where

$$e_n(x) = e^{2i\pi nx}$$

for $n \in \mathbf{Z}$ is an orthonormal subset.

PROPOSITION 6.2.3. *Let $V$ be a complex vector space. If $S$ is an orthogonal subset in $V$ such that $0 \notin S$, then $S$ is linearly independent. Moreover, if $w \in \langle S\rangle$, then the decomposition of $w$ as a linear combination of vectors in $S$ is*

$$w = \sum_{v \in S} \frac{\langle v|w\rangle}{\|v\|^2} v.$$

*In particular, if $(v_1, \ldots, v_d)$ is an ordered orthonormal basis of $V$, then we have the decomposition*

$$w = \sum_{i=1}^{d} \langle v_i|w\rangle v_i$$

*for all $w \in V$. Further, we then have*

$$\|w\|^2 = \sum_{i=1}^{d} |\langle w|v_i\rangle|^2, \qquad \langle v|w\rangle = \sum_{i=1}^{d} \langle v_i|v\rangle\langle w|v_i\rangle = \sum_{i=1}^{d} \overline{\langle v_i|v\rangle}\langle v_i|w\rangle$$

*for all $v$ and $w$ in $V$.*

This proposition means that if $\dim(V) = d$, then a tuple $(v_1, \ldots, v_d)$ is an ordered orthogonal basis if and only if

$$v_i \neq 0 \text{ for all } i, \qquad \langle v_i|v_j\rangle = 0 \text{ for } i \neq j,$$

and it is an ordered orthonormal basis if and only if we have

$$\langle v_i|v_j\rangle = \delta(i, j),$$

since the proposition shows that these vectors are then linearly independent.

PROOF. Let $(t_v)_{v \in S}$ be complex numbers, all but finitely many of which are zero, such that

$$\sum_{v \in S} t_v v = 0.$$

Fix $v_0 \in S$. Computing $\langle v_0|w\rangle$, we get

$$0 = \langle v_0|\sum_{v\in S} t_v v\rangle = \sum_{v\in S} t_v\langle v_0|v\rangle$$

which by orthogonality means that $0 = t_{v_0}\langle v_0|v_0\rangle$. Since $v_0 \neq 0$, we deduce that $t_{v_0} = 0$. This holds for all $v_0 \in S$, which means that $S$ is linearly independent.

Now let

$$w = \sum_{v\in S} t_v v$$

be an element of $\langle S\rangle$. Computing $\langle v|w\rangle$ for $v \in S$, we get similarly

$$\langle v|w\rangle = t_v\langle v|v\rangle,$$

which gives the formula we stated.

Finally, we compute the scalar product for any $v$ and $w$ in $V$:

$$\langle v|w\rangle = \sum_i\sum_j \overline{\langle v_i|v\rangle}\langle v_j|w\rangle\,\langle v_i|v_j\rangle = \sum_i \overline{\langle v_i|v\rangle}\langle v_i|w\rangle,$$

since $\langle v_i|v_j\rangle$ is zero unless $i = j$. The case of $\|w\|^2$ follows by taking $v = w$. ☐

THEOREM 6.2.4 (Gram-Schmidt orthonormalization). *Let $V$ be a finite-dimensional unitary space. Let $B = (v_1, \ldots, v_n)$ be an ordered basis of $V$. There exists a unique ordered* orthonormal *basis $(w_1, \ldots, w_n)$ of $V$ such that for $1 \leqslant i \leqslant n$, we have*

$$w_i \in \langle v_1, \ldots, v_i\rangle,$$

*and such that the coefficient of $v_i$ in the linear combination representing $w_i$ is a real number that is $> 0$. In particular, this shows that orthonormal bases of $V$ exist.*

PROOF. We use induction on $n$. For $n = 1$, the vector $w_1$ is of the form $cv_1$, and $c$ must satisfy

$$1 = \|w_1\|^2 = \langle cv_1|cv_1\rangle = |c_1|^2\|v_1\|^2,$$

so that $|c_1|^2 = \|v_1\|^{-2}$; since the last requirement is that $c_1 > 0$, the unique choice is $c_1 = \|v_1\|^{-1}$.

Now assume that $n \geqslant 2$ and that the result is known for spaces of dimension $n-1$. Applying it to $\langle v_1, \ldots, v_{n-1}\rangle$, we deduce that there exist unique orthonormal vectors $(w_1, \ldots, w_{n-1})$ such that $w_i$ is a linear combination of $(v_1, \ldots, v_i)$ for $1 \leqslant i \leqslant n-1$ and such that the coefficient of $v_i$ in $w_i$ is $> 0$.

We search for $w$ as a linear combination

$$w = t_1 w_1 + \cdots + t_{n-1}w_{n-1} + t_n v_n$$

for some $t_i \in \mathbf{C}$, with $t_n$ a real number that is $> 0$. The conditions to be satisfied are that $\langle w_i|w\rangle = 0$ for $1 \leqslant i \leqslant n-1$ and that $\langle w|w\rangle = 1$. The first $n-1$ equalities translate to

$$0 = \langle w_i|w\rangle = t_i + t_n\langle w_i|v_n\rangle,$$

which holds provided $t_i = -t_n\langle w_i|v_n\rangle$ for $1 \leqslant i \leqslant n-1$. We assume this condition, so that

$$w = t_n\Big(v_n - \sum_{i=1}^{n-1}\langle w_i|v_n\rangle w_i\Big).$$

Then $t_n$ is the only remaining parameter and can only take the positive value such that

$$\frac{1}{t_n} = \Big\|v_n - \sum_{i=1}^{n-1}\langle v_n|w_i\rangle w_i\Big\|.$$

This concludes the proof, provided the vector

$$x = v_n - \sum_{i=1}^{n-1} \langle v_n | w_i \rangle w_i$$

is non-zero. But by construction, this is a linear combination of $v_1$, ..., $v_n$ where the coefficient of $v_n$ is 1, hence non-zero. Since the vectors $v_i$ for $1 \leqslant i \leqslant n$ are linearly independent, it follows that $x \neq 0$. ☐

REMARK 6.2.5. In practice, one may proceed as follows to find the vectors $(w_1, \ldots, w_n)$: one computes

$$w_1 = \frac{v_1}{\|v_1\|}$$

$$w_2' = v_2 - \langle w_1 | v_2 \rangle w_1, \qquad w_2 = \frac{w_2'}{\|w_2'\|}$$

and so on

$$w_n' = v_n - \langle w_1 | v_n \rangle w_1 - \cdots - \langle w_{n-1} | v_n \rangle w_{n-1}, \qquad w_n = \frac{w_n'}{\|w_n'\|}.$$

Indeed, these vectors satisfy the required conditions: first, the vectors are of norm 1, then the coefficient of $v_n$ in $w_n$ is $1/\|w_n'\| > 0$ (once one knows it is defined!) and finally, we have orthogonality because, for instance for $i < n$, we get

$$\langle w_i | w_n \rangle = \frac{1}{\|w_i\| \|w_n\|} \langle w_i' | w_n' \rangle = \langle w_i | v_n \rangle - \langle w_i | v_n \rangle \langle w_i | w_i \rangle = 0.$$

COROLLARY 6.2.6. *Let $V$ be a finite-dimensional unitary space. Let $W \subset V$ be a subspace of $V$, and let $B$ be an ordered orthonormal basis of $W$. Then there is an orthonormal ordered basis of $V$ containing $B$.*

PROOF. Write $B = (w_1, \ldots, w_m)$. Let $B'$ be such that $(B_0, B')$ is an ordered basis of $V$, and let $\tilde{B} = (v_1, \ldots, v_n)$ be the ordered orthonormal basis given by Theorem 5.4.4. Because of the uniqueness property, we have in fact $v_i = w_i$ for $1 \leqslant i \leqslant m$: indeed, if we consider $(w_1, \ldots, w_m, v_{m+1}, \ldots, v_n)$, the vectors also satisfy the conditions of Theorem 6.2.4 for the basis $B_0$. ☐

COROLLARY 6.2.7 (Complex Cholesky decomposition). *Let $n \geqslant 1$ and let $A \in M_{n,n}(\mathbf{C})$ be a hermitian matrix such that the sesquilinear form $b(x, y) = {}^t\bar{x}Ay$ is a scalar product on $\mathbf{C}^n$. Then there exists a unique upper-triangular matrix $R \in M_{n,n}(\mathbf{C})$ with diagonal coefficients $> 0$ such that $A = {}^t\bar{R}R$.*

*Conversely, for any invertible matrix $R \in M_{n.n}(\mathbf{C})$, the sesquilinear form on $\mathbf{C}^n$ defined by $b(x, y) = {}^t\bar{x}({}^t\bar{R}R)y$ is a scalar product on $\mathbf{C}^n$.*

PROOF. We consider the unitary space $V = \mathbf{C}^n$ with the scalar product

$$\langle x | y \rangle = {}^t\bar{x}Ay.$$

We then consider the standard basis $E = (e_1, \ldots, e_n)$ of $\mathbf{C}^n$. Let $B = (v_1, \ldots, v_n)$ be the ordered orthonormal basis of $V$ obtained from this standard basis by Gram-Schmidt orthonormalization (Theorem 6.2.4). Let $R = \mathrm{M}_{E,B}$ be the change of basis matrix from $E$ to $B$. Because $v_i \in \langle e_1, \ldots, e_i \rangle$, the matrix $R$ is upper-triangular, and since the coefficient of $e_i$ in $v_i$ is $> 0$, the diagonal coefficients of $R$ are $> 0$.

We now check that $A = {}^t\bar{R}R$. The point is that since $B$ is an orthonormal basis of $V$, we have

$$\langle x|y\rangle = \sum_i \bar{t}_i s_i = {}^t\bar{t}s$$

if we denote by $t = (t_i)$ and $s = (s_j)$ the vectors such that

$$x = \sum_i t_i v_i, \qquad y = \sum_j s_j v_j.$$

We have also $t = Rx$ and $s = Ry$ by definition of the change of basis. It follows therefore that

$${}^t\bar{x}Ay = {}^t\overline{Rx}Ry = {}^t\bar{x}{}^t\bar{R}Ry.$$

Because this is true for *all* $x$ and $y$, it follows that $A = {}^t\bar{R}R$. This proves the existence of $R$. For the uniqueness, we will use some facts proved below. Note that if ${}^t\bar{R}R = {}^t\bar{S}S$ with $R$ and $S$ upper-triangular and with $> 0$ diagonal entries, then we obtain ${}^t\bar{Q} = Q^{-1}$ where $Q = RS^{-1}$. The matrix $Q$ is upper-triangular with $> 0$ diagonal entries, and the equation means that it is unitary, in the sense of Definition 6.5.1 below. Then Corollary 6.5.5 below means that $Q$ is diagonal with diagonal coefficients of modulus 1. But since it has positive diagonal coefficients, it must be the identity.

Conversely, let $b(x, y) = {}^t\bar{x}({}^t\bar{R}R)y$ for $R \in M_{n,n}(\mathbf{C})$. Since ${}^t({}^t\bar{R}R) = {}^tR\bar{R}$, the matrix $A = {}^t\bar{R}R$ is hermitian, and therefore $b$ is a hermitian form. Moreover, we can write $b(x, y) = {}^t\overline{Rx}Ry$, and hence $b(x, x) = \langle Rx|Rx\rangle$, where the scalar product is the standard euclidean scalar product on $\mathbf{C}^n$. This implies that $b(x, x) \geqslant 0$ and that $b(x, x) = 0$ if and only if $Rx = 0$. If $R$ is invertible, it follows that $R$ is a scalar product. ☐

## 6.3. Orthogonal complement, II

Definition 6.3.1 (Orthogonal of a subspace). Let $V$ be a unitary space. The **orthogonal** $W^\perp$ of a subspace $W$ of $V$ is the set of all vectors orthogonal to all $v \in W$:

$$W^\perp = \{v \in V \mid \langle v|w\rangle = 0 \text{ for all } w \in W\}.$$

Proposition 6.3.2. *Let $V$ be a unitary space.*

(1) *We have $\{0\}^\perp = V$ and $V^\perp = \{0\}$.*

(2) *For any subspaces $W_1$ and $W_2$ of $V$ such that $W_1 \subset W_2$, we have $W_2^\perp \subset W_1^\perp$;*

(3) *If $V$ is finite-dimensional then $(W^\perp)^\perp = W$; in particular, $W_1 = W_2$ if and only if $W_2^\perp = W_1^\perp$.*

(4) *If $V$ is finite-dimensional then $V = W \oplus W^\perp$ for any subspace $W$ of $V$. In particular, we have then $\dim(W^\perp) = \dim(V) - \dim(W)$.*

Proof. (1) By definition, all vectors are orthogonal to 0; because the scalar product is non-degenerate, only 0 is orthogonal to all of $V$.

(2) If $W_1 \subset W_2$, all vectors orthogonal to $W_2$ are orthogonal to $W_1$, so $W_2^\perp \subset W_1^\perp$.

(3) Let $(v_1, \ldots, v_m, v_{m+1}, \ldots, v_n)$ be an orthonormal ordered basis of $V$ such that $(v_1, \ldots, v_m)$ is an orthonormal ordered basis of $W$ (Corollary 6.2.6). By linearity, a vector $v \in W$ belongs to $W^\perp$ if and only if $\langle v_i|v\rangle = 0$ for $1 \leqslant i \leqslant m$. But since $B$ is an orthonormal basis of $V$, we can write

$$v = \sum_{i=1}^{n} \langle v_i|v\rangle v_i$$

and this shows that $v \in W^{\perp}$ if and only if

$$v = \sum_{i=m+1}^{n} \langle v_i | v \rangle v_i.$$

Hence $(v_{m+1}, \ldots, v_n)$ is an orthonormal basis of $W^{\perp}$. Repeating this argument, it follows that $v \in (W^{\perp})^{\perp}$ if and only if

$$v = \sum_{i=1}^{m} \langle v_i | v \rangle v_i,$$

which means if and only if $v \in W$.

(4) We first see that $W$ and $W^{\perp}$ are in direct sum: indeed, an element $v \in W \cap W^{\perp}$ satisfies $\langle v | v \rangle = 0$, so $v = 0$. Then we have $W + W^{\perp} = V$ by the argument in (3): using the notation introduced in that argument, we can write

$$v = \sum_{i=1}^{m} \langle v_i | v \rangle v_i + \sum_{i=m+1}^{n} \langle v_i | v \rangle v_i$$

where the first term belongs to $W$ and the second to $W^{\perp}$. ☐

Because of (3), one also says that $W^{\perp}$ is the **orthogonal complement** of $W$ in $V$.

Definition 6.3.3 (Orthogonal direct sum). Let $V$ be a unitary space and $I$ an arbitrary set. If $(W_i)_{i \in I}$ are subspaces of $V$, we say that they are in **orthogonal direct sum** if for all $i \neq j$ and $w \in W_i$, $w' \in W_j$, we have $\langle w | w' \rangle = 0$, or equivalently if $W_i \subset W_j^{\perp}$ for all $i \neq j$.

Lemma 6.3.4. *If $(W_i)_{i \in I}$ are subspaces of $V$ in orthogonal direct sum, then they are linearly independent, i.e., they are in direct sum.*

Proof. This is because of Proposition 6.2.3, since any choice of vectors $w_i$ in $W_i$ will form an orthogonal subset of $V$. ☐

Definition 6.3.5 (Orthogonal projection). Let $V$ be a finite-dimensional unitary space and let $W$ be a subspace of $V$. The projection $p_W$ on $W$ with kernel $W^{\perp}$ is called the **orthogonal projection** on $W$.

The orthogonal projection $p_W$ on $W$ is therefore characterized as the unique map $p_W$ from $V$ to $V$ such that $p_W(v) \in W$ and $v - p_W(v) \perp w$ for all $w \in W$.

Lemma 6.3.6. *Let $V$ be a finite-dimensional unitary space and let $W$ be a subspace of $V$. If $(v_1, \ldots, v_m)$ is an orthonormal ordered basis of $W$, then the orthogonal projection on $W$ is given by*

$$p_W(v) = \sum_{i=1}^{m} \langle v_i | v \rangle v_i$$

*for all $v \in V$.*

Proof. Indeed, since $p_W(v)$ belongs to $W$, Proposition 6.2.3, applied to $W$ and the basis $(v_1, \ldots, v_m)$, shows that

$$p_W(v) = \sum_{i=1}^{m} \langle v_i | p_W(v) \rangle v_i.$$

But since $v = p_W(v) + v'$ where $v' \in W^{\perp}$, we have

$$\langle v_i | v \rangle = \langle v_i | p_W(v) \rangle + \langle v_i | v' \rangle = \langle v_i | v \rangle$$

for $1 \leqslant i \leqslant m$. ☐

## 6.4. Adjoint, II

In this section, we consider only *finite-dimensional* unitary spaces. Let $f\colon V_1 \to V_2$ be a linear map between finite-dimensional unitary spaces. For any $v \in V_2$, we can define a linear form $\lambda_v\colon V_1 \to \mathbf{C}$ by

$$\lambda_v(w) = \langle v|f(w)\rangle,$$

where the scalar product is the one on $V_2$. According to Proposition 6.1.12, there exists a unique vector $f^*(v) \in V_1$ such that

$$\langle v|f(w)\rangle = \lambda_v(w) = \langle f^*(v)|w\rangle$$

for all $w \in V_1$. Because of the uniqueness, we can see that the map $v \mapsto f^*(v)$ is a linear map from $V_2$ to $V_1$.

Definition 6.4.1 (Adjoint). The linear map $f^*$ is called the **adjoint** of $f$.

If $V$ is a unitary space, then $f \in \mathrm{End}_{\mathbf{C}}(V)$ is called **normal** if and only if $f^*f = ff^*$, and it is called **self-adjoint** if $f^* = f$.

So the adjoint of $f\colon V_1 \to V_2$ is characterized by the equation

$$\langle f^*(v)|w\rangle = \langle v|f(w)\rangle \tag{6.2}$$

for all $w \in V_1$ and $v \in V_2$.

Note that we also obtain

$$\langle w|f^*(v)\rangle = \langle f(w)|v\rangle$$

by applying the hermitian property of the scalar product.

Example 6.4.2. Let $A \in M_{m,n}(\mathbf{C})$ and let $f = f_A\colon \mathbf{C}^n \to \mathbf{C}^m$, where $\mathbf{C}^n$ and $\mathbf{C}^m$ are viewed as unitary spaces with the standard scalar product. Then for $x \in \mathbf{C}^n$ and $y \in \mathbf{C}^m$, we have

$$\langle f(x)|y\rangle = {}^t(\overline{f(x)})y = {}^t\overline{(Ax)}y = {}^t\bar{x}{}^t\bar{A}y = \langle x|{}^t\bar{A}y\rangle.$$

This means that $f^*(y) = {}^t\bar{A}y$, or in other words, that the adjoint of $f_A$ is $f_{{}^t\bar{A}}$.

The meaning of normal endomorphisms is made clearer by the following lemma:

Lemma 6.4.3. *Let $V$ be a finite-dimensional unitary space. An endomorphism $f \in \mathrm{End}_{\mathbf{C}}(V)$ is normal if and only if*

$$\|f(v)\| = \|f^*(v)\|$$

*for all $v \in V$.*

Proof. For $v \in V$, we have

$$\|f(v)\|^2 = \langle f(v)|f(v)\rangle = \langle f^*f(v)|v\rangle$$

and

$$\|f^*(v)\|^2 = \langle f^*(v)|f^*(v)\rangle = \langle ff^*(v)|v\rangle$$

so that we have $\|f(v)\| = \|f^*(v)\|$ for all $v$ if $f$ is normal.

Conversely, if $\|f(v)\| = \|f^*(v)\|$ for all $v \in V$, the same computation shows that

$$\langle f^*f(v)|v\rangle = \langle ff^*(v)|v\rangle.$$

Define $b_1(v,w) = \langle f^*f(v)|w\rangle$ and $b_2(v,w) = \langle ff^*(v)|w\rangle$. Both are positive hermitian forms on $V$, from what we just saw, and $b_1(v,v) = b_2(v,v)$ for all $v \in V$. By Remark 6.1.15, this implies $b_1 = b_2$. This means that

$$\langle (f^*f - ff^*)(v)|w\rangle = 0$$

for all $v$ and $w \in V$, and taking $w = (f^*f - ff^*)(v)$ leads to the conclusion that $ff^* = f^*f$, so that $f$ is normal. ☐

Lemma 6.4.4. (1) *The map* $f \mapsto f^*$ *is an isomorphism*

$$\mathrm{Hom}_{\mathbf{C}}(V_1, V_2) \to \overline{\mathrm{Hom}_{\mathbf{C}}(V_2, V_1)},$$

*with inverse also given by the adjoint. In other words, we have*

$$(f_1 + f_2)^* = f_1^* + f_2^*, \qquad (tf)^* = \bar{t}f^*, \qquad (f^*)^* = f$$

*for any* $f$, $f_1$, $f_2 \in \mathrm{Hom}_{\mathbf{C}}(V_1, V_2)$ *and* $t \in \mathbf{C}$. *We also have* $\mathrm{Id}^* = \mathrm{Id}$.

(2) *The adjoint of the identity* $\mathrm{Id}_V$ *is* $\mathrm{Id}_V$.

(3) *For* $V_1$, $V_2$, $V_3$ *finite-dimensional unitary spaces and* $f \in \mathrm{Hom}_{\mathbf{C}}(V_1, V_2)$, $g \in \mathrm{Hom}_{\mathbf{C}}(V_2, V_3)$, *we have*

$$(g \circ f)^* = f^* \circ g^*.$$

Proof. (1) The additivity follows easily from the characterization (6.2) and is left as an exercise. To check that $(tf)^* = \bar{t}f$, note that

$$\langle(\bar{t}f^*)(v)|w\rangle = t\langle f^*(v)|w\rangle = t\langle v|f(w)\rangle = \langle v|(tf)(w)\rangle$$

for all $v \in V_2$ and $w \in V_1$. Using the characterization of the adjoint, this means that $(tf)^* = \bar{t}f^*$.

To prove the last part, it is enough to check that $(f^*)^* = f$. But the adjoint $g = (f^*)^*$ of $f^*$ is the linear map from $V_1$ to $V_2$ characterized by the relation

$$\langle g(w)|v\rangle = \langle w|f^*(v)\rangle$$

for $w \in V_1$ and $v \in V_2$, or in other words by the relation

$$\langle v|g(w)\rangle = \langle f^*(v)|w\rangle = \langle v|f(w)\rangle.$$

Fixing $w$ and taking $v = g(w) - f(w)$, we get $\|g(w) - f(w)\|^2 = 0$, hence $g(w) = f(w)$ for all $w \in V_1$. So $g = f$.

(2) It is immediate from the definition that $\mathrm{Id}_V^* = \mathrm{Id}_V$.

(3) The composition $g \circ f$ is a linear map from $V_1$ to $V_3$. For any $v \in V_3$ and $w \in V_1$, we have

$$\langle v|g(f(w))\rangle = \langle g^*(v)|f(w)\rangle = \langle f^*(g^*(v))|w\rangle,$$

which shows that $(g \circ f)^*(v) = f^*(g^*(v))$. □

Proposition 6.4.5. *Let* $f : V_1 \to V_2$ *be a linear map between finite-dimensional unitary spaces.*

(1) *We have*

$$\mathrm{Ker}(f^*) = \mathrm{Im}(f)^\perp, \qquad \mathrm{Im}(f^*) = \mathrm{Ker}(f)^\perp,$$

*and in particular* $f^*$ *is surjective if and only if* $f$ *is injective, and* $f^*$ *is injective if and only if* $f$ *is surjective.*

(2) *We have* $\mathrm{rank}(f) = \mathrm{rank}(f^*)$.

(3) *If* $V_1 = V_2$, *then a subspace* $W$ *of* $V_1$ *is stable for* $f$ *if and only if* $W^\perp$ *is stable for* $f^*$.

Proof. (1) To say that an element $v \in V_2$ belongs to $\mathrm{Ker}(f^*)$ is to say that, for all $w \in V_1$, we have

$$\langle v|f(w)\rangle = \langle f^*(v)|w\rangle = 0.$$

This means precisely that $v$ is orthogonal in $V_2$ to all vectors $f(w)$, i.e., that $v \in \mathrm{Im}(f)^\perp$.

If we then apply this property to $f^* : V_2 \to V_1$, we obtain $\mathrm{Ker}((f^*)^*) = \mathrm{Im}(f^*)^\perp$, or in other words $\mathrm{Ker}(f) = \mathrm{Im}(f^*)^\perp$. Computing the orthogonal and using Proposition 6.3.2 (3), we get $\mathrm{Ker}(f)^\perp = \mathrm{Im}(f^*)$.

From this we see that $f^*$ is injective if and only if $\mathrm{Im}(f)^\perp = 0$, which means (Proposition 6.3.2) if and only if $\mathrm{Im}(f) = V_2$, i.e., if $f$ is surjective. Similarly, $f^*$ is surjective if and only if $f$ is injective.

(2) We compute, using (1) and Proposition 6.3.2 (4), that

$$\begin{aligned}\mathrm{rank}(f^*) &= \dim(V_1) - \dim \mathrm{Ker}(f^*)\\ &= \dim(V_1) - \dim(\mathrm{Im}(f)^\perp) = \dim \mathrm{Im}(f) = \mathrm{rank}(f).\end{aligned}$$

(3) Since $V_1 = (V_1^\perp)^\perp$, we have $f(W) \subset W$ if and only if $f(W) \perp W^\perp$. Similarly, $f^*(W^\perp) \subset W^\perp$ if and only $f^*(W^\perp) \perp W$. But for $w_1 \in W$ and $w_2 \in W^\perp$, we have

$$\langle f(w_1)|w_2\rangle = \langle w_1|f^*(w_2)\rangle,$$

which shows that these two conditions are equivalent. ☐

Proposition 6.4.6. *Let $V_1$ and $V_2$ be finite-dimensional unitary spaces of dimension $n$ and $m$ respectively. Let $f\colon V_1 \to V_2$ be a linear map. Let $B_1 = (v_1, \ldots, v_n)$ be an ordered orthonormal basis of $V_1$ and $B_2 = (w_1, \ldots, w_m)$ an ordered orthonormal basis of $V_2$. We then have*

$$\mathrm{Mat}(f; B_1, B_2) = (\langle w_i|f(v_j)\rangle)_{\substack{1\leqslant i\leqslant \dim(V_2)\\ 1\leqslant j\leqslant \dim(V_1)}}.$$

*In particular, we have*

$$\mathrm{Mat}(f^*; B_2, B_1) = {}^t\overline{\mathrm{Mat}(f; B_1, B_2)}$$

*and if $V_1 = V_2$, the endomorphism $f$ is self-adjoint if and only if $\mathrm{Mat}(f; B_1, B_1)$ is hermitian.*

Note that this proposition *only* applied to orthornomal bases!

Proof. Write $\mathrm{Mat}(f; B_1, B_2) = (a_{ij})$ with $1 \leqslant i \leqslant m$ and $1 \leqslant j \leqslant n$. Then for $1 \leqslant j \leqslant n$, we have

$$f(v_j) = \sum_{i=1}^{m} a_{ij} w_i.$$

Since the basis $B_2$ is orthornomal, the coefficients $a_{ij}$ are therefore given by

$$a_{ij} = \langle w_i|f(v_j)\rangle$$

(see Proposition 6.3.2).

Similarly, the matrix $\mathrm{Mat}(f^*; B_2, B_1) = (b_{ji})$ has coefficients

$$b_{ji} = \langle v_j|f^*(w_i)\rangle = \langle f(v_j)|w_i\rangle = \bar{a}_{ij}.$$

This means that $\mathrm{Mat}(f^*; B_2, B_1) = {}^t\bar{A}$. ☐

The following definition is then useful:

Definition 6.4.7 (Adjoint matrix). Let $A \in M_{m,n}(\mathbf{C})$. The **adjoint matrix** is $A^* = {}^t\bar{A}$.

Note that

$$(A_1 + A_2)^* = A_1^* + A_2^*, \quad (tA)^* = \bar{t}A^*, \quad (AB)^* = B^*A^*$$
$$\det(A^*) = \overline{\det(A)}, \quad (A^*)^{-1} = (A^{-1})^*$$

if $A$ is invertible.

Corollary 6.4.8. *Let $V$ be a finite-dimensional unitary space and $f \in \mathrm{End}_{\mathbf{C}}(V)$. We have then $\det(f) = \overline{\det(f^*)}$.*

*If $A \in M_{n,n}(\mathbf{C})$, then $\det(A^*) = \overline{\det(A)}$.*

Proof. This follows from the proposition and the facts that $\det({}^tA) = \det(A)$ and $\det(\bar{A}) = \overline{\det(A)}$. ☐

## 6.5. Unitary endomorphisms

Definition 6.5.1 (Unitary transformation). Let $V$ be a unitary space. An endomorphism $f$ of $V$ is a **unitary transformation** if $f$ is an isomorphism and

$$\langle f(v)|f(w)\rangle = \langle v|w\rangle$$

for all $v$ and $w \in V$. The set of all unitary transformations of $V$ is denoted $\mathrm{U}(V)$ and called the **unitary group of** $V$. *It depends on the scalar product!*

If $V = \mathbf{C}^n$ with the standard scalar product, that we denote $\mathrm{U}_n(\mathbf{C})$ the set of all matrices $A$ such that $f_A$ is a unitary transformation of $V$; these are called **unitary matrices**.

Lemma 6.5.2. *Let $V$ be a finite-dimensional unitary space.*

(1) *An endomorphism $f$ of $V$ is a unitary transformation if and only if it is invertible and $f^{-1} = f^*$. If $f \in \mathrm{U}(V)$, then its determinant is a complex number of modulus 1.*

(2) *An endomorphism $f$ of $V$ is a unitary transformation if and only $\langle f(v)|f(w)\rangle = \langle v|w\rangle$ for all $v$ and $w \in V$.*

(3) *A matrix $A \in M_{n,n}(\mathbf{C})$ is unitary if and only if it is invertible and $A^{-1} = {}^t\bar{A}$, if and only if $A{}^t\bar{A} = {}^t\bar{A}A = 1_n$. We then have $|\det(A)| = 1$.*

(4) *Any unitary transformation is a normal endomorphism of $V$.*

Proof. (1) If $f$ is invertible, then it is a unitary transformation if and only if

$$\langle v|f^*f(w)\rangle = \langle v|w\rangle$$

for all $v$, $w \in V$. This condition is equivalent to $f^*f = \mathrm{Id}_V$. This is also equivalent with $f$ invertible with inverse $f^*$ (since $V$ is finite-dimensional).

If $f \in \mathrm{U}(V)$, we deduce that $\det(f)^{-1} = \det(f^{-1}) = \det(f^*) = \overline{\det(f)}$, which means that $|\det(f)| = 1$.

(2) It suffices to show that the condition $\langle f(v)|f(w)\rangle = \langle v|w\rangle$ implies that $f$ is invertible if $V$ is finite-dimensional. It implies in particular that $\|f(v)\|^2 = \|v\|^2$ for all $v \in V$. In particular, $f(v) = 0$ if and only if $v = 0$, so that $f$ is injective, and hence invertible since $V$ is finite-dimensional.

(3) The statement follows from (1) using Proposition 6.4.6.

(4) If $f$ is unitary, then we have $ff^* = f^*f = 1_n$, so $f$ is normal. ☐

Proposition 6.5.3. *Let $V$ be a unitary space.*

(1) *The identity 1 belongs to $\mathrm{U}(V)$; if $f$ and $g$ are elements of $\mathrm{U}(V)$, then the product $fg$ is also one. If $V$ is finite-dimensional, then all $f \in \mathrm{U}(V)$ are bijective and $f^{-1} = f^*$ belongs to $\mathrm{U}(V)$.*

(2) *If $f \in \mathrm{U}(V)$, then $d(f(v), f(w)) = d(v, w)$ for all $v$ and $w$ in $V$, and the angle between $f(v)$ and $f(w)$ is equal to the angle between $v$ and $w$.*

Proof. (1) It is elementary that $1 \in \mathrm{U}(V)$; if $f$ and $g$ are unitary transformations, then

$$\langle fg(v)|fg(w)\rangle = \langle f(g(v))|f(g(w))\rangle = \langle g(v)|g(w)\rangle = \langle v|w\rangle$$

for all $v$ and $w$ in $V$, so that $fg$ is unitary. If $f$ is unitary then $(f^{-1})^* = (f^*)^* = f = (f^{-1})^{-1}$ so that $f^*$ is unitary.

(2) is elementary from the definitions. ☐

Lemma 6.5.4. *Let $n \geqslant 1$. A matrix $A \in M_{n,n}(\mathbf{C})$ is unitary if and only if $A^*A = 1_n$, if and only if the column vectors of $A$ form an orthonormal basis of the unitary space $\mathbf{C}^n$ with the standard scalar product.*

Proof. We have already seen the first part. If $A \in M_{n,n}(\mathbf{C})$ is unitary, then the column vectors $C_i$ of $A$ satisfy

$$\langle C_i | C_j \rangle = \langle Ae_i | Ae_j \rangle = \langle e_i | e_j \rangle = \delta(i,j)$$

where $(e_1, \ldots, e_n)$ is the standard basis of $\mathbf{C}^n$. So these vectors form an orthonormal basis of $\mathbf{C}^n$.

Conversely, the condition $\langle C_i | C_j \rangle = \delta(i,j)$ means that $\langle Ae_i | Ae_j \rangle = \langle e_i | e_j \rangle$ for all $i$ and $j$, and using sesquilinearity we deduce that $f_A$ is a unitary transformation. $\square$

This allows us in particular to deduce the uniqueness in the Cholesky Decomposition (Corollary 6.2.7):

Corollary 6.5.5. *If $A \in M_{n,n}(\mathbf{C})$ is an upper-triangular matrix and is unitary, then $A$ is diagonal and its diagonal coefficients are complex numbers of modulus 1.*

Proof. Let $(e_1, \ldots, e_n)$ denote the standard basis of $\mathbf{C}^n$. Let $A = (a_{ij})$; we therefore have $a_{ij} = 0$ if $i > j$ since $A$ is upper-triangular. We will prove by induction on $i$, $1 \leqslant i \leqslant n$, that the $i$-column vector $C_i$ of $A$ is of the form $t_i e_i$ for some $t_i \in \mathbf{C}$ with $|t_i| = 1$, which for $i = n$ will establish the statement.

For $i = 1$, since $A$ is unitary, we have

$$1 = \|C_1\|^2 = |a_{11}|^2$$

since $a_{i1} = 0$ for all $i > 2$. This proves the desired property for $i = 1$. Now assume that $2 \leqslant i \leqslant n$, and that the property holds for $C_1, \ldots, C_{i-1}$. Since $A$ is unitary, we have

$$\langle C_j | C_i \rangle = 0$$

for $1 \leqslant j \leqslant i-1$. But the induction hypothesis shows that $C_j = t_j e_j$, and hence we obtain $\langle C_j | C_i \rangle = t_j a_{ji} = 0$ for $1 \leqslant j \leqslant i-1$. Since $t_j \neq 0$, it follows that $a_{ji} = 0$ for $j \leqslant i-1$, and with the vanishing for $j \geqslant i+1$, this means that $C_i = t_i e_i$ for some $t_i \in \mathbf{C}$. The conditions $\|C_i\|^2 = 1$ impliest that $|t_i| = 1$, which therefore concludes the induction step. $\square$

Proposition 6.5.6 (Complex QR or Iwasawa decomposition). *Let $A \in M_{n,n}(\mathbf{C})$ be any matrix. There exists a unitary matrix $Q \in \mathrm{U}_n(\mathbf{C})$ and an upper-triangular matrix $R$ such that $A = QR$.*

Proof. We prove this in the case where $A$ is invertible. Consider the matrix $T = A^*A = {}^t\bar{A}A$. It is hermitian. By the complex Cholesky decomposition (Corollary 6.2.7), there exists an upper-triangular matrix $R$ with positive diagonal coefficients such that $T = {}^t\bar{R}R$. This means that $R^*R = A^*A$. Since $R$ and $R^*$ are invertible, with the inverse of $R^*$ equal to $(R^{-1})^*$, we get

$$1_n = (AR^{-1})^* AR^{-1}.$$

This means that $Q = AR^{-1}$ is a unitary matrix. Consequently, we have $A = QR$ as claimed. $\square$

## 6.6. Normal and self-adjoint endomorphisms, II

Lemma 6.6.1. *Let $V$ be a finite-dimensional unitary space and let $f \in \mathrm{End}_{\mathbf{C}}(V)$ be a normal endomorphism. We have* $\mathrm{Ker}(f) = \mathrm{Ker}(f^*)$. *In particular, a complex number $\lambda$ is an eigenvalue of $f$ if and only if $\bar{\lambda}$ is an eigenvalue of $f^*$, and we have then* $\mathrm{Eig}_{\lambda,f} = \mathrm{Eig}_{\bar{\lambda},f^*}$.

Proof. The relation $\mathrm{Ker}(f) = \mathrm{Ker}(f^*)$ follows from Lemma 6.4.3. For any $\lambda \in \mathbf{C}$, the endomorphism $f - \lambda \cdot 1$ is also normal since

$$\begin{aligned}(f-\lambda\cdot 1)(f-\lambda\cdot 1)^* &= (f-\lambda\cdot 1)(f^*-\bar{\lambda}\cdot 1)\\ &= ff^* + |\lambda|^2\cdot 1 - \lambda f^* - \bar{\lambda} f\\ &= (f^*-\bar{\lambda}\cdot 1)(f-\lambda\cdot 1) = (f-\lambda\cdot 1)^*(f-\lambda\cdot 1).\end{aligned}$$

Therefore

$$\mathrm{Ker}(f-\lambda\cdot 1) = \mathrm{Ker}((f-\lambda\cdot 1)^*) = \mathrm{Ker}(f^*-\bar{\lambda}\cdot 1).$$

□

Proposition 6.6.2. *Let $V$ be a finite-dimensional unitary space and $f \in \mathrm{End}_{\mathbf{R}}(V)$ a normal endomorphism.*

(1) *The eigenspaces of $f$ are orthogonal to each other. In other, words, if $t_1 \neq t_2$ are eigenvalues of $f$, and $v_i \in \mathrm{Eig}_{t_i,f}$, then we have $\langle v_1|v_2\rangle = 0$.*

(2) *If $f$ is self-adjoint, then the eigenvalues of $f$ are real.*

(3) *If $f$ is unitary, then the eigenvalues of $f$ are complex numbers of modulus 1.*

Proof. (1) We may assume that $v_1$ and $v_2$ are non-zero. We then get

$$t_1\langle v_1|v_2\rangle = \langle f(v_1)|v_2\rangle = \langle v_1|f^*(v_2)\rangle = \langle v_1|\bar{t}_2 v_2\rangle = t_2\langle v_1|v_2\rangle,$$

since $v_2 \in \mathrm{Eig}_{\bar{t}_2,f^*}$ by the previous lemma. Since $t_1 \neq t_2$, it follows that $v_1 \perp v_2$.

(2) If $f$ is self-adjoint then we have $\mathrm{Ker}(f-\lambda\cdot 1) = \mathrm{Ker}(f-\bar{\lambda}\cdot 1)$ for any $\lambda \in \mathbf{C}$. If $\lambda$ is an eigenvalue and $v$ an eigenvector, then we get

$$f(v) = \lambda v = \bar{\lambda} v,$$

which means that $\lambda = \bar{\lambda}$, or equivalently that $\lambda \in \mathbf{R}$.

(3) If $f$ is unitary (hence normal), then if $\lambda$ is an eigenvalue of $f$ and $v$ a $\lambda$-eigenvector, then we have

$$v = f^*(f(v)) = f^*(\lambda v) = |\lambda|^2 v,$$

so that $|\lambda|^2 = 1$. □

Theorem 6.6.3 (Spectral theorem for normal endomorphisms). *Let $V$ be a finite-dimensional unitary space and $f \in \mathrm{End}_{\mathbf{C}}(V)$ a normal endomorphism. There exists an orthonormal basis $B$ of $V$ such that the elements of $B$ are eigenvectors of $f$; in particular, the endomorphism $f$ is diagonalizable.*

Proof of Theorem 6.6.3. We use induction on $n = \dim(V) \geqslant 1$. If $n = 1$, all linear maps are diagonal. Suppose now that $n \geqslant 2$ and that the result holds for normal endomorphisms of unitary vector spaces of dimension $\leqslant n-1$. Let $V$ be a unitary space of dimension $n$ and $f \in \mathrm{End}_{\mathbf{C}}(V)$ a normal endomorphism.

By Theorem 4.3.14, there exists an eigenvalue $t \in \mathbf{C}$ of $f$. Let $W = \mathrm{Eig}_{t,f} \subset V$ be the $t$-eigenspace of $f$. We then have $V = W \oplus W^\perp$ and $W^\perp$ is stable for $f$ since for $w_1 \in W^\perp$ and $w_2 \in W = \mathrm{Eig}_{\bar{t},f^*}$, we have

$$\langle f(w_1)|w_2\rangle = \langle w_1|f^*(w_2)\rangle = \bar{t}\langle w_1|w_2\rangle = 0.$$

Let $g\colon W^\perp \to W^\perp$ be the endomorphism induced by $f$ on $W^\perp$.

We claim that this is still a normal endomorphism of the unitary space $W^\perp$. Indeed, from Proposition 6.4.5 (3), the space $W^\perp$ is also stable under $f^*$. For $w_1$ and $w_2$ in $W^\perp$, we have

$$\langle w_1|g(w_2)\rangle = \langle w_1|f(w_2)\rangle = \langle f^*(w_1)|w_2\rangle.$$

Since $f^*(w_1) \in W^\perp$, this means that the adjoint of $g$ is the endomorphism induced by $f^*$ on $W^\perp$. Now since the scalar product on $W^\perp$ is the restriction of that of $V$, we have

$$\|g(w)\| = \|f(w)\| = \|f^*(w)\| = \|g^*(w)\|$$

for all $w \in W^\perp$, so that $g$ is normal.

Now we use the induction hypothesis: there is an orthonormal basis $B_1$ of eigenvectors of $g$ on $W^\perp$, and then if $B_0$ is an orthonormal basis of $W$, the basis $(B_0, B_1)$ is an orthonormal basis of $V$, and its elements are eigenvectors of $f$. $\square$

Corollary 6.6.4. *Let $A \in M_{n,n}(\mathbf{C})$ be a hermitian matrix. Then $A$ is diagonalizable, and there is a basis of eigenvectors which is an orthonormal basis of $\mathbf{C}^n$ for the standard unitary scalar product. Equivalently, there exists a unitary matrix $X$ such that $D = XAX^{-1} = XA^t\bar{X}$ is diagonal. If $A$ is hermitian, then the matrix $D$ has real coefficients. If $A$ is unitary, then the matrix $D$ has coefficients which are complex number of modulus 1.*

Remark 6.6.5. Be careful that if $A \in M_{n,n}(\mathbf{C})$ is *symmetric* then it is *not* always diagonalizable! An example is the matrix

$$A = \begin{pmatrix} 2 & i \\ i & 0 \end{pmatrix} \in M_{2,2}(\mathbf{C}),$$

which is symmetric but not diagonalizable, as one can easily check.

Example 6.6.6. For $t \in \mathbf{R}$, let

$$r(t) = \begin{pmatrix} \cos(t) & -\sin(t) \\ \sin(t) & \cos(t) \end{pmatrix} \in M_{2,2}(\mathbf{C}).$$

Then $r(t)$ is unitary, hence normal. Therefore we know that for any $t$, there exists an orthonormal basis $B$ of $\mathbf{C}^2$ such that $f_{r(t)}$ is represented by a diagonal matrix in the basis $B$. In fact, by computing the eigenvalues, we found the basis

$$B_0 = \left(\begin{pmatrix} 1 \\ i \end{pmatrix}, \begin{pmatrix} 1 \\ -i \end{pmatrix}\right)$$

of eigenvectors (see Example 4.2.11), with

$$r(t)v_1 = e^{-it}v_1, \qquad r(t)v_2 = e^{it}v_2.$$

This basis is orthogonal but not orthonormal; the associated orthonormal basis is $B = (v_1, v_2)$ where

$$v_1 = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ i \end{pmatrix}, \quad v_2 = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ -i \end{pmatrix}.$$

One notices here the remarkable fact that the basis $B$ is *independent* of $t$! This is explained by the next theorem, and by the fact that

$$r(t)r(s) = r(t+s) = r(s)r(t)$$

for all $s$ and $t \in \mathbf{R}$.

THEOREM 6.6.7 (Spectral theorem for families of commuting normal endomorphisms). *Let $V$ be a finite-dimensional unitary space and let $M \subset \mathrm{End}_{\mathbf{C}}(V)$ be any set of normal endomorphisms such that $fg = gf$ for all $f \in M$ and $g \in M$. There exists an orthonormal basis $B$ of $V$ such that the elements of $B$ are simultaneously eigenvectors of $f$ for* any *$f \in M$.*

PROOF. We will prove the statement by induction on $n = \dim(V)$. For $n = 1$, all linear maps are diagonal, so the statement is true. Assume now that $\dim(V) = n$ and that the result holds for all unitary spaces of dimension $\leqslant n - 1$.

If $M$ is empty, or if all elements of $M$ are of the form $f = t\mathrm{Id}$ for some $t \in \mathbf{C}$, then any orthonormal basis works. Otherwise, let $f_0 \in M$ be any fixed element which is not a multiple of the identity. Since $f_0$ is normal, there exists an orthonormal basis $B_0$ of eigenvectors of $f_0$ by Theorem 6.6.3. Let

$$t_1, \ldots, t_k$$

be the different eigenvalues of $f_0$, and $W_1, \ldots, W_k$ be the corresponding eigenspaces. We have then

$$V = W_1 \oplus \cdots \oplus W_k,$$

and the spaces $W_i$ are mutually orthogonal. The assumption on $f_0$ implies that $k \geqslant 2$ and that $\dim W_i \leqslant n - 1$ for all $i$.

For any $f \in M$ and $v \in W_i$, we get

$$f_0(f(v)) = f(f_0(v)) = t_i f(v),$$

so that $f(v) \in W_i$. Hence the restriction of $f$ to any $W_i$ is an endomorphism, denoted $f_i$, of $W_i$. Let $f_i^*$ be the adjoint of $f_i$ in $\mathrm{End}_{\mathbf{C}}(W_i)$. For

$$v = v_1 + \cdots + v_k, \quad v_i \in W_i, \text{ and} \quad w = w_1 + \cdots + w_k, \quad w_i \in W_i,$$

we compute

$$\begin{aligned}\langle f(v)|w\rangle &= \langle f_1(v_1) + \cdots + f_k(v_k)|w_1 + \cdots + w_k\rangle \\ &= \sum_{i,j}\langle f_i(v_i)|w_j\rangle = \sum_i \langle f_i(v_i)|w_i\rangle = \sum_i \langle v_i|f_i^*(w_i)\rangle,\end{aligned}$$

because $\langle f_i(v_i)|w_j\rangle = 0$ if $i \neq j$, by the orthogonality of the decomposition of $V$ into eigenspaces of $f_0$. This shows that

$$f^*(w) = \sum_i f_i^*(w_i).$$

In particular, the adjoint of $f$ restricted to $W_i$ is also an endomorphism (namely, $f_i^*$) of $W_i$. Since $f$ and $f^*$ commute, we deduce that for all $i$, $f_i$ is a normal endomorphism of $W_i$.

We conclude by induction (applied to the sets of normal endomorphisms $f|W_i$ of $W_i$ for $1 \leqslant i \leqslant k$) that the exist orthonormal bases $B_i$ of $W_i$ such that, for all $f \in M$, the restriction of $f$ to $W_i$ is represented by a diagonal matrix in the basis $B_i$.

Let finally $B = (B_1, \ldots, B_k)$. This is an orthonormal basis of $V$, and for every $f \in M$, the matrix $\mathrm{Mat}(f; B, B)$ is diagonal. ∎

COROLLARY 6.6.8. *Let $A = (a_{ij}) \in M_{n,n}(\mathbf{C})$ be a hermitian matrix. Then the sesquilinear form $b(x, y) = {}^t\bar{x}Ay$ is a scalar product if and only if, for $1 \leqslant k \leqslant n$, we have $\det(A_k) > 0$, where $A_k \in M_{k,k}(\mathbf{C})$ is the matrix defined by $A_k = (a_{ij})_{\substack{1\leqslant i\leqslant k\\ 1\leqslant j\leqslant k}}$.*

The matrices $A_k$ are called the "principal minors" of $A$.

Proof. Let $B = (v_1, \dots, v_n)$ be a basis of $\mathbf{R}^n$ formed of eigenvectors of $A$, with $Av_i = \lambda_i v_i$. Using the standard scalar product, we have

$$b(x, y) = \langle x | Ay \rangle$$

and therefore

$$b(v_i, v_j) = \lambda_i \delta(i, j).$$

It follows that $b$ is a scalar product if (and only if) the eigenvalues $\lambda_i$ are all $> 0$.

We now prove the "if" direction by induction with respect to $n$. For $n = 1$, the result is clear. Assume now that $n \geqslant 2$, and that the result holds for matrices of size $\leqslant n - 1$. Let $A$ be such that $\det(A_k) > 0$ for $1 \leqslant k \leqslant n$. By induction, the sesquilinear form defined by $A_{n-1}$ on $\mathbf{C}^{n-1}$ is a scalar product. The product of the eigenvalues is equal to the determinant of $A$, which is $\det(A_n) > 0$. Hence, all eigenvalues are non-zero, and if there is one eigenvalue $< 0$, then there is at least another one. Assume for instance that $\lambda_1 \neq \lambda_2$ are two eigenvalues $< 0$. The vectors $v_1$ and $v_2$ are linearly independent, so there exist $a$ and $b$ in $\mathbf{C}$, not both zero, such that $w = av_1 + bv_2 \in \mathbf{C}^n$ is a non-zero vector where the last coordinate is 0. Hence we can view $w$ as a non-zero element of $\mathbf{C}^{n-1}$. But then we have

$${}^t\bar{w} A_{n-1} w = {}^t\bar{w} A w = |a|^2 b(v_1, v_1) + |b|^2 b(v_2, v_2) = -|a|^2 - |b|^2 < 0,$$

and this contradicts the fact that $A_{n-1}$ defines a scalar product on $\mathbf{C}^{n-1}$. Therefore $A$ has only positive eigenvalues, and $b$ is a scalar product.

Conversely, assume that $b$ is a scalar product on $\mathbf{C}^n$. Then its restriction $b_k$ to the subspace $W_k$ generated by the first $k$ basis vectors of the standard basis is a scalar product. If we identify $W_k$ with $\mathbf{C}^k$, then we get

$$b_k(x, y) = {}^t\bar{x} A_k y$$

for all $x$, $y \in \mathbf{C}^k$. From the remarks at the beginning, we therefore have $\det(A_k) > 0$. □

Example 6.6.9. This criterion is convenient when $n$ is relatively small. For instance, the matrix

$$A = \begin{pmatrix} 2 & 3 & i \\ 3 & 5 & -1+i \\ -i & -1-i & 5 \end{pmatrix}$$

defines a scalar product since $2 > 0$, $10 - 9 > 0$ and the determinant of $A$ is $2 > 0$, but the matrix

$$A' = \begin{pmatrix} 2 & 3 & i \\ 3 & 3 & -1+i \\ -i & -1-i & 5 \end{pmatrix}$$

doesn't (because $\det(A'_2) = -3 < 0$).

## 6.7. Singular values decomposition, II

THEOREM 6.7.1 (Unitary Singular value or Cartan decomposition). *Let $V$ be a finite-dimensional unitary space and $f \in \mathrm{End}_{\mathbf{C}}(V)$. Let $n = \dim(V)$ and $r = \mathrm{rank}(f)$. There exist orthonormal bases*

$$B_1 = (v_1, \dots, v_n)$$
$$B_2 = (w_1, \dots, w_n)$$

*of $V$, possibly different, and $r$ strictly positive real numbers $\sigma_1$, ..., $\sigma_r$ such that for all $v \in V$, we have*

$$f(v) = \sum_{i=1}^{r} \sigma_i \langle v_i | v \rangle w_i.$$

*Equivalently we have $f(v_i) = \sigma_i w_i$ for $1 \leqslant i \leqslant r$ and $f(v_i) = 0$ for $i > r$, so that the matrix $\mathrm{Mat}(f; B_1, B_2)$ is diagonal with diagonal coefficients*

$$(\sigma_1, \dots, \sigma_r, 0, \dots, 0).$$

The numbers $\sigma_1$, ..., $\sigma_r$ are called the **singular values** of $f$. Up to ordering, they are uniquely defined.

PROOF. Consider the endomorphism $g = f^* f$ of $V$. Then $g^* = f^*(f^*)^* = f^* f$, so that $g$ is self-adjoint. Let $B_1 = (v_1, \dots, v_n)$ be an orthonormal basis of $V$ of eigenvectors of $g$, say $g(v_i) = \lambda_i v_i$ for $1 \leqslant i \leqslant n$. Because

$$\lambda_i \|v_i\|^2 = \langle g(v_i) | v_i \rangle = \langle f^*(f(v_i)) | v_i \rangle = \|f(v_i)\|^2,$$

the eigenvalues are $\geqslant 0$. We can order them so that the first $s$ eigenvalues are $> 0$, and the eigenvalues $\lambda_{s+1}$, ..., $\lambda_n$ are zero. We then see from the equation above that $f(v_i) = 0$ for $i > s$.

Let $v \in V$. We have

$$v = \sum_{i=1}^{n} \langle v_i | v \rangle v_i,$$

since the basis $B_1$ is orthonormal, hence

$$f(v) = \sum_{i=1}^{n} \langle v_i | v \rangle f(v_i) = f(v) = \sum_{i=1}^{s} \langle v_i | v \rangle f(v_i).$$

For $1 \leqslant i \leqslant s$ and $1 \leqslant j \leqslant s$, we have

$$\langle f(v_i) | f(v_j) \rangle = \langle g(v_i) | v_j \rangle = \lambda_i \langle v_i | v_j \rangle = \lambda_i \delta(i, j),$$

again because $B_1$ is an orthonormal basis. This means that if we define

$$w_i = \frac{1}{\sqrt{\lambda_i}} f(v_i)$$

for $1 \leqslant i \leqslant s$ (which is possible since $\lambda_i > 0$), then we have

$$\langle w_i | w_j \rangle = \delta(i, j).$$

Now we can write the formula for $f(v)$ in the form

$$f(v) = \sum_{i=1}^{s} \sqrt{\lambda_i} \langle v_i | v \rangle w_i.$$

This gives the desired result with $\sigma_i = \sqrt{\lambda_i}$ (completing the orthonormal set $(w_1, \dots, w_s)$ to an orthonormal basis $B_2$ of $V$).

Finally, the description shows that $\mathrm{Im}(f) \subset \langle\{w_1, \ldots, w_s\}\rangle$, and since $f(v_i) = \sigma_i w_i$, we have in fact equality. Since $(w_1, \ldots, w_s)$ are linearly independent (as they are orthonormal), it follows that $s = \dim \mathrm{Im}(f) = r$. ☐

Corollary 6.7.2. *Let $n \geqslant 1$ and let $A \in M_{n,n}(\mathbf{C})$. There exist unitary matrices $X_1$ and $X_2$ and a diagonal matrix $D \in M_{n,n}(\mathbf{C})$ with diagonal entries*

$$(\sigma_1, \ldots, \sigma_r, 0, \ldots, 0)$$

*where $\sigma_i > 0$ for $1 \leqslant i \leqslant r$, such that $A = X_1 D X_2$.*

Proof. This is the theorem applied to $f = f_A$ on $\mathbf{C}^n$ with the standard scalar product, the matrices $X_1$ and $X_2$ being the change of basis matrices from the standard basis to $B_1$ and $B_2$, which are orthogonal matrices since $B_1$ and $B_2$ are orthonormal bases. ☐

CHAPTER 7

# The Jordan normal form

## 7.1. Statement

The Jordan Normal Form of a matrix has a different form for different fields. The simplest is the case $\mathbf{K} = \mathbf{C}$, and we will state and prove the general result only in that case. However, some of the definitions make sense for any field, and we begin with these.

DEFINITION 7.1.1 (Jordan blocks). Let $n \geqslant 1$ and let $\lambda \in \mathbf{K}$. The Jordan block of size $n$ and eigenvalue $\lambda$ is the matrix

$$J_{n,\lambda} = \begin{pmatrix} \lambda & 1 & 0 & \cdots & \cdots \\ 0 & \lambda & 1 & & \vdots \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & \cdots & \cdots & \lambda & 1 \\ 0 & \cdots & \cdots & 0 & \lambda \end{pmatrix} \in M_{n,n}(\mathbf{K})$$

or in other words $J_{n,\lambda} = (a_{ij})$ with

$$a_{ii} = \lambda, \text{ for } 1 \leqslant i \leqslant n, \quad a_{i,i+1} = 1 \text{ for } 1 \leqslant i \leqslant n-1,$$

and $a_{i,j} = 0$ if $j \neq i$ and $j \neq i+1$.

EXAMPLE 7.1.2. For instance, for $\mathbf{K} = \mathbf{R}$, we have

$$J_{3,\pi} = \begin{pmatrix} \pi & 1 & 0 \\ 0 & \pi & 1 \\ 0 & 0 & \pi \end{pmatrix}, \qquad J_{4,0} = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix}.$$

Note that $\det(J_{n,\lambda}) = \lambda^n$ and $\mathrm{Tr}(J_{n,\lambda}) = n\lambda$.

LEMMA 7.1.3. (1) *The only eigenvalue of $J_{n,\lambda}$ is $\lambda$. Its geometric multiplicity is 1 and its algebraic multiplicity is $n$.*
(2) *We have $(J_{n,\lambda} - \lambda 1_n)^n = 0_{n,n}$.*

PROOF. (1) By computing a triangular determinant (Corollary 3.4.3), we have

$$\mathrm{char}_{J_{n,\lambda}}(t) = (t-\lambda)^n.$$

In particular, $\lambda$ is the unique eigenvalue of $J_{n,\lambda}$, and its algebraic multiplicity is $n$.

Let $v = (t_i)_{1 \leqslant i \leqslant n} \in \mathbf{K}^n$ be an eigenvector (for the eigenvalue $\lambda$) of $J_{n,\lambda}$. This means that $J_{n,\lambda} v = \lambda v$, which translates to the equations

$$\begin{cases} \lambda t_1 + t_2 & = \lambda t_1 \\ \lambda t_2 + t_3 & = \lambda t_2 \\ \quad\vdots & \quad\vdots \\ \lambda t_{n-1} + t_n & = \lambda t_{n-1} \\ \lambda t_n & = \lambda t_n \end{cases}$$

which means that $t_2 = \cdots = t_n = 0$. So $v$ is a multiple of the first standard basis vector. In particular, the $\lambda$-eigenspace is the one-dimensional space generated by this basis vector, so the geometric multiplicity of $\lambda$ is 1.

(2) By definition, we have $J_{n,\lambda} - \lambda 1_n = J_{n,0}$, so it suffices to prove that $J_{n,0}^n = 0$. But if $(e_1, \ldots, e_n)$ are the standard basis vectors of $\mathbf{K}^n$, we have

$$J_{n,0}e_1 = 0, \quad J_{n,0}e_i = e_{i-1} \text{ for } 1 \leqslant i \leqslant n.$$

Therefore $J_{n,0}^2 e_2 = J_{n,0}e_1 = 0$, and by induction we get $J_{n,0}^i e_i = 0$ for $1 \leqslant i \leqslant n$. Then

$$J_{n,0}^n e_i = J_{n,0}^{n-i} J_{n,0}^i e_i = 0$$

for $1 \leqslant i \leqslant n$, so that $J_{n,0}^n$ is the zero matrix. □

The following lemma describes what Jordan blocks "mean" as endomorphisms; another interpretation is given below in Example 10.3.13.

LEMMA 7.1.4. *Let $V$ be a finite-dimensional $\mathbf{K}$-vector space of dimension $n \geqslant 1$ and $f \in \mathrm{End}_{\mathbf{K}}(V)$. Let $\lambda \in \mathbf{K}$. Then there exists an ordered basis $B$ of $V$ such that $\mathrm{Mat}(f; B, B) = J_{n,\lambda}$ if and only if there exists a vector $v \in V$ such that $(f - \lambda \cdot 1)^n(v) = 0$ and*

$$B = ((f - \lambda \cdot 1)^{n-1}(v), (f - \lambda \cdot 1)^{n-2}(v), \ldots, (f - \lambda \cdot 1)(v), v).$$

PROOF. We denote $g = f - \lambda \cdot 1 \in \mathrm{End}_{\mathbf{K}}(V)$. First assume that there exists $v$ such that $(g^{n-1}(v), g^{n-2}(v), \ldots, v)$ is an ordered basis of $V$ and $g^n(v) = 0$. Then we get

$$\begin{aligned} \mathrm{Mat}(f; B, B) - \lambda \cdot 1_n &= \mathrm{Mat}(f - \lambda \cdot 1; B, B) \\ &= \mathrm{Mat}(g; B, B) = J_{n,0} \end{aligned}$$

and so $\mathrm{Mat}(f; B, B) = J_{n,0} + \lambda \cdot 1_n = J_{n,\lambda}$.

Conversely, if $\mathrm{Mat}(f; B, B) = J_{n,\lambda}$, then we have $\mathrm{Mat}(g; B, B) = J_{n,0}$. If we denote $B = (v_1, \ldots, v_n)$, this means that

$$g(v_1) = 0, \quad g(v_2) = v_1, \quad \cdots \quad g(v_n) = v_{n-1},$$

and hence it follows that

$$v_{n-1} = g(v_n), \quad \cdots \quad v_1 = g^{n-1}(v_n), \quad g^n(v_n) = 0.$$

which gives the result with $v = v_n$. □

DEFINITION 7.1.5 (Sums of Jordan blocks). Let $k \geqslant 1$ be an integer, and let $n_1, \ldots, n_k$ be positive integers and $\lambda_1, \ldots, \lambda_k$ complex numbers. Let $n$ be the sum of the $n_i$'s. We denote by

$$J_{n_1,\lambda_1} \boxplus J_{n_2,\lambda_2} \boxplus \cdots \boxplus J_{n_k,\lambda_k}$$

the matrix $A \in M_{n,n}(\mathbf{K})$ which is block diagonal with the indicated Jordan blocks:

$$A = \begin{pmatrix} J_{n_1,\lambda_1} & 0 & 0 & \cdots & \cdots \\ 0 & J_{n_2,\lambda_2} & 0 & & \vdots \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & \cdots & \cdots & J_{n_{k-1},\lambda_{k-1}} & 0 \\ 0 & \cdots & \cdots & 0 & J_{n_k,\lambda_k} \end{pmatrix}.$$

Lemma 7.1.6. *Let*

$$A = J_{n_1,\lambda_1} \boxplus J_{n_2,\lambda_2} \boxplus \cdots \boxplus J_{n_k,\lambda_k}.$$

*The spectrum of $A$ is $\{\lambda_1, \ldots, \lambda_k\}$; the geometric multiplicity of an eigenvalue $\lambda$ is the number of indices $i$ such that $\lambda_i = \lambda$, and the algebraic multiplicity is the sum of the $n_i$ for these indices.*

*In particular, the matrix $A$ is diagonalizable if and only if $k = n$ and $n_i = 1$ for all $i$.*

Proof. This follows from Lemma 7.1.3. To be more precise, since $A$ is upper-triangular, we have

$$\mathrm{char}_A(t) = \prod_{i=1}^{k} (t - \lambda_i)^{n_i},$$

so the set of eigenvalues is $\{\lambda_1, \ldots, \lambda_k\}$, and the algebraic multiplicity of one eigenvalue $\lambda$ is the sum of the $n_i$ where $\lambda_i = \lambda$.

To compute the geometric multiplicity of $\lambda$, we decompose $\mathbf{C}^n = V_1 \oplus \cdots \oplus V_k$, where $V_i$ is generated by the standard basis vectors $B_i$ corresponding to the $i$-th Jordan block, then $V_i$ is invariant under $f_A$. Hence, for $v = v_1 + \cdots + v_k$ with $v_i \in V_i$, we have

$$f(v_1 + \cdots + v_k) = \lambda(v_1 + \cdots + v_k)$$

if and only if $f(v_i) = \lambda v_i$ for all $i$. Since the restriction of $f$ to $V_i$ has matrix $J_{n_i,\lambda_i}$ with respect to $B_i$, Lemma 7.1.3 shows that $v_i = 0$ unless $\lambda = \lambda_i$, and that the corresponding vector $v_i$ is then determined up to multiplication by an element of $\mathbf{K}$. ☐

Example 7.1.7. For instance, for $\mathbf{K} = \mathbf{R}$, we have

$$J_{3,\pi} \boxplus J_{1,\pi} \boxplus J_{2,0} = \begin{pmatrix} \pi & 1 & 0 & 0 & 0 & 0 \\ 0 & \pi & 1 & 0 & 0 & 0 \\ 0 & 0 & \pi & 0 & 0 & 0 \\ 0 & 0 & 0 & \pi & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

This has eigenvalues $\pi$ and 0; the geometric multiplicity of $\pi$ is 2 (there are two Jordan blocks for the eigenvalue $\pi$), and the algebraic multiplicity is 4; the geometric multiplicity of 0 is 1 (there is one Jordan block for the eigenvalue 0), and the algebraic multiplicity is 2.

Now we can state the Jordan Normal Form for complex matrices:

Theorem 7.1.8 (Complex Jordan Normal Form). *Let $n \geqslant 1$ and $A \in M_{n,n}(\mathbf{C})$. There exists $k \geqslant 1$ and integers $n_1, \ldots, n_k \geqslant 1$ with $n = n_1 + \cdots + n_k$, and there exist complex numbers $\lambda_1, \ldots, \lambda_k$ such that $A$ is similar to the matrix*

$$J_{n_1,\lambda_1} \boxplus J_{n_2,\lambda_2} \boxplus \cdots \boxplus J_{n_k,\lambda_k}.$$

*In particular, $A$ is diagonalizable if and only if $k = n$.*

*Equivalently, if $V$ is a finite-dimensional $\mathbf{C}$-vector space of dimension $n \geqslant 1$ and $f \in \mathrm{End}_{\mathbf{C}}(V)$, then there exist an ordered basis $B$ of $V$, an integer $k \geqslant 1$, integers $n_1, \ldots, n_k \geqslant 1$ with $n = n_1 + \cdots + n_k$, and complex numbers $\lambda_1, \ldots, \lambda_k$ such that*

$$\mathrm{Mat}(f; B, B) = J_{n_1,\lambda_1} \boxplus J_{n_2,\lambda_2} \boxplus \cdots \boxplus J_{n_k,\lambda_k}.$$

This will be proved in the next section. For the moment, we present some applications:

Corollary 7.1.9 (Cayley-Hamilton Theorem). *Let $n \geqslant 1$ and let $A \in M_{n,n}(\mathbf{C})$. Write*

$$\mathrm{char}_A(t) = t^n + a_{n-1}t^{n-1} + \cdots + a_1 t + a_0.$$

*Then we have*

$$A^n + a_{n-1}A^{n-1} + \cdots + a_1 A + a_0 1_n = 0_n.$$

This theorem is in fact valid for any field $\mathbf{K}$. (Indeed, for $\mathbf{K} = \mathbf{Q}$ or $\mathbf{K} = \mathbf{R}$, it suffices to view $A$ as a complex matrix to get the result.)

For any field $\mathbf{K}$, any polynomial $P = \sum_i c_i X^i \in \mathbf{K}[X]$ and any matrix $A \in M_{n,n}(\mathbf{K})$, we denote

$$P(A) = \sum_i c_i A^i.$$

Lemma 7.1.10. *For any polynomials $P$ and $Q$ in $\mathbf{K}[X]$ and any $A \in M_{n,n}(\mathbf{K})$, we have $(P+Q)(A) = P(A) + Q(A)$ and $(PQ)(A) = P(A)Q(A) = Q(A)P(A)$. Moreover, if $X$ is an invertible matrix and $B = XAX^{-1}$, then $P(B) = XP(A)X^{-1}$.*

Proof. The first property follows immediately from the definition. For the second, write

$$P = \sum_i c_i X^i, \qquad Q = \sum_j d_j X^j.$$

Then

$$PQ = \sum_{i,j} c_i d_j X^{i+j}.$$

Similarly, we have

$$P(A) = \sum_i c_i A^i, \qquad Q(A) = \sum_j d_j A^j,$$

and computing the product using the rule $A^{i+j} = A^i A^j$, we find

$$(PQ)(A) = \sum_{i,j} c_i d_j A^{i+j} = P(A)Q(A).$$

Finally, for any $i \geqslant 0$, we first check (for instance by induction on $i$) that

$$XA^iX^{-1} = (XAX^{-1})\cdots(XAX^{-1}) = (XAX^{-1})^i.$$

Then using linearity, it follows that $P(XAX^{-1}) = XP(A)X^{-1}$ for any polynomial $P \in \mathbf{K}[X]$. ∎

Proof of the Cayley-Hamilton Theorem. Since $P(XAX^{-1}) = XP(A)X^{-1}$ and $\mathrm{char}_A = \mathrm{char}_{XAX^{-1}}$ for any invertible matrix $X$ (similar matrices have the same characteristic polynomial), we may assume using Theorem 7.1.8 that $A$ is in Jordan Normal Form, namely

$$A = J_{n_1,\lambda_1} \boxplus J_{n_2,\lambda_2} \boxplus \cdots \boxplus J_{n_k,\lambda_k},$$

for some $k \geqslant 1$, integers $(n_i)$ and complex numbers $(\lambda_i)$. We then have

$$P(A) = (A - \lambda_1)^{n_1} \cdots (A - \lambda_k)^{n_k}.$$

For any $i$ with $1 \leqslant i \leqslant k$, we can reorder the product so that

$$P(A) = (A - \lambda_1 \cdot 1)^{n_1} \cdots (A - \lambda_{i-1} \cdot 1)^{n_{i-1}} \\ (A - \lambda_{i+1} \cdot 1)^{n_{i+1}} \cdots (A - \lambda_k)^{n_k} (A - \lambda_i \cdot 1)^{n_i}.$$

Let $i$ be an integer with $1 \leqslant i \leqslant k$. For the standard basis vectors $v$ corresponding to the block $J_{n_i,\lambda_i}$, namely

$$v = e_j \text{ where } n_1 + \cdots + n_{i-1} < j \leqslant n_1 + \cdots + n_i,$$

we have

$$P(A)v = (A - \lambda_1 \cdot 1)^{n_1} \cdots (A - \lambda_{i-1} \cdot 1)^{n_{i-1}}$$
$$(A - \lambda_{i+1} \cdot 1)^{n_{i+1}} \cdots (A - \lambda_k \cdot 1)^{n_k} ((A - \lambda_i \cdot 1)^{n_i} v) = 0,$$

by Lemma 7.1.3 (2). Therefore the matrix $P(A)$ has all columns zero, which means that $P(A) = 0$. ☐

EXAMPLE 7.1.11. Let $n \geqslant 1$ and let $A \in M_{n,n}(\mathbf{C})$ with

$$\mathrm{char}_A(t) = t^n + a_{n-1}t^{n-1} + \cdots + a_1 t + a_0.$$

If $a_0 = (-1)^n \det(A) \neq 0$, it follows from the Cayley-Hamilton Theorem that

$$1_n = -\frac{1}{a_0}(A^n + a_{n-1}A^{n-1} + \cdots + a_1 A) = AB$$

where $B = -a_0^{-1}(A^{n-1} + a_{n-1}A^{n-2} + \cdots + a_1 1_n)$. Hence $B$ is the inverse of $A$ (but in practice this is not very convenient to compute it!) For $n = 2$, since

$$\mathrm{char}_A(t) = t^2 - \mathrm{Tr}(A)t + \det(A),$$

this gives the formula

$$A^{-1} = -\frac{1}{\det(A)}(A - \mathrm{Tr}(A)1_2)$$

for an invertible matrix in $M_{2,2}(\mathbf{C})$, which can of course be checked directly.

REMARK 7.1.12. A common idea to prove the Cayley-Hamilton Theorem is to write $\mathrm{char}_A(A) = \det(A - A) = \det(0) = 0$. This does not work! One reason is that it is not allowed to mix numbers, like determinants, and matrices ($\mathrm{char}_A(A)$ is a matrix), in this manner. To see this concretely, consider the following question: for a matrix

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_{2,2}(\mathbf{C}),$$

define $q(A) = ad + bc$. Then there exists a polynomial $P_A(t)$ such that

$$q(t1_2 - A) = P_A(t),$$

namely

$$P_A(t) = (t - a)(t - d) + bc = t^2 - (a + d)t + ad + bc.$$

*If* the naive argument for the Cayley-Hamilton Theorem was correct, one should also expect that $P_A(A) = q_A(A - A) = 0$. But this almost never true! For instance, when

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

one checks that $P_A(t) = t^2 - 4t + 5$, and that $P_A(A) = \begin{pmatrix} 4 & 0 \\ 0 & 4 \end{pmatrix}$.

COROLLARY 7.1.13. *Let $n \geqslant 1$ and let $A \in M_{n,n}(\mathbf{C})$. Then $A$ and ${}^tA$ are similar.*

PROOF. We first see that this property is true when $A = J_{n,\lambda}$ is a Jordan block: the matrix of $f_A$ in the basis $(e_n, e_{n-1}, \ldots, e_1)$ of $\mathbf{C}^n$ is the transpose of $J_{\lambda,n}$.

Now we reduce to this case. By Theorem 7.1.8, there exists an invertible matrix $X \in M_{n.n}(\mathbf{C})$ such that $XAX^{-1} = C$, where

$$C = J_{n_1,\lambda_1} \boxplus J_{n_2,\lambda_2} \boxplus \cdots \boxplus J_{n_k,\lambda_k}$$

for some integer $k \geqslant 1$, integers $n_i \geqslant 1$, and complex numbers $\lambda_i$. For each $i$, we can find an invertible matrix $X_i$ in $M_{n_i,n_i}(\mathbf{C})$ such that

$$X_i J_{n_i,\lambda_i} X_i^{-1} = {}^t J_{n_i,\lambda_i},$$

since (as we saw at the beginning) a Jordan block is similar to its transpose. Then the block diagonal matrix

$$Y = \begin{pmatrix} X_1 & 0 & \cdots & 0 \\ 0 & X_2 & \cdots & 0 \\ \vdots & & \vdots & \\ 0 & \cdots & 0 & X_k \end{pmatrix}$$

satisfies $YCY^{-1} = {}^tC$. This means that

$$YXAX^{-1}Y^{-1} = {}^tXAX^{-1} = {}^tX^{-1t}A^tX,$$

and therefore ${}^tA = ZAZ^{-1}$ with $Z = {}^tXYX$. Hence $A$ is similar to ${}^tA$. ☐

The final two applications concern the exponential of a complex matrix. Recall from analysis that for any $n \geqslant 1$ and any $A \in M_{n,n}(\mathbf{C})$, the series

$$\sum_{j=0}^{+\infty} \frac{1}{j!} A^j$$

converges, in the sense that all coefficients converge, to a matrix $\exp(A)$ called the *exponential* of $A$.

Since the multiplication of matrices is continuous, for any invertible matrix $X \in M_{n,n}(\mathbf{C})$, we have

$$X\exp(A)X^{-1} = \sum_{j=0}^{+\infty} \frac{1}{j!} XA^jX^{-1} = \sum_{j=0}^{+\infty} \frac{1}{j!} (XAX^{-1})^j = \exp(XAX^{-1}). \tag{7.1}$$

PROPOSITION 7.1.14. *Let $n \geqslant 1$ and let $A \in M_{n,n}(\mathbf{C})$. The exponential of $A$ is invertible, and in fact we have* $\det(\exp(A)) = \exp(\mathrm{Tr}(A))$.

PROOF. The formula (7.1) shows that $\det(\exp(A)) = \det(\exp(XAX^{-1}))$. By Theorem 7.1.8, using a suitable $X$, we reduce to the case

$$A = J_{n_1,\lambda_1} \boxplus J_{n_2,\lambda_2} \boxplus \cdots \boxplus J_{n_k,\lambda_k}.$$

This matrix is upper-triangular with diagonal coefficients

$$\lambda_1 \text{ repeated } n_1 \text{ times}, \ldots, \lambda_k \text{ repeated } n_k \text{ times}$$

Hence, for any $j \geqslant 0$, the matrix $A^j$ is upper-triangular with diagonal coefficients

$$\lambda_1^j \text{ repeated } n_1 \text{ times}, \ldots, \lambda_k^j \text{ repeated } n_k \text{ times}.$$

Summing over $k$, this means that $\exp(A)$ is upper-triangular with diagonal coefficients

$$e^{\lambda_1} \text{ repeated } n_1 \text{ times}, \ldots, e^{\lambda_k} \text{ repeated } n_k \text{ times}.$$

Hence

$$\det(A) = (e^{\lambda_1})^{n_1} \cdots (e^{\lambda_k})^{n_k} = e^{n_1\lambda_1 + \cdots + n_k\lambda_k} = \exp(\mathrm{Tr}(A)).$$

∎

Finally, we sketch a proof of the following fact:

PROPOSITION 7.1.15. *Let $n \geqslant 1$ be an integer. The exponential on $M_{n,n}(\mathbf{C})$ has image equal to the set of* invertible *matrices. In other words, for any invertible matrix $A \in M_{n,n}(\mathbf{C})$, there exists a matrix $L \in M_{n,n}(\mathbf{C})$ such that* $\exp(L) = A$.

SKETCH OF PROOF. Because of (7.1) and Theorem 7.1.8, it suffices to show that if

$$A = J_{n_1,\lambda_1} \boxplus J_{n_2,\lambda_2} \boxplus \cdots \boxplus J_{n_k,\lambda_k},$$

with $\lambda_i \neq 0$ for all $i$, then $A = \exp(L)$ for some matrix $L$. If we note further that the exponential of a block-diagonal matrix

$$L = \begin{pmatrix} L_1 & 0 & \cdots & 0 \\ 0 & L_2 & \cdots & 0 \\ \vdots & & \vdots & \\ 0 & \cdots & 0 & L_k \end{pmatrix}$$

with $L_i \in M_{n_i,n_i}(\mathbf{C})$ is

$$\exp(L) = \begin{pmatrix} \exp(L_1) & 0 & \cdots & 0 \\ 0 & \exp(L_2) & \cdots & 0 \\ \vdots & & \vdots & \\ 0 & \cdots & 0 & \exp(L_k) \end{pmatrix},$$

it is sufficient to prove that any Jordan block $J_{n,\lambda}$ with $\lambda \neq 0$ is the exponential of some matrix.

We only check that this is true for $n \leqslant 3$, the general case requiring some more algebraic details. For $n = 1$, this is because any non-zero complex number is the exponential of some complex number. For $n = 2$, one computes

$$\exp\Bigl(\begin{pmatrix} a & t \\ 0 & a \end{pmatrix}\Bigr) = \begin{pmatrix} e^a & e^a t \\ 0 & e^a \end{pmatrix},$$

and hence for $\lambda \neq 0$, writing $\lambda = \exp(z)$ for some $z \in \mathbf{C}$, we have

$$J_{2,\lambda} = \exp\Bigl(\begin{pmatrix} z & \lambda^{-1} \\ 0 & z \end{pmatrix}\Bigr).$$

For $n = 3$, similarly, we have

$$\exp\Bigl(\begin{pmatrix} a & t_1 & t_2 \\ 0 & a & t_3 \\ 0 & 0 & a \end{pmatrix}\Bigr) = \begin{pmatrix} e^a & e^a t_1 & e^a(t_3 + t_1 t_2/2) \\ 0 & e^a & e^a t_3 \\ 0 & 0 & e^a \end{pmatrix}$$

(to see this, it is useful to know that $\exp(A_1 + A_2) = \exp(A_1)\exp(A_2)$ if $A_1$ and $A_2$ commute; apply this $A_1 = a1_3$ and $A_2$ the upper-triangular matrix with zero diagonal). So in that case, we get

$$J_{3,\lambda} = \exp\Bigl(\begin{pmatrix} z & \lambda^{-1} & -(2\lambda^2)^{-1} \\ 0 & z & \lambda^{-1} \\ 0 & 0 & z \end{pmatrix}\Bigr).$$

∎

## 7.2. Proof of the Jordan normal form

A first key observation is that a Jordan block $J_{n,\lambda}$ has the property that $J_{n,\lambda} - \lambda 1_n$ is a *nilpotent* matrix with $(J_{n,\lambda} - \lambda 1_n)^n = 0$. This implies that in a matrix

$$A = J_{n_1,\lambda_1} \boxplus J_{n_2,\lambda_2} \boxplus \cdots \boxplus J_{n_k,\lambda_k},$$

any vector $v \in \mathbf{C}^n$ which is a linear combination the basis vectors corresponding to the block $J_{n_i,\lambda_i}$ verifies

$$(A - \lambda_i 1_n)^{n_i} v = 0$$

So these vectors are not quite eigenvectors (which would be the case $n_i = 1$), but they are not very far from that. We will find the Jordan decomposition by looking for such vectors.

Definition 7.2.1 (Generalized eigenspace). Let $V$ be a $\mathbf{K}$-vector space and $t \in \mathbf{K}$. Let $f$ be an endomorphism of $V$. The $t$**-generalized eigenspace** of $f$ is the union over $k \geqslant 0$ of the kernel of $(f - t \cdot 1)^k$.

The crucial properties of generalized eigenspaces are the following facts, where one should note that the second is *not* true of the eigenspace:

Lemma 7.2.2. *Let $V$ be a $\mathbf{K}$-vector space and $t \in \mathbf{K}$. Let $f$ be an endomorphism of $V$.*

(1) *The $t$-generalized eigenspace $W$ of $f$ is a subspace of $V$ that is stable for $f$.*

(2) *If $v \in V$ is such that $f(v) - tv \in W$, then we have $v \in W$. In other words, $(f - t \cdot 1)^{-1}(W) \subset W$.*

(3) *The $t$-generalized eigenspace is non-zero if and only if $t$ is an eigenvalue of $f$.*

Proof. (1) Let $W$ be the $t$-generalized eigenspace of $f$. It is immediate from the definition that if $t \in \mathbf{K}$ and $v \in W$, then $tv \in W$. Now let $v_1$ and $v_2$ be elements of $W$. There exist $k_1 \geqslant 0$ and $k_2 \geqslant 0$ such that $(f - t \cdot 1)^{k_1}(v_1) = 0$ and $(f - t \cdot 1)^{k_2}(v_2) = 0$. Let $k$ be the maximum of $k_1$ and $k_2$. Then we have

$$(f - t \cdot 1)^k(v_1) = (f - t \cdot 1)^k(v_2) = 0,$$

and by linearity we get

$$(f - t \cdot 1)^k(v_1 + v_2) = 0.$$

This shows that $W$ is a vector subspace of $V$.

Let $v \in W$ and $k \geqslant 0$ be such that $(f - t \cdot 1)^k(v) = 0$. Let $w = f(v)$. We then have

$$(f - t \cdot 1)^k(w) = (f - t \cdot 1)^k((f - t \cdot 1)(v)) + t(f - t \cdot 1)^k(v) = (f - t \cdot 1)^{k+1}(v) = 0.$$

Hence $w = f(v) \in W$, which means that $W$ is $f$-invariant.

(2) Assume that $f(v) - tv \in W$. Let $k \geqslant 0$ be such that $(f - t \cdot 1)^k(f(v) - tv) = 0$. Then

$$(f - t \cdot 1)^{k+1}(v) = (f - t \cdot 1)^k(f(v) - tv) = 0,$$

so that $v \in W$.

(3) If $t$ is an eigenvalue of $f$, then any eigenvector is a non-zero element of the $t$-generalized eigenspace. Conversely, suppose that there exists a vector $v \neq 0$ and an integer $k \geqslant 1$ such that

$$(f - \lambda \cdot 1)^k(v) = 0.$$

We may assume that $k$ is the smallest positive integer with this property. Then for $w = (f - \lambda \cdot 1)^{k-1}(v)$, which is non-zero because of this condition, we have $(f - \lambda \cdot 1)(w) = 0$, so that $w$ is a $t$-eigenvector of $f$. $\square$

The next result is the Jordan Normal Form in the special case of a nilpotent endomorphism. Its proof is, in fact, the most complicated part of the proof of Theorem 7.1.8, but it is valid for any field.

Proposition 7.2.3. *Let $n \geqslant 1$. Let $V$ be an $n$-dimensional $\mathbf{K}$-vector space and let $f \in \operatorname{End}_{\mathbf{K}}(V)$ be a nilpotent endomorphism of $V$. There exists an integer $k \geqslant 1$, integers $n_1, \ldots, n_k \geqslant 1$ with $n = n_1 + \cdots + n_k$ and a basis $B$ of $V$ such that*

$$\operatorname{Mat}(f; B, B) = J_{n_1,0} \boxplus \cdots \boxplus J_{n_k,0}.$$

Example 7.2.4. For instance, if $m = 5$, and $k = 3$ with $n_1 = 3$, $n_2 = n_3 = 1$, then we get the matrix

$$J_{3,0} \boxplus J_{1,0} \boxplus J_{1,0} = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

We give two proofs of Proposition 7.2.3 – one is more abstract (using subspaces and linear maps), but slightly shorter, while the second is more concrete (using vectors and constructing a suitable basis "by hand"), but slightly longer.

First proof of Proposition 7.2.3. Let $d \geqslant 0$ be the integer such that $f^d = 0$ but $f^{d-1} \neq 0$. We may assume that $d \geqslant 2$ (otherwise we get $f = 0$, this has matrix $J_{1,0} \boxplus \cdots \boxplus J_{1,0}$ in any basis).

Then we have an increasing sequence of subspaces of $V$ given by the kernels $W_i = \operatorname{Ker}(f^i)$ of the successive powers of $f$:

$$\{0\} = \operatorname{Ker}(f^0) \subset \operatorname{Ker}(f) \subset \cdots \subset \operatorname{Ker}(f^i) \subset \cdots \subset \operatorname{Ker}(f^d) = V.$$

Note that $W_i \neq W_{i+1}$ for $0 \leqslant i \leqslant d-1$: indeed, for any $v \in V$, we have $f^{d-(i+1)}(v) \in W_{i+1}$ since $f^d(v) = 0$, and if $W_{i+1} = W_i$, it follows that $f^i f^{d-(i+1)}(v) = 0$, which means that $f^{d-1} = 0$. For any $i$, we have also $f(W_i) \subset W_{i-1}$.

Using these properties, we will construct by induction on $i$ with $1 \leqslant i \leqslant d$, a sequence of direct sum decompositions

$$V = \tilde{W}_{d-1} \oplus \cdots \oplus \tilde{W}_{d-i} \oplus W_{d-i}, \tag{7.2}$$

such that, for $d - i \leqslant j \leqslant d-1$, we have

(1) the space $\tilde{W}_j$ is a subspace of $W_{j+1}$ and $\tilde{W}_j \cap W_j = \{0\}$;
(2) the restriction of $f$ to $\tilde{W}_j$ is injective;
(3) the image $f(\tilde{W}_j)$ lies in $\tilde{W}_{j-1}$ if $j > d-i$, while $f(\tilde{W}_{d-i}) \subset W_{d-i}$

(note that these conditions are not independent; but some parts are useful for the conclusion, and others better adapted to the inductive construction).

Let us first explain how this leads to the Jordan form of $f$. For $i = d$, we have $W_0 = \{0\}$, and we get the decomposition

$$V = \tilde{W}_{d-1} \oplus \cdots \oplus \tilde{W}_0, \tag{7.3}$$

such that (by Conditions (2) and (3)) the restrictions of $f$ are injective linear maps

$$\tilde{W}_{d-1} \xrightarrow{f} \tilde{W}_{d-2} \xrightarrow{f} \cdots \xrightarrow{f} \tilde{W}_1 \xrightarrow{f} \tilde{W}_0.$$

We then construct a basis $B$ of $V$ as follows:

- Let $B_{d-1}$ be a basis of $\tilde{W}_{d-1}$;

- The set $f(B_{d-1})$ is linearly independent in $\tilde{W}_{d-2}$, since $f$ is injective restricted to $\tilde{W}_{d-1}$; let $B_{d-2}$ be vectors such that $(f(B_{d-1}), B_{d-2})$ is a basis of $\tilde{W}_{d-2}$, so that
$$(B_{d-1}, f(B_{d-1}), B_{d-2})$$
is a basis of $\tilde{W}_{d-1} \oplus \tilde{W}_{d-2}$;
- The vectors in $(f^2(B_{d-1}), f(B_{d-2}))$ are linearly independent in $\tilde{W}_{d-3}$, since $f$ is injective restricted to $\tilde{W}_{d-2}$; let $B_{d-3}$ be vectors such that $(f^2(B_{d-1}), f(B_{d-2}), B_{d-3})$ is a basis of $\tilde{W}_{d-3}$, so that
$$(B_{d-1}, f(B_{d-1}), f^2(B_{d-1}), B_{d-2}, f(B_{d-2}), B_{d-3})$$
is a basis of $\tilde{W}_{d-1} \oplus \tilde{W}_{d-2}$;
- Inductively, we construct similarly $B_{d-1}, \dots, B_0$ linearly independent vectors in $\tilde{W}_{d-1}, \dots, \tilde{W}_0$, such that
$$B = (B_{d-1}, f(B_{d-1}), \dots, f^{d-1}(B_{d-1}), B_{d-2}, \dots, f^{d-2}(B_{d-2}), \cdots, B_1, f(B_1), B_0)$$
is a basis of $V$.

Finally, for any $i \geqslant 1$ and for any basis vector $v$ of $B_{d-i}$, consider the vectors
$$(f^{d-i}(v), \dots, f(v), v)$$
which are all basis vectors of $B$. These generate a subspace of $V$ that is invariant under $f$: indeed, it suffices to check that $f(f^{d-i}(v)) = 0$, and this holds because $v \in \tilde{W}_{d-i} \subset W_{d-i+1} = \mathrm{Ker}(f^{d-i+1})$ (see Condition (1)).

The matrix of $f$ restricted to the subspace generated by
$$(f^{d-i}(v), \dots, f(v), v)$$
is $J_{0,d-i+1}$ (see Lemma 7.1.4). If we reorder the basis $B$ by putting such blocks of vectors one after the other, the matrix of $f$ with respect to $B$ will be in Jordan Normal Form.

This concludes the proof of Proposition 7.2.3, up to the existence of the decompositions (7.2). We now establish this by induction on $i$. For $i = 1$, we select $\tilde{W}_{d-1}$ as any complement of $W_{d-1}$ in $W_d = V$, so that $V = \tilde{W}_{d-1} \oplus W_{d-1}$. This gives the direct sum decomposition and Condition (1). The image of $\tilde{W}_{d-1}$ is then a subspace of $W_{d-1}$ (Condition (3)), and the kernel of the restriction of $f$ to $\tilde{W}_{d-1}$ is then $W_1 \cap \tilde{W}_{d-1} \subset W_{d-1} \cap \tilde{W}_{d-1} = \{0\}$, which gives Condition (2) (recall that we assumed that $d \geqslant 2$, so $1 \leqslant d-1$).

Suppose now that $i \leqslant d$ and that we have constructed
$$V = \tilde{W}_{d-1} \oplus \cdots \oplus \tilde{W}_{d-(i-1)} \oplus W_{d-(i-1)}, \tag{7.4}$$
satisfying the desired properties. The image $F = f(\tilde{W}_{d-(i-1)})$ and the subspace $W_{d-i}$ are both contained in $W_{d-(i-1)}$. Moreover, we have $F \cap W_{d-i} = \{0\}$: indeed, if $v \in F \cap W_{d-i}$, then we can write $v = f(w)$ with $w \in \tilde{W}_{d-(i-1)}$. Then $f^{d-(i-1)}(w) = f^{d-i}(v) = 0$ and therefore $w \in \tilde{W}_{d-(i-1)} \cap W_{d-(i-1)} = \{0\}$ (by induction from Condition (1) for (7.4)), so $v = 0$.

Hence $F$ and $W_{d-i}$ are in direct sum. We define $\tilde{W}_{d-i}$ to be any complement of $W_{d-i}$ in $W_{d-(i-1)}$ that contains $F$. Condition (1) holds since $\tilde{W}_{d-i} \subset W_{d-(i-1)}$ and $\tilde{W}_{d-i} \cap W_{d-i} = \{0\}$. From
$$W_{d-(i-1)} = \tilde{W}_{d-i} \oplus W_{d-i},$$
and (7.4), we get the further decomposition
$$V = \tilde{W}_{d-1} \oplus \cdots \oplus \tilde{W}_{d-i} \oplus W_{d-i}.$$

The linear map $f$ sends $\tilde{W}_{d-(i-1)}$ to $F \subset \tilde{W}_{d-i}$ by construction. Since $f$ sends also $\tilde{W}_{d-i} \subset W_{d-(i-1)}$ to $W_{d-i}$, we obtain Condition (3).

To conclude, we check Condition (2). First, since $\tilde{W}_{d-1}, \ldots, \tilde{W}_{d-(i-1)}$ are unchanged, the induction hypothesis implies that the restriction of $f$ to $\tilde{W}_j$ is injective for $d-(i-1) \leqslant j \leqslant d-1$. And finally, for $j = d-i$, the kernel of the restriction of $f$ to $\tilde{W}_{d-i}$ is

$$\operatorname{Ker}(f) \cap \tilde{W}_{d-i} = W_1 \cap \tilde{W}_{d-i} \subset W_{d-(i-1)} \cap \tilde{W}_{d-i} = \{0\}$$

by construction. □

Second proof of Proposition 7.2.3. The idea is to identify vectors that are associated to the Jordan blocks as in Lemma 7.1.4, and the difficulty is that they are not unique in general. The basic observation that we use is that each block $J_{n_i,0}$ must correspond to a single vector in $\operatorname{Ker}(f)$, up to multiplication by an element of $\mathbf{K}$. We will then start from a basis of $\operatorname{Ker}(f)$, and construct the blocks carefully "backwards".

To be precise, for a vector $v \neq 0$ in $V$, define the *height* $\mathrm{H}(v)$ of $v$ as the largest integer $m \geqslant 0$ such that there exists $w \in V$ with $f^m(w) = v$ (so that $m = 0$ corresponds to the case $w = v$, i.e., $v$ does not belong to the image of $f$). This is finite, and indeed $\mathrm{H}(v) \leqslant n-1$ because we know that $f^n = 0$ (Proposition 4.4.6).

Note that if $\mathrm{H}(v) = h$ and $f^h(w) = v$, then we have $f^i(w) = 0$ for all $i > h$, and also $\mathrm{H}(f^i(w)) = i$ for $0 \leqslant i \leqslant h$. Moreover, if $f$ is the linear map on $\mathbf{K}^n$ corresponding to a Jordan block $J_{n,0}$, then the first standard basis vector $e_1$ of $\mathbf{K}^n$ satisfies $\mathrm{H}(e_1) = n-1$ (since $e_1 = f^{n-1}(e_n)$), and is (up to multiplication by non-zero elements of $\mathbf{K}$) the only vector with this height, all others having height $\leqslant n-2$ (because $f^n = 0$). Therefore we can try to "recover" the size of a Jordan block from the heights of vectors.

Let $k = \dim \operatorname{Ker}(f)$. Let then $(v_1, \ldots, v_k)$ be a basis of $\operatorname{Ker}(f)$ chosen so that the sum

$$\sum_{i=1}^{k} \mathrm{H}(v_i)$$

of the heights of the basis vectors is *as large as possible* – this is possible because the set of possible sums of this type is a finite set of integers (since the height of a non-zero vector is finite). For $1 \leqslant i \leqslant k$, let $n_i = \mathrm{H}(v_i) \geqslant 0$ and let $w_i \in V$ be such that $f^{n_i}(w_i) = v_i$. Since $f$ is nilpotent, we know that the vectors

$$B_i = (f^{n_i}(w_i), f^{n_i-1}(w_i), \ldots, f(w_i), w_i)$$

are linearly independent (Proposition 4.4.6). Let $W_i$ be the $(n_i+1)$-dimensional subspace of $V$ with basis $B_i$. We may re-order the vectors $(v_i)$ to ensure that

$$n_1 \geqslant n_2 \geqslant \cdots \geqslant n_k \geqslant 1.$$

We first claim that the vectors in $B = (B_1, \ldots, B_k)$ are linearly independent (in particular, the spaces $W_1, \ldots, W_k$ are in direct sum). To see this, note that these vectors are $f^{n_i-j}(w_i)$ for $1 \leqslant i \leqslant k$ and $0 \leqslant j \leqslant n_i$. Let $t_{ij}$ be elements of $\mathbf{K}$ such that

$$\sum_{i=1}^{k} \sum_{j=0}^{n_i} t_{i,j} f^{n_i-j}(w_i) = 0. \tag{7.5}$$

We apply $f^{n_1}$ to the identity (7.5); since $f^{n_1+n_i-j}(w_i) = 0$ unless $n_i - j = 0$ and $n_i = n_1$, the resulting formula is

$$\sum_{\substack{1 \leqslant i \leqslant k \\ n_i = n_1}} t_{i,n_1} v_i = 0.$$

Since $(v_i)$ is a basis of $\mathrm{Ker}(f)$, this means that $t_{i,n_i} = 0$ whenever $n_i = n_1$. Now apply $f^{n_1-1}$ to (7.5); the vanishing of $t_{i,n_i}$ when $n_i = n_1$ shows that the resulting equation is

$$\sum_{\substack{1\leqslant i\leqslant k\\ n_i\geqslant n_1-1}} t_{i,n_1-1}v_i = 0,$$

and hence $t_{i,n_1-1} = 0$ whenever $n_1 - 1 \leqslant n_i$. Iterating, we obtain $t_{i,n_1-l} = 0$ whenever $n_1 - l \leqslant n_i$, and in the end, it follows that $t_{i,j} = 0$ for all $i$ and $j$.

Now we claim that the direct sum $W$ of the spaces $W_1, \dots, W_k$ is equal to $V$. This will conclude the proof of the proposition, since the matrix of $f$ with respect to $(B_1, \dots, B_k)$ is simply

$$J_{n_1+1,0} \boxplus \cdots \boxplus J_{n_k+1,0}.$$

To prove the claim, we will show by induction on $r \geqslant 1$ that $\mathrm{Ker}(f^r) \subset W$. Since $f$ is nilpotent, this will imply that $V \subset W$ by taking $r$ large enough (indeed, $r = n$ is enough, according to Proposition 4.4.6).

For $r = 1$, we have $\mathrm{Ker}(f) \subset W$ by construction, so we assume that $r > 1$ and that $\mathrm{Ker}(f^{r-1}) \subset W$.

We first decompose $W$ in two parts: we have

$$W = E \oplus F$$

where $E$ is the space generated by $(w_1, \dots, w_k)$, and $F$ is the space generated by $f^j(w_i)$ with $1 \leqslant i \leqslant k$ and $1 \leqslant j < n_i$. Note that $F$ is contained in $f(W)$, since all its basis vectors are in $f(W)$. On the other hand, we claim that $E \cap \mathrm{Im}(f) = \{0\}$. If this is true, then we conclude that $\mathrm{Ker}(f^r) \subset W$ as follows: let $v \in \mathrm{Ker}(f^r)$; then $f(v)$ belongs to $\mathrm{Ker}(f^{r-1})$. By induction, $f(v)$ therefore belongs to $W$. Now write $f(v) = w_1 + w_2$ with $w_1 \in E$ and $w_2 \in F$. By the first observation about $F$, there exists $w_3 \in W$ such that $f(w_3) = w_2$. Then $w_1 = f(v - w_3) \in E \cap \mathrm{Im}(f)$, so that $w_1 = 0$. Therefore $v - w_3 \in \mathrm{Ker}(f) \subset W$, so that $v = (v - w_3) + w_3 \in W$.

We now check the claim. Assume that there exists $v \neq 0$ in $E \cap \mathrm{Im}(f)$. Then there exists $w \in V$ such that

$$f(w) = v = t_1w_1 + \cdots + t_kw_k$$

with $t_i \in \mathbf{K}$ not all zero. Let $j$ be the smallest integer with $t_j \neq 0$, so that

$$f(w) = v = t_jw_j + \cdots + t_kw_k.$$

Applying $f^{n_j}$, we get

$$f^{n_j+1}(w) = f^{n_j}(v) = t_jv_j + \cdots + t_lv_l \neq 0, \tag{7.6}$$

where $l \geqslant j$ is the integer such that $n_j = \cdots = n_l$ and $n_{l+1} < n_l$. But then the vectors $(v_i)_{i\neq j}$, together with $v'_j = f^{n_j+1}(w)$, form another basis of $\mathrm{Ker}(f)$: the formula (7.6) shows that $v'_j \in \mathrm{Ker}(f)$ and that

$$v_j = \frac{1}{t_j}(v'_j - t_{j+1}v_{j+1} - \cdots t_lv_l),$$

so that these $k$ vectors generate $\mathrm{Ker}(f)$. Since $v'_j = f^{n_j+1}(w)$, we have $mathrmH(v'_j) \geqslant n_j + 1$. Hence the sum of the heights of the elements of this new basis is strictly larger than $n_1 + \cdots + n_k$. This contradicts our choice of the basis $(v_1, \dots, v_k)$ of $\mathrm{Ker}(f)$, and therefore concludes the proof that $E \cap \mathrm{Im}(f) = \{0\}$. ☐

The second lemma is also valid for any field.

Lemma 7.2.5. *Let $V$ be a $\mathbf{K}$-vector space. Let $f$ be an endomorphism of $V$. The generalized eigenspaces of $f$ are linearly independent.*

Proof. Let $\lambda_1, \ldots, \lambda_k$ be the distinct eigenvalues of $f$ and $V_i$ the $\lambda_i$-generalized eigenspace. Let $n_i \geqslant 1$ be such that $V_i = \mathrm{Ker}((f - \lambda_i \cdot 1)^{n_i})$. Suppose $v_i \in V_i$ are elements such that

$$v_1 + \cdots + v_k = 0.$$

Fix $i$ with $1 \leqslant i \leqslant n$. Consider then the endomorphism

$$g_i = (f - \lambda_1 \cdot 1)^{n_1} \cdots (f - \lambda_{i-1} \cdot 1)^{n_{i-1}} (f - \lambda_{i+1} \cdot 1)^{n_{i+1}} \cdots (f - \lambda_k \cdot 1)^k \in \mathrm{End}_{\mathbf{K}}(V)$$

(omitting the factor with $\lambda_i$). Since the factors $f - \lambda_i$ commute, we can rearrange the order of the composition as we wish, and it follows that for $j \neq i$, we have $g_i(v_j) = 0$. On the other hand, since $V_i$ is stable under $f$ (Lemma 7.2.2 (1)), it is stable under $g_i$, and since none of the $\lambda_j$, $j \neq i$, is a generalized eigenvalue of $f|V_i$, the restriction of $g_i$ to $V_i$ is invertible as an endomorphism of $V_i$. Since applying $g_i$ to the equation above gives

$$g_i(v_i) = 0,$$

we deduce that $v_i = 0$. Since this holds for all $i$, it follows that the generalized eigenspaces are linearly independent. ☐

Using these lemmas, we can now conclude the proof:

Proof of Theorem 7.1.8. Let $\lambda_1, \ldots, \lambda_k$ be the distinct eigenvalues of $f$ and $V_i$ the $\lambda_i$-generalized eigenspace. Let

$$W = V_1 \oplus \cdots \oplus V_k,$$

where the sum is direct by the previous lemma. By Proposition 7.2.3 applied to the restriction of $f - \lambda_i$ to $V_i$, which is nilpotent, there exist integers $k_i \geqslant 1$, integers $n_{i,1}$, $\ldots n_{1,k_i} \geqslant 1$ with $n_{i,1} + \cdots + n_{i,k} = \dim V_i$ and a basis $B_i$ of $V_i$ such that

$$\mathrm{Mat}(f|V_i; B_i, B_i) = J_{n_{i,1},\lambda_i} \boxplus \cdots \boxplus J_{n_{i,k_i},\lambda_i}.$$

Therefore the restriction of $f$ to the stable subspace $W$ has a Jordan Normal Form decomposition in the basis $(B_1, \ldots, B_k)$ of $W$. The proof will be finished by proving that $W = V$.

Suppose that $W \neq V$. Then we can find a complement $\tilde{W}$ of $W$ in $V$ with $\dim(\tilde{W}) \geqslant 1$. Consider the projection $p$ on $\tilde{W}$ parallel to $W$ and the endomorphism $\tilde{f} = p \circ (f|\tilde{W})$ of $\tilde{W}$. By Theorem 4.3.14, since $\dim(\tilde{W}) \geqslant 1$ and we are considering $\mathbf{C}$-vector spaces, there exists an eigenvalue $\lambda \in \mathbf{C}$ of $\tilde{f}$. Let $v \in \tilde{W}$ be an eigenvector of $\tilde{f}$ with respect to $\lambda$. The condition $\tilde{f}(v) = \lambda v$ means that

$$f(v) = \lambda v + w$$

where $w \in \mathrm{Ker}(p) = W$. Therefore

$$w = \sum_{i=1}^{k} w_i,$$

where $w_i \in V_i$. Define $g = f - \lambda \cdot 1$, so that

$$g(v) = \sum_{i=1}^{k} w_i.$$

For any $i$ such that $\lambda_i \neq \lambda$, the restriction of $g = f - \lambda \cdot 1$ to $V_i$ is invertible so there exists $v_i \in V_i$ such that $g(v_i) = w_i$. If this is the case for all $i$, then we get

$$g\Big(v - \sum_{i=1}^{k} v_i\Big) = 0,$$

which means that the vector

$$v - \sum_{i=1}^{k} v_i$$

is in $\mathrm{Ker}(g) = \mathrm{Ker}(f - \lambda \cdot 1) = \{0\}$. This would mean $v \in W$, which is a contradiction.

So there exists $i$ such that $\lambda_i = \lambda$, and we may assume that $\lambda = \lambda_1$ by reordering the spaces $V_i$ if needed. Then $g = f - \lambda_1 \cdot 1$, and we get

$$g\Big(v - \sum_{i=2}^{k} v_i\Big) = g(v_1) \in V_1.$$

But then

$$g^{n_1}\Big(v - \sum_{i=2}^{k} v_i\Big) = g^{n_1}(v_1) = 0,$$

which means by definition of generalized eigenspaces that

$$v - \sum_{i=2}^{k} v_i \in V_1,$$

so $v \in W$, again a contradiction. ☐

Example 7.2.6. How does one compute the Jordan Normal Form of a matrix $A$, whose existence is ensured by Theorem 7.1.8? There are two aspects of the question: (1) either one is looking "only" for the invariants $k$, $\lambda_1$, ..., $\lambda_k$ and $n_1$, ..., $n_k$; or (2) one wants also to find the change of basis matrix $X$ such that $XAX^{-1}$ is in Jordan Normal Form.

The first problem can often be solved, for small values of $n$ at least, by simple computations that use the fact there the number of possibilities for $k$ and the integers $n_i$ is small. The second requires more care. We will illustrate this with one example of each question.

(1) Assume that we have a matrix $A \in M_{7,7}(\mathbf{C})$, and we compute the characteristic polynomial to be $\mathrm{char}_A(t) = (t - i)^4(t + 2)^2(t - \pi)$. We can then determine the Jordan Normal Form (without computing a precise change of basis) by arguing for each eigenvalue $\lambda$ in turn, and determining the "part" of the Jordan Normal Form involving only $\lambda$:

- For the eigenvalue $\lambda = \pi$, the algebraic and geometric multiplicities are 1, and therefore the corresponding contribution is $J_{1,\pi}$.
- For the eigenvalue $\lambda = -2$, there are two possibilities: either $J_{2,-2}$ or $J_{1,-2} \boxplus J_{1,-2}$; they can be distinguished by computing the eigenspace $\mathrm{Eig}_{-2,A}$: the first case corresponds to a 1-dimensional eigenspace, and the second to a 2-dimensional eigenspace (since each Jordan block brings a one-dimensional eigenspace).
- For the eigenvalue $\lambda = i$, there are more possibilities, as follows:

$$J_{4,i}, \quad J_{3,i} \boxplus J_{1,i}, \quad J_{2,i} \boxplus J_{2,i}, \quad J_{2,i} \boxplus J_{1,i} \boxplus J_{1,i}, \quad J_{1,i} \boxplus J_{1,i} \boxplus J_{1,i} \boxplus J_{1,i}.$$

  Most can be distinguished using the dimension of $\mathrm{Eig}_{i,A}$, which is, respectively

$$1, \quad 2, \quad 2, \quad 3, \quad 4.$$

- If the $i$-eigenspace has dimension 2, we can distinguish between $J_{3,i} \boxplus J_{1,i}$ and $J_{2,i} \boxplus J_{2,i}$ by the dimension of the kernel of $(A - i1_n)^2$: it is 3 for the first case, and 4 for the second case.

(2) Now we discuss the actual computation of the Jordan Normal Form together with the associated basis. Besides general remarks, we apply it to the matrix

$$A = \begin{pmatrix} 3 & 1 & -3 & 0 & 0 \\ 0 & -2 & 16 & 0 & 0 \\ 0 & -1 & 6 & 0 & 0 \\ 2 & -3 & 14 & 2 & 1 \\ 0 & 0 & 0 & 0 & 2 \end{pmatrix} \in M_{5,5}(\mathbf{C}). \tag{7.7}$$

We use the following steps:

- We compute the characteristic polynomial $P$ of $A$ and factor it, in the form

$$P(t) = \prod_{j=1}^{m} (t - \lambda_j)^{m_j}$$

where the $\lambda_j$ are *distinct* complex numbers, and $m_j \geqslant 1$ is the algebraic multiplicity of $\lambda_j$ as eigenvalue of $A$.

For the matrix $A$ of (7.7), we find

$$P = (t-2)^4(t-3).$$

- For each eigenvalue $\lambda$, we compute $\mathrm{Eig}_{\lambda,A}$; its dimension is the number of Jordan blocks of $A$ with eigenvalue $\lambda$; if the dimension is equal to the algebraic multiplicity, then a basis of corresponding eigenvectors gives the Jordan blocks

$$J_{1,\lambda} \boxplus \cdots \boxplus J_{1,\lambda}.$$

Here, $\lambda = 3$ is an eigenvalue with geometric and algebraic multiplicity 1, so the corresponding Jordan block is $J_{1,3}$. Solving the linear system $Av = 3v$ (which we leave as an exercise) gives the basis vector

$$v_1 = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 2 \\ 0 \end{pmatrix}$$

of $\mathrm{Eig}_{3,A}$.

- To determine further the Jordan blocks with eigenvalue $\lambda$, if needed, we compute the successive matrices $(A - \lambda \cdot 1_n)^k$ for $k = 2, \ldots,$ and their kernels. When these stabilize, we have found the $\lambda$-generalized eigenspace. We can then either exploit the small number of possibilities (see below for an example), or else use the construction in the first proof of Proposition 7.2.3 for $A - \lambda \cdot 1_n$ to find a basis of the generalized eigenspace in which the matrix has a Jordan decomposition.

For our example, if $\lambda = 2$, the possibilities for the Jordan blocks are

$$J_{4,2}, \quad J_{3,2} \boxplus J_{1,2}, \quad J_{2,2} \boxplus J_{2,2}, \quad J_{2,2} \boxplus J_{1,2} \boxplus J_{1,2}, \quad J_{1,2} \boxplus J_{1,2} \boxplus J_{1,2} \boxplus J_{1,2}.$$

We solve the linear system $Av = 2v$ using the REF method for $(A - 2 \cdot 1_5)v = 0$. Since

$$A - 2 \cdot 1_5 = \begin{pmatrix} 1 & 1 & -3 & 0 & 0 \\ 0 & -4 & 16 & 0 & 0 \\ 0 & -1 & 4 & 0 & 0 \\ 2 & -3 & 14 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}, \tag{7.8}$$

we forget the last row which is identically zero. The reduction (where we exchange rows at some point to avoid denominators) goes:

$$A - 2 \cdot 1_5 \rightsquigarrow \begin{array}{r} R_1 \\ R_2 \\ R_3 \\ R_4 - 2R_1 \end{array} \begin{pmatrix} 1 & 1 & -3 & 0 & 0 \\ 0 & -4 & 16 & 0 & 0 \\ 0 & -1 & 4 & 0 & 0 \\ 0 & -5 & 20 & 0 & 1 \end{pmatrix} \rightsquigarrow \begin{array}{r} R_1 \\ R_3 \\ R_2 \\ R_4 \end{array} \begin{pmatrix} 1 & 1 & -3 & 0 & 0 \\ 0 & -1 & 4 & 0 & 0 \\ 0 & -4 & 16 & 0 & 0 \\ 0 & -5 & 20 & 0 & 1 \end{pmatrix}$$

$$\rightsquigarrow \begin{array}{r} R_1 \\ R_2 \\ R_3 - 4R_2 \\ R_4 - 5R_2 \end{array} \begin{pmatrix} 1 & 1 & -3 & 0 & 0 \\ 0 & -1 & 4 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix} \rightsquigarrow \begin{array}{r} R_1 \\ R_2 \\ R_4 \\ R_3 \end{array} \begin{pmatrix} 1 & 1 & -3 & 0 & 0 \\ 0 & -1 & 4 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

If we now use Theorem 2.10.12, we see that $\dim \mathrm{Eig}_{2,A} = 2$, with basis vectors

$$v_2 = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} = e_4, \qquad v_3 = \begin{pmatrix} -1 \\ 4 \\ 1 \\ 0 \\ 0 \end{pmatrix}$$

(the fourth and third columns of the REF matrix are the free columns). As a check, note that it is indeed clear from the form of $A$ that $e_4$ is an eigenvector for the eigenvalue 2.

This shows in particular that the only possibilities for the Jordan blocks are

$$J_{3,2} \boxplus J_{1,2}, \qquad J_{2,2} \boxplus J_{2,2}.$$

To go further, we compute the kernel of $(A - 2 \cdot 1_5)^2$, since we know (see the discussion above) that its dimension will distinguish between the two possibilities. We compute

$$(A - 2 \cdot 1_5)^2 = \begin{pmatrix} 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 2 & 0 & 2 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

It is clear that the rank of this matrix is 1, so its kernel $W$ has dimension 4. Indeed, a basis is

$$(f_1, f_2, f_3, f_4) = (e_1 - e_3, e_2, e_4, e_5)$$

in terms of the standard basis vectors. Since the kernel has dimension 4, it is in fact the generalized eigenspace for the eigenvalue 2, which confirms that the corresponding Jordan blocks are $J_{2,2} \boxplus J_{2,2}$. There only remains to find a suitable basis where these Jordan blocks appear.

For the block associated to $v_2 = e_4$, this means we must find a vector $w_2$ in $W$ with $(A - 2 \cdot 1_5)w_2 = v_2$. Looking at $A - 2 \cdot 1_5$ (namely (7.8)), we see that we can take $w_2 = e_5$, which is indeed in $W_2$.

For the block associated to $v_3$, we must find $w_3 \in W$ with $(A - 2 \cdot 1_5)w_3 = v_3$. Writing

$$w_3 = af_1 + bf_2 + cf_3 + df_4,$$

we compute

$$(A - 2 \cdot 1_5)w_3 = \begin{pmatrix} 4a + b \\ -16a - 4b \\ -4a - b \\ -12a - 3b + d \\ 0 \end{pmatrix}$$

To satisfy $(A - 2 \cdot 1_5)w_3 = v_3$, the equations become

$$\begin{cases} 4a + b = -1 \\ -12a - 3b + d = 0 \end{cases}$$

(the others following from these two). These equation are satisfied if and only if $d = -3$ and $4a + b = -1$. Hence, a suitable choice is

$$w_3 = -f_2 - 3f_4 = \begin{pmatrix} 0 \\ -1 \\ 0 \\ 0 \\ -3 \end{pmatrix}.$$

In conclusion, if we take the basis

$$B = (v_1, v_2, w_2, v_3, w_3) = \left( \begin{pmatrix} 1 \\ 0 \\ 0 \\ 2 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}, \begin{pmatrix} -1 \\ 4 \\ 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ -1 \\ 0 \\ 0 \\ -3 \end{pmatrix} \right)$$

of $\mathbf{C}^5$, then the matrix of $f_A$ with respect to $B$ is the Jordan Normal Form matrix

$$J_{1,3} \boxplus J_{2,2} \boxplus J_{2,2}.$$

CHAPTER 8

# Duality

In this short chapter, we consider an important "duality" between vector spaces and linear maps. In particular, this is the theoretic explanation of the transpose of a matrix and of its properties.

In this chapter, $\mathbf{K}$ is an arbitrary field.

## 8.1. Dual space and dual basis

DEFINITION 8.1.1 (Dual space; linear form). Let $V$ be a $\mathbf{K}$-vector space. The **dual space** $V^*$ of $V$ is the space $\mathrm{Hom}_{\mathbf{K}}(V, \mathbf{K})$ of linear maps from $V$ to $\mathbf{K}$. An element of $V^*$ is called a **linear form** on $V$.

If $V$ is finite-dimensional, then $V^*$ is also finite dimensional, and $\dim(V^*) = \dim(V)$, and in particular, $V^*$ is isomorphic to $V$. *This is not true for infinite-dimensional spaces.*

Let $\lambda \in V^*$ be a linear form and $v \in V$. It is often convenient to use the notation

$$\langle \lambda, v \rangle = \lambda(v)$$

for the value of $\lambda$ at the vector $v$.

EXAMPLE 8.1.2. (1) Let $V = \mathbf{K}^n$ for some $n \geqslant 1$. For $1 \leqslant j \leqslant n$, let $\lambda_j$ be the $j$-th coordinate map $(t_i)_{1 \leqslant i \leqslant n} \mapsto t_j$; then $\lambda_j$ is a linear form on $V$, hence an element of $V^*$. More generally, if $s_1$, $\ldots$, $s_n$ are elements of $\mathbf{K}$, the map

$$(t_i) \mapsto s_1 t_1 + \cdots + s_n t_n$$

is an element of $V^*$. In fact, all linear forms on $\mathbf{K}^n$ are of this type: this linear form is the unique linear map $V \to \mathbf{K}$ such that the standard basis vector $e_i$ is mapped to $s_i$.

(2) Let $V = M_{n,n}(\mathbf{K})$. Then the trace is an element of $V^*$; similarly, for any finite-dimensional vector space $V$, the trace is an element of $\mathrm{End}_{\mathbf{K}}(V)^*$.

(3) Let $V = \mathbf{K}[X]$ be the space of polynomials with coefficients in $\mathbf{K}$. For any $t_0 \in \mathbf{K}$, the map $P \mapsto P(t_0)$ is a linear form on $V$. Similarly, the map $P \mapsto P'(t_0)$ is a linear form.

(4) Let $V$ be a vector space and let $B$ be a basis of $V$. Let $v_0$ be an element of $B$. For any $v \in V$, we can express $v$ uniquely as a linear combination of the vectors in $B$; let $\lambda(v)$ be the coefficient of $v_0$ in this representation (which may of course be 0):

$$v = \lambda(v) v_0 + w,$$

where $w$ is a linear combination of the vectors of $B' = B - \{v_0\}$. Then $\lambda$ is an element of $V^*$, called the **$v_0$-coordinate linear form associated to** $B$. Indeed, if $v_1$ and $v_2$ are elements of $V$ such that

$$v_i = \lambda(v_i) v_0 + w_i,$$

with $w_i$ a linear combination of the vectors in $B'$, then we get

$$t v_1 + s v_2 = (t\lambda(v_1) + s\lambda(v_2)) v_0 + (t w_1 + s w_2),$$

where $tw_1 + sw_2$ also belongs to $\langle B' \rangle$, which means that

$$\lambda(tv_1 + sv_2) = t\lambda(v_1) + s\lambda(v_2).$$

Note that $\lambda$ depends not only on $v_0$, but on all of $B$.

(5) Let $V = \mathbf{K}[X]$. Consider the basis $B = (X^i)_{i \geqslant 0}$ of $V$. Then for $i \geqslant 0$, the $X^i$-coordinate linear form associated to $B$ is the linear form that maps a polynomial $P$ to the coefficient of $X^i$ in the representation of $P$ as a sum of monomials $\sum_j a_j X^j$.

(6) Let $V$ be the $\mathbf{C}$-vector space of all continuous functions $f\colon [0,1] \to \mathbf{C}$. On $V$, we have many linear forms: for instance, for any $a \in [0,1]$, the map $f \mapsto f(a)$ is a linear form on $V$. For any function $g \in V$, we can also define the linear form

$$\lambda_g(f) = \int_0^1 f(t)g(t)dt.$$

We will now show how to construct a basis of $V^*$ when $V$ is finite-dimensional.

Proposition 8.1.3. *Let $V$ be a finite-dimensional vector space and let $B = (e_1, \ldots, e_n)$ be an ordered basis of $V$. For $1 \leqslant i \leqslant n$, let $\lambda_i$ be the $e_i$-coordinate linear form associated to $V$, i.e., the elements $\lambda_i(v)$ of $\mathbf{K}$ are such that*

$$v = \lambda_1(v)e_1 + \cdots + \lambda_n(v)e_n.$$

*Then $B^* = (\lambda_1, \ldots, \lambda_n)$ is an ordered basis of $V^*$. It satisfies*

$$\langle \lambda_j, e_i \rangle = \begin{cases} 1 & \text{if } i = j \\ 0 & \text{otherwise} \end{cases} \tag{8.1}$$

*and it is characterized by this property, in the sense that if $(\mu_1, \ldots, \mu_n)$ is any ordered sequence elements of $V^*$ such that*

$$\langle \mu_j, e_i \rangle = \begin{cases} 1 & \text{if } i = j \\ 0 & \text{otherwise,} \end{cases}$$

*then we have $\mu_j = \lambda_j$ for all $j$.*

One says that $(\lambda_1, \ldots, \lambda_n)$ is the **dual basis** to the given ordered basis $B$.

Proof. We saw in Example 8.1.2 (4) that $\lambda_i \in V^*$. The property (8.1), namely

$$\langle \lambda_j, e_i \rangle = \begin{cases} 1 & \text{if } i = j \\ 0 & \text{otherwise,} \end{cases}$$

follows from the definition, since the coefficients of the representation of $e_i$ in the basis $B$ are 1 for the $i$-th basis vector $e_i$ itself and 0 for all other vectors.

Since $V$ and $V^*$ both have dimension $n$, to show that $B^* = (\lambda_j)_{1 \leqslant j \leqslant n}$ is an ordered basis of $V^*$, it is enough to check that the linear forms $\lambda_j$ are linearly independent in $V^*$. Therefore, let $t_1, \ldots, t_n$ be elements of $\mathbf{K}$ such that

$$t_1\lambda_1 + \cdots + t_n\lambda_n = 0 \in V^*.$$

This means that, for all $v \in V$, we have

$$t_1\lambda_1(v) + \cdots + t_n\lambda_n(v) = 0 \in \mathbf{K}.$$

Applied to $v = e_i$ for $1 \leqslant i \leqslant n$, this leads to $t_i = 0$.

Finally, we check that $B^*$ is characterized by the condition (8.1): let $(\mu_j)_{1\leqslant j\leqslant n}$ be a sequence in $V^*$ such that

$$\langle \mu_j, e_i\rangle = \begin{cases} 1 & \text{if } i = j \\ 0 & \text{otherwise.} \end{cases}$$

Then $\lambda_j$ and $\mu_j$ are linear maps on $V$ that take the same values for all elements of the basis $B$: they are therefore equal. ☐

Given an ordered basis $B = (e_1, \ldots, e_n)$ of a finite-dimensional vector space $V$, we can also summarize the definition of the dual basis $(\lambda_j)_{1\leqslant j\leqslant n}$ by the relation

$$v = \sum_{i=1}^{n} \langle \lambda_i, v\rangle e_i. \tag{8.2}$$

EXAMPLE 8.1.4. (1) Let $V = \mathbf{K}^n$ and let $B = (e_1, \ldots, e_n)$ be the standard basis of $V$. Consider the ordered basis $B_0 = (1)$ of $\mathbf{K}$. For $\lambda \in V^*$, the matrix $\mathrm{Mat}(\lambda; B, B_0)$ is a matrix with one row and $n$ columns, namely

$$\mathrm{Mat}(\lambda; B, B_0) = (\lambda(e_1),\ \lambda(e_2),\ \cdots,\ \lambda(e_n)).$$

Let $(\lambda_1, \cdots, \lambda_n)$ be the dual basis of $B$. These are just the coordinate maps:

$$\lambda_j((t_i)_{1\leqslant i\leqslant n}) = t_j$$

for $1 \leqslant j \leqslant n$, since the coordinate maps satisfy the characteristic property (8.1). These linear forms are often denoted $dx_1, \ldots, dx_n$, so that the representation formula becomes

$$v = \begin{pmatrix} t_1 \\ \vdots \\ t_n \end{pmatrix} = t_1 dx_1(v) + \cdots + t_n dx_n(v).$$

The corresponding matrices are

$$\mathrm{Mat}(dx_1; B, B_0) = (1,\ 0, \cdots,\ 0), \quad \mathrm{Mat}(dx_2; B, B_0) = (0,\ 1,\ 0, \cdots,\ 0), \quad \ldots$$
$$\mathrm{Mat}(dx_n; B, B_0) = (0,\ 0, \cdots,\ 0,\ 1).$$

For a linear form $\lambda$ represented by the row matrix $t = (t_1\ \cdots\ t_n)$ as above and a column vector $x = (x_i)_{1\leqslant i\leqslant n} \in \mathbf{K}^n$, the value $\lambda(v)$ is

$$t_1x_1 + \cdots + t_nx_n = t \cdot x,$$

where the product on the right is the product of matrices.

(2) If $V$ is infinite-dimensional and $B$ is a basis of $V$, then the corresponding coordinate linear forms do not form a generating set of $V^*$. For instance, let $V = \mathbf{R}[X]$. Consider the linear form

$$\lambda(P) = \int_0^1 P(t)dt,$$

and the basis $(X^i)_{i\geqslant 0}$, so that $\lambda(X^i) = \frac{1}{i+1}$ for $i \geqslant 0$. We claim that $\lambda$ is not a linear combination of the coordinate linear forms $\lambda_i$, which map $P$ to the coefficient of $X^i$ in the representation of $P$. Intuitively, this is because such a linear combination only involves finitely many coefficients, whereas $\lambda$ involves all the coefficients of $P$. To be precise, a linear combination of the $\lambda_i$'s is a linear form of the type

$$\ell(P) = \sum_{i=0}^{m} t_i \lambda_i(P)$$

where the integer $m$ and the coefficients $t_i \in \mathbf{R}$ are *fixed*. So we have $\ell(X^{m+1}) = 0$, for instance, whereas $\lambda(X^{m+1}) = 1/(m+2)$.

(3) Let $V = M_{m,n}(\mathbf{K})$, and consider the basis $(E_{i,j})$ (Example 2.5.8 (3)). The corresponding dual basis (after choosing a linear ordering of the pair of indices $(i,j)$...) is given by the $(k,l)$-th coefficient linear maps for $1 \leqslant k \leqslant m$ and $1 \leqslant l \leqslant n$:

$$\lambda_{k,l}((a_{ij})_{1 \leqslant i,j \leqslant n}) = a_{k,l}.$$

(4) Let $\mathbf{K} = \mathbf{R}$, and let $n \geqslant 1$ be an integer and let $V$ be the vector space of polynomials $P \in \mathbf{R}[X]$ with degree $\leqslant n$. Then

$$B = (1, X-1, \ldots, (X-1)^n)$$

is an ordered basis of $V$ (to see this, note that the linear map

$$f \begin{cases} V \to V \\ P \mapsto P(X-1) \end{cases}$$

is an isomorphism, with inverse given by $P \mapsto P(X+1)$, and that $(X-1)^i = f(X^i)$ for all $i$; since $(1, X, \ldots, X^n)$ is a basis of $V$, the result follows). To find the dual basis, we must represent a polynomial $P \in V$ as a linear combination of powers of $X-1$; this can be done using the Taylor formula:

$$P(X) = P(1) + P'(1)(X-1) + \frac{P''(1)}{2}(X-1)^2 + \cdots + \frac{P^{(n)}(1)}{n!}(X-1)^n.$$

From the coefficients, we see that the dual basis $B^*$ is given by $B^* = (\lambda_0, \ldots, \lambda_n)$ where

$$\lambda_i(P) = \frac{P^{(i)}(1)}{i!}.$$

Lemma 8.1.5. *Let $V$ be a vector space.*

(1) *Let $\lambda \in V^*$. Then $\lambda = 0$ if and only if $\langle \lambda, v \rangle = 0$ for all $v \in V$.*

(2) *Let $v \in V$. Then $v = 0$ if and only if $\langle \lambda, v \rangle = 0$ for all $\lambda \in V^*$.*

(3) *More generally, if $v$ is an element of $V$ and if $W \subset V$ is a subspace of $V$ such that $v \notin W$, then there exists a non-zero linear form $\lambda \in V^*$ with $\lambda(v) \neq 0$ and $W \subset \mathrm{Ker}(\lambda)$.*

Proof. (1) is the definition of the zero linear form. The assertion (2) is the special case of (3) when $W = \{0\}$.

To prove (3), let $B_0$ be an ordered basis of $W$. Because $v \notin W$, the elements of $B_0$ and $v$ are linearly independent (assuming

$$tv + \sum_{w \in B_0} t_w w = 0,$$

we would get $v \in W$ if $t$ were non-zero; so $t = 0$, and then the linear independence of $B_0$ shows that all $t_w = 0$). Let $B$ be an ordered basis of $V$ containing $B_0$ and $v$. Now let $\lambda$ be the $v$-coordinate linear form associated to $B$ (Example 8.1.2 (3)). We have $\lambda(v) = 1 \neq 0$, so $\lambda$ is non-zero, but $\lambda(w) = 0$ if $w \in B_0$, hence $W \subset \mathrm{Ker}(\lambda)$. ☐

A vector space has a dual, which is another vector space, hence has also a dual. What is it? This seems complicated, but in fact the dual of the dual space is often nicer to handle than the dual space itself.

Theorem 8.1.6. *Let $V$ be a vector space and $V^*$ the dual space. For any $v \in V$, the map* $\mathrm{ev}_v\colon V^* \to \mathbf{K}$ *defined by*

$$\mathrm{ev}_v(\lambda) = \langle \lambda, v\rangle = \lambda(v)$$

*is an element of $(V^*)^*$. Moreover, the map* $\mathrm{ev}\colon v \mapsto \mathrm{ev}_v$ *is an injective linear map $V \to (V^*)^*$. If $V$ is finite-dimensional, then* ev *is an isomorphism.*

Proof. It is easy to check that $\mathrm{ev}_v$ is a linear form on $V^*$. Let $v \in V$ be such that $\mathrm{ev}_v = 0 \in (V^*)^*$. This means that $\lambda(v) = 0$ for all $\lambda \in V^*$, and by the lemma, this implies $v = 0$. So ev is injective. If $V$ is finite-dimensional, we have $\dim(V) = \dim(V^*)$, and therefore ev is an isomorphism (Corollary 2.8.5). ☐

If $V$ is infinite-dimensional, then one can show that ev is injective but not surjective. In particular, it is not an isomorphism. In a similar direction, we deduce the following property:

Corollary 8.1.7. *Let $V$ be a vector space. The space $V^*$ is finite-dimensional if and only if $V$ is finite-dimensional.*

Proof. If $V$ is finite-dimensional, then we know that $V^*$ is also. Conversely, assume that $V^*$ is finite-dimensional. Then $(V^*)^*$ is also finite dimensional, and since Theorem 8.1.6 gives an injective linear map $\mathrm{ev}\colon V \to (V^*)^*$, we deduce that $V$ is finite-dimensional. ☐

Remark 8.1.8. Note the relation

$$\langle \mathrm{ev}_v, \lambda\rangle = \langle \lambda, v\rangle,$$

so that if we "identify" $V$ and $(V^*)^*$ using the isomorphism of the theorem, we get a symmetric relation

$$\langle v, \lambda\rangle = \langle \lambda, v\rangle$$

for $\lambda \in V^*$ and $v \in V$.

Lemma 8.1.9. *Let $V$ be a finite-dimensional vector space and $B = (e_1, \ldots, e_n)$ an ordered basis of $V$. The dual basis $B^{**}$ of the dual basis $B^*$ of $B$ is the ordered basis $(\mathrm{ev}_{e_i})_{1\leqslant i\leqslant n}$ of $(V^*)^*$.*

If we identify $V$ and $(V^*)^*$ using $v \mapsto \mathrm{ev}_v$, this means that the dual of the dual basis of $B$ "is" the original basis $B$.

Proof. The vectors $(\mathrm{ev}_{e_1}, \ldots, \mathrm{ev}_{e_n})$ satisfy

$$\langle \mathrm{ev}_{e_i}, \lambda_j\rangle = \langle \lambda_j, e_i\rangle = \begin{cases} 1 & \text{if } i = j \\ 0 & \text{otherwise,} \end{cases}$$

for all $i$ and $j$, and so by the last part of Proposition 8.1.3, $(\mathrm{ev}_{e_1}, \ldots, \mathrm{ev}_{e_n})$ is the dual basis of $B^*$. ☐

Definition 8.1.10 (Hyperplane). Let $V$ be a vector space. A subspace $W$ of $V$ is called a **hyperplane** if there exists a complement of dimension 1.

If $V$ is finite-dimensional, this means that a hyperplane is a subspace of dimension $\dim(V) - 1$.

Lemma 8.1.11. *Let $W \subset V$ be a subspace. Then $W$ is a hyperplane if and only if there exists a non-zero $\lambda \in V^*$ such that $W = \mathrm{Ker}(\lambda)$.*

Proof. Suppose first that $\lambda \neq 0$ is a linear form. Let $W = \mathrm{Ker}(\lambda)$. Since $\lambda \neq 0$, there exists $v_0 \in V$ such that $\lambda(v_0) \neq 0$. Then the formula

$$v = \left(v - \frac{\lambda(v)}{\lambda(v_0)} v_0\right) + \frac{\lambda(v)}{\lambda(v_0)} v_0$$

shows that the line generated by $v_0$ is a one-dimensional complement to $W$.

Conversely, let $W$ be a hyperplane in $V$. Let $v_0 \notin W$ be fixed. There exists a linear form $\lambda \in V^*$ with $\lambda(v_0) \neq 0$ and $W \subset \mathrm{Ker}(\lambda)$ (Lemma 8.1.5 (3)). Then $W = \mathrm{Ker}(\lambda)$, since $W$ is a hyperplane, so that $W \oplus \langle v_0 \rangle = V$, and

$$\lambda(w + tv_0) = t\lambda(v_0)$$

for $w \in W$ and $t \in \mathbf{K}$. □

Definition 8.1.12 (Orthogonal). Let $V$ be a vector space and $W$ a subspace of $V$. The **orthogonal of $W$ in $V^*$** is the subspace

$$W^{\perp} = \{\lambda \in V^* \mid \langle \lambda, w \rangle = 0 \text{ for all } w \in W\}.$$

In other words, $W^{\perp}$ is the space of all linear forms with kernel containing $W$.

Proposition 8.1.13. *Let $V$ be a vector space.*

(1) *We have $\{0\}^{\perp} = V^*$ and $V^{\perp} = \{0\}$.*

(2) *We have $W_1 \subset W_2$ if and only if $W_2^{\perp} \subset W_1^{\perp}$, and $W_1 = W_2$ if and only if $W_1^{\perp} = W_2^{\perp}$.*

(3) *Suppose $V$ is finite-dimensional. Then we have $(W^{\perp})^{\perp} = \{\mathrm{ev}_w \in (V^*)^* \mid w \in W\}$ and*

$$\dim(W^{\perp}) = \dim(V) - \dim(W). \tag{8.3}$$

The last assertion shows that if $V$ is finite-dimensional and we identify $(V^*)^*$ and $V$ using the isomorphism of Theorem 8.1.6, then $(W^{\perp})^{\perp} = W$.

Proof. (1) It is elementary that $\{0\}^{\perp} = V*$ (all linear forms take value 0 at $0_V$) and that $V^{\perp} = \{0\}$ (only the zero linear form maps all elements of $V$ to 0).

(2) If $W_1 \subset W_2$, then any linear form $\lambda$ that is zero on $W_2$ is also zero on $W_1$, which means that $W_2^{\perp}$ is contained in $W_1^{\perp}$. Conversely, if $W_1$ is not contained in $W_2$, then there exists $w \neq 0$ in $W_1$ and not in $W_2$. There exists a linear form $\lambda \in V^*$ with $\lambda(w) \neq 0$ and $W_2 \subset \mathrm{Ker}(\lambda)$ (lemma 8.1.5 (3)). Then $\lambda \in W_2^{\perp}$ but $\lambda \notin W_1^{\perp}$.

Since (exchanging $W_1$ and $W_2$) we also have $W_2 \subset W_1$ if and only if $W_1^{\perp} \subset W_2^{\perp}$, we get the equality $W_1 = W_2$ if and only if $W_1^{\perp} = W_2^{\perp}$.

(3) By definition and Theorem 8.1.6, $(W^{\perp})^{\perp}$ is the set of elements $\mathrm{ev}_v$ of $(V^*)^*$ such that $\langle \mathrm{ev}_v, \lambda \rangle = 0$ for all $\lambda \in W^{\perp}$, or in other words, the space of all $\mathrm{ev}_v$ for $v \in V$ such that $\langle \lambda, v \rangle = 0$ for all $\lambda \in W^{\perp}$. This condition is satisfied if $v \in W$. Conversely, if $v \notin W$, there exists a linear form $\lambda \in V^*$ with $\lambda(v) \neq 0$ but $W \subset \mathrm{Ker}(\lambda)$ (lemma 8.1.5 (3)). Then $\lambda \in W^{\perp}$, but $\lambda(v) \neq 0$. This means that it is not the case that $\lambda(v) = 0$ for all $\lambda \in W^{\perp}$, so $\mathrm{ev}_v \notin (V^{\perp})^{\perp}$.

We now prove (8.3). Let $\tilde{W}$ be a complement of $W$. Let $f\colon W^{\perp} \to \tilde{W}^*$ be the restriction linear map $\lambda \mapsto \lambda|W$. We claim that $f$ is an isomorphisme: this will imply that $\dim(W^{\perp}) = \dim(\tilde{W}^*) = \dim(\tilde{W}) = \dim(V) - \dim(W)$ (by Proposition 4.1.11).

We now check the claim. First, $f$ is injective: if $f(\lambda) = 0$, then the linear form $\lambda$ is zero on $\tilde{W}$, but since $\lambda \in W^{\perp}$, it is also zero on $W$, and since $W \oplus \tilde{W} = V$, we get $\lambda = 0 \in V^*$.

Now we check that $f$ is surjective. Let $\mu \in \tilde{W}^*$ be a linear form. We define $\lambda \in V^*$ by

$$\lambda(w + \tilde{w}) = \mu(\tilde{w}),$$

which is well-defined (and linear) because $W \oplus \tilde{W} = V$. The restriction of $\lambda$ to $\tilde{W}$ coincides with $\mu$, so that $f(\lambda) = \mu$. Hence $f$ is surjective. $\square$

REMARK 8.1.14. In particular, from (2) we see that, for a subspace $W$ of $V$, we have $W = \{0\}$ if and only if $W^\perp = V^*$, and $W = V$ if and only if $W^\perp = \{0\}$.

EXAMPLE 8.1.15. (1) Consider for instance $V = M_{n,n}(\mathbf{K})$ for $n \geqslant 1$ and the subspace

$$W = \{A \in V \mid \mathrm{Tr}(A) = 0\}.$$

The orthogonal of $W$ is the space of all linear forms $\lambda$ on $V$ such that $\lambda(A) = 0$ whenever $A$ has trace 0. It is obvious then that $W^\perp$ contains the trace itself $\mathrm{Tr} \in V^*$. In fact, this element generates $W^\perp$. Indeed, since the trace is a surjective linear map from $V$ to $\mathbf{K}$, we have $\dim(W) = \dim(\mathrm{Ker}(\mathrm{Tr})) = \dim(V) - 1$, and hence

$$\dim(W^\perp) = \dim(V) - \dim(W) = \dim(V) - (\dim(V) - 1) = 1.$$

Since $\mathrm{Tr} \in W^\perp$ is a non-zero element of this one-dimensional space, it is basis of $W^\perp$.

(2) It is often useful to interpret elements of $W^\perp$ as "the linear relations satisfied by all elements of $W$". For instance, in the previous example, all elements of $W$ satisfy the linear relation

"the sum of the diagonal coefficients is 0",

but they do not *all* satisfy

"the sum of the coefficients in the first row is 0"

(unless $n = 1$, in which case the two relations are the same...) The fact that $W^\perp$ is generated by the trace means then that the *only* linear relations satisfied by all matrices of trace 0 are those that follow from the relation "being of trace 0", namely its multiples (e.g., "twice the sum of diagonal coefficients is 0").

## 8.2. Transpose of a linear map

Let $V_1$ and $V_2$ be $\mathbf{K}$-vector spaces and $V_1^*$ and $V_2^*$ their respective dual spaces. Let $f\colon V_1 \to V_2$ be a linear map. If we have a linear form $\lambda\colon V_2 \to \mathbf{K}$, we can compose with $f$ to obtain a linear form $\lambda \circ f\colon V_1 \to \mathbf{K}$. This means that to every element of $V_2^*$ is associated an element of $V_1^*$.

LEMMA 8.2.1. *The map $\lambda \mapsto \lambda \circ f$ is a linear map from $V_2^*$ to $V_1^*$.*

PROOF. By definition, for $\lambda_1$ and $\lambda_2$ in $V_2^*$, and for $v$, $w \in V_1$ and $s$, $t \in \mathbf{K}$, we get

$$((t\lambda_1 + s\lambda_2) \circ f)(v) = t\lambda_1(f(v)) + s\lambda_2(f(v)),$$

which is the desired linearity. $\square$

DEFINITION 8.2.2 (Transpose). Let $V_1$ and $V_2$ be $\mathbf{K}$-vector spaces and $V_1^*$ and $V_2^*$ their respective dual spaces. Let $f\colon V_1 \to V_2$ be a linear map. The linear map $V_2^* \to V_1^*$ defined by $\lambda \mapsto \lambda \circ f$ is called the **transpose** of $f$, and denoted ${}^t f$.

Concretely, the definition translates to:

$$\langle ({}^t f)(\lambda), v \rangle = \langle \lambda, f(v) \rangle \tag{8.4}$$

for all $\lambda \in V_2^*$ and $v \in V_1$.

Example 8.2.3. (1) Let $V = \mathbf{K}^n$ and $f = f_A$ for some matrix $A \in M_{n,n}(\mathbf{K})$. We will see in Section 8.3 that ${}^t f$ is the linear map on $V^*$ represented by the transpose matrix ${}^t A$ in the dual basis of the standard basis of $V$.

(2) Let $V$ be any $\mathbf{K}$-vector space and let $\lambda \in V^*$. Then $\lambda$ is a linear map $V \to \mathbf{K}$, hence the transpose of $\lambda$ is a linear map ${}^t\lambda \colon \mathbf{K}^* \to V^*$. To compute it, note that a linear map $\mu \in \mathbf{K}^* = \mathrm{Hom}_{\mathbf{K}}(\mathbf{K}, \mathbf{K})$ satisfies $\mu(t) = t\mu(1)$ for all $t \in \mathbf{K}$, so that $\mu(t) = at$ for some $a \in \mathbf{K}$. We then get ${}^t\lambda(\mu) = \mu \circ \lambda$, or in other words

$$\langle {}^t\lambda(\mu), v\rangle = \langle \mu, \lambda(v)\rangle = a\lambda(v).$$

This means that ${}^t\lambda(\mu) = a\lambda = \mu(1)\lambda$.

Proposition 8.2.4. *The transpose has the following properties:*

(1) *For all vector spaces $V$, we have ${}^t\mathrm{Id}_V = \mathrm{Id}_{V^*}$.*

(2) *The map $f \mapsto {}^t f$ is a linear map*

$$\mathrm{Hom}_{\mathbf{K}}(V_1, V_2) \to \mathrm{Hom}_{\mathbf{K}}(V_2^*, V_1^*).$$

(3) *For all vector spaces $V_1$, $V_2$ and $V_3$ and linear maps $f \colon V_1 \to V_2$ and $g \colon V_2 \to V_3$, we have*

$${}^t(g \circ f) = {}^t f \circ {}^t g \colon V_3^* \to V_1^*.$$

*In particular, if $f$ is an isomorphism, then ${}^t f$ is an isomorphism, with inverse the transpose ${}^t(f^{-1})$ of the inverse of $f$.*

Proof. (1) and (2) are elementary consequences of the definition.

(3) Let $\lambda \in V_3^*$. We get by definition (8.4)

$${}^t(g \circ f)(\lambda) = \lambda \circ (g \circ f) = (\lambda \circ g) \circ f = {}^t f(\lambda \circ g) = {}^t f({}^t g(\lambda)).$$

The remainder of the follows from this and (1), since for $f \colon V_1 \to V_2$ and $g \colon V_2 \to V_1$, the condition $g \circ f = \mathrm{Id}_{V_1}$ (resp. $f \circ g = \mathrm{Id}_{V_2}$) implies ${}^t f \circ {}^t g = \mathrm{Id}_{V_1^*}$ (resp. ${}^t g \circ {}^t f = \mathrm{Id}_{V_2^*}$). ☐

Proposition 8.2.5 (Transpose of the transpose). *Let $V_1$ and $V_2$ be $\mathbf{K}$-vector spaces, and $f \colon V_1 \to V_2$ a linear map. For any $v \in V$, we have*

$$({}^t({}^t f))(\mathrm{ev}_v) = \mathrm{ev}_{f(v)}.$$

*In other words, if $V_1$ and $V_2$ are finite-dimensional and if we identify $(V_i^*)^*$ with $V_i$ using the respective isomorphisms $\mathrm{ev} \colon V_i \to (V_i^*)^*$, then the transpose of the transpose of $f$ is $f$.*

Proof. The transpose of ${}^t f$ is defined by $({}^t({}^t f))(x) = x \circ {}^t f$ for $x \in (V_1^*)^*$. Assume that $x = \mathrm{ev}_v$ for some vector $v \in V_1$ (recall from Theorem 8.1.6 that if $V_1$ is finite-dimensional, then any $x \in (V_1^*)^*$ can be expressed in this manner for some unique vector $v \in V_1$). Then $x \circ {}^t f = \mathrm{ev}_v \circ {}^t f$ is a linear form $V_2^* \to \mathbf{K}$, and it is given for $\lambda \in V_2^*$ by

$$(\mathrm{ev}_v \circ {}^t f)(\lambda) = \mathrm{ev}_v({}^t f(\lambda)) = \mathrm{ev}_v(\lambda \circ f) = (\lambda \circ f)(v) = \lambda(f(v)) = \mathrm{ev}_{f(v)}(\lambda).$$

This means that ${}^t({}^t f)(\mathrm{ev}_v) = \mathrm{ev}_{f(v)}$, as claimed. ☐

Proposition 8.2.6. *Let $f \colon V_1 \to V_2$ be a linear map between vector spaces.*

(1) *The kernel of ${}^t f$ is the space of linear forms $\lambda \in V_2^*$ such that* $\mathrm{Im}(f) \subset \mathrm{Ker}(\lambda)$, *i.e.,* $\mathrm{Ker}({}^t f) = \mathrm{Im}(f)^\perp$. *In particular, ${}^t f$ is injective if and only if $f$ is surjective.*

(2) *The image of ${}^t f$ is the space of linear forms $\mu \in V_1^*$ such that* $\mathrm{Ker}(f) \subset \mathrm{Ker}(\mu)$, *i.e.,* $\mathrm{Im}({}^t f) = \mathrm{Ker}(f)^\perp$. *In particular, ${}^t f$ is surjective if and only if $f$ is injective.*

PROOF. (1) To say that ${}^t f(\lambda) = 0$ is to say that, for any $v \in V_1$, we have

$$\langle ({}^t f)(\lambda), v\rangle = \langle \lambda, f(v)\rangle = 0,$$

or equivalently that $\lambda(w) = 0$ if $w$ belongs to the image of $f$, hence the first assertion. Then ${}^t f$ is injective if and only if its kernel $\mathrm{Im}(f)^\perp$ is $\{0\}$, and by Proposition 8.1.13, this is if and only if $\mathrm{Im}(f) = V_2$, i.e., if and only if $f$ is surjective.

(2) Let $\lambda \in V_2^*$ and let $\mu = ({}^t f)(\lambda)$. For $v \in V_1$, we have

$$\langle \mu, v\rangle = \langle \lambda, f(v)\rangle,$$

which shows that $\mu(v) = 0$ if $f(v) = 0$, so that $\mathrm{Ker}(f) \subset \mathrm{Ker}(\mu)$ for any $\mu \in \mathrm{Im}({}^t f)$. This means that $\mathrm{Im}({}^t f) \subset \mathrm{Ker}(f)^\perp$. Conversely, assume that $\mu \in V_1^*$ is in $\mathrm{Ker}(f)^\perp$. Let $W \subset V_2$ be the image of $f$, and let $\tilde{W}$ be a complement of $W$ in $V_2$. Any $v \in V_2$ can be written uniquely $v = w + \tilde{w}$ where $w \in W$ and $\tilde{w} \in \tilde{W}$. There exists $v_1 \in V_1$ such that $w = f(v_1)$. We claim that the map

$$\lambda \colon v \mapsto \mu(v_1)$$

is well-defined, and is an element of $V_2^*$ such that $({}^t f)(\lambda) = \mu$. To see that it is well-defined, we must check that $\lambda(v)$ is independent of the choice of $v_1$ such that $f(v_1) = w$. But if $v_1'$ is another such element, we have $f(v_1 - v_1') = 0$, hence $v_1 - v_1'$ is in the kernel of $f$, and consequently (by the assumption $\mu \in \mathrm{Ker}(f)^\perp$) in the kernel of $\mu$, so that $\mu(v_1 - v_1') = 0$.

Since $\lambda$ is well-defined, it follows easily that it is linear (left as exercise). So $\lambda \in V_2^*$. Also, it follows that $\lambda(f(v)) = \mu(v)$ for all $v \in V_1$, since for the vector $f(v) \in V_2$, we can take $v_1 = v$ itself to define $\lambda(f(v))$. Now we get for all $v \in V_1$ the relation

$$\langle ({}^t f)(\lambda), v\rangle = \langle \lambda, f(v)\rangle = \mu(v),$$

so that ${}^t f = \mu$, as desired.

Finally, this result shows that ${}^t f$ is surjective if and only if $\mathrm{Ker}(f)^\perp = V_1^*$, i.e., if and only if $\mathrm{Ker}(f) = \{0\}$ by Proposition 8.1.13. ☐

REMARK 8.2.7. We can deduce prove (2) from (1) in the finite-dimensional case by duality: identifying $V_i$ and $V_i^{**}$, we have

$$\mathrm{Ker}(f)^\perp = \mathrm{Ker}({}^{tt} f)^\perp = (\mathrm{Im}({}^t f)^\perp)^\perp = \mathrm{Im}({}^t f),$$

where we used the identification of Proposition 8.2.5, then applied (1) to ${}^t f$, and then the identification from Proposition 8.1.13 (3).

EXAMPLE 8.2.8. As in Example 8.1.15 (1), consider $V = M_{n,n}(\mathbf{K})$ and the linear map $\mathrm{Tr}\colon V \to \mathbf{K}$. From Example 8.2.3 (2), the image of ${}^t\mathrm{Tr}$ is the set of linear forms of the type $a\,\mathrm{Tr}$ for some $a \in \mathbf{K}$, which means that it is the space generated by the trace. Hence $\mathrm{Ker}(\mathrm{Tr})^\perp = \mathrm{Im}({}^t\mathrm{Tr})$ is one-dimensional and generated by the trace, which recovers the result of the example.

COROLLARY 8.2.9. *Let $f\colon V_1 \to V_2$ be a linear map between finite-dimensional vector spaces. We have* $\dim \mathrm{Ker}({}^t f) = \dim(V_2) - \mathrm{rank}(f)$ *and* $\mathrm{rank}({}^t f) = \dim(V_1) - \dim \mathrm{Ker}(f) = \mathrm{rank}(f)$.

PROOF. We prove the first assertion. We have, by the previous proposition, $\mathrm{Ker}({}^t f) = \mathrm{Im}(f)^\perp$. From Proposition 8.1.13 (3), we then deduce

$$\dim(\mathrm{Ker}({}^t f)) = \dim(\mathrm{Im}(f)^\perp) = \dim(V_2) - \dim(\mathrm{Im}(f)).$$

To prove the second assertion, we use duality: we apply the formula to ${}^t f$ instead of $f$, and get

$$\operatorname{rank}({}^t({}^t f)) = \dim(V_2^*) - \dim \operatorname{Ker}({}^t f).$$

But Proposition 8.2.5 shows that the rank of ${}^t({}^t f)$ is the same as the rank of $f$. So we get

$$\dim \operatorname{Ker}({}^t f) = \dim(V_2^*) - \operatorname{rank}(f),$$

as claimed. ☐

## 8.3. Transpose and matrix transpose

LEMMA 8.3.1. *Let $V_1$ and $V_2$ be finite-dimensional vector spaces with ordered bases $B_1$ and $B_2$ and $\dim(V_1) = n$, $\dim(V_2) = m$. Let $B_i^*$ be the dual bases of the dual spaces. If $f\colon V_1 \to V_2$ is a linear map and $A = \operatorname{Mat}(f; B_1, B_2)$, then we have $A = (a_{ij})_{i,j}$ with*

$$a_{ij} = \langle \mu_i, f(e_j)\rangle$$

*for $1 \leqslant i \leqslant m$ and $1 \leqslant j \leqslant n$.*

PROOF. We write $B_1 = (e_1, \ldots, e_n)$, $B_2 = (f_1, \ldots, f_m)$ and $B_1^* = (\lambda_j)_{1\leqslant j\leqslant n}$, $B_2^* = (\mu_i)_{1\leqslant i\leqslant m}$. Let $A = \operatorname{Mat}(f; B_1, B_2) = (a_{ij})_{1\leqslant i\leqslant n}$. The columns of $A$ are the vectors $f(e_j)$ for $1 \leqslant j \leqslant n$, which means that

$$f(e_j) = \sum_{i=1}^{n} a_{ij} f_i.$$

If we compare with the definition of the dual basis, this means that

$$a_{ij} = \langle \mu_i, f(e_j)\rangle.$$

☐

PROPOSITION 8.3.2. *Let $V_1$ and $V_2$ be finite-dimensional vector spaces with ordered bases $B_1$ and $B_2$. Let $B_i^*$ be the dual bases of the dual spaces. If $f\colon V_1 \to V_2$ is a linear map then we have*

$$\operatorname{Mat}({}^t f; B_2^*, B_1^*) = {}^t\operatorname{Mat}(f; B_1, B_2).$$

PROOF. We write $B_1 = (e_1, \ldots, e_n)$, $B_2 = (f_1, \ldots, f_m)$ and $B_1^* = (\lambda_j)$, $B_2^* = (\mu_j)$. Let $A = \operatorname{Mat}(f; B_1, B_2) = (a_{ij})$. By the previous lemma, we know that

$$a_{ij} = \langle \mu_i, f(e_j)\rangle.$$

On the other hand, if we apply this to ${}^t f$ and to $A' = \operatorname{Mat}({}^t f; B_2^*, B_1^*) = (b_{ji})$, using the fact that the dual basis of $B_1^*$ is $(\operatorname{ev}_{e_j})$ and that of $B_2^*$ is $(\operatorname{ev}_{f_i})$ (Lemma 8.1.9), we get

$$b_{ji} = \langle \operatorname{ev}_{e_j}, {}^t f(\mu_i)\rangle = \langle {}^t f(\mu_i), e_j\rangle = \langle \mu_i, f(e_j)\rangle = a_{ij}.$$

This means that $A'$ is the transpose of the matrix $A$. ☐

COROLLARY 8.3.3. *Let $V$ be a finite-dimensional vector space and $f \in \operatorname{End}_{\mathbf{K}}(V)$. Then $\det({}^t f) = \det(f)$ and $\operatorname{Tr}({}^t f) = \operatorname{Tr}(f)$.*

PROOF. This follows from the fact that one can compute the determinant or the trace of ${}^t f$ with respect to any basis of $V^*$, by combining the proposition with Proposition 3.4.10. ☐

We then recover "without computation" the result of Proposition 5.1.1 (1).

COROLLARY 8.3.4. *Let $n, m, p \geqslant 1$ and $A \in M_{m,n}(\mathbf{K})$, $B \in M_{p,m}(\mathbf{K})$. Then*

$${}^t(BA) = {}^t A\, {}^t B \in M_{p,n}(\mathbf{K}).$$

Proof. Let $B_m$, $B_n$, $B_p$ denote the standard bases of $\mathbf{K}^m$, $\mathbf{K}^n$ and $\mathbf{K}^p$ respectively, and let $B_m^*$, $B_n^*$, and $B_p^*$ denote the dual bases.

We compute

$$\begin{aligned}{}^t(BA) = \mathrm{Mat}({}^tf_{BA}; B_p^*, B_n^*) &= \mathrm{Mat}({}^t(f_B \circ f_A); B_p^*, B_n^*) \\ &= \mathrm{Mat}({}^tf_A \circ {}^tf_B; B_p^*, B_n^*) = \mathrm{Mat}({}^tf_A; B_m^*, B_n^*)\,\mathrm{Mat}({}^tf_B; B_p^*, B_m^*) \\ &= {}^t\mathrm{Mat}(f_A; B_n, B_m){}^t\mathrm{Mat}(f_B; B_m, B_p) = {}^tA{}^tB,\end{aligned}$$

using the last proposition and Proposition 8.2.4 (2). ☐

Corollary 8.3.5 (Row rank equals column rank). *Let $A \in M_{m,n}(\mathbf{K})$ be a matrix. The dimension of the subspace of $\mathbf{K}^n$ generated by the columns of $A$ is equal to the dimension of the subspace of $\mathbf{K}_m$ generated by the rows of $A$.*

Proof. Denote again $B_m$ (resp. $B_n$) the standard basis of $\mathbf{K}^m$ (resp. $\mathbf{K}^n$) and $B_m^*$ (resp. $B_n^*$) the dual basis. The dimension $r$ of the subspace of $\mathbf{K}_m$ generated by the rows of $A$ is the rank of the transpose matrix ${}^tA$. Since ${}^tA = \mathrm{Mat}({}^tf_A; B_m^*, B_n^*)$, it follows that $r$ is the rank of ${}^tf_A$ (Proposition 2.11.2 (2)). By Corollary 8.2.9, this is the same as the rank of $f_A$, which is the dimension of the subspace of $\mathbf{K}^n$ generated by the columns of $A$. ☐

CHAPTER 9

# Fields

It is now time to discuss what are fields precisely. Intuitively, these are the sets of "numbers" with operations behaving like addition and multiplication so that all[1] the results of linear algebra work equally well for all fields as they do for $\mathbf{Q}$, $\mathbf{R}$ or $\mathbf{C}$ (except for euclidean or unitary spaces).

## 9.1. Definition

DEFINITION 9.1.1 (Field). A **field** $\mathbf{K}$ is a set, also denoted $\mathbf{K}$, with two special elements $0_{\mathbf{K}}$ and $1_{\mathbf{K}}$, and two operations

$$+_{\mathbf{K}} \colon (x, y) \mapsto x +_{\mathbf{K}} y, \qquad \cdot_{\mathbf{K}} \colon (x, y) \mapsto x \cdot_{\mathbf{K}} y$$

from $\mathbf{K} \times \mathbf{K}$ to $\mathbf{K}$, such that all of the following conditions hold:

(1) $0_{\mathbf{K}} \neq 1_{\mathbf{K}}$ (so a field has at least 2 elements);
(2) For any $x \in \mathbf{K}$, we have $x +_{\mathbf{K}} 0_{\mathbf{K}} = 0_{\mathbf{K}} +_{\mathbf{K}} x = x$;
(3) For any $x$ and $y$ in $\mathbf{K}$, we have

$$x +_{\mathbf{K}} y = y +_{\mathbf{K}} x;$$

(4) For any $x$, $y$ and $z$ in $\mathbf{K}$, we have

$$x +_{\mathbf{K}} (y +_{\mathbf{K}} z) = (x +_{\mathbf{K}} y) +_{\mathbf{K}} z;$$

(5) For any $x$ in $\mathbf{K}$, there exists a unique element denoted $-x$ such that

$$x +_{\mathbf{K}} (-x) = (-x) +_{\mathbf{K}} x = 0_{\mathbf{K}};$$

(6) For any $x \in \mathbf{K}$, we have $x \cdot_{\mathbf{K}} 0_{\mathbf{K}} = 0_{\mathbf{K}} \cdot_{\mathbf{K}} x = 0_{\mathbf{K}}$ and $x \cdot_{\mathbf{K}} 1_{\mathbf{K}} = 1_{\mathbf{K}} \cdot_{\mathbf{K}} x = x$;
(7) For any $x$ and $y$ in $\mathbf{K}$, we have

$$x \cdot_{\mathbf{K}} y = y \cdot_{\mathbf{K}} x;$$

(8) For any $x$, $y$ and $z$ in $\mathbf{K}$, we have

$$x \cdot_{\mathbf{K}} (y \cdot_{\mathbf{K}} z) = (x \cdot_{\mathbf{K}} y) \cdot_{\mathbf{K}} z;$$

(9) For any $x$ in $\mathbf{K} - \{0\}$, there exists a unique element denoted $x^{-1}$ in $\mathbf{K}$ such that

$$x \cdot_{\mathbf{K}} x^{-1} = x^{-1} \cdot_{\mathbf{K}} x = 1_{\mathbf{K}};$$

(10) For any $x$, $y$ and $z$ in $\mathbf{K}$, we have

$$x \cdot_{\mathbf{K}} (y +_{\mathbf{K}} z) = x \cdot_{\mathbf{K}} y + x \cdot_{\mathbf{K}} z, \qquad (x +_{\mathbf{K}} y) \cdot_{\mathbf{K}} z = x \cdot_{\mathbf{K}} z + y \cdot_{\mathbf{K}} z.$$

EXAMPLE 9.1.2. (1) One can immediately see that, with the usual addition and multiplication, the sets $\mathbf{Q}$, $\mathbf{R}$ and $\mathbf{C}$ satisfy all of these conditions. On the other hand, the set $\mathbf{Z}$ (with the usual addition and multiplication) *does not*: condition (9) fails for $x \in \mathbf{Z}$, except if $x = 1$ or $x = -1$, since the inverse of an integer is in general a rational number that is not in $\mathbf{Z}$.

[1] Or almost all: we will see that there are very few exceptions.

(2) The simplest example of a field different from $\mathbf{Q}$, $\mathbf{R}$ or $\mathbf{C}$ is the following: we take the set $\mathbf{F}_2 = \{0, 1\}$, and we define $+$ and $\cdot$ according to the following rules:

$$\begin{array}{c|c|c} + & 0 & 1 \\ \hline 0 & 0 & 1 \\ 1 & 1 & 0 \end{array} \qquad \begin{array}{c|c|c} \cdot & 0 & 1 \\ \hline 0 & 0 & 0 \\ 1 & 0 & 1 \end{array}$$

Note that these are easy to remember for at least two reasons: (1) if one takes the convention that 0 represents "even integers" and 1 represents "odd integers", then the result always give the parity of the sum or the product of integers with the given parity; (2) since only the elements 0 and 1 occur, the conditions (2) and (6) in the definition of a field determine all the rules, except $1 + 1 = 0$. But condition (5) implies that we must have $-1 = 1$ if the field has only two elements 0 and 1 (because (2) shows that 0 does not work as opposite of 1), and therefore $1 + 1 = 0$.

It is not difficult to check that $\mathbf{F}_2$ is a field with these definitions of addition and multiplication.

(3) Let

$$\mathbf{K} = \{z = x + iy \in \mathbf{C} \mid x \in \mathbf{Q} \text{ and } y \in \mathbf{Q}\}.$$

This is a subset of $\mathbf{C}$, containing $\mathbf{Q}$, and it is not difficult to see that it is a field with the addition and multiplication of complex numbers. Indeed, the main points are that $z_1 + z_2$ and $z_1 z_2$ are in $\mathbf{K}$ if both $z_1$ and $z_2$ are in $\mathbf{K}$ (which follow immediately from the definition of addition and multiplication), and that if $z \neq 0$ is in $\mathbf{K}$, then the inverse $z^{-1} \in \mathbf{C}$ of $z$ is also in $\mathbf{K}$, and this is true because if $z = x + iy$, then

$$z^{-1} = \frac{x - iy}{x^2 + y^2}$$

has rational real and imaginary parts. Most conditions are then consequences of the fact that addition and multiplication of complex numbers are known to satisfy the properties required in the definition. This fields is called the field of *Gaussian numbers* and is denoted $\mathbf{K} = \mathbf{Q}(i)$.

(4) Let

$$\mathbf{K} = \Big\{\frac{P(\pi)}{Q(\pi)} \in \mathbf{R} \mid P \in \mathbf{Q}[X],\ Q \in \mathbf{Q}[X] \text{ and } Q(\pi) \neq 0\Big\}.$$

This set is a subset of $\mathbf{R}$. It is a field, when addition and multiplication are defined as addition and multiplication of real numbers. Again, the main point is that the sum or product of two elements of $\mathbf{K}$ is in $\mathbf{K}$, because for instance

$$\frac{P_1(\pi)}{Q_1(\pi)} + \frac{P_2(\pi)}{Q_2(\pi)} = \frac{P_1(\pi)Q_2(\pi) + P_2(\pi)Q_1(\pi)}{Q_1(\pi)Q_2(\pi)},$$

and we have $(Q_1 Q_2)(\pi) \neq 0$. This field is denoted $\mathbf{Q}(\pi)$.

Remark 9.1.3. If $-1_{\mathbf{K}}$ denotes the opposite of the element $1_{\mathbf{K}}$ in a field, then we have

$$-x_{\mathbf{K}} = (-1_{\mathbf{K}}) \cdot x$$

for any $x \in \mathbf{K}$.

A very important property following from the definition is that if $x \cdot_{\mathbf{K}} y = 0_{\mathbf{K}}$, then either $x = 0_{\mathbf{K}}$ or $y = 0_{\mathbf{K}}$ (or both); indeed, if $x_{\mathbf{K}} \neq 0_{\mathbf{K}}$, then multiplying on the left by $x^{-1}$, we obtain:

$$x^{-1} \cdot_{\mathbf{K}} (x \cdot_{\mathbf{K}} y) = x^{-1} \cdot_{\mathbf{K}} 0_{\mathbf{K}} = 0_{\mathbf{K}}$$

by (6), and using (8), (9) and (6) again, this becomes

$$0_{\mathbf{K}} = (x^{-1} \cdot_{\mathbf{K}} x) \cdot y = 1_{\mathbf{K}} \cdot y = y.$$

### 9.2. Characteristic of a field

Let $\mathbf{K}$ be a field. Using the element $1_{\mathbf{K}}$ and addition we define by induction

$$2_{\mathbf{K}} = 1_{\mathbf{K}} + 1_{\mathbf{K}}, \qquad \ldots \qquad n_{\mathbf{K}} = (n-1)_{\mathbf{K}} + 1_{\mathbf{K}}$$

for any integer $n \geqslant 1$, and

$$n_{\mathbf{K}} = -((-n)_{\mathbf{K}}) = (-1_{\mathbf{K}}) \cdot n_{\mathbf{K}}$$

for any integer $n \leqslant 0$. It follows then that

$$(n+m)_{\mathbf{K}} = n_{\mathbf{K}} +_{\mathbf{K}} m_{\mathbf{K}}, \qquad (nm)_{\mathbf{K}} = n_{\mathbf{K}} \cdot_{\mathbf{K}} m_{\mathbf{K}}$$

for any integers $n$ and $m$ in $\mathbf{Z}$.

Two cases may occur when we do this for all $n \in \mathbf{Z}$: either the elements $n_{\mathbf{K}}$ are non-zero in $\mathbf{K}$ whenever $n \neq 0$; or there exists some non-zero integer $n \in \mathbf{Z}$ such that $n_{\mathbf{K}} = 0_{\mathbf{K}}$.

In the first case, one says that $\mathbf{K}$ *is a field of characteristic zero.* This is the case for $\mathbf{K} = \mathbf{Q}$, or $\mathbf{R}$ or $\mathbf{C}$.

The second case seems surprising at first, but it may arise: for $\mathbf{K} = \mathbf{F}_2$, we have $2_{\mathbf{K}} = 1_{\mathbf{K}} + 1_{\mathbf{K}} = 0$. When this happens, we say that $\mathbf{K}$ has *positive characteristic.*

Suppose now that $\mathbf{K}$ has positive characteristic. Consider the set $I$ of all integers $n \in \mathbf{Z}$ such that $n_{\mathbf{K}} = 0_{\mathbf{K}}$. This is then a subset of $\mathbf{Z}$ that contains at least one non-zero integer. This set has the following properties:

(1) We have $0 \in I$;
(2) If $n$ and $m$ are elements of $I$, then $n+m$ is also in $I$;
(3) If $n$ is in $I$, then $-n \in I$.
(4) Consequently, by induction and using the previous property, if $n$ is in $I$ and $k \in \mathbf{Z}$, then $kn \in I$.

Since $I$ contains at least one non-zero integer, (3) shows that there exists an integer $n \geqslant 1$ in $I$. It follows that there is a *smallest* integer $k \geqslant 1$ in $I$. Then, by (4), all multiples $qn$ of $n$ are in $I$, for $q \in \mathbf{Z}$. Consider then an arbitrary $n \in I$. By division with remainder, we can express

$$n = qk + r$$

where $q$ and $r$ are in $\mathbf{Z}$ and $0 \leqslant r \leqslant k-1$. Since $k \in I$ and $n \in I$, then the properties above show that $r = n - qk$ is also in $I$. But since $0 \leqslant r \leqslant k-1$, and $k$ is the smallest positive integer in $I$, this is only possible if $r = 0$. This means that $n = qk$.

What this means is that if $k$ is as defined above, we have

$$I = \{qk \mid q \in \mathbf{Z}\}.$$

The integer $k$ is not arbitrary: it is a *prime number*, which means that $k \geqslant 2$ and has no positive integral divisor except 1 and $k$. Indeed, first we have $k \neq 1$ because $0_{\mathbf{K}} \neq 1_{\mathbf{K}}$. Next, assume that $k = ab$ where $a$ and $b$ are positive integers. Then

$$0_{\mathbf{K}} = k_{\mathbf{K}} = a_{\mathbf{K}} \cdot_{\mathbf{K}} b_{\mathbf{K}},$$

and therefore, from the properties of fields, either $a_{\mathbf{K}} = 0$ or $b_{\mathbf{K}} = 0$, or in other words, either $a \in I$ or $b \in I$. Since $I$ is the set of multiples of $k$ and $a$ and $b$ are non-zero, this means that either $a$ or $b$ is divisible by $k$. But then the equation $ab = k$ is only possible if the other is equal to 1, and that means that $k$ is prime.

Definition 9.2.1 (Characteristic of a field). The **characteristic of a field K** is either 0, if $n_{\mathbf{K}} \neq 0$ for all $n \in \mathbf{Z}$, or the prime number $p$ such that $n_{\mathbf{K}} = 0$ if and only if $n = pm$ is a multiple of $p$.

Example 9.2.2. (1) The fields $\mathbf{Q}$, $\mathbf{R}$, $\mathbf{C}$, $\mathbf{Q}(i)$ and $\mathbf{Q}(\pi)$ are all fields of characteristic 0.

(2) The characteristic of $\mathbf{F}_2$ is 2. One can show that, for any prime number $p$, there exist fields of characteristic $p$; some are finite, and some are infinite (in particular, it is *not* true that all infinite fields are of characteristic 0).

## 9.3. Linear algebra over arbitrary fields

From now, we denote by $\mathbf{K}$ an arbitrary field, and we denote simply $0 = 0_{\mathbf{K}}$, $1 = 1_{\mathbf{K}}$ and write the addition and multiplication without subscripts $\mathbf{K}$. We can then look back to the definition 2.3.1 of a vector space and see that it involves no further data concerning $\mathbf{K}$ than the elements 0 and 1 (see (2.3)), and the addition and multiplication (for instance in (2.6) and (2.8)). In other words, the definition does make sense for any field.

We denote by $p$ the characteristic of $\mathbf{K}$, which is either 0 or a prime number $p \geqslant 2$. The whole developpment of linear algebra is then independent of the choice of field, with very few exceptions, which we now indicate:

- Remark 3.1.5 (which states that a multilinear map $f$ on $V^n$ is alternating if and only if

$$f(v_1, \ldots, v_n) = -f(v_1, \ldots, v_{i-1}, v_j, v_{i+1}, \ldots, v_{j-1}, v_i, v_{j+1}, \ldots, v_n) \tag{9.1}$$

  whenever $1 \leqslant i \neq j \leqslant n$) holds only when the characteristic is not equal to 2. Indeed, if $\mathbf{K} = \mathbf{F}_2$, for instance, then since $1+1 = 0$ in $\mathbf{K}$, we have $1 = -1$ in $\mathbf{K}$, and the condition (9.1) always holds. Conversely, if the characteristic is not 2, then $2 = 1+1 \neq 0$ in $\mathbf{K}$, and therefore has an inverse $1/2$, so that the condition

$$2f(v_1, \ldots, v_n) = 0$$

  coming from (9.1) if $v_i = v_j$ with $i \neq j$ implies $f(v_1, \ldots, v_n) = 0$ if $v_i = v_j$.
- Proposition 4.4.3 is also only valid for fields of characteristic different from 2, since the proof uses a division by 2 (see (4.4)). Indeed, if $\mathbf{K} = \mathbf{F}_2$, the endomorphism $f_A \in \mathrm{End}_{\mathbf{F}_2}(\mathbf{F}_2^2)$ given by the matrix

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

  is an involution, since

$$A^2 = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1+1 \\ 0 & 1 \end{pmatrix} = 1_2$$

  (in $M_{2,2}(\mathbf{F}_2)$) and it is not diagonalizable.
- The most delicate issue is that if the field $\mathbf{K}$ is finite (which implies that the characteristic is not zero), then the definition of polynomials (and therefore the construction of the characteristic polynomial) requires some care. We discuss this in the next section.
- Properties that require the existence of an eigenvalue for an endomorphism of a finite-dimensional vector space of dimension 1 (e.g., the Jordan Normal Form as in Theorem 7.1.8) are only applicable if all polynomials of degree $\geqslant 1$ with coefficients in $\mathbf{K}$ (as defined precisely in the next section) have a root in $\mathbf{K}$ –

such fields are called *algebraically closed*, and $\mathbf{C}$ is the standard example of such field.

## 9.4. Polynomials over a field

Let $\mathbf{K}$ be an arbitrary field. When $\mathbf{K}$ is $\mathbf{Q}$ or $\mathbf{R}$ or $\mathbf{C}$, we have viewed polynomials with coefficients in $\mathbf{K}$ as a function $P\colon \mathbf{K} \to \mathbf{K}$ such that there exist an integer $d \geqslant 0$ and coefficients

$$a_0, \ldots, a_d$$

in $\mathbf{K}$ with

$$P(x) = a_0 + a_1 x + \cdots + a_d x^d$$

for all $x \in \mathbf{K}$. This definition is reasonable because the power functions $x \mapsto x^i$ are linearly independent, which means that the function $P$ *determines uniquely* the coefficients $a_i$.

This property is not true any more for finite fields. For instance, consider $\mathbf{K} = \mathbf{F}_2$. Then consider the functions from $\mathbf{F}_2$ to $\mathbf{F}_2$ defined by

$$P_1(x) = x^2, \qquad P_2(x) = x.$$

These do not have the same coefficients, but $P_1(0) = P_2(0) = 0$ and $P_1(1) = P_2(1) = 1$, so that the *functions* are identical.

This behavior is not what we want, in particular because it leads to a considerable loss of information. So one defines polynomials more abstractly by *identifying* them with the sequence of coefficients. To do this, we make the following definition:

Definition 9.4.1 (Polynomial). Let $\mathbf{K}$ be a field. A **polynomial** $P$ with coefficients in $\mathbf{K}$ and in one indeterminate $X$ is a finite linear combination of "symbols" $X^i$ for $i$ integer $\geqslant 0$, which are linearly independent over $\mathbf{K}$. Polynomials are added in the obvious way, and multiplied using the rule

$$X^i \cdot X^j = X^{i+j}$$

together with the commutativity rule $P_1 P_2 = P_2 P_1$, the associativity rule $P_1(P_2 P_3) = (P_1 P_2) P_3$ and the distributivity rule $P_1(P_2 + P_3) = P_1 P_2 + P_1 P_3$.

The set of all polynomials with coefficients in $\mathbf{K}$ is denoted $\mathbf{K}[X]$. It is a $\mathbf{K}$-vector space of infinite dimension with

$$t \cdot \sum_{i=0}^{d} a_i X^i = \sum_i (t a_i) X^i$$

for $t \in \mathbf{K}$ and

$$\Bigl(\sum_i a_i X^i\Bigr) + \Bigl(\sum_i b_i X^i\Bigr) = \sum_i (a_i + b_j) X^i,$$

where only finitely many coefficients are non-zero. One often writes simply $a_0$ instead of $a_0 X^0$ for $a_0 \in \mathbf{K}$.

Let $P \in \mathbf{K}[X]$ be a non-zero polynomial. The **degree** of $P$, denoted $\deg(P)$, is the largest integer $i \geqslant 0$ such that the coefficient of $X^i$ is non-zero.

An abstract formula for the product is simply

$$\Bigl(\sum_i a_i X^i\Bigr) \cdot \Bigl(\sum_i b_i X^i\Bigr) = \sum_i c_i X^i,$$

where

$$c_i = \sum_{j+k=i} a_j b_k$$

(both $j$ and $k$ ranging over integers $\geqslant 0$, which means that $j \leqslant i$ and $k \leqslant i$, so the sum is a finite sum).

EXAMPLE 9.4.2. (1) The degree of $P = a_0$ is equal to 0 for all $a_0 \neq 0$, but is not defined if $a_0 = 0$.

(2) Consider the polynomial $P = X^2 + X + 1$ in $\mathbf{F}_2[X]$ of degree 2 (note that the corresponding function is $0 \mapsto 1$ and $1 \mapsto 1$, but it is not a constant polynomial, which would be of degree 0).

We have

$$P^2 = (X^2 + X + 1)(X^2 + X + 1) = \\ X^4 + X^3 + X^2 + X^3 + X^2 + X + X^2 + X + 1 = X^4 + 1$$

because $X^3 + X^3 = 2X^3 = 0$ in $\mathbf{F}_2[X]$ and similarly $X^2 + X^2 = 0$ and $X + X = 0$.

LEMMA 9.4.3. *The degree of $P_1 + P_2$ is $\leqslant \max(\deg(P_1), \deg(P_2))$, if $P_1 + P_2 \neq 0$; the degree of $P_1P_2$ is $\deg(P_1) + \deg(P_2)$ if $P_1$ and $P_2$ are non-zero.*

PROOF. We leave the case of the sum as exercise. For the product, if $P_1$ and $P_2$ are non-zero, we write

$$P_1 = a_dX^d + \cdots + a_1X + a_0, \qquad P_2 = b_eX^e + \cdots + b_1X + b_0$$

where $d = \deg(P_1) \geqslant 0$ and $e = \deg(P_2) \geqslant 0$, so that $a_d \neq 0$ and $b_e \neq 0$ by definition. If we compute the product, we obtain

$$P_1P_2 = a_db_eX^{d+e} + (a_db_{e-1} + a_{d-1}b_e)X^{d-1} + \cdots$$

where $a_db_e \neq 0$ (as a product of two non-zero elements of $\mathbf{K}$!). Hence $\deg(P_1P_2) = d + e$. ☐

DEFINITION 9.4.4 (Polynomial function). Let $P \in \mathbf{K}[X]$ be a polynomial, with

$$P = a_0 + a_1X + \cdots + a_dX^d.$$

The associated **polynomial function** $\tilde{P}$ is the function $\mathbf{K} \to \mathbf{K}$ defined by

$$\tilde{P}(x) = a_0 + a_1x + \cdots + a_dx^d.$$

We often write simply $P(x) = \tilde{P}(x)$.

LEMMA 9.4.5. *The map $P \mapsto \tilde{P}$ from $\mathbf{K}[X]$ to the vector space $V$ of all functions $\mathbf{K} \to \mathbf{K}$ is linear and satisfies $\widetilde{P_1P_2} = \tilde{P}_1\tilde{P}_2$. It is injective if and only if $\mathbf{K}$ is infinite.*

PROOF. The linearity and the assertion $\widetilde{P_1P_2} = \tilde{P}_1\tilde{P}_2$ are elementary – they come essentially from the fact that both the powers $X^i$ of the indeterminate and the powers $x^i$ of a fixed element of $\mathbf{K}$ satisfy the same rules of multiplication (exponents are added).

To prove the other assertion, we will show the following: if $P \neq 0$, then the number $N_P$ of $x \in \mathbf{K}$ such that $\tilde{P}(x) = 0$ is at most the degree of $P$. This will show that the map $P \mapsto \tilde{P}$ is injective if $\mathbf{K}$ is infinite.

We proceed by induction on the degree of $P$. If the degree is 0, then $P = a_0$ with $a_0 \neq 0$, and hence $\tilde{P}(x) = a_0 \neq 0$ for all $x \in \mathbf{K}$, so the number $N_P$ is $0 = \deg(P)$ in that case.

Now assume that $P$ has degree $d \geqslant 1$ and that $N_Q \leqslant \deg(Q)$ for all non-zero polynomials $Q$ of degree $\leqslant d - 1$. Write

$$P = a_dX^d + \cdots + a_1X + a_0$$

with $a_d \neq 0$. If $N_P$ is zero, then obviously $N_P \leqslant d$, so we assume that $N_P \geqslant 1$. This means that there exists $x_0 \in \mathbf{K}$ such that $\tilde{P}(x_0) = 0$. We may assume that $x_0 = 0$ (by replacing $P$ by

$$P_1 = \sum_{i=0}^{d} a_i (X + x_0)^i,$$

otherwise, since $\tilde{P}_1(x) = 0$ if and only if $\tilde{P}(x + x_0) = 0$, so that $N_P = N_{P_1}$). But $\tilde{P}(0) = a_0 = 0$ means that

$$P = a_1 X + \cdots + a_d X^d = X(a_1 + \cdots + a_d X^{d-1}) = XQ$$

where $Q$ has degree $d - 1$. Then $\tilde{P}(x) = 0$ if and only if either $x = 0$ or $\tilde{Q}(x) = 0$. Therefore $N_P \leqslant 1 + N_{Q_1} \leqslant 1 + d - 1 = d$ by induction.

For the converse, if $\mathbf{K}$ is finite, define

$$P = \prod_{x \in \mathbf{K}} (X - x) \in \mathbf{K}[X].$$

This is a polynomial of degree $\mathrm{Card}(\mathbf{K})$, in particular non-zero. But for any $x \in \mathbf{K}$, we have $\tilde{P}(x) = 0$, so that $\tilde{P} = 0$. ☐

A "proper" definition of the characteristic polynomial of a matrix $A \in M_{n,n}(\mathbf{K})$ can then be given as follows: (1) $\mathbf{K}[X]$ can be seen as a subset of a field $\mathbf{K}(X)$, with elements the fractions $P/Q$ where $P$ and $Q$ are polynomials with $Q \neq 0$, and the "obvious" addition and multiplication of such fractions, which moreover satisfy $P_1/Q_1 = P_2/Q_2$ if and only if $P_1 Q_2 = P_2 Q_1$; (2) the polynomial $X = X/1$ belongs to $\mathbf{K}(X)$, and so $X \cdot 1_n - A$ is a matrix in $M_{n,n}(\mathbf{K}(X))$; as such, it has a determinant, which is an element of $\mathbf{K}(X)$, and one can check that in fact this determinant belongs to $\mathbf{K}[X]$. This is the characteristic polynomial of $A$.

Example 9.4.6. Consider $\mathbf{K} = \mathbf{F}_2$ and

$$A = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 0 \end{pmatrix} \in M_{3,3}(\mathbf{K}).$$

To compute the characteristic polynomial of $A$ in practice, we write the usual determinant with the "indeterminate" $X$ and then we compute it by the usual rules, e.g., the Leibniz formula: since $-1 = +1$ and $2 = 0$ in $\mathbf{K}$, we get

$$\begin{aligned} \mathrm{char}_A(X) = \begin{vmatrix} X+1 & 0 & 1 \\ 0 & X+1 & 1 \\ 1 & 1 & X \end{vmatrix} &= X(X+1)^2 + 0 + 0 - (X+1) - (X+1) - 0 \\ &= X(X^2+1) = X^3 + X. \end{aligned}$$

We finish with a fundamental result about polynomials:

Theorem 9.4.7 (Euclidean division for polynomials). *Let $\mathbf{K}$ be a field, let $P_1$ and $P_2$ be polynomials in $\mathbf{K}[X]$ with $P_2 \neq 0$. There exist a unique pair $(Q, R)$ of polynomials in $\mathbf{K}[X]$ such that $R$ is either $0$ or has degree $< \deg(P_1)$, and such that*

$$P_2 = QP_1 + R.$$

One says that $Q$ is the quotient and that $R$ is the remainder in the euclidean division of $P_2$ by $P_1$.

Proof. We first prove the existence. For this purpose, we use induction with respect to the degree of $P_2$. If $P_2 = 0$ or if $0 \leqslant \deg(P_2) < \deg(P_1)$, then we may define $Q = 0$ and $R = P_2$.

Now assume that $\deg(P_2) = d \geqslant \deg(P_1) = e$ and that the result holds for polynomials of degree $\leqslant d-1$. We write

$$P_2 = a_e X^e + \cdots + a_1 X + a_0, \qquad a_e \neq 0,$$

and

$$P_1 = b_d X^d + \cdots + b_1 X + b_0, \qquad b_d \neq 0.$$

Since $d \geqslant e$, the polynomial

$$P_3 = P_1 - \frac{b_d}{a_e} X^{d-e} P_2$$

is well-defined. We have

$$P_3 = b_d X^d + \cdots + b_0 - \Big( b_d X^d + \frac{b_d a_{e-1}}{a_e} X^{d-1} + \cdots \Big)$$

which shows that $P_3 = 0$ or $\deg(P_3) \leqslant d-1$. By induction, there exist $Q_3$ and $R_3$ such that $R_3 = 0$ or has degree $< \deg(P_2)$ and

$$P_3 = P_2 Q_3 + R_3.$$

It follows that

$$P_1 = P_2 Q_3 + R_3 + \frac{b_d}{a_e} X^{d-e} P_2 = \Big( Q_3 + \frac{b_d}{a_e} X^{d-e} \Big) P_2 + R_3$$

which is of the desired form with $R = R_3$ and $Q = Q_3 + b_d a_e^{-1} X^{d-e}$.

We now prove the uniqueness. Assume that

$$P_1 = QP_2 + R = Q'P_2 + R'$$

with $R$ and $R'$ either 0 or with degree $< \deg(P_2)$. We then get

$$P_2(Q - Q') = R' - R.$$

But the left-hand side is either 0 or a polynomial of degree $< \deg(P_2)$, whereas the right-hand side is either 0 or a polynomial of degree $\deg(P_2) + \deg(Q - Q') \geqslant \deg(P_2)$. So the only possibility is that both sides are 0, which means that $R = R'$ and $Q = Q'$. $\square$

Example 9.4.8. In practice, one can find $Q$ and $R$ by successively cancelling the terms of higher degree, as done in the proof. For instance, with

$$P_1 = X^5 - 12X^4 + X^2 - 2, \qquad P_2 = X^2 + X - 1,$$

we get

$$\begin{aligned} P_1 = X^5 - 12X^4 + X^2 - 2 &= X^3(X^2 + X - 1) - 13X^4 + X^3 + X^2 - 2 \\ &= (X^3 - 13X^2)(X^2 + X - 1) + 14X^3 - 12X^2 - 2 \\ &= (X^3 - 13X^2 + 14X)(X^2 + X - 1) - 26X^2 + 14X - 2 \\ &= (X^3 - 13X^2 + 14X - 26)(X^2 + X - 1) + 40X - 28 \end{aligned}$$

so that $Q = X^3 - 13X^2 + 14X - 26$ and $R = 40X - 28$.

CHAPTER 10

# Quotient vector spaces

What we will discuss in this chapter is an example of one of the most important general construction in algebra (and mathematics in general), that of *quotient sets modulo an equivalence relation*. The idea involved is, in some sense, very simple, but is often considered quite abstract. We will focus on the special case of vector spaces where some geometric intuition may help understand what is happening. In turn, this helps understanding the general case.

In all this chapter, $\mathbf{K}$ is an arbitrary field.

## 10.1. Motivation

We will first present the general idea in a very special case. We consider $\mathbf{K} = \mathbf{R}$ and the real vector space $V = \mathbf{R}^2$. Let $W \subset V$ be a one-dimensional subspace, namely a line through the origin. We will explain what is the quotient vector space $V/W$.

We define first a set $X$ as the set of all lines in $\mathbf{R}^2$ parallel to $W$, where lines do not necessarily pass through the origin. So an element of $X$ is a subset of $V$. There is an obvious map $p$ from $V$ to $X$: to every point $x \in \mathbf{R}^2$, we associate the line $p(x)$ that is parallel to $W$ and passing through $x$; it is an axiom of euclidean geometry that such a line exists and is unique, and below we will check this algebraically. Note that $p$ is surjective, since if $\ell \in X$ is any line parallel to $W$, we obtain $p(x) = \ell$ for any point $x$ that belongs to $\ell$.

We will show that there is on the set $X$ a unique structure of $\mathbf{R}$-vector space such that the map $p\colon V \to X$ is a linear map.

In order to do this, in a way that will allow us to generalize the construction easily to any vector space $V$ with subspace $W$, we begin by describing $X$ and the map $p$ more algebraically. Let $v_0 \neq 0$ be a vector generating the line $W$. This means that

$$W = \{tv_0 \mid t \in \mathbf{R}\}.$$

For $v_1 \in \mathbf{R}^2$, the line $\ell = p(v_1)$ parallel to $W$ and passing through $v_1$ is the subset

$$\ell = \{v \in \mathbf{R}^2 \mid v = v_1 + w \text{ for some } w \in W\} = \{v_1 + tv_0 \mid t \in \mathbf{R}\} \subset \mathbf{R}^2.$$

Example 10.1.1. Suppose that $W$ is the horizontal axis, which means that we can take $v_0 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$. Then the elements of $X$ are horizontal lines. For any $v_1 = \begin{pmatrix} x_1 \\ y_1 \end{pmatrix}$, the horizontal line through $v_1$ is

$$\left\{\begin{pmatrix} x \\ y_1 \end{pmatrix} \mid x \in \mathbf{R}\right\} = \left\{\begin{pmatrix} x_1 \\ y_1 \end{pmatrix} + (x - x_1)\begin{pmatrix} 1 \\ 0 \end{pmatrix} \mid x \in \mathbf{R}\right\} = \left\{\begin{pmatrix} x_1 \\ y_1 \end{pmatrix} + t\begin{pmatrix} 1 \\ 0 \end{pmatrix} \mid t \in \mathbf{R}\right\}.$$

To define a vector space structure on $X$, we need to define the zero vector $0_X$, and the addition $+_X$ and multiplication $\cdot_X$ of a real number with an element of $X$. Asking that the map $p$ is linear will tell us that there is only one possibility.

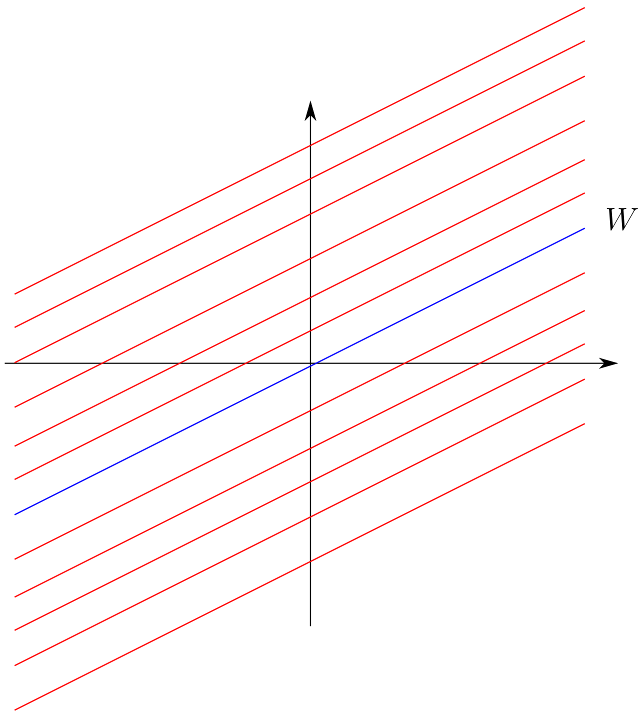


FIGURE 10.1. The red lines are non-zero elements of $X$, the blue line is the zero vector in $X$

To begin with, we must have $0_X = p(0)$, since $p$ is linear; that means that $0_X$ must be the line parallel to $W$ through the origin, in other words, that we must have $0_X = W$, seen as an element of $X$.

Now consider addition. If $\ell_1$ and $\ell_2$ are elements of $X$, we can find $v_1$ and $v_2$ in $\mathbf{R}^2$ such that $\ell_1 = p(v_1)$ and $\ell_2 = p(v_2)$ (in other words, $v_1$ is a point on $\ell_1$, and $v_2$ is a point on $\ell_2$). Since $p$ should be linear we must have

$$\ell_1 +_X \ell_2 = p(v_1) +_X p(v_2) = p(v_1 + v_2),$$

or in other words: $\ell_1 +_X \ell_2$ must be the line parallel to $W$ through the vector $v_1 + v_2$ in $\mathbf{R}^2$.

Similarly, consider $\ell \in X$ and $t \in \mathbf{R}$. If $v \in \mathbf{R}^2$ is an element of $\ell$, so that $\ell = p(v)$, we must have

$$t \cdot_X \ell = t \cdot_X p(v) = p(tv),$$

which means that the product $t \cdot_X \ell$ should be the line parallel to $W$ through the vector $tv$.

This reasoning tells us that there is at most one vector space structure on $X$ for which $p$ is linear. It does not yet say that it exists, because the definitions of addition and multiplication that it suggests might not be well-defined. The point (say for addition) is that there are many choices of vectors $v_1$ and $v_2$ in $\ell_1$ and $\ell_2$ respectively. It could then be that if we chose other points $w_1$ and $w_2$, the line parallel to $W$ through $w_1 + w_2$ would be different from the line parallel to $W$ through $v_1 + v_2$; this would be a contradiction, since we saw that either of them is supposed to be $\ell_1 +_X \ell_2$.

We now show that this does not happen. So suppose $w_1 \in \ell_1$ and $w_2 \in \ell_2$ are arbitrary. By the description above, the line in $X$ through $w_1 + w_2$ is

$$\{w_1 + w_2 + tv_0 \mid t \in \mathbf{R}\},$$

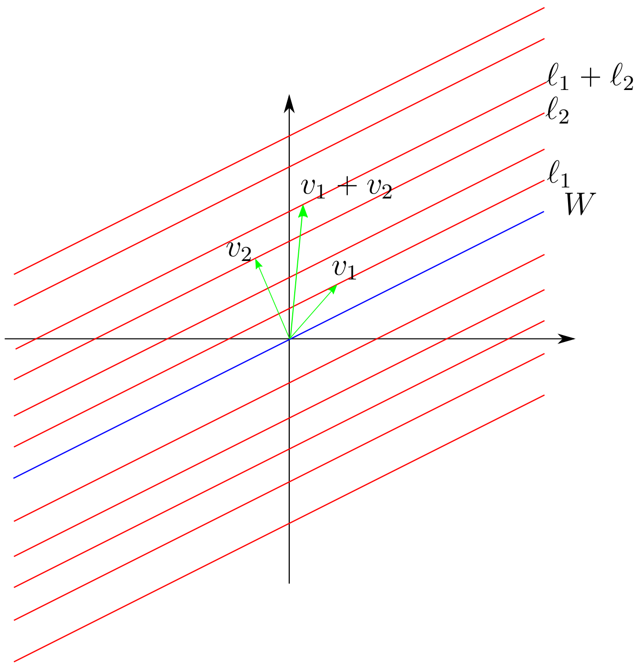


FIGURE 10.2. The sum of $\ell_1$ and $\ell_2$

and the line through $v_1 + v_2$ is

$$p(v_1 + v_2) = \{v_1 + v_2 + tv_0 \mid t \in \mathbf{R}\}.$$

To show that these lines are identical, it suffices to check that they contain a common point, since they are parallel. We will show that indeed $w_1 + w_2 \in p(v_1 + v_2)$. For this we know that $w_1$ is in the line $\ell_1$ in $X$ through $v_1$; this means that

$$w_1 \in \{v_1 + tv_0 \mid t \in \mathbf{R}\},$$

or in other words, that there exists $a \in \mathbf{R}$ such that $w_1 = v_1 + av_0$. Similarly, there exists $b \in \mathbf{R}$ such that $w_2 = v_2 + bv_0$. It follows that $w_1 + w_2 = v_1 + v_2 + (a+b)v_0$, which belongs to $p(v_1 + v_2)$.

In other words, we have constructed a well-defined map

$$+_X : X \times X \to X$$

such that

$$p(v_1) +_X p(v_2) = p(v_1 + v_2). \tag{10.1}$$

The definition is as above: the sum of two lines $\ell_1$ and $\ell_2$ in $X$ is the line parallel to $W$ passing through the sum $v_1 + v_2$ of $v_1 \in \ell_1$ and $v_2 \in \ell_2$, this definition being independent of the choice of $v_1$ in $\ell_1$ and $v_2 \in \ell_2$.

A similar reasoning applies to the product of $t \in \mathbf{R}$ with $\ell \in X$. Recall that it should be the line in $X$ passing through $tv$, and the question is whether this is well-defined: what happens if we replace $v \in \ell$ by another point $w$ in $\ell$? The answer is that since $w$ belongs to the line in $X$ through $v$, we have $w = v + av_0$ for some $a \in \mathbf{R}$, and therefore $tw = tv + atv_0$, which shows that $p(tw) = p(tv)$. Therefore the map

$$\cdot_X : \mathbf{R} \times X \to X$$

is well-defined and satisfies

$$p(tv) = t \cdot_X p(v) \tag{10.2}$$

for $t \in \mathbf{R}$ and $v \in \mathbf{R}^2$.

It now remains to check that $X$, with the zero vector $0_X = W$ and the addition and multiplication just defined, is indeed a vector space according to Definition 2.3.1. This is the case, and all axioms are verified in the same manner: by writing the points of $X$ as $p(v)$ for some $v \in \mathbf{R}^2$, by using the vector space properties of $\mathbf{R}^2$, and then using the fact that addition and multiplication have been constructed so that the map $p\colon \mathbf{R}^2 \to X$ preserves addition and multiplication (by (10.1) and (10.2)).

For instance, let us check (2.8). Fix first $t \in \mathbf{R}$ and $\ell_1$, $\ell_2$ in $X$. Write $\ell_i = p(v_i)$. Then

$$\begin{aligned} t \cdot_X (\ell_1 +_X \ell_2) = t \cdot_X (p(v_1) +_X p(v_2)) &= t \cdot_X p(v_1 + v_2) \\ = p(t(v_1 + v_2)) = p(tv_1 + tv_2) &= p(tv_1) +_X p(tv_2) \\ &= t \cdot_X p(v_1) +_X t \cdot_X p(v_2) = t \cdot_X \ell_1 +_X t \cdot_X \ell_2, \end{aligned}$$

which is the first part of (2.8). If $t_1$ and $t_2$ are in $\mathbf{R}$ and $\ell = p(v)$ in $X$, then

$$\begin{aligned} (t_1 + t_2) \cdot_X \ell &= (t_1 + t_2) \cdot_X p(v) = p((t_1 + t_2)v) = p(t_1 v + t_2 v) \\ &= p(t_1 v) +_X p(t_2 v) = t_1 \cdot_X p(v) +_X t_2 \cdot_X p(v) = t_1 \cdot_X \ell +_X t_2 \cdot_X \ell, \end{aligned}$$

which establishes the second part of (2.8).

All remaining conditions are proved in the same way, and we leave them as exercises. And finally, from (10.1) and (10.2), we next see that $p\colon V \to X$ is a linear map with respect to this vector space structure on $X$.

Before we continue to the general case, now that we now that $X$ is a vector space, and $p\colon \mathbf{R}^2 \to X$ is a surjective linear map, we can ask what is the kernel of $p$? By definition, this is the space of all $v \in \mathbf{R}^2$ such that $p(v) = 0_X = W$, which means the space of all $v$ so that the line parallel to $W$ through $v$ is $W$ itself. This means that $\mathrm{Ker}(p) = W$.

The vector space we just constructed is called the *quotient space of $V$ by $W$* and denoted $V/W$ ("$V$ modulo $W$"), and the linear map $p$ the *canonical surjection* of $V$ to $V/W$. One should always think of these are coming together.

Note that since $p\colon V \to V/W$ is surjective, we have

$$\dim(V/W) = \dim(V) - \dim \mathrm{Ker}(p) = \dim(V) - \dim(W) = 1.$$

## 10.2. General definition and properties

We now consider the general case. Let $\mathbf{K}$ be any field, $V$ a vector space over $\mathbf{K}$ and $W \subset V$ a subspace. To generalize the discussion from the previous section, we first explain the meaning of "affine subspace parallel to $W$", and the crucial property of these subspaces that generalizes the parallel axiom for lines in plane.

Definition 10.2.1 (Affine space). Let $V$ be a vector space. An **affine subspace** $A$ of $V$ is a subset of $V$ of the form

$$A_{W,v_0} = \{v \in V \mid v = v_0 + w \text{ for some } w \in W\}$$

for some vector subspace $W \subset V$ and some $v_0 \in V$. The **dimension** of $A_{W,v_0}$ is defined to be the dimension of $W$. We then say that the affine subspace $A$ is **parallel** to $W$.

If $A$ is an affine subspace of $V$, then the corresponding vector subspace is uniquely determined by $A$. Indeed, if $A = A_{W,v_0}$, then

$$W = \{v - v_0 \mid v \in A\}.$$

We call $W$ the **vector subspace associated** to the affine subspace $A$.

The crucial property is the following:

LEMMA 10.2.2. *Let $V$ be a $\mathbf{K}$ vector space and $W$ a vector subspace of $V$. Then any $v \in V$ belongs to a unique affine subspace parallel to $W$, namely $A_{W,v}$. In particular, two parallel affine subspaces $A_1$ and $A_2$ are either equal or have empty intersection.*

PROOF. Since $v \in A_{W,v}$, any $v \in V$ belongs to some affine subspace parallel to $W$. We then need to show that it belongs to only one such affine subspace. But assume $v \in A_{W,v'}$ for some $v' \in V$. This means that $v = v' + w_0$ for some $w_0 \in W$. But then for any $w$ in $W$, we get

$$v + w = v' + (w + w_0) \in A_{W,v'}, \qquad v' + w = v + (w - w_0) \in A_{W,v},$$

which means that in fact $A_{W,v} = A_{W,v'}$. So $v$ belongs only to the affine subspace $A_{W,v}$ parallel to $W$. ☐

Now we define a map $p\colon V \to X$ by $p(v) = A_{W,v}$, which is therefore the unique affine subspace of $V$ parallel to $W$ containing $v$. Note that $p$ is surjective since any affine subspace $A$ parallel to $W$ contains some point $v$, which then satisfies $p(v) = A$.

We will now define a new vector space $X$ and a linear map $p\colon V \to X$ as follows:

- The set $X$ is the set of all affine subspaces of $V$ parallel to $W$;
- The zero element of $X$ is the affine subspace $A_{W,0} = W$;
- The sum of $A_{W,v_1}$ and $A_{W,v_2}$ in $X$ is $A_{W,v_1+v_2}$;
- The product of $t \in \mathbf{K}$ and $A_{W,v} \in X$ is $A_{W,tv} \in X$;

and we will check that $p\colon V \to X$ is linear, and that its kernel is equal to $W$.

To check that this makes sense we must first check that the operations we defined make sense (namely, that $A_{W,v_1+v_2}$ is independent of the choice of vectors $v_1$ and $v_2$ in the respective affine subspaces $A_{W,v_1}$ and $A_{W,v_2}$, and similarly for the product), and then that $p$ is linear. These checks will be exactly similar to those in the previous section, and justify the following definition:

DEFINITION 10.2.3 (Quotient space). The vector space $X$ is denoted $V/W$ and called the **quotient space of $V$ by $W$**. The linear map $p\colon V \to V/W$ is called the **canonical surjection** from $V$ to $V/W$.

PROOF OF THE ASSERTIONS. We begin by checking that the addition on $X$ is well-defined. Let $A_1$ and $A_2$ be two affine subspaces parallel to $W$. Let $v_1$ and $w_1$ be two elements of $V$ such that $A_1 = A_{W,v_1} = A_{W,w_1}$ and let $v_2$ and $w_2$ be two elements of $V$ such that $A_2 = A_{W,v_2} = A_{W,w_2}$. We want to check that $A_{W,v_1+v_2} = A_{W,w_1+w_2}$, so that the sum

$$A_1 + A_2 = A_{W,v_1+v_2}$$

in $X$ is well-defined. By Lemma 10.2.2, it suffices to show that $w_1 + w_2 \in A_{W,v_1+v_2}$. This is indeed the case: since $w_1 \in A_1 = A_{W,v_1}$, there exists $x_1 \in W$ such that $w_1 = v_1 + x_1$, and similarly there exists $x_2 \in W$ such that $w_2 = v_2 + x_2$. But then $w_1 + w_2 = v_1 + v_2 + (x_1 + x_2) \in A_{W,v_1+v_2}$.

Similarly, we check that the multiplication of $A \in X$ by $t \in \mathbf{R}$ is well-defined.

These two facts imply in particular the compatibility of $p\colon V \to X$ with addition and multiplication:

$$p(v_1 + v_2) = p(v_1) + p(v_2), \qquad p(tv) = tp(v),$$

where the addition on the right-hand side of the first formula is the addition in $X$.

From this, it follows easily as in the previous section that this addition and multiplication satisfy of the conditions for a vector space structure on $X$. For instance, we check (2.6) this time. Let $t_1$ and $t_2$ be elements of $\mathbf{K}$, and $A \in X$. Write $A = p(v)$ for some $v \in V$, which is possible since $p$ is surjective. Then we have

$$\begin{aligned}(t_1t_2)\cdot A = (t_1t_2)\cdot p(v) = p((t_1t_2)v) = p(t_1(t_2v))\\ = t_1p(t_2v) = t_1\cdot(t_2\cdot p(v)) = t_1\cdot(t_2\cdot A).\end{aligned}$$

Now that we know that $X$ is a vector space, the compatibility relations of $p$ mean that $p$ is linear. Moreover, we have $\mathrm{Ker}(p) = \{v \in V \mid p(v) = W \in X\} = W$. ☐

Corollary 10.2.4. *Let $V$ and $W$ be finite-dimensional vector spaces. Then $V/W$ is finite-dimensional and*

$$\dim(V/W) = \dim(V) - \dim(W).$$

Proof. Since $p\colon V \to V/W$ is linear and surjective, the space $V/W$ has finite dimension $\leqslant \dim V$. Then from Theorem 2.8.4 we get

$$\dim(V) = \dim \mathrm{Im}(p) + \dim \mathrm{Ker}(p) = \dim(V/W) + \dim(W)$$

since $\mathrm{Ker}(p) = W$ and $p$ is surjective. ☐

Example 10.2.5. The simplest examples of quotient spaces are when $W = V$ and $W = \{0\}$. In the first case, the only element of $V/W$ is $W = V$ itself, so that $V/W = \{0_{V/W}\}$. In the second case, the elements of $V/W$ are the sets $\{x\}$ for $x \in V$, and the map $p$ is $x \mapsto \{x\}$. Hence $p$ is an isomorphism $V \to V/\{0\}$. In general, one simply identifies $V$ and $V/\{0\}$, although properly speaking these are not the same sets.

## 10.3. Examples

Quotient spaces are examples of these mathematical objects that seem to be very abstract at first, but that turn out to occur, implicitly or explicitly, everywhere, including where one didn't suspect their presence. We will give some instances of this here.

Example 10.3.1. First, recall that we constructed $V/W$ not in a vacuum, but with a surjective linear map $p\colon V \to V/W$ with kernel $W$. It turns out that this data is enough to characterize very strongly $V/W$:

Proposition 10.3.2 (First isomorphism theorem). *Let $V$ be a $\mathbf{K}$-vector space and $W \subset V$ a subspace. Let $X$ be a $\mathbf{K}$-vector space and $f\colon V \to X$ a surjective linear map such that $\mathrm{Ker}(f) = W$. Then there exists a unique isomorphism*

$$g\colon V/W \to X$$

*such that $g \circ p = f$, where $p\colon V \to V/W$ is the canonical surjection.*

It is very convenient to draw diagrams to understand this type of statements, in this case the following:

$$\begin{tikzcd} V \arrow[r, "f"] \arrow[d, "p"] & X \\ V/W \arrow[ur, "g"] & \end{tikzcd}$$

In other words, if a vector space $X$, coming with a surjective linear map $V \to X$ "looks like $V/W$", then it is isomorphic to $V/W$, and the isomorphism is "natural", in the sense that it involves no choice (of a basis, or of a complement, or of anything else).

Proof. Let $A \in V/W$. To define $g(A)$, we write $A = p(v)$ for some $v \in V$; then the only possible choice for $g(A)$, in order that the relation $g \circ p = f$ holds, is that $g(A) = g(p(v)) = f(v)$.

The question is then whether this definition makes sense: one more, the issue is that there are many $v \in V$ with $p(v) = A$, and we must check that $f(v)$ is independent of this choice, and only depends on $A$. To see this, let $v' \in V$ by any other element with $p(v') = A$. Then $A = A_{W,v}$, and $v' \in V$, means that there exists $w \in W$ such that $v' = v + w$. We now deduce that $f(v') = f(v) + f(w) = f(v)$ *because* $\mathrm{Ker}(f) = W$.

So the application $g\colon V/W \to X$ is well-defined. By construction, we see that $g\circ p = f$. We now check that it is linear: if $A_1 = A_{W,v_1}$ and $A_2 = A_{W,v_2}$ are elements of $V/W$, and $t_1$, $t_2$ elements of $\mathbf{K}$, then we know that

$$t_1A_1 + t_2A_2 = p(t_1v_1 + t_2v_2).$$

Therefore, our definition implies that $g(t_1A_1 + t_2A_2) = f(t_1v_1 + t_2v_2) = t_1f(v_1) + t_2f(v_2)$ since $f$ is linear. This means that $g(t_1A_1 + t_2A_2) = t_1g(A_1) + t_2g(A_2)$.

Finally, we prove that $g$ is an isomorphism. First, since $f$ is surjective, for any $x \in X$, we can write $x = f(v)$ for some $v \in V$, and then $x = g(p(v))$, so that $x$ belongs to the image of $g$. Therefore $g$ is surjective. Second, let $A \in \mathrm{Ker}(g)$. If we write $A = p(v)$, this means that $0 = g(A) = f(v)$, and therefore $v \in \mathrm{Ker}(f) = W$. But then $A = p(v) = 0_{V/W}$. Hence $g$ is also injective. ☐

Using this, we can often identify even the most familiar spaces with a quotient space.

Corollary 10.3.3. *Let $f\colon V_1 \to V_2$ be any linear map. There exists a unique isomorphism $g\colon V_1/\mathrm{Ker}(f) \to \mathrm{Im}(f)$ such that $f = g \circ p$, where $p\colon V_1 \to V_1/\mathrm{Ker}(f)$ is the canonical surjection:*

$$\begin{tikzcd} V_1 \arrow[r, "f"] \arrow[d, "p"'] & \mathrm{Im}(f) \\ V_1/\mathrm{Ker}(f) \arrow[ur, "g"'] & \end{tikzcd}$$

Proof. The linear map $f$ defines a surjective map $V_1 \to \mathrm{Im}(f)$, which we still denote $f$. Since the kernel of this linear map is indeed the kernel of $f$, the proposition shows that there exists a unique isomorphism $g\colon V_1/W \to \mathrm{Im}(f)$ such that $g\circ p = f$, or in other words an isomorphism $V_1/\mathrm{Ker}(f) \to \mathrm{Im}(f)$. ☐

Example 10.3.4. Another way to interpret a quotient space is a an analogue of a complementary subspace.

Proposition 10.3.5. *Let $W \subset V$ be a subspace and $W' \subset V$ a complementary subspace so that $W \oplus W' = V$. The restriction $p|W'$ of the canonical surjection $p\colon V \to V/W$ is an isomorphism $p|W'\colon W' \to V/W$.*

Proof. The restriction $p|W'$ is linear. Its kernel is $\mathrm{Ker}(p) \cap W' = W \cap W' = \{0\}$, by definition of the complement, so that it is injective. To show that $p|W'$ is surjective, let $A \in V/W$. There exists $v \in V$ such that $p(v) = A$, and we can write $v = w + w'$ where $w \in W$ and $w' \in W'$. Then $A = p(v) = p(w')$ (since $p(w) = 0$), which means that $A$ is in the image of $p|W'$. Therefore $p|W'$ is surjective, hence is an isomorphism. ☐

Example 10.3.6 (Linear maps from a quotient space). One can also think of $V/W$ in terms of the linear maps from this space to any other space.

Proposition 10.3.7. *Let $V$ be a vector space and $W$ a subspace. Let $p\colon V \to V/W$ be the canonical surjection. For any vector space $V_1$, the map*

$$f \mapsto f \circ p$$

*is an isomorphism*

$$\mathrm{Hom}_{\mathbf{K}}(V/W, V_1) \to \{g \in \mathrm{Hom}_{\mathbf{K}}(V, V_1) \mid W \subset \mathrm{Ker}(g)\}.$$

What this means is that it is equivalent to give a linear map $V/W \to V_1$ (which is a data involving the quotient space $V/W$) or to give a linear map $V \to V_1$ whose kernel contains $W$ (which does not refer to the quotient space at all). This makes is often possible to argue about properties of quotient spaces without referring to their specific definitions!

Definition 10.3.8 (Linear maps defined by passing to the quotient). Given a linear map $g\colon V \to V_1$ with $W \subset \mathrm{Ker}(g)$, the linear map $f\colon V/W \to V_1$ with $f \circ p = g$ is called the **linear map obtained from $g$ by passing to the quotient modulo $W$**.

Proof. It is elementary that $f \mapsto f \circ p$ is a linear map

$$\phi\colon\ \mathrm{Hom}_{\mathbf{K}}(V/W, V_1) \to \mathrm{Hom}_{\mathbf{K}}(V, V_1).$$

What we claim is that $\phi$ is injective and that its image consists of the subspace $E$ of $\mathrm{Hom}_{\mathbf{K}}(V, V_1)$ made of those $g\colon V \to V_1$ such that $W \subset \mathrm{Ker}(g)$. Note that it is also elementary that $E$ is a subspace of $\mathrm{Hom}_{\mathbf{K}}(V, V_1)$.

To prove injectivity, assume that $f \circ p = 0 \in \mathrm{Hom}_{\mathbf{K}}(V, V_1)$. This means that $f(p(v)) = 0$ for all $v \in V$. Since $p$ is surjective, this implies that $f(A) = 0$ for all $A \in V/W$, and hence that $f = 0$. So $\mathrm{Ker}(\phi) = \{0\}$, and $\phi$ is injective.

If $g = f \circ p$ belongs to $\mathrm{Im}(\phi)$, then for any $w \in W$, we get $g(w) = f(p(w)) = f(0) = 0$, so that the kernel of $g$ contains $W$. Therefore $g \in E$. Conversely, let $g\colon V \to V_1$ be a linear map such that $W \subset \mathrm{Ker}(g)$. We wish to define $f\colon V/W \to V_1$ such that $f \circ p = g$.

Let $A \in V/W$, and let $v \in V$ be such that $p(v) = A$. We must define $f(A) = g(v)$ if we want $f \circ p = g$. As usual, we must check that this is well-defined. But if $v' \in V$ is another element of $A$, then $v - v'$ belongs to $W$, so that $g(v) = g(v')$ since $W \subset \mathrm{Ker}(g)$. Hence $g$ is indeed well-defined. It satisfies $g = f \circ p$, so that it is a linear map and $\phi(f) = g$. Therefore $E \subset \mathrm{Im}(\phi)$, and the proof is finished. ☐

It is useful to know the kernel and image of a linear map obtained in such a way.

Proposition 10.3.9. *Let $V_1$ and $V_2$ be vector spaces and $W$ a subspace of $V_1$. Let $f\colon V_1 \to V_2$ be a linear map with $W \subset \mathrm{Ker}(f)$, and let $\tilde{f}\colon V_1/W \to V_2$ be the linear map obtained from $f$ by passing to the quotient modulo $W$.*

(1) *The image of $\tilde{f}$ is equal to the image of $f$; in particular, $\tilde{f}$ is surjective if and only if $f$ is surjective.*

(2) *The restriction to $\mathrm{Ker}(f)$ of the canonical surjection $p\colon V_1 \to V_1/W$ induces by passing to the quotient an isomorphism*

$$\mathrm{Ker}(f)/W \to \mathrm{Ker}(\tilde{f}).$$

*In particular, $\tilde{f}$ is injective if and only if the kernel of $f$ is exactly equal to $W$.*

Proof. By definition, we have $f = \tilde{f} \circ p$.

(1) Since $p$ is surjective, any $\tilde{f}(A)$ is of the form $\tilde{f}(p(v)) = f(v)$ for some $v \in V_1$, and hence the image of $\tilde{f}$ is contained in the image of $f$. On the other hand, $f(v) = \tilde{f}(p(v))$ shows that $\mathrm{Im}(\tilde{f}) \supset \mathrm{Im}(f)$, so there is equality.

(2) If $v \in \mathrm{Ker}(f)$, then $\tilde{f}(p(v)) = f(v) = 0$, so that $p(v) \in \mathrm{Ker}(\tilde{f})$. Therefore the restriction $\tilde{p}$ of $p$ to $\mathrm{Ker}(f)$ defines a linear map $\tilde{p}\colon \mathrm{Ker}(f) \to \mathrm{Ker}(\tilde{f})$. The kernel of this linear map is $W$ (since $W = \mathrm{Ker}(p)$ and $W \subset \mathrm{Ker}(f)$). Moreover, $\tilde{p}$ is surjective: if $A \in \mathrm{Ker}(\tilde{f})$, then writing $A = p(v)$, we obtain $f(v) = \tilde{f}(A) = 0$, so that $v \in \mathrm{Ker}(f)$, and then $A = \tilde{p}(v)$. By Proposition 10.3.2, we obtain an isomorphism

$$\mathrm{Ker}(f)/W \to \mathrm{Ker}(\tilde{f}).$$

∎

Example 10.3.10. Taking $V_1 = \mathbf{K}$ in Proposition 10.3.7, we obtain a description of the dual space of $V/W$: the map $\ell \mapsto \ell \circ p$ is an isomorphism

$$(V/W)^* \to \{\lambda \in V^* \mid \lambda(W) = 0\} = W^\perp,$$

in other words, the dual of $V/W$ is the subspace of the dual of $V$ consisting of linear maps that are zero on $W$.

Dually we have the description of the dual of a subspace:

Proposition 10.3.11. *Let $V$ be a $\mathbf{K}$-vector space and $W \subset V$ a subspace of $V$. Then the restriction map $\lambda \mapsto \lambda|W$ from $V^*$ to $W^*$ induces by passing to the quotient an isomorphism*

$$V^*/W^\perp \to W^*.$$

Proof. We first check that the restriction map, which we denote $f\colon V^* \to W^*$, passes to the quotient modulo $W^\perp \subset V^*$, which means that $W^\perp$ is a subset of $\mathrm{Ker}(f)$ (Definition 10.3.8). In fact, by definition, we have $\lambda \in W^\perp$ if and only if $\lambda$ is zero on $W$, and so we have the equality $W^\perp = \mathrm{Ker}(f)$. In particular, it follows (Proposition 10.3.9 (2)) that the induced linear map $\tilde{f}\colon V^*/W^\perp \to W^*$ is injective.

To prove surjectivity, it suffices to prove that $f$ itself is surjective. But $f$ is the transpose of the linear inclusion $W \to V$, which is injective, and hence it is surjective by Proposition 8.2.6 (2). ∎

Example 10.3.12. Let $V$ be a vector space, $W \subset V$ a subspace and $f \in \mathrm{End}_{\mathbf{K}}(V)$ an endomorphism of $V$. We assume that $W$ is stable under $f$n, namely that we have $f(W) \subset W$.

Let $p\colon V \to V/W$ be the canonical surjection. We obtain a composite linear map

$$V \xrightarrow{f} V \xrightarrow{p} V/W,$$

and for all $w \in W$, we have $f(w) \in W$, and therefore $p(f(w)) = 0$ in $V/W$. By Proposition 10.3.7, there exists therefore a unique linear map $\tilde{f}\colon V/W \to V/W$ such that $\tilde{f} \circ p = p \circ f$. This endomorphism $\tilde{f}$ of $V/W$ is called the *endomorphism of* $V/W$ induced by $f$. It is computed, according to the proposition, in the following manner: for $A \in V/W$, one writes $A = p(v)$ for some $v \in V$; one computes $f(v) \in V$; then $\tilde{f}(v) = p(f(v))$. In other words, $\tilde{f}(A)$ is the affine subspace parallel to $W$ that contains $f(v)$ for any element $v$ of $A$.

This is summarized by the diagram

$$\begin{tikzcd} V \arrow[r, "f"] \arrow[d, "p"] & V \arrow[d, "p"] \\ V/W \arrow[r, "\tilde{f}"] & V/W. \end{tikzcd}$$

We can "visualize" this endomorphism as follows if $V$ is finite-dimensional. Let $n = \dim(V)$, $m = \dim(W)$, and let $B = (B_1, B_2)$ be an ordered basis of $V$ such that $B_1$ is a basis of $W$. The matrix of $f$ with respect to $B$ has a block form

$$\begin{pmatrix} A_1 & A_2 \\ 0_{n-m,m} & A_4 \end{pmatrix}$$

where $A_1 = \mathrm{Mat}(f|W; B_1, B_1)$ (where $f|W$ is the endomorphism of $W$ induced by $f$, which is defined since $f(W) \subset W$), $A_2 \in M_{m,n-m}(\mathbf{K})$ and $A_4 = M_{n-m,n-m}(\mathbf{K})$.

The space $W'$ generated by $B_2$ is a complement to $W$ in $V$. So the restriction of $p$ to $W'$ is an isomorphism $p|W' \colon W' \to V/W$ (Proposition 10.3.5). In particular, if we write $B_2 = (x_1, \ldots, x_{m-n})$, the vectors

$$B_3 = (p(x_1), \ldots, p(x_{m-n}))$$

form an ordered basis of $V/W$. We then have the relation

$$A_4 = \mathrm{Mat}(\tilde{f}; B_3, B_3).$$

In other words, the "lower right" block of $\mathrm{Mat}(f; B, B)$ is the matrix representing the action of $f$ on $V/W$.

Example 10.3.13. We now give a very concrete example. Let $V = \mathbf{K}[X]$ be the space of polynomials with coefficients in $\mathbf{K}$. Let $n \geqslant 1$ and let $W_n$ be the subspace generated by $X^i$ for $i \geqslant n+1$. There is an obvious complementary subspace $W_n'$ to $W_n$, namely the subspace generated by $1, \ldots, X^n$. By Proposition 10.3.5, the restriction of the canonical projection to $W_n'$ is therefore an isomorphism $p_n \colon W_n' \to V/W_n$.

Consider the endomorphism $f$ of $V$ defined by $f(P) = XP$. Since $f(X^i) = X^{i+1}$, it follows that $f(W_n) \subset W_n$. Let $\tilde{f}_n$ be the endomorphism of $V/W_n$ obtained from $f$ by passing to the quotient, as in the previous example.

The vectors $(v_0, \ldots, v_n)$, where $v_i = p_n(X^i)$ for $0 \leqslant i \leqslant n$, form a basis $B_n$ of $V/W_n$. We will compute the matrix $\mathrm{Mat}(\tilde{f}_n; B_n, B_n)$ as an example of concrete computation with quotient spaces.

For $0 \leqslant i \leqslant n-1$, we have $f(X^i) = X^{i+1}$, which implies that $\tilde{f}_n(v_i) = v_{i+1}$. For $i = n$, we have $f(X^n) = X^{n+1} \in W_n$, and this means that $\tilde{f}_n(v_n) = 0$. Therefore the matrix is

$$\mathrm{Mat}(\tilde{f}_n; B_n, B_n) = \begin{pmatrix} 0 & 0 & 0 & \cdots & \cdots \\ 1 & 0 & 0 & & \cdots \\ 0 & 1 & 0 & & \cdots \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & \cdots & 1 & 0 & 0 \\ 0 & \cdots & \cdots & 1 & 0 \end{pmatrix} \in M_{n+1,n+1}(\mathbf{K}).$$

This is the transpose of the Jordan block $J_{n+1,0}$. What is interesting here is that it shows that the Jordan blocks (or their transposes) of *all* sizes are defined uniformly in terms of the single endomorphism $f$ of the space $V$.

Example 10.3.14. Consider a $\mathbf{K}$-vector space $V$ and two subspaces $W_1$ and $W_2$. Then $W_1$ is a subspace of $W_1 + W_2$. The following important proposition identifies the quotient space $(W_1 + W_2)/W_1$.

Proposition 10.3.15 (Second isomorphism theorem). *The composition*

$$f\colon W_2 \to W_1 + W_2 \to (W_1 + W_2)/W_1,$$

*where the first map is the inclusion of $W_2$ in $W_1 + W_2$ and the second is the canonical surjection $p$, passes to the quotient by $W_2 \cap W_1$ and induces an isomorphism*

$$W_2/(W_1 \cap W_2) \to (W_1 + W_2)/W_1.$$

Proof. The kernel of the composition $f$ is the set of vectors $v \in W_2$ which belong to the kernel $W_1$ of the canonical surjection $p$, which means that $\mathrm{Ker}(f) = W_1 \cap W_2$. Hence by Proposition 10.3.9 (2), $f$ passes to the quotient to define an injective linear map

$$\tilde{f}\colon W_2/(W_1 \cap W_2) \to (W_1 + W_2)/W_1.$$

It remains to check that $\tilde{f}$ is surjective. Thus let $x \in (W_1+W_2)/W_1$. There exists $w_1 \in W_1$ and $w_2 \in W_2$ such that $x = p(w_1 + w_2)$. But since $w_1 \in W_1$, we have in fact $x = p(w_2)$, and that means $f(w_2) = p(w_2) = x$. Hence $f$ is surjective, and (Proposition 10.3.9 (1)) so is $\tilde{f}$. ☐

Example 10.3.16. We now consider the *subspaces* of a quotient space. These are very simply understood:

Proposition 10.3.17. *Let $V$ be a $\mathbf{K}$-vector space and $W$ a subspace of $V$. Let $\pi\colon V \to V/W$ be the canonical projection. Let $X$ be the set of all vector subspaces of $V/W$ and let $Y$ be the set of all vector subspaces of $V$ which contain $W$.*

(1) *The maps*

$$I \begin{cases} Y \to X \\ E \mapsto \pi(E) \end{cases} \qquad \text{and} \qquad J \begin{cases} X \to Y \\ F \mapsto \pi^{-1}(F) \end{cases}$$

*are reciprocal bijections.*

(2) *These bijections preserve inclusion: for subspaces $E_1$ and $E_2$ of $V$, both containing $W$, we have $E_1 \subset E_2$ if and only if $\pi(E_1) \subset \pi(E_2)$.*

(3) *For a subspace $E \in Y$ of $V$, the restriction of $\pi$ to $E$ passes to the quotient to induce an injective linear map*

$$E/W \to V/W,$$

*with image equal to $\pi(E)$.*

Proof. (1) It is elementary that $I$ and $J$ are well-defined, since the image and inverse images of subspaces are subspaces, and since $\pi^{-1}(F)$ contains $\pi^{-1}(\{0\}) = \mathrm{Ker}(\pi) = W$ for any subspace $F$ of $V/W$.

We first check that $I \circ J = \mathrm{Id}_X$. Let $F$ be a subspace of $V/W$; then $J(F) = \pi^{-1}(F)$. Let $F_1 = I(J(F)) = \pi(\pi^{-1}(F))$. Since $v \in \pi^{-1}(F)$ if and only if $\pi(v) \in F$, we obtain $F_1 \subset F$. Conversely, let $w \in F$. Write $w = \pi(v)$ for some $v \in V$. Then $v \in \pi^{-1}(F)$, and hence $w \in \pi(\pi^{-1}(F))$. This means that $F \subset F_1$, and therefore $F = F_1$. This means that $I \circ J = \mathrm{Id}_X$.

Now we check that $J \circ I = \mathrm{Id}_Y$. So let $E$ be a subspace of $V$ containing $W$ and $E_1 = \pi^{-1}(\pi(E))$. We have $v \in E_1$ if and only if $\pi(v) \in \pi(E)$. In particular, this immediately implies that $E \subset E_1$. Conversely, let $v \in E_1$ be any vector. Since $\pi(v) \in \pi(E)$, there exists $v_1 \in E$ such that $\pi(v) = \pi(v_1)$. This means that $v - v_1 \in \mathrm{Ker}(\pi) = W \subset E$ (since $E \in Y$), and hence

$$v = (v - v_1) + v_1 \in E.$$

We conclude that $E_1 \subset E$, so that $E_1 = E$, and this gives $J \circ I = \mathrm{Id}_Y$.

(2) This is an elementary property.

(3) The restriction of $\pi$ to $E$ is a linear map $E \to V/W$. Its kernel is $E \cap W = E$ (since $E \in Y$), and therefore it induces an injective linear map $E/W \to V/W$ (Proposition 10.3.7 and Proposition 10.3.9 (2)). The image of this map is the image of $\pi|E$, which is $\pi(E)$ (Proposition 10.3.9 (1)). $\square$

REMARK 10.3.18. One must be careful that if $E$ is an arbitrary subspace of $V$, it is not always the case that $\pi^{-1}(\pi(E)) = E$! For instance, $\pi^{-1}(\pi(\{0\})) = \pi^{-1}(\{0\}) = W$.

The meaning of this proposition is that subspaces of $V/W$ "correspond" exactly to subspaces of $V$ which contain $W$. One can also determine *quotients* of subspaces of $V/W$.

PROPOSITION 10.3.19 (Third isomorphism theorem). *Let $V$ be a vector space and $W$ a subspace. Let $\pi$ denote the canonical projection $V \to V/W$. Let $E_1 \subset E_2$ be two subspaces of $V$ containing $W$. Denote $F_i = \pi(E_i)$. Then $F_1 \subset F_2$. Let $\pi_1 \colon F_2 \to F_2/F_1$ be the canonical surjection modulo $F_1$. The linear map $f \colon E_2 \to F_2/F_1$ defined as the composition*

$$E_2 \xrightarrow{\pi} F_2 \xrightarrow{\pi_1} F_2/F_1$$

*passes to the quotient modulo $E_1$ and induces an isomorphism*

$$E_2/E_1 \to F_2/F_1.$$

One often writes the result of this proposition in the form

$$(E_2/W)/(E_1/W) = E_2/E_1.$$

PROOF. First, the composition defining $f$ makes sense since $\pi(E_2) = F_2$. The kernel of $f$ is the set of vectors $v \in E_2$ such that $\pi(v) \in \mathrm{Ker}(\pi_1) = F_1$, or in other words it is $\pi^{-1}(F_1)$, which is equal to $E_1$ by Proposition 10.3.17 (1) since $F_1 = \pi(E_1)$. So (by Proposition 10.3.9 (2)) the map $f$ passes to the quotient modulo $E_1$ and induces an injective linear map $E_2/E_1 \to F_2/F_1$. The image of this map is the same as the image of $f$. Since $f$ is surjective (because $\pi$ maps $E_2$ to $F_2$ by definition and $\pi_1$ is surjective), it follows that $f$ is an isomorphism. $\square$

CHAPTER 11

# Tensor products and multilinear algebra

In this chapter, we use quotient spaces for the very important construction of the *tensor product* of vector spaces over a field.

## 11.1. The tensor product of vector spaces

Let $\mathbf{K}$ be a field and let $V_1$ and $V_2$ be $\mathbf{K}$-vector spaces. For any $\mathbf{K}$-vector space $W$, we denote by $\mathrm{Bil}_{\mathbf{K}}(V_1, V_2; W)$ the vector space of all $\mathbf{K}$-bilinear maps $V_1 \times V_2 \to W$, i.e., the space of all maps $b\colon V_1 \times V_2 \to W$ such that

$$\begin{aligned} b(tv_1 + sv_1', v_2) &= tb(v_1, v_2) + sb(v_1', v_2) \\ b(v_1, tv_2 + sv_2') &= tb(v_1, v_2) + sb(v_1, v_2') \end{aligned}$$

for all $s$, $t \in \mathbf{K}$ and $v_1$, $v_1' \in V_1$, $v_2$, $v_2' \in V_2$.

This space is a vector subspace of the space of all (set-theoretic) maps from $V_1 \times V_2$ to $W$ (Example 2.3.6 (3)).

Example 11.1.1. (1) We already saw examples of bilinear forms in the study of euclidean spaces for instance: if $V$ is a $\mathbf{R}$-vector space, then a scalar product on $V$ is an element of $\mathrm{Bil}_{\mathbf{R}}(V, V; \mathbf{R})$.

(2) For any field $\mathbf{K}$ and any $\mathbf{K}$-vector space $V$, the map

$$b \begin{cases} V \times V^* \to \mathbf{K} \\ (v, \lambda) \mapsto \langle \lambda, v \rangle \end{cases}$$

is in $\mathrm{Bil}_{\mathbf{K}}(V, V^*; \mathbf{K})$.

(3) For any field $\mathbf{K}$ and any $\mathbf{K}$-vector space $V$, the map

$$\begin{cases} \mathrm{End}_{\mathbf{K}}(V) \times \mathrm{End}_{\mathbf{K}}(V) \to \mathrm{End}_{\mathbf{K}}(V) \\ (f, g) \mapsto f \circ g \end{cases}$$

is an element of $\mathrm{Bil}_{\mathbf{K}}(\mathrm{End}_{\mathbf{K}}(V), \mathrm{End}_{\mathbf{K}}(V); \mathrm{End}_{\mathbf{K}}(V))$.

(4) Let $m$, $n$, $p \geqslant 1$ be integers. The map

$$\begin{cases} M_{m,n}(\mathbf{K}) \times M_{p,m}(\mathbf{K}) \to M_{p,n}(\mathbf{K}) \\ (A_1, A_2) \mapsto A_2 A_1 \end{cases}$$

is bilinear, and is an element of $\mathrm{Bil}_{\mathbf{K}}(M_{m,n}(\mathbf{K}), M_{p,m}(\mathbf{K}); M_{p,n}(\mathbf{K}))$.

If $b\colon V_1 \times V_2 \to W_1$ is a bilinear map in $\mathrm{Bil}_{\mathbf{K}}(V_1, V_2; W_1)$ and $f\colon W_1 \to W_2$ is a linear map, then

$$f \circ b\colon V_1 \times V_2 \to W_2$$

is an element of $\mathrm{Bil}_{\mathbf{K}}(V_1, V_2; W_2)$.

The tensor product construction creates a vector space $V_1 \times_{\mathbf{K}} V_2$, called the "tensor product of $V_1$ and $V_2$ over $\mathbf{K}$", in such a way that, for any $\mathbf{K}$-vector space $W$, the *linear* *maps* correspond exactly and naturally to the *bilinear maps* from $V_1 \times V_2$ to $W$ using this composition.

The precise statement is the following result, that we will first prove before discussing with examples *why*, despite the abstract appearance of this construction, this is in fact a very useful thing to know.

THEOREM 11.1.2 (Construction of tensor product). *Let* $\mathbf{K}$ *be a field. Let* $V_1$ *and* $V_2$ *be* $\mathbf{K}$*-vector spaces. There exists a* $\mathbf{K}$*-vector space* $V_1 \otimes_{\mathbf{K}} V_2$ *and a bilinear map*

$$b_0 \colon V_1 \times V_2 \to V_1 \otimes_{\mathbf{K}} V_2,$$

*denoted* $b_0(v_1, v_2) = v_1 \otimes v_2$*, such that for any* $\mathbf{K}$*-vector space* $W$*, the composition application* $f \mapsto f \circ b_0$ *is an isomorphism*

$$\mathrm{Hom}_{\mathbf{K}}(V_1 \otimes_{\mathbf{K}} V_2, W) \to \mathrm{Bil}_{\mathbf{K}}(V_1, V_2; W)$$

*of* $\mathbf{K}$*-vector spaces.*

*Moreover, the vector space* $V_1 \otimes_{\mathbf{K}} V_2$ *is generated by the set of vectors* $v_1 \otimes v_2$ *for* $(v_1, v_2) \in V_1 \times V_2$*.*

The following diagram illustrates the statement:

$$\begin{tikzcd} V_1 \times V_2 \arrow[r, "b"] \arrow[d, "b_0"] & W \\ V_1 \otimes_{\mathbf{K}} V_2 \arrow[ur, "f"] & \end{tikzcd}$$

DEFINITION 11.1.3 (Tensor product). The space $V_1 \otimes_{\mathbf{K}} V_2$, together with the bilinear map $b_0$, is called the **tensor product of** $V_1$ **and** $V_2$ **over** $\mathbf{K}$.

(We emphasize the bilinear map $b_0$ also in the definition, because it is necessary to characterize the tensor product by the property of the theorem, as we will see.)

PROOF. We will construct $V_1 \otimes_{\mathbf{K}} V_2$ and $b$ by a quotient space construction. We first consider a vector space $E$ over $\mathbf{K}$ with basis $B = V_1 \times V_2$. This means that an element of $E$ is a finite sum of the type

$$\sum_{i=1}^{n} t_i(v_i, w_i)$$

where $n \geqslant 0$ (with $n = 0$ corresponding to the zero vector $0_E$), $t_i \in \mathbf{K}$ and $v_i \in V_1$, $w_i \in V_2$ for $1 \leqslant i \leqslant n$, and the only rules that can be used to operate such sums are those of vector spaces. For instance, $(0, 0) \in E$ is a basis vector, and not the zero vector $0_E$.

In $E$, we define a set of vectors $S = S_1 \cup S_2 \cup S_3 \cup S_4$, where

$$\begin{aligned}
S_1 &= \{(tv_1, v_2) - t(v_1, v_2) \mid t \in \mathbf{K}, \quad (v_1, v_2) \in V_1 \times V_2\},\\
S_2 &= \{(v_1 + v_1', v_2) - (v_1, v_2) - (v_1', v_2) \mid \quad (v_1, v_1', v_2) \in V_1 \times V_1 \times V_2\},\\
S_3 &= \{(v_1, tv_2) - t(v_1, v_2) \mid t \in \mathbf{K}, \quad (v_1, v_2) \in V_1 \times V_2\},\\
S_4 &= \{(v_1, v_2 + v_2') - (v_1, v_2) - (v_1, v_2') \mid \quad (v_1, v_2, v_2') \in V_1 \times V_2 \times V_2\}.
\end{aligned}$$

We define a subspace $F$ of $E$ as being the vector space generated by $S$ in $E$. We then define $V_1 \otimes_{\mathbf{K}} V_2 = E/F$, and we define a map $b_0 \colon V_1 \times V_2 \to V_1 \otimes_{\mathbf{K}} V_2$ by

$$b_0(v_1, v_2) = p((v_1, v_2)),$$

where $p \colon E \to E/F$ is the canonical surjective map. Note already that since the vectors $(v_1, v_2)$ generate $E$ and $p$ is surjective, the vectors $b_0(v_1, v_2)$ generate $E/F$.

By definition, $V_1 \otimes_{\mathbf{K}} V_2$ is a $\mathbf{K}$-vector space. What remains to be proved is that $b$ is bilinear, and that $V_1 \otimes_{\mathbf{K}} V_2$ with the bilinear map $b$ satisfies the stated property concerning bilinear maps to any $\mathbf{K}$-vector space $W$.

Bilinearity of $b_0$ means that the following four conditions should hold:

$$\begin{aligned} b_0(tv_1, v_2) &= tb_0(v_1, v_2) \\ b_0(v_1 + v_1', v_2) &= b_0(v_1, v_2) + b_0(v_1', v_2) \\ b_0(v_1, tv_2) &= tb_0(v_1, v_2) \\ b_0(v_1, v_2 + v_2') &= b_0(v_1, v_2) + b_0(v_1, v_2'). \end{aligned}$$

It is of course not a coincidence that the shape of the formulas look like the definition of the sets $S_i$; each set $S_i$ is defined to be a subset of $S$ in order that one of these formulas become true.

Indeed, we have by definition

$$b_0(tv_1, v_2) - tb_0(v_1, v_2) = p((tv_1, v_2) - t(v_1, v_2)) = 0_{E/F}$$

since $(tv_1, v_2) - t(v_1, v_2) \in S_1 \subset F$, and similarly

$$b_0(v_1 + v_1', v_2) - (b_0(v_1, v_2) + b_0(v_1', v_2)) = p((v_1 + v_1', v_2) - (v_1, v_2) - (v_1', v_2)) = 0_{E/F}$$

because the vector belongs to $S_2 \subset F$, and so on.

This being done, let $W$ be a $\mathbf{K}$-vector space. We denote by $\phi$ the map

$$\mathrm{Hom}_{\mathbf{K}}(V_1 \otimes_{\mathbf{K}} V_2, W) \xrightarrow{\phi} \mathrm{Bil}_{\mathbf{K}}(V_1, V_2; W)$$

given by $f \mapsto f \circ b_0$. We leave it to the reader to check that, indeed, $f \circ b_0$ is bilinear if $f$ is linear (this follows from the bilinearity of $b_0$ and the linearity of $f$). We then need to show that $\phi$ is an isomorphism. We leave as an elementary exercise to check that it is linear.

We next show that $\phi$ is injective: if $f \in \mathrm{Ker}(\phi)$, then we have $f(b_0(v_1, v_2)) = 0$ for all $(v_1, v_2) \in V_1 \times V_2$. This means that $p((v_1, v_2)) \in \mathrm{Ker}(f)$ for all $v_1$ and $v_2$. Since the basis vectors $(v_1, v_2)$ generate $E$ by definition, and $p$ is surjective, this implies that $f = 0$.

Finally, we show that $\phi$ is surjective. Let $b\colon V_1 \times V_2 \to W$ be a bilinear map. We can define a linear map $\tilde{f}\colon E \to W$ by putting $\tilde{f}((v_1, v_2)) = b(v_1, v_2)$ for any $(v_1, v_2) \in V_1 \times V_2$, since these elements of $E$ form a basis of $E$.

We then observe that $S \subset \mathrm{Ker}(\tilde{f})$, so that $F \subset \mathrm{Ker}(\tilde{f})$. Indeed, for a vector $r = (tv_1, v_2) - t(v_1, v_2) \in S_1$, we get by linearity of $\tilde{f}$ the relation

$$\tilde{f}(r) = \tilde{f}((tv_1, v_2)) - t\tilde{f}(v_1, v_2) = b(tv_1, v_2) - tb(v_1, v_2) = 0$$

because $b$ is bilinear, and similarly for the vectors in $S_2$, $S_3$ or $S_4$.

Since $F \subset \mathrm{Ker}(\tilde{f})$, the linear map $\tilde{f}$ passes to the quotient modulo $F$ (Proposition 10.3.7): there exists a linear map $f\colon E/F = V_1 \otimes_{\mathbf{K}} V_2 \to W$ such that $\tilde{f} = f \circ p$. We claim that $\phi(f) = f \circ b_0 = b$, which will show that $\phi$ is surjective. Indeed, for $(v_1, v_2) \in V_1 \times V_2$, we have

$$f(b_0(v_1, v_2)) = f(p((v_1, v_2))) = \tilde{f}((v_1, v_2)) = b(v_1, v_2)$$

by the definitions of $b_0$ and of $\tilde{f}$. ☐

The definition and construction of the tensor product seem very abstract. Here is a simple consequence that shows how they can be used; as we will see in all of this chapter, it is only the *statement* of Theorem 11.1.2 that is important: the details of the quotient space construction are never used.

Corollary 11.1.4. *Let $V_1$ and $V_2$ be $\mathbf{K}$-vector spaces. Let $v_1$ and $v_2$ be non-zero vectors in $V_1$ and $V_2$ respectively. Then $v_1 \otimes v_2$ is non-zero in $V_1 \otimes_{\mathbf{K}} V_2$.*

Proof. It suffices to find a vector space $W$ and a bilinear map $b\colon V_1 \times V_2 \to W$ such that $b(v_1, v_2) \neq 0$, since in that case, the linear map

$$f\colon V_1 \otimes V_2 \to W$$

such that $f(v_1 \otimes v_2) = b(v_1, v_2)$ (whose existence is given by Theorem 11.1.2) will satisfy $f(v_1 \otimes v_2) \neq 0$, which would not be possible if $v_1 \otimes v_2$ were zero.

To find $b$, we first note that, since $v_2 \neq 0$, there exists $\lambda \in V_2^*$ such that $\lambda(v_2) \neq 0$. Then we define $b\colon V_1 \times V_2 \to V_1$ by

$$b(v, w) = \lambda(w)v.$$

This map is bilinear, and we have $b(v_1, v_2) = \lambda(v_2)v_1 \neq 0$. ☐

Another corollary gives the dimension of the tensor product if the factors are finite-dimensional.

Corollary 11.1.5. *Let $V_1$ and $V_2$ be finite-dimensional $\mathbf{K}$-vector spaces. Then the tensor product $V_1 \otimes_{\mathbf{K}} V_2$ is finite-dimensional and*

$$\dim(V_1 \otimes_{\mathbf{K}} V_2) = \dim(V_1)\dim(V_2).$$

Proof. Apply the characterization in Theorem 11.1.2 to $W = \mathbf{K}$: we find then an isomorphism

$$(V_1 \otimes_{\mathbf{K}} V_2)^* \to \mathrm{Bil}_{\mathbf{K}}(V_1, V_2; \mathbf{K}).$$

The right-hand side is the space of bilinear maps $V_1 \times V_2 \to \mathbf{K}$, and it is finite-dimensional (by extending to this case Proposition 5.2.3, which provides the result when $V_1 = V_2$: one maps a bilinear map $b$ to the matrix $(b(v_i, w_j))$ with respect to a basis of $V_1$ and a basis of $V_2$). By Theorem 8.1.6, this means that the space $V_1 \otimes_{\mathbf{K}} V_2$ itself is finite-dimensional. Then it has the same dimension as $\mathrm{Bil}_{\mathbf{K}}(V_1, V_2; \mathbf{K})$, and the generalization of Proposition 5.2.3 shows that this dimension is $\dim(V_1)\dim(V_2)$. ☐

We next show that the property highlighted in Theorem 11.1.2 characterizes the tensor product – this is similar to Proposition 10.3.2 that showed that the properties (kernel and surjectivity) of the canonical surjection $V \to V/W$ are sufficient to characterize the quotient space.

Proposition 11.1.6. *Let $V_1$ and $V_2$ be $\mathbf{K}$-vector spaces. Let $X$ be a $\mathbf{K}$-vector space with a bilinar map $\beta\colon V_1 \times V_2 \to X$ such that for any $\mathbf{K}$-vector space $W$, the composition application $f \mapsto f \circ \beta$ is an isomorphism*

$$\mathrm{Hom}_{\mathbf{K}}(X, W) \to \mathrm{Bil}_{\mathbf{K}}(V_1, V_2; W)$$

*of $\mathbf{K}$-vector spaces. There exists then a unique isomorphism $f\colon V_1 \otimes_{\mathbf{K}} V_2 \to X$ such that*

$$\beta(v_1, v_2) = f(v_1 \otimes v_2)$$

*for $(v_1, v_2) \in V_1 \times V_2$.*

Proof. Apply first Theorem 11.1.2 to $W = X$ and to the bilinear map $\beta$: this shows that there exists a unique linear map $f\colon V_1 \otimes_{\mathbf{K}} V_2 \to X$ such that $\beta = f \circ b_0$, or in other words such that $\beta(v_1, v_2) = f(v_1 \otimes v_2)$.

Next, apply the assumption of the proposition to $W = V_1 \otimes_{\mathbf{K}} V_2$ and to the bilinear form $b_0$; this shows that there exists a unique linear map $g\colon X \to V_1 \otimes_{\mathbf{K}} V_2$ such that

$$g(\beta(v_1, v_2)) = v_1 \otimes v_2$$

for $(v_1, v_2) \in V_1 \times V_2$. We then claim that $f$ and $g$ are reciprocal isomorphisms, which will prove the proposition.

Indeed, consider the composite $i = f \circ g \colon X \to X$. It satisfies

$$i(\beta(v_1, v_2)) = f(v_1 \otimes v_2) = \beta(v_1, v_2),$$

or in other words, $i \circ \beta = \beta = \mathrm{Id}_X \circ \beta$. Since $f \mapsto f \circ \beta$ is supposed to be an isomorphism, this means that $f \circ g = i = \mathrm{Id}_X$. Similarly, arguing with $g \circ f$, we see that $g \circ f = \mathrm{Id}_{V_1 \otimes_{\mathbf{K}} V_2}$. This concludes the proof of the claim. □

The next proposition is also very important as a way of understanding linear maps involving tensor products.

Proposition 11.1.7. *Let $f_1 \colon V_1 \to W_1$ and $f_2 \colon V_2 \to W_2$ be two linear maps. There exists a unique linear map*

$$f \colon V_1 \otimes_{\mathbf{K}} V_2 \to W_1 \otimes_{\mathbf{K}} W_2$$

*such that*

$$f(v_1 \otimes v_2) = f_1(v_1) \otimes f_2(v_2)$$

*for all $(v_1, v_2) \in V_1 \times V_2$.*

We will denote $f = f_1 \otimes f_2$ the linear map constructed in this proposition.

Proof. Define

$$\tilde{f} \colon V_1 \times V_2 \to W_1 \otimes_{\mathbf{K}} W_2$$

by $\tilde{f}(v_1, v_2) = f_1(v_1) \otimes f_2(v_2)$. Since $f_1$ and $f_2$ are linear, and $(w_1, w_2) \mapsto w_1 \otimes w_2$ is bilinear, the map $\tilde{f}$ belongs to $\mathrm{Bil}_{\mathbf{K}}(V_1, V_2; W_1 \otimes_{\mathbf{K}} W_2)$. From Proposition 11.1.6, applied to $W = W_1 \otimes_{\mathbf{K}} W_2$ and $\tilde{f}$, there exists a unique linear map

$$f \colon V_1 \otimes_{\mathbf{K}} V_2 \to W_1 \otimes_{\mathbf{K}} W_2$$

such that $f(v_1 \otimes v_2) = \tilde{f}(v_1, v_2) = f_1(v_1) \otimes f_2(v_2)$, as we wanted to show. The following diagram summarizes the construction:

$$\begin{tikzcd} V_1 \times V_2 \arrow[r, "\tilde{f}"] \arrow[d] & W_1 \otimes_{\mathbf{K}} W_2 \\ V_1 \otimes_{\mathbf{K}} V_2 \arrow[ur, "f_1 \otimes f_2"'] & \end{tikzcd}$$

□

Example 11.1.8. (1) If either $f_1 = 0$ or $f_2 = 0$, we have $f_1 \otimes f_2 = 0$, since we then get $(f_1 \otimes f_2)(v_1 \otimes v_2) = f_1(v_1) \otimes f_2(v_2) = 0$ for all $(v_1, v_2) \in V_1 \times V_2$; since the pure tensors generate $V_1 \otimes V_2$, the linear map $f_1 \otimes f_2$ is zero.

(2) If $f_1 = \mathrm{Id}_{V_1}$ and $f_2 = \mathrm{Id}_{V_2}$, then $f_1 \otimes f_2 = \mathrm{Id}_{V_1 \otimes V_2}$. Indeed, we have

$$(\mathrm{Id}_{V_1} \otimes \mathrm{Id}_{V_2})(v_1 \otimes v_2) = v_1 \otimes v_2$$

and since the pure tensors generate $V_1 \otimes V_2$, this implies that $\mathrm{Id}_{V_1} \otimes \mathrm{Id}_{V_2}$ is the identity on all of $V_1 \otimes V_2$.

(3) Suppose that we have pairs of spaces $(V_1, V_2)$, $(W_1, W_2)$ and $(H_1, H_2)$, and linear maps $f_i \colon V_i \to W_i$ and $g_i \colon W_i \to H_i$. Then we can compute

$$(g_1 \circ f_1) \otimes (g_2 \circ f_2) \colon V_1 \otimes V_2 \to H_1 \otimes H_2,$$

and $(g_1 \otimes g_2) \circ (f_1 \otimes f_2)$. These linear maps are the same: indeed, the first one maps $v_1 \otimes v_2$ to

$$(g_1 \circ f_1)(v_1) \otimes (g_2 \circ f_2)(v_2),$$

while the second maps this vector to

$$(g_1 \otimes g_2)(f_1(v_1) \otimes f_2(v_2)) = g_1(f_1(v_1)) \otimes g_2(f_2(v_2)).$$

## 11.2. Examples

We will discuss some examples and simple applications of tensor products in this section.

EXAMPLE 11.2.1. When $V_1$ and $V_2$ are finite-dimensional $\mathbf{K}$-vector spaces, the tensor product $V_1 \otimes_{\mathbf{K}} V_2$ is not such a mysterious space.

PROPOSITION 11.2.2. *Let $V_1$ and $V_2$ be finite-dimensional $\mathbf{K}$-vector spaces. Let $(v_1, \ldots, v_n)$ be a basis of $V_1$ and $(w_1, \ldots, w_m)$ a basis of $V_2$. Then the vectors $(v_i \otimes w_j)_{\substack{1 \leqslant i \leqslant n \\ 1 \leqslant j \leqslant m}}$ form a basis of $V_1 \otimes_{\mathbf{K}} V_2$.*

PROOF. In Theorem 11.1.2, we saw that the vectors $v \otimes w$, for $(v, w) \in V_1 \times V_2$, generate $V_1 \otimes_{\mathbf{K}} V_2$. Writing

$$v = \sum_i t_i v_i, \qquad w = \sum_j s_j w_j,$$

the bilinearity gives

$$v \otimes w = \sum_{i,j} t_i s_j \; v_i \otimes w_j,$$

so that $(v_i \otimes w_j)$ is a generating set of $V_1 \otimes_{\mathbf{K}} V_2$. Since this set has $nm = \dim(V_1 \otimes_{\mathbf{K}} V_2)$ elements (by Corollary 11.1.5), it is a basis. $\square$

One can show that this result is also true in the general case when $V_1$ or $V_2$ (or both) might be infinite-dimensional.

Here is a an example that gives an intuition of the difference between pure tensors and all tensors. Consider $V_1 = V_2 = \mathbf{K}^2$, with standard basis $(e_1, e_2)$. Then $V_1 \otimes V_2$ is 4-dimensional with basis $(f_1, f_2, f_3, f_4)$ where, for example, we have

$$f_1 = e_1 \otimes e_1, \quad f_2 = e_1 \otimes e_2, \quad f_3 = e_2 \otimes e_1, \quad f_4 = e_2 \otimes e_2.$$

A pure tensor in $V_1 \otimes V_2$ is an element of the form

$$\begin{pmatrix} a \\ b \end{pmatrix} \otimes \begin{pmatrix} c \\ d \end{pmatrix} = (ae_1 + be_2) \otimes (ce_1 + de_2) = acf_1 + adf_2 + bcf_3 + bdf_4.$$

Not all vectors in $V_1 \otimes V_2$ are of this form! Therefore $x_1 f_1 + \cdots + x_4 f_4$ is a pure tensor if and only if there exist $(a, b, c, d) \in \mathbf{K}^4$ such that

$$\begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} = \begin{pmatrix} ac \\ ad \\ bc \\ bd \end{pmatrix} \in \mathbf{K}^4. \tag{11.1}$$

An obvious necessary condition is that $x_1 x_4 = x_2 x_3$ (since both products are equal to $abcd$ in the case of pure tensors). In fact, it is also a sufficient condition, namely if $x_1$, $\ldots$, $x_4$ satisfy $x_1 x_4 = x_2 x_3$, we can find $(a, b, c, d)$ with the relation (11.1). To see this, we consider various cases:

- If $x_1 \neq 0$, then we take

$$a = 1, \quad b = \frac{x_3}{x_1}, \quad c = x_1, \quad d = x_2.$$

The relation (11.1) then holds (e.g., $bd = x_3 x_2 / x_1 = x_1 x_4 / x_1 = x_4$).

- If $x_1 = 0$, then since $0 = x_2x_3$, we have either $x_2 = 0$ or $x_3 = 0$; in the first case, take
$$a = 0, \quad b = 1, \quad c = x_3, \quad d = x_4$$
and in the second, take
$$a = x_2, \quad b = x_4, \quad c = 0, \quad d = 1.$$

Example 11.2.3. Since we have found (in the finite-dimensional case) an explicit basis of the tensor product, we can think of the matrices representing linear maps.

Let $V_1$ and $V_2$ be finite-dimensional $\mathbf{K}$-vector space. Consider two endomorphisms $f_1 \in \mathrm{End}_{\mathbf{K}}(V_1)$ and $f_2 \in \mathrm{End}_{\mathbf{K}}(V_2)$, and let $f = f_1 \otimes f_2 \in \mathrm{End}_{\mathbf{K}}(V_1 \otimes_{\mathbf{K}} V_2)$.

Let $B_1 = (v_1, \ldots, v_n)$ be a basis of $V_1$ and $B_2 = (w_1, \ldots, w_m)$ a basis of $V_2$. Define $A_i = \mathrm{Mat}(f_i; B_i, B_i)$. Write $A_1 = (a_{ij})$ and $A_2 = (b_{ij})$. We consider the basis $B$ of $V_1 \otimes_{\mathbf{K}} V_2$ consisting of the vectors $v_i \otimes w_j$, and we want to write down the matrix of $f$ with respect to $B$. For simplicity of notation, we present the computation for $n = 2$ and $m = 3$.

We must first order the basis vectors in $B$. We select the following ordering:
$$B = (x_1, \ldots, x_6) = (v_1 \otimes w_1, v_1 \otimes w_2, v_1 \otimes w_3, v_2 \otimes w_1, v_2 \otimes w_2, v_2 \otimes w_3)$$
(i.e., we order first with respect to increasing $j$ for $i = 1$, and then with $i = 2$).

Let $C \in M_{6,6}(\mathbf{K})$ be the matrix representing $f$ with respect to this ordered basis of $V_1 \otimes_{\mathbf{K}} V_2$.

We begin with the first basis vector $v_1 \otimes w_1$. By definition, we have
$$\begin{aligned} f(v_1 \otimes w_1) = f_1(v_1) \otimes f_2(w_1) &= \Big(a_{11}v_1 + a_{21}v_2\Big) \otimes \Big(b_{11}w_1 + b_{21}w_2 + b_{31}w_3\Big) \\ &= a_{11}b_{11}x_1 + a_{11}b_{21}x_2 + a_{11}b_{31}x_3 + a_{21}b_{11}x_4 + a_{21}b_{21}x_5 + a_{21}b_{31}x_6 \end{aligned}$$
in terms of our ordering. The first column of $C$ is therefore the transpose of the row vector
$$(a_{11}b_{11}, a_{11}b_{21}, a_{11}b_{31}, a_{21}b_{11}, a_{21}b_{21}, a_{21}b_{31}).$$
Similarly, for $x_2$, we obtain
$$\begin{aligned} f(x_2) = f(v_1 \otimes w_2) = f_1(v_1) \otimes f_2(w_2) &= \Big(a_{11}v_1 + a_{21}v_2\Big) \otimes \Big(b_{12}w_1 + b_{22}w_2 + b_{32}w_3) \\ &= a_{11}b_{12}x_1 + a_{11}b_{22}x_2 + a_{11}b_{32}x_3 + a_{21}b_{12}x_4 + a_{21}b_{22}x_5 + a_{21}b_{32}x_6, \end{aligned}$$
and
$$f(x_3) = a_{11}b_{13}x_1 + a_{11}b_{23}x_2 + a_{11}b_{33}x_3 + a_{21}b_{13}x_4 + a_{23}b_{23}x_5 + a_{21}b_{33}x_6.$$
This gives us the first three columns of $C$:
$$\begin{pmatrix} a_{11}b_{11} & a_{11}b_{12} & a_{11}b_{13} \\ a_{11}b_{21} & a_{11}b_{22} & a_{11}b_{23} \\ a_{11}b_{31} & a_{11}b_{32} & a_{11}b_{33} \\ a_{21}b_{11} & a_{21}b_{12} & a_{21}b_{13} \\ a_{21}b_{21} & a_{21}b_{22} & a_{21}b_{23} \\ a_{21}b_{31} & a_{21}b_{32} & a_{21}b_{33} \end{pmatrix} = \begin{pmatrix} a_{11}A_2 \\ a_{21}A_2 \end{pmatrix}$$
in block form. Unsurprisingly, finishing the computation leads to
$$C = \begin{pmatrix} a_{11}A_2 & a_{12}A_2 \\ a_{21}A_2 & a_{22}A_2 \end{pmatrix}$$
in block form. This type of matrix (in terms of $A_1$ and $A_2$) is called, in old-fashioned terms, the Kronecker product of $A_1$ and $A_2$.

In the general case, with the "same" ordering of the basis vectors, one finds

$$C = \begin{pmatrix} a_{11}A_2 & \cdots & a_{1n}A_2 \\ \vdots & \vdots & \vdots \\ a_{n1}A_2 & \cdots & a_{nn}A_2 \end{pmatrix}$$

in block form.

EXAMPLE 11.2.4. Another way to "recognize" the tensor product is the following:

PROPOSITION 11.2.5. *Let $V_1$ and $V_2$ be finite-dimensional $\mathbf{K}$-vector spaces. There exists a unique isomorphism*

$$\alpha\colon V_1^* \otimes_{\mathbf{K}} V_2 \to \mathrm{Hom}_{\mathbf{K}}(V_1, V_2)$$

*such that $\alpha(\ell \otimes w)$ is the linear map $f_{\ell,w}$ from $V_1$ to $V_2$ that sends $v$ to*

$$\langle \ell, v\rangle w = \ell(v)w.$$

PROOF. The map $\alpha$ is well-defined (and linear) by Theorem 11.1.2, because the map

$$(\ell, w) \mapsto f_{\ell,w}$$

is bilinear from $V_1^* \times V_2$ to $\mathrm{Hom}_{\mathbf{K}}(V_1, V_2)$. To prove that it is an isomorphism, we will construct an inverse $\beta$. For this purpose, let $(v_1, \ldots, v_n)$ be a basis of $V_1$. Denote $(\ell_1, \ldots, \ell_n)$ the dual basis.

For $f\colon V_1 \to V_2$, we then define

$$\beta(f) = \sum_{i=1}^{n} \ell_i \otimes f(v_i) \in V_1^* \otimes V_2.$$

The map $\beta\colon \mathrm{Hom}_{\mathbf{K}}(V_1, V_2) \to V_1^* \otimes_{\mathbf{K}} V_2$ is linear. We will show that it is the inverse of $\alpha$. First we compute $\alpha \circ \beta$. This is a linear map from $\mathrm{Hom}_{\mathbf{K}}(V_1, V_2)$ to itself. Let $f\colon V_1 \to V_2$ be an element of this space, and $g = (\alpha \circ \beta)(f)$. We have

$$g = \sum_{i=1}^{n} \alpha(\ell_i \otimes f(v_i)),$$

and therefore

$$g(v) = \sum_{i=1}^{n} \ell_i(v) f(v_i) = f\Big(\sum_{i=1}^{n} \langle \ell_i, v\rangle v_i\Big) = f(v)$$

by definition of the dual basis (8.2). There $g = f$, which means that $\alpha \circ \beta$ is the identity.

Now consider $\beta \circ \alpha$, which is an endomorphism of $V_1^* \otimes_{\mathbf{K}} V_2$. To show that $\beta \circ \alpha$ is the identity, it suffices to check that it is so for vectors $\ell \otimes w$. We get

$$\begin{aligned}(\beta \circ \alpha)(\ell \otimes w) &= \beta(f_{\ell,w}) \\ &= \sum_{i=1}^{n} \ell_i \otimes f_{\ell,w}(v_i) \\ &= \sum_{i=1}^{n} \ell_i \otimes \ell(v_i) w = \Big(\sum_{i=1}^{n} \langle \ell, v_i\rangle \ell_i\Big) \otimes w.\end{aligned}$$

But for any $v \in V_1$, using (8.2), we get

$$\ell(v) = \sum_{i=1}^{n} \langle \ell_i, v\rangle \langle \ell, v\rangle = \langle \sum_{i=1}^{n} \langle \ell, v_i\rangle \ell_i, v\rangle$$

which means that

$$\ell = \sum_{i=1}^{n} \langle \ell, v_i \rangle \ell_i \in V_1^*.$$

Hence $(\beta \circ \alpha)(\ell \otimes w) = \ell \otimes w$, which means that $\beta \circ \alpha$ is also the identity. $\square$

For instance, if $V$ is finite-dimensional, this gives an isomorphism

$$V^* \otimes_{\mathbf{K}} V \to \mathrm{End}_{\mathbf{K}}(V).$$

Now consider the trace $\mathrm{Tr}\colon \mathrm{End}_{\mathbf{K}}(V) \to \mathbf{K}$. This is a linear form, and hence, by composition we obtain a linear form

$$V^* \otimes_{\mathbf{K}} V \to \mathbf{K},$$

which by Theorem 11.1.2 corresponds to a unique bilinear form

$$\tau\colon V^* \times V \to \mathbf{K}.$$

What linear form is that? If we follow the definition, for any $w \in V$ and $\ell \in V^*$, we have

$$\tau(\ell \otimes w) = \mathrm{Tr}(f)$$

where $f \in \mathrm{End}_{\mathbf{C}}(V)$ is given by

$$f(v) = \ell(v)w.$$

The trace of this endomorphism is simply $\ell(w) = \langle \ell, w \rangle$. Indeed, this is clear if $w = 0$, and otherwise, let $B = (w, w_2, \ldots, w_n)$ be a basis of $V$; then the matrix of $f$ with respect to $B$ is

$$\begin{pmatrix} \ell(w) & \ell(v_2) & \cdots & \ell(v_n) \\ 0 & 0 & \cdots & 0 \\ \vdots & & \vdots & \end{pmatrix},$$

which has trace $\ell(w)$.

So we see that, by means of the tensor product, the meaning of the trace map is clarified, and it does not look as arbitrary as the "sum of diagonal coefficients" suggests.

Another useful consequence of this proposition is that it clarifies the difference between "pure tensors" of the form $v_1 \otimes v_2$ in a tensor product, and the whole space $V_1 \otimes_{\mathbf{K}} V_2$. Indeed, the linear maps $f_{\ell,w}$ associated to a pure tensor are exactly the linear maps $V_1 \to V_2$ of rank $\leqslant 1$ (the rank is 1, unless $w = 0$ or $\ell = 0$), since the image of $f_{\ell,w}$ is contained in the space generated by $w$. In particular this shows that most elements of $V_1 \otimes_{\mathbf{K}} V_2$ are *not* of the special form $v_1 \otimes v_2$!

Example 11.2.6. A very useful construction based on the tensor product is that it can be used to associate naturally to a vector space over $\mathbf{Q}$ or $\mathbf{R}$ a vector space over $\mathbf{C}$ that is "the same", except that one can multiply vectors with complex numbers instead of just real vectors.

Proposition 11.2.7. *Let* $\mathbf{K} = \mathbf{Q}$ *or* $\mathbf{K} = \mathbf{R}$*. Let* $V$ *be a* $\mathbf{K}$*-vector space. View* $\mathbf{C}$ *as a* $\mathbf{K}$*-vector space. Let* $V_{\mathbf{C}} = V \otimes \mathbf{C}$*. Then* $V_{\mathbf{C}}$ *has a structure of vector space over* $\mathbf{C}$ *such that the zero vector and the addition are the same as the zero vector and addition as* $\mathbf{K}$*-vector space, and such that*

$$z \cdot (v \otimes 1) = v \otimes z \tag{11.2}$$

*for all* $z \in \mathbf{C}$ *and* $v \in V$*. Moreover:*

(1) *If* $B$ *is a basis of* $V$*, then the set* $B_{\mathbf{C}} = \{v \otimes 1 \mid v \in B\}$ *is a basis of* $V_{\mathbf{C}}$*, and in particular*

$$\dim_{\mathbf{K}} V = \dim_{\mathbf{C}} V_{\mathbf{C}};$$

(2) *If* $V_1$ *and* $V_2$ *are real vector spaces and* $f \in \mathrm{Hom}_{\mathbf{K}}(V_1, V_2)$*, then the linear map* $f \otimes \mathrm{Id}_{\mathbf{C}} \colon V_{1,\mathbf{C}} \to V_{2,\mathbf{C}}$ *is* $\mathbf{C}$*-linear.*

(3) *If* $f \colon V_1 \to V_2$ *is a linear map of finite-dimensional* $\mathbf{K}$*-vector spaces, and* $B_i$ *is an ordered basis of* $V_i$*, then*

$$\mathrm{Mat}(f; B, B) = \mathrm{Mat}(f_{\mathbf{C}}; B_{1,\mathbf{C}}, B_{2,\mathbf{C}})$$

*where we denote* $f_{\mathbf{C}}$ *the* $\mathbf{C}$*-linear map* $f \otimes \mathrm{Id}_{\mathbf{C}}$*.*

Proof. We first interpret (11.2) more precisely: for any $z \in \mathbf{C}$, we have a multiplication map $m_z$ on $\mathbf{C}$ such that $m_z(w) = zw$. This map is also a $\mathbf{K}$-linear endomorphism of $\mathbf{C}$. Hence, we have a $\mathbf{K}$-linear endomorphism $n_z = \mathrm{Id}_V \otimes m_z$ of $V_{\mathbf{C}}$, which satisfies

$$n_z(v \otimes w) = v \otimes zw$$

for all $v \in V$ and $w \in \mathbf{C}$. In particular, we have $n_z(v \otimes 1) = v \otimes z$. We will show that the definition

$$z \cdot v = n_z(v)$$

gives $V_{\mathbf{C}}$ a structure of $\mathbf{C}$-vector space. It then satisfies (11.2) in particular.

By construction, $V_{\mathbf{C}}$ is a $\mathbf{K}$-vector space, so the addition and the zero vector satisfy conditions (2.2) and (2.5) in Definition 2.3.1, which only involve addition and zero.

We check some of the other conditions, leaving a few as exercises:

- (Condition (2.3)): we have $0 \cdot v = n_0(v)$; but $n_0 = \mathrm{Id}_V \otimes m_0 = \mathrm{Id}_V \otimes 0 = 0$, as endomorphism of $V_{\mathbf{C}}$ (Example 11.1.8 (1)), so $0 \cdot v = 0$ for all $v \in V$; similarly, we have $m_1 = \mathrm{Id}_{\mathbf{C}}$ (Example (11.1.8) (2)), hence $n_1 = \mathrm{Id}_V \otimes \mathrm{Id}_{\mathbf{C}}$ is the identity on $V_{\mathbf{C}}$, and $1 \cdot v = v$ for all $v \in V$;
- (Condition (2.6)): for $z_1$ and $z_2 \in \mathbf{C}$, we have $m_{z_1 z_2} = m_{z_1} \circ m_{z_2}$ (this is Example 11.1.8 (3)), and from this we deduce that $n_{z_1 z_2} = n_{z_1} \circ n_{z_2}$; then
$$(z_1 z_2) \cdot v = n_{z_1}(n_{z_2}(v)) = n_{z_1}(z_2 \cdot v) = z_1 \cdot (z_2 \cdot v).$$
- (First part of Condition (2.8)): since $n_z$ is $\mathbf{K}$-linear, we have
$$z \cdot (v_1 + v_2) = n_z(v_1 + v_2) = n_z(v_1) + n_z(v_2) = z \cdot v_1 + z \cdot v_2.$$

We now discuss the complements of the statement. First, let $B$ be a basis of $V$ as $\mathbf{K}$-vector space, and $B_0$ a basis of $\mathbf{C}$ as $\mathbf{K}$-vector space. Then the $\mathbf{K}$-vector space $V_{\mathbf{C}}$ has $\{v \otimes w \mid v \in B,\ w \in B_0\}$ as basis (this is the remark following Proposition 11.2.2). Since

$$v \otimes w = w \cdot (v \otimes 1),$$

in $V_{\mathbf{C}}$, this shows that $\{v \otimes 1 \mid v \in B\}$ generates $V_{\mathbf{C}}$ as a $\mathbf{C}$-vector space. But moreover, for any finite distinct vectors $v_1, \ldots, v_n$ in $B$, and any $z_j$ in $\mathbf{C}$, writing

$$z_j = \sum_{w \in B_0} a_{j,w} w$$

for some $a_{j,w} \in \mathbf{K}$, with all but finitely many equal to 0, we have

$$\sum_j z_j(v_j \otimes 1) = \sum_{w \in B_0} \sum_j a_{j,w}(v_j \otimes w)$$

and therefore the linear combination is zero if and only if $a_{j,w} = 0$ for all $j$ and all $w$, which means that $z_j = 0$ for all $j$. So the vectors $\{v \otimes 1 \mid v \in B\}$ are also linearly independent in $V_{\mathbf{C}}$.

Now consider a $\mathbf{K}$-linear map $V_1 \to V_2$. The map $f \otimes \mathrm{Id}_{\mathbf{C}}$ is then at least $\mathbf{K}$-linear. But furthermore, for $z \in \mathbf{C}$ and $v \in V_1$, we get

$$(f \otimes \mathrm{Id}_{\mathbf{C}})(z \cdot (v \otimes 1)) = (f \otimes \mathrm{Id}_{\mathbf{C}})(v \otimes z) = f(v) \otimes z = z \cdot (f(v) \otimes 1).$$

Since the vectors $v \otimes 1$ generate $V_{\mathbf{C}}$ as a $\mathbf{C}$-vector space, we deduce that $f \otimes \mathrm{Id}_{\mathbf{C}}$ is $\mathbf{C}$-linear.

Finally, let $B_1 = (v_1, \ldots, v_n)$ and $B_2 = (w_1, \ldots, w_m)$ and write $\mathrm{Mat}(f; B_1, B_2) = (a_{ij})$. Then for a basis vector $v_j \otimes 1$ of $B_{1,\mathbf{C}}$, we have

$$f_{\mathbf{C}}(v_j \otimes 1) = f(v_j) \otimes 1 = \sum_{i=1}^{m} a_{ij}(w_i \otimes 1),$$

which means that the $j$-th column of $\mathrm{Mat}(f_{\mathbf{C}}; B_{1,\mathbf{C}}, B_{2,\mathbf{C}})$ is $(a_{ij})_{1 \leqslant i \leqslant m}$, hence that

$$\mathrm{Mat}(f_{\mathbf{C}}; B_{1,\mathbf{C}}, B_{2,\mathbf{C}}) = \mathrm{Mat}(f; B_1, B_2).$$

$\square$

In some cases, this construction is not really needed: nothing prevents us to view a real matrix as a complex matrix and to speak of its eigenvalues as complex numbers. But in more abstract cases, it can be very useful. We illustrate this in the next example.

Example 11.2.8. We now present a simple and quite concrete application of the tensor product. We begin with a definition:

Definition 11.2.9 (Algebraic number). A complex number $z$ is an algebraic number if there exists a non-zero polynomial $P \in \mathbf{Q}[X]$ with rational coefficients such that $P(z) = 0$.

For instance, $z = \sqrt{2}$ is algebraic (one can take $P = X^2 - 2$), $z = e^{2i\pi/n}$ is algebraic for any $n \geqslant 1$ (one can take $P = X^n - 1$); moreover $\sqrt{2 + \sqrt{2}}$ is also (take $P = (X^2 - 2)^2 - 2$). What about $\sqrt{2 + \sqrt{2}} + e^{2i\pi/n}$, or $e^{2i\pi/n}\sqrt{2 + \sqrt{2}}$ or more complicated sum or product?

Theorem 11.2.10. *Let $z_1$ and $z_2$ be algebraic numbers. Then $z_1 + z_2$ and $z_1 z_2$ are also algebraic numbers.*

We give a simple proof using tensor products, although more elementary arguments do exist. For this we need a lemma showing that algebraic numbers are eigenvalues of rational matrices.

Lemma 11.2.11. *Let $z$ be an algebraic number and $Q \neq 0$ a polynomial with rational coefficients of degree $n \geqslant 1$ such that $Q(z) = 0$. There exists a matrix $A \in M_{n,n}(\mathbf{Q})$ such that $z$ is an eigenvalue of $A$.*

Proof. Let $V = \mathbf{Q}[X]$ and let $W \subset V$ be the subspace

$$W = \{QP \mid P \in \mathbf{Q}[X]\}$$

(in other words, the image of the linear map $P \mapsto PQ$ on $V$). Consider the quotient space $E = V/W$ and the quotient map $p \colon V \to E$. The space $E$ is finite-dimensional, and in fact the space $W_n$ of polynomials of degree $\leqslant n - 1$ is a complement to $W$, so that the restriction of $p$ to $W_n$ is an isomorphism $W_n \to E$. To see this, note that for any polynomial $P \in V$, by Euclidean Division of $P$ by $Q$ (Theorem 9.4.7), we see that there exist unique polynomials $P_1 \in \mathbf{Q}[X]$ and $R \in V_n$ such that

$$P = P_1 Q + R.$$

This means that $P \in W + W_n$. Since $W \cap W_n = \{0\}$ (because non-zero elements of $W$ have degree $\geqslant \deg(Q) = n$), this gives the formula $W \oplus W_n = V$.

Now consider the endomorphism $f(P) = XP$ of $V$. Since $f(QP) = (XP)Q$, the image of $W$ is contained in $W$. Let then $f_1$ be the endomorphism of the $n$-dimensional space $E$ induced by $f$ by passing to the quotient modulo $W$.

We claim that $z$ is an eigenvalue of the matrix $\mathrm{Mat}(f; B, B)$ for any basis $B$ of $E$. This can be checked by a direct computation of this matrix for a specific basis, but it has also a nice explanation in terms of "change of field", as in the previous example, although we will avoid using the formal construction.

Precisely, let $V_{\mathbf{C}} = \mathbf{C}[X]$ and $W_{\mathbf{C}} = \{PQ \mid P \in V_{\mathbf{C}}\}$, and define $E_{\mathbf{C}} = V_{\mathbf{C}}/W_{\mathbf{C}}$. As above, we define $f_{\mathbf{C}}(P) = XP$ for $P \in V_{\mathbf{C}}$, and we obtain an induced quotient endomorphism $f_{1,\mathbf{C}} \in \mathrm{End}_{\mathbf{C}}(E_{\mathbf{C}})$.

Since $Q(z) = 0$, there exists a polynomial $Q_1 \in \mathbf{C}[X]$ (of degree $n-1$) such that $Q = (X-z)Q_1$ (e.g., by euclidean division of $Q$ by $X - z$ in $\mathbf{C}[X]$, we get $Q = (X-z)Q_1 + R$ where $R$ is constant; but then $Q(z) = 0 + R(z)$ so that $R = 0$; note that we cannot do this division in $V$, since $z$ is in general not in $\mathbf{Q}$). Since $Q_1$ is non-zero and of degree $< \deg(Q)$, the vector $v = p_{\mathbf{C}}(Q_1) \in E_{\mathbf{C}}$ is non-zero. Now we compute

$$f_{1,\mathbf{C}}(v) = f_{1,\mathbf{C}}(p_{\mathbf{C}}(Q_1)) = p)\mathbf{C}(f_{\mathbf{C}}(Q_1)) = p_{\mathbf{C}}(XQ_1).$$

But $XQ_1 = (X-z)Q_1 + zQ_1 = Q + zQ_1$ implies that $p_{\mathbf{C}}(XQ_1) = p_{\mathbf{C}}(zQ_1) = zp_{\mathbf{C}}(Q_1)$. Hence $v$ is an eigenvector of $f_{1,\mathbf{C}}$ for the eigenvalue $z$.

Now take the basis

$$B = (p_{\mathbf{C}}(1), \ldots, p_{\mathbf{C}}(X^{n-1}))$$

of $E_{\mathbf{C}}$. If we compute any matrix $A$ representing $f_{1,\mathbf{C}}$ with respect to this basis, we see that this is the same as the matrix representing $f$ in the basis $(p(1), \ldots, p(X^{n-1})$ of $E$, and therefore $A \in M_{n,n}(\mathbf{Q})$, and $z$ is an eigenvalue of $A$. ☐

Proof of Theorem 11.2.10. Suppose $P_i \neq 0$ are polynomials with rational coefficients of degree $n_i \geqslant 1$ such that $P_i(z_i) = 0$.

By Lemma 11.2.11, there exist matrices $A_i \in M_{n_i}(\mathbf{Q})$ such that $z_i$ is an eigenvalue of $A_i$, *viewed as a complex matrix*, say for the eigenvector $v_i \in V_i = \mathbf{C}^{n_i}$. Denote $f_i = f_{A_i} \in \mathrm{End}_{\mathbf{C}}(V_i)$. Now form the endomorphism

$$f = f_1 \otimes f_2 \in \mathrm{End}_{\mathbf{C}}(V), \quad V = V_1 \otimes V_2 = \mathbf{C}^{n_1} \otimes \mathbf{C}^{n_2}.$$

Let $w = v_1 \otimes v_2 \in V$. This is a non-zero element of $V$ since $v_1$ and $v_2$ are non-zero in their respective spaces (Corollary 11.1.4). We have

$$f(w) = f(v_1 \otimes v_2) = f_1(v_1) \otimes f_2(v_2) = (z_1 v_1) \otimes (z_2 v_2) = (z_1 z_2)(v_1 \otimes v_2) = z_1 z_2 w$$

by bilinearity of $(v_1, v_2) \mapsto v_1 \otimes v_2$. So $w$ is an eigenvector of $f$ with respect to $z_1 z_2$. Consequently $z_1 z_2$ is a root of the characteristic polynomial of $f$. However, this polynomial has rational coefficients, because if we take for instance the standard bases $B_1 = (e_i)$ and $B_2 = (e'_j)$ of $V_1$ and $V_2$, and the basis

$$B = (e_i \otimes e'_j)$$

of $V$, the fact that $A_i$ has rational coefficients implies that $\mathrm{Mat}(f; B, B)$ has rational coefficients: $f(e_i \otimes e'_j)$ is a linear combination involving the coefficients of $A_1$ and $A_2$ of the basis vectors of $B$. Hence $z_1 z_2$ is an eigenvalue of the rational matrix $A = \mathrm{Mat}(f; B, B)$, therefore a root of its characteristic polynomial, and hence is algebraic.

For the sum, we consider

$$g = f_1 \otimes \mathrm{Id}_{V_2} + \mathrm{Id}_{V_1} \otimes f_2 \in \mathrm{End}_{\mathbf{C}}(V).$$

Then we get

$$g(w) = f_1(v_1) \otimes v_2 + v_1 \otimes f_2(v_2) = z_1(v_1 \otimes v_2) + z_2(v_1 \otimes v_2) = (z_1 + z_2)w,$$

so that $z_1 + z_2$ is an eigenvalue of $g$, hence a root of the (non-zero) characteristic polynomial of $g$, and a similar argument shows that this is a rational polynomial. ☐

## 11.3. Exterior algebra

For the last section of the course, we consider another very important abstract construction that is essential in many applications, especially in differential geometry: the *exterior algebra* of a vector space. We only present the simplest aspects.

Let $\mathbf{K}$ be a field. For a $\mathbf{K}$-vector space $V$, an integer $k \geqslant 0$ and any other $\mathbf{K}$-vector space, we define $\mathrm{Alt}_k(V; W)$ to be the space of all alternating $k$-multilinear maps

$$a \colon V^k \to W.$$

(see Definition 3.1.3). This is a vector subspace of the space of all maps $V^k \to W$.

If $a \in \mathrm{Alt}_k(V; W)$ and $f \colon W \to E$ is a linear map, then $f \circ a$ in a $k$-multilinear map from $V$ to $E$, and it is in fact in $\mathrm{Alt}_k(V; E)$.

Proposition 11.3.1 (Exterior powers). *Let $V$ be a $\mathbf{K}$-vector space and $k \geqslant 0$ an integer. There exists a $\mathbf{K}$-vector space $\bigwedge^k V$ and an alternating $k$-multilinear map*

$$a_0 \colon V^k \to \bigwedge^k V$$

*such that, for any $\mathbf{K}$-vector space $W$, the map*

$$f \mapsto f \circ a_0$$

*is an isomorphism $\mathrm{Hom}_{\mathbf{K}}(\bigwedge^k V, W) \to \mathrm{Alt}_k(V; W)$.*

We denote

$$a_0(v_1, \ldots, v_k) = v_1 \wedge v_2 \wedge \cdots \wedge v_k.$$

Proof. This is a variant of the construction of the tensor product: let $E$ be the $\mathbf{K}$-vector space with basis $V^k$, and $E_0$ the subspace generated by the vectors of the type

$$\begin{aligned}(v_1, \ldots, v_{i-1}, tv_i, v_{i+1}, \ldots, v_k) - t(v_1, \ldots, v_k),\\ (v_1, \ldots, v_{i-1}, v_i + v'_i, v_{i+1}, \ldots, v_k) - (v_1, \ldots, v_{i-1}, v_i, v_{i+1}, \ldots, v_k)\\ -(v_1, \ldots, v_{i-1}, v'_i, v_{i+1}, \ldots, v_k),\\ (v_1, \ldots, v_{i-1}, v_i, v_{i+1}, \ldots, v_{j-1}, v_i, v_{j+1}, \ldots, v_k),\end{aligned}$$

(where in the last case we have $i < j$). Define then $\bigwedge^k V = E/E_0$ and $a_0(v_1, \ldots, v_k) = p((v_1, \ldots, v_k))$, where $p$ is the canonical surjective quotient map. The definition of $E_0$ shows that $a_0$ is a $k$-multilinear alternating map on $V$, and it is then a computation similar to that in the proof of Theorem 11.1.2 to check that the space $\bigwedge^k V$ and this $k$-multilinear map have the desired properties. ☐

Corollary 11.3.2. *Let $V_1$ and $V_2$ be $\mathbf{K}$-vector spaces and $f\colon V_1 \to V_2$ be a $\mathbf{K}$-linear map. For any $k \geqslant 0$, there exists a unique $\mathbf{K}$-linear map $\bigwedge^k f\colon \bigwedge^k V_1 \to \bigwedge^k V_2$ such that*

$$(\bigwedge^k f)(v_1 \wedge \cdots \wedge v_k) = f(v_1) \wedge \cdots \wedge f(v_k).$$

*Moreover, for $f\colon V_1 \to V_2$ and $g\colon V_2 \to V_3$, we have*

$$\bigwedge^k (g \circ f) = \bigwedge^k g \circ \bigwedge^k f,$$

*and $\bigwedge^k \mathrm{Id} = \mathrm{Id}$. In particular, if $f$ is an isomorphism, then so is $\bigwedge^k f$, and*

$$\Big(\bigwedge^k f\Big)^{-1} = \bigwedge^k f^{-1}.$$

Proof. This is entirely similar to the proof of Proposition 11.1.7 for the tensor product: the map

$$V_1^k \to \bigwedge^k V_2$$

mapping $(v_1, \ldots, v_k)$ to $f(v_1) \wedge \cdots \wedge f(v_k)$ is $k$-multilinear and alternating, so by Proposition 11.3.1, there exists a unique linear map

$$\bigwedge^k V_1 \to \bigwedge^k V_2$$

that maps $v_1 \wedge \cdots \wedge v_k$ to $f(v_1) \wedge \cdots \wedge f(v_k)$.

The composition properties then follows from the uniqueness, as in Example 11.1.8, (3). ☐

Proposition 11.3.3. *Let $V$ be a finite-dimensional $\mathbf{K}$-vector space, with $\dim(V) = n \geqslant 0$. Let $B = (v_1, \ldots, v_n)$ be an ordered basis of $V$.*

(1) *We have $\bigwedge^k V = \{0\}$ if $k > n$; for $0 \leqslant k \leqslant n$, we have*

$$\dim \bigwedge^k V = \binom{n}{k}.$$

(2) *For $0 \leqslant k \leqslant n$, and for $I \subset \{1, \ldots, n\}$ a subset with cardinality $k$, let*

$$v_I = v_{i_1} \wedge \cdots \wedge v_{i_k}$$

*where $I = \{i_1, \ldots, i_k\}$ with $i_1 < \cdots < i_k$. Then*

$$B_k = (v_I)_{\mathrm{Card}(I)=k}$$

*is a basis of $\bigwedge^k V$.*

For the proof, we will need the following property that also shows that the notation $v_1 \wedge \cdots \wedge v_k$ is not ambiguous if we think of grouping some of the factors together.

Proposition 11.3.4. *Let $V$ be a $\mathbf{K}$-vector space and $k \geqslant 0$, $\ell \geqslant 0$ integers. There exists a bilinear map*

$$\alpha\colon \bigwedge^k V \times \bigwedge^\ell V \to \bigwedge^{k+\ell} V$$

*such that*

$$\alpha(v_1 \wedge \cdots v_k, v_{k+1} \wedge \cdots \wedge v_{k+\ell}) = v_1 \wedge \cdots \wedge v_{k+\ell}$$

*for all vectors $v_i \in V$, $1 \leqslant i \leqslant k + \ell$.*

One denotes in general $\alpha(x, y) = x \wedge y$ for any $x \in \bigwedge^k V$ and $y \in \bigwedge^\ell V$, and one calls this the *exterior product* or *wedge product* of $x$ and $y$.

PROOF. We begin with a fixed $x \in \bigwedge^k V$ of the form

$$x = v_1 \wedge \cdots \wedge v_k,$$

and consider the map

$$\alpha_x \colon V^\ell \to \bigwedge^{k+\ell} V$$

so that

$$\alpha_x(w_1, \ldots, w_\ell) = v_1 \wedge \cdots \wedge v_k \wedge w_1 \wedge \cdots \wedge w_\ell.$$

One sees that $\alpha_x$ is $\ell$-multilinear and alternating (because the "wedge product") ist. Hence by Proposition 11.3.1, there exists a linear map (that we still denote $\alpha_x$ for simplicity)

$$\bigwedge^\ell V \to \bigwedge^{k+\ell} V$$

such that

$$\alpha_x(w_1 \wedge \cdots \wedge w_\ell) = v_1 \wedge \cdots \wedge v_k \wedge w_1 \wedge \cdots \wedge w_\ell.$$

We can now define a map

$$\alpha \colon V^k \to \mathrm{Hom}_{\mathbf{K}}(\bigwedge^\ell V, \bigwedge^{k+\ell} V)$$

with

$$\alpha(v_1, \ldots, v_k) = \alpha_{v_1 \wedge \cdots \wedge v_k}.$$

It is again an elementary check that the map $\alpha$ itself is $k$-multilinear and alternating. Therefore there exists a linear map (again denoted $\alpha$)

$$\alpha \colon \bigwedge^k V \to \mathrm{Hom}_{\mathbf{K}}(\bigwedge^\ell V, \bigwedge^{k+\ell} V)$$

with $\alpha(v_1 \wedge \cdots \wedge v_k) = \alpha_{v_1 \wedge \cdots \wedge v_k}$. Now we just define

$$x \wedge y = \alpha(x)(y),$$

and the result holds. $\square$

PROOF OF PROPOSITION 11.3.3. The second part of course implies the first since we get a basis with the right number of elements. To prove the second part, we first observe that the alternating property of the wedge product implies that the vectors $v_I$ generate $\bigwedge^k V$. So the problem is to prove that they are linearly independent. Let $t_I$ be elements of $\mathbf{K}$ such that

$$\sum_I t_I v_I = 0,$$

where the sets $I$ are all the $k$-elements subsets of $\{1, \ldots, n\}$. Take any such set $J$, and let $K \subset \{1, \ldots, n\}$ be the complement. Apply the "wedge with $v_K$" operation to the relation: this gives

$$\sum_I t_I v_K \wedge v_I = 0.$$

For any set $I$ *except* $I = J$, the vector $v_K \wedge v_I$ is a wedge product of $n$ vectors, two of which are repeated, hence is zero by the alternating property. So we get

$$t_J v_K \wedge v_J = 0.$$

It is therefore enough to show that $v_K \wedge v_J \neq 0$ in $\bigwedge^n V$. This is an ordered wedge product of $n$ vectors which form an ordered basis $B'$ of $V$. To show that this is non-zero, we use determinants: by Theorem 3.1.7, there exists an $n$-multilinear alternating map $D\colon V^n \to \mathbf{K}$ such that $D(B') = 1$. By Proposition 11.3.1, there is therefore a linear form $D\colon \bigwedge^n V \to \mathbf{K}$ such that $D(v_K \wedge v_J) = 1$. This implies that the vector $v_K \wedge v_J$ is non-zero. ☐

EXAMPLE 11.3.5. One important use of exterior powers is that they can reduce a problem about a finite-dimensional subspace $W$ of a vector space $V$ to a problem about a one-dimension space, or a single vector.

PROPOSITION 11.3.6. *Let $V$ be a finite-dimensional vector space.*

(1) *Let $(v_1, \ldots, v_k)$ be vectors in $V$. Then $(v_1, \ldots, v_k)$ are linearly independent if and only if $v_1 \wedge \cdots \wedge v_k \neq 0$ in $\bigwedge^k V$.*

(2) *Let $(v_1, \ldots, v_k)$ and $(w_1, \ldots, w_k)$ be vectors in $V$, which are linearly independent. Then the $k$-dimensional spaces generated by $(v_1, \ldots, v_k)$ and by $(w_1, \ldots, w_k)$ are equal if and only if there exists $t \neq 0$ in $\mathbf{K}$ such that*

$$w_1 \wedge \cdots \wedge w_k = t\, v_1 \wedge \cdots \wedge v_k.$$

We begin with a lemma:

LEMMA 11.3.7. *Let $W \subset V$ be a subspace of $V$. If $f$ denotes the linear map $W \to V$ that corresponds to the inclusion of $W$ in $V$, then the map $\bigwedge^k f\colon \bigwedge^k W \to \bigwedge^k V$ is injective.*

In other words, we may view $\bigwedge^k W$ as a subspace of $\bigwedge^k V$ by the "obvious" linear map

$$w_1 \wedge \cdots \wedge w_k \to w_1 \wedge \cdots \wedge w_k$$

for $w_1, \ldots, w_k$ in $W$, where the right-hand side is viewed as an element of $\bigwedge^k V$.

PROOF. Let $(v_1, \ldots, v_m)$ be an ordered basis of $W$ and $(v_1, \ldots, v_n)$ an ordered basis of $V$. Then the vectors $v_I$, where $I \subset \{1, \ldots, n\}$ has cardinality $k$, form a basis of $\bigwedge^k V$. Among them we have the vectors $v_I$ where $I \subset \{1, \ldots, m\}$ has cardinality $k$, which are therefore linearly independent. However, by construction, such a vector in $\bigwedge^k V$ is the image by $\bigwedge^k f$ of the corresponding vector in $\bigwedge^k W$. Hence $\bigwedge^k f$ sends a basis of $\bigwedge^k W$ to linearly independent vectors in $\bigwedge^k V$, and this means that this is an injective linear map. ☐

This result means that for some questions at least, the $k$-th exterior power can be used to reduce problems about a $k$-dimensional subspace of a vector space to a problem about a single vector in $\bigwedge^k V$ (or about a one-dimensional subspace). For instance, this gives a nice parameterization of the set of all $k$-dimensional subspaces of an $n$-dimensional space, by non-zero vectors of $\bigwedge^k V$, up to multiplication by a non-zero element of $\mathbf{K}$.

PROOF. (1) If $v_1, \ldots, v_k$ are linearly dependent, we can find elements $t_i$ in $\mathbf{K}$, not all zero, with

$$t_1 v_1 + \cdots + t_k v_k = 0.$$

Assume for instance that $t_j \neq 0$. Then

$$v_j = -\frac{1}{t_j} \sum_{i \neq j} t_i v_i,$$

and hence

$$v_1 \wedge \cdots \wedge v_k = -\frac{1}{t_j} \sum_{i \neq j} v_1 \wedge \cdots \wedge v_{j-1} \wedge v_i \wedge v_{j+1} \wedge \cdots \wedge v_k = 0$$

by the alternating property of the wedge product, since each term contains twice the vector $v_i$.

Conversely, assume that $v_1, \ldots, v_k$ are linearly independent. Let then $v_{k+1}, \ldots, v_n$ be vectors such that $(v_1, \ldots, v_n)$ is an ordered basis of $V$. From Proposition 11.3.3, the vector $v_1 \wedge \cdots \wedge v_k$ is an element of a basis of $\bigwedge^k V$, and therefore it is non-zero.

(2) If $\langle\{v_1, \ldots, v_k\}\rangle = \langle\{w_1, \ldots, w_k\}\rangle$, then both $v_1 \wedge \cdots \wedge v_k$ and $w_1 \wedge \cdots \wedge w_k$ are non-zero elements of the space $\bigwedge^k W$, seen as a subspace of $\bigwedge^k V$ by Lemma 11.3.7. Since $\bigwedge^k W$ has dimension one by Proposition 11.3.3, this means that there exists $t \neq 0$ such that

$$w_1 \wedge \cdots \wedge w_k = t\; v_1 \wedge \cdots \wedge v_k,$$

as claimed.

Conversely, suppose that

$$w_1 \wedge \cdots \wedge w_k = t\; v_1 \wedge \cdots \wedge v_k$$

for some $t \neq 0$. Let $i$ be an integer such that $1 \leqslant i \leqslant k$. Assume that $v_i \notin \langle\{w_1, \ldots, w_k\}\rangle$. Then, since $(w_1, \ldots, w_k)$ are linearly independent, the vectors $(v_i, w_1, \ldots, w_k)$ are linearly independent. But then there exists a basis of $V$ containing them, and in particular the vector

$$v_i \wedge w_1 \wedge \cdots \wedge w_k \in \bigwedge^{k+1} V$$

is non-zero. However, this is also the exterior product $v_i \wedge y$ where $y = w_1 \wedge \cdots \wedge w_k$ (Proposition 11.3.4). Since $y = tv_1 \wedge \cdots \wedge v_k$, the vector is

$$t\; v_i \wedge (v_1 \wedge \cdots \wedge v_k) = 0,$$

by the alternating property. This is a contradiction, so we must have $v_i \in \langle\{w_1, \ldots, w_k\}\rangle$ for all $i$, and this means that

$$\langle\{v_1, \ldots, v_k\}\rangle \subset \langle\{w_1, \ldots, w_k\}\rangle.$$

Since both spaces have dimension $k$, they are equal. $\square$

This can be used very concretely. For instance, consider $V = \mathbf{K}^3$ and the space $W = \langle\{v_1, v_2\}\rangle$ generated by two vectors

$$v_1 = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix}, \quad v_2 = \begin{pmatrix} y_1 \\ y_2 \\ y_3 \end{pmatrix}.$$

When is $W$ of dimension two? In other words, when are $v_1$ and $v_2$ linearly independent? To answer, we compute $v_1 \wedge v_2$ using the basis

$$e_1 \wedge e_2, \qquad e_1 \wedge e_3, \qquad e_2 \wedge e_3$$

of $\bigwedge^2 \mathbf{K}^3$, where $(e_1, e_2, e_3)$ is the standard basis of $\mathbf{K}^3$. We get first

$$\begin{aligned} v_1 \wedge v_2 &= (x_1e_1 + x_2e_2 + x_3e_3) \wedge (y_1e_1 + y_2e_2 + y_3e_3) \\ &= x_1y_1e_1 \wedge e_1 + x_1y_2e_1 \wedge e_2 + x_1y_3e_1 \wedge y_3 \\ &+ x_2y_1e_2 \wedge e_1 + x_2y_2e_2 \wedge e_2 + x_2y_3e_2 \wedge y_3 \\ &+ x_3y_1e_1 \wedge e_3 + x_3y_2e_3 \wedge e_2 + x_3y_3e_3 \wedge y_3 \end{aligned}$$

since the wedge product is multilinear. Since it is also alternating, this becomes

$$v_1 \wedge v_2 = a\ e_1 \wedge e_2 + b\ e_1 \wedge e_3 + c\ e_2 \wedge e_3$$

where

$$a = x_1y_2 - x_2y_1, \qquad b = x_1y_3 - x_3y_1, \qquad c = x_2y_3 - x_3y_2.$$

Hence the space $W$ has dimension 2 if and only if at least one of the numbers $a$, $b$, $c$ is non-zero. (Note that these are the determinants of the $2 \times 2$ matrices obtained from

$$(v_1\ v_2) = \begin{pmatrix} x_1 & y_1 \\ x_2 & y_2 \\ x_3 & y_3 \end{pmatrix}$$

by removing one row; this illustrates a general feature.)

Moreover, the spaces generated by $v_1$, $v_2$ and

$$w_1 = \begin{pmatrix} x_1' \\ x_2' \\ x_3' \end{pmatrix}, \quad w_2 = \begin{pmatrix} y_1' \\ y_2' \\ y_3' \end{pmatrix}$$

are then equal if and only if there exists a non-zero element $t \in \mathbf{K}$ such that

$$\begin{pmatrix} x_1y_2 - x_2y_1 \\ x_1y_3 - x_3y_1 \\ x_2y_3 - x_3y_2 \end{pmatrix} = t \begin{pmatrix} x_1'y_2' - x_2'y_1' \\ x_1'y_3' - x_3'y_1' \\ x_2'y_3' - x_3'y_2' \end{pmatrix}$$

(because this condition implies also that the right-hand side is non-zero in $\mathbf{K}^3$, so $w_1$ and $w_2$ also generate a 2-dimensional space, and the proposition applies).

Example 11.3.8. Our last example is also very important.

Proposition 11.3.9. *Consider $n \geqslant 1$ and an $n$-dimensional $\mathbf{K}$-vector space $V$. Let $f \in \mathrm{End}_{\mathbf{K}}(V)$ be an endomorphism of $V$. Then the endomorphism $\bigwedge^n f$ of the 1-dimensional vector space $\bigwedge^n V$ is the multiplication by $\det(f)$. In other words, for any $(v_1, \ldots, v_n)$ in $V^n$, we have*

$$f(v_1) \wedge \cdots \wedge f(v_n) = \det(f)\ v_1 \wedge \cdots \wedge v_n.$$

In particular, this provides a definition of the determinant of an endomorphism that is independent of the choice of a basis of $V$!

Proof. We illustrate this in the case $n = 2$ first: if $B = (v_1, v_2)$ is an ordered basis of $V$, and

$$\mathrm{Mat}(f; B, B) = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

then

$$\begin{aligned}\Big(\bigwedge^2 f\Big)(e_1 \wedge e_2) = f(e_1) \wedge f(e_2) &= (ae_1 + ce_2) \wedge (be_1 + de_2) \\ &= ab\ e_1 \wedge e_1 + ad\ e_1 \wedge e_2 + bc\ e_2 \wedge e_1 + cd\ e_2 \wedge e_2 \\ &= ad\ e_1 \wedge e_2 + bc\ e_2 \wedge e_1 \\ &= (ad - bc)\ e_1 \wedge e_2.\end{aligned}$$

Since $e_1 \wedge e_2$ is a basis of the one-dimensional space $\bigwedge^2 V$, this implies that $\bigwedge^2 f(x) = \det(f)x$ for all $x \in \bigwedge^2 V$.

Now we consider the general case. One possibility is to generalize the previous computation; this will lead to the result using the Leibniz Formula. Another approach is to use the "axiomatic" characterization of Theorem 3.1.7, and this is what we will do.

We first consider $V = \mathbf{K}^n$. Let $(e_i)$ be the standard basis of $V$. For a matrix $A \in M_{n,n}(\mathbf{K})$, since $\bigwedge^n f_A$ is an endomorphism of the 1-dimensional space $\bigwedge^n V$ generated by $x = e_1 \wedge \cdots \wedge e_n$, there exists an element $\Delta(A) \in \mathbf{K}$ such that $(\bigwedge^n f_A)(y) = \Delta(A)y$ for all $y \in \bigwedge^n V$. Equivalently, this means that $(\bigwedge^n f_A)(x) = \Delta(A)x$, namely, that

$$f_A(e_1) \wedge f_A(e_2) \wedge \cdots \wedge f_A(e_n) = \Delta(A)\ e_1 \wedge e_2 \wedge \cdots \wedge e_n.$$

We consider the map

$$\Delta\colon \mathbf{K}^n \to \mathbf{K}$$

defined by mapping $(v_1, \ldots, v_n)$ to $\Delta(A)$ for the matrix with column vectors $(v_1, \ldots, v_n)$, in other words, to the element $t$ of $\mathbf{K}$ such that

$$v_1 \wedge \cdots \wedge v_n = f_A(e_1) \wedge \cdots \wedge f_A(e_n) = t\ e_1 \wedge \cdots \wedge e_n.$$

Then $\Delta$ is $n$-multilinear: for instance, for the vectors $(tv_1 + sv_1', v_2, \ldots, v_n)$, the relation

$$\begin{aligned}(tv_1 + sv_1') \wedge \cdots \wedge v_n &= t(v_1 \wedge \cdots \wedge v_n) + s(v_1' \wedge \cdots \wedge v_n) \\ &= (t\Delta(v_1, \ldots, v_n) + s\Delta(v_1', v_2, \ldots, v_n))e_1 \wedge \cdots \wedge e_n\end{aligned}$$

shows the multilinearity with respect to the first variable. Moreover, $\Delta$ is alternating, because if $v_i = v_j$, then

$$0 = v_1 \wedge \cdots \wedge v_n = \Delta(v_1, \ldots, v_n)e_1 \wedge \cdots \wedge e_n$$

means that $\Delta(v_1, \ldots, v_n) = 0$. Finally, it is clear that $\Delta(e_1, \ldots, e_n) = 1$, and hence by Theorem 3.1.7 and Corollary 3.1.8, we deduce that

$$\Delta(v_1, \ldots, v_n) = \det(A) = \det(f_A),$$

where $A$ is the matrix with column vectors $(v_1, \ldots, v_n)$.

We now come to the general case. Let $B = (v_1, \ldots, v_n)$ be an ordered basis of $V$ and $j\colon \mathbf{K}^n \to V$ be the isomorphism mapping the vector $(t_i)$ to

$$x = \sum_i t_i v_i \in V.$$

Consider $f \in \mathrm{End}_{\mathbf{K}}(V)$ and the diagram

$$\begin{tikzcd} \mathbf{K}^n \arrow[r, "f_A"] \arrow[d, "j"] & \mathbf{K}^n \arrow[d, "j"] \\ V \arrow[r, "f"] & V \end{tikzcd}$$

where $j^{-1} \circ f \circ j = f_A$ for the matrix $A = \mathrm{Mat}(f; B, B)$. Applying Corollary 11.3.2, we obtain

$$\begin{tikzcd} \bigwedge^n \mathbf{K}^n \arrow[r, "\bigwedge^n f_A"] \arrow[d, "\bigwedge^n j"] & \bigwedge^n \mathbf{K}^n \arrow[d, "\bigwedge^n j"] \\ \bigwedge^n V \arrow[r, "\bigwedge^n f"] & \bigwedge^n V \end{tikzcd},$$

and $\bigwedge^n f$ is an isomorphism, so that

$$\bigwedge^n f = \Big(\bigwedge^n j\Big)^{-1} \circ \bigwedge^n f_A \circ \bigwedge^n j.$$

From the special case previously considered, we know that $\bigwedge^n f_A$ is the multiplication by $\det(f_A) = \det(f)$. It follows that $\bigwedge^n f$ is also the multiplication by $\det(f)$. $\square$

REMARK 11.3.10. The computation we did shows also that the coordinates $(a, b, c)$ of $v_1 \wedge v_2$ with respect to the basis

$$(e_1 \wedge e_2, e_1 \wedge e_3, e_2 \wedge_3)$$

are the same as the coordinates of the classical *vector product* $v_1 \times v_2$ defined as a map

$$\mathbf{K}^3 \times \mathbf{K}^3 \to \mathbf{K}^3.$$

This fact explains the appearance of the cross product in classical vector calculus in $\mathbf{R}^3$, as representing concretely certain aspects of the general differential calculus of differential forms on $\mathbf{R}^n$.

EXAMPLE 11.3.11. As a final remark, without proof, we note an alternative approach to exterior powers, in the case of the dual space of an $n$-dimensional vector space $V$ over a field with characteristic 0. This is sometimes used in differential geometry (in the theory of differential forms).

PROPOSITION 11.3.12. *Let $V$ be an $n$-dimensional $\mathbf{K}$-vector space. There is an isomorphism*

$$\beta \colon \bigwedge^k V^* \to \mathrm{Alt}_k(V; \mathbf{K})$$

*such that for linear forms $\lambda_1, \ldots, \lambda_k$ on $V$, and for $(w_1, \ldots, w_k) \in V^k$, we have*

$$\beta(\lambda_1 \wedge \cdots \wedge \lambda_k)(w_1, \ldots, w_k) = \sum_{\sigma \in \mathrm{S}_k} \varepsilon(\sigma) \lambda_1(w_{\sigma(1)}) \cdots \lambda_k(w_{\sigma(k)}).$$

One may then want to describe the exterior product

$$\bigwedge^k V^* \times \bigwedge^\ell V^* \to \bigwedge^{k+\ell} V^*$$

in terms of $\mathrm{Alt}_k(V; \mathbf{K})$ and $\mathrm{Alt}_\ell(V; \mathbf{K})$ only. This is a rather unpleasant formula: if $a_1 = \beta(x)$ and $a_2 = \beta(y)$, then we have

$$\beta(x \wedge y)(v_1, \ldots, v_{k+\ell}) = \sum_{\sigma \in H_{k,\ell}} \varepsilon(\sigma) a_1(v_{\sigma(1)}, \ldots, v_{\sigma(k)}) a_2(v_{\sigma(k+1)}, \ldots, v_{\sigma(k+\ell)}),$$

where $H_{k,\ell}$ is the subset of permutations $\sigma \in \mathrm{S}_{k+\ell}$ such that

$$\sigma(1) < \cdots < \sigma(k), \qquad \sigma(k+1) < \cdots < \sigma(k+\ell).$$

Hence, although the description seems more concrete, the resulting formulas and properties are much less obvious!

# Appendix: dictionary

We give here a short English–German–French dictionary of important terms in linear algebra.

- Field / Körper / Corps
- Vector space / Vektorraum / Espace vectoriel
- Vector subspace / Unterraum / Sous-espace vectoriel
- Linear map / Lineare Abbildung / Application linéaire
- Matrix, matrices / Matrix, Matrizen / Matrice, matrices
- Kernel / Kern / Noyau
- Image / Bild / Image
- Linear combination / Linearkombination / Combinaison linéaire
- Generating set / Erzeugendensystem / Ensemble générateur
- Linearly (in)dependent set / Linear (un)abhängig Menge / Ensemble linéairement (in)dépendant
- Basis (plural bases) / Basis (pl. Basen) / Base (pl. bases)
- Ordered basis / Geordnete Basis / Base ordonnée
- Dimension / Dimension / Dimension
- Isomorphism / Isomorphismus / Isomorphisme
- Isomorphic to... / Isomorph zu... / Isomorphe à...
- Endomorphism / Endomorphismus / Endomorphisme
- Change of basis matrix / Basiswechselmatrix / Matrice de changement de base
- Row echelon form / Zeilenstufenform / Forme échelonnée
- Upper/lower triangular matrix / Obere-/Untere-/Dreiecksmatrix / Matrices triangulaire supérieure / inférieure
- Determinant / Determinante / Déterminant
- Permutation / Permutation / Permutation
- Signature / Signum / Signature
- Transpose matrix / Transponierte Matrix / Matrice transposée
- Trace / Spur / Trace
- Direct sum / Direkte Summe / Somme directe
- Complement / Komplement / Complément
- Stable or invariant subspace / Invarianter Unterraum / Sous-espace stable ou invariant
- Matrices similaires / Ähnliche Matrizen / Matrices similaires
- Conjugate matrices / Konjugierte Matrizen / Matrices conjuguées
- Eigenvalue / Eigenwert / Valeur propre
- Eigenvector / Eigenvektor / Vecteur propre
- Eigenspace / Eigenraum / Espace propre
- Spectrum / Spektrum / Spectre
- Characteristic polynomial / Charakteristisches Polynom / Polynôme caractéristique
- Diagonalizable / Diagonalisierbar / Diagonalisable

- Multiplicity / Vielfachheit / Multiplicité
- Involution / Involution / Involution
- Projection / Projektion / Projection
- Nilpotent / Nilpotent / Nilpotent
- Dual space / Dualraum / Espace dual
- Linear form / Linearform / Forme linéaire
- Bilinear form / Bilinearform / Forme bilinéaire
- Non-degenerate / Nicht-ausgeartet / Non-dégénérée
- Positive definite / Positiv definit / Définie positive
- Positive demi-definite / Positiv semi-definit / Semi-définie positive
- Scalar product / Skalarprodukt / Produit scalaire
- Euclidean space / Euklidisches Raum / Espace euclidien
- Adjoint / Adjungierte / Adjoint
- Orthogonal group / Orthogonale Gruppe / Groupe orthogonal
- Self-adjoint map / Selbstadjungierte Abbildung / Application auto-adjointe
- Quadratic form / Quadratische Form / Forme quadratique
- Quadric / Quadrik / Quadrique
- Singular values / Singulärwerte / Valeurs singulières
- Sesquilinear form / Sesquilinearform / Forme sesquilinéaire
- Hermitian form / Hermitesche Form / Forme hermitienne
- Unitary space / Unitärer Raum / Espace hermitien ou pré-hilbertien
- Unitary group / Unitäre Gruppe / Groupe unitaire
- Normal map / Normale Abbildung / Application linéaire normale
- Jordan Block / Jordanblock / Bloc de Jordan
- Jordan Normal Form / Jordansche Normalform / Forme de Jordan
- Dual basis / Duale Basis / Base duale
- Transpose of a linear map / Duale Abbildung / Transposée d'une application linéaire
- Characteristic of a field / Charakteristik eines Körpers / Caractéristique d'un corps
- Euclidean division of polynomials / Polynomdivision / Division euclidienne des polynômes
- Quotient space / Quotientenraum / Espace quotient
- Tensor product / Tensorprodukt / Produit tensoriel
- Exterior powers / Äussere Potenzen / Puissances extérieures
- Exterior or wedge product / "Wedge" Produkt / Produit extérieur