Linear Algebra 2

University of Luxembourg

Gabor Wiese[*]
gabor.wiese@uni.lu

Version of 7th July 2017

Contents

[*] translated from the French original by Luca and Massimo Notarnicola

Preface

This is an English translation of my lecture notes *Algèbre linéaire 2*, as taught in the Summer Term 2017 in the academic Bachelor programme at the University of Luxembourg in the tracks mathematics and physics (with mathematical focus).

These notes have developed over the years. They draw on various sources, most notably on Fischer's book *Lineare Algebra* (Vieweg-Verlag) and lecture notes by B. H. Matzat from the University of Heidelberg.

I would like to thank Luca and Massimo Notarnicola for taking the time to translate these notes from French to English, and correcting some errors in the process.

Esch-sur-Alzette, 7 July 2017, Gabor Wiese

References

Here are some references: these books are available at the university library.

- Lelong-Ferrand, Arnaudiès. *Cours de mathématiques, Tome 1, Algèbre*. Dunod. Ce livre est très complet et très détaillé. On peut l'utiliser comme ouvrage de référence.
- Siegfried Bosch: *Algebra* (en allemand), Springer-Verlag. Ce livre est très complet et bien lisible.
- Serge Lang: *Algebra* (en anglais), Springer-Verlag. C'est comme une encyclopédie de l'algèbre; on y trouve beaucoup de sujets rassemblés, écrits de façon concise.
- Siegfried Bosch. *Lineare Algebra*, Springer-Verlag.
- Jens Carsten Jantzen, Joachim Schwermer. *Algebra*.
- Christian Karpfinger, Kurt Meyberg. *Algebra: Gruppen - Ringe - Körper*, Spektrum Akademischer Verlag.
- Gerd Fischer. *Lehrbuch der Algebra: Mit lebendigen Beispielen, ausführlichen Erläuterungen und zahlreichen Bildern*, Vieweg+Teubner Verlag.
- Gerd Fischer. *Lineare Algebra: Eine Einführung für Studienanfänger*, Vieweg+Teubner Verlag.
- Gerd Fischer, Florian Quiring. *Lernbuch Lineare Algebra und Analytische Geometrie: Das Wichtigste ausführlich für das Lehramts- und Bachelorstudium*, Springer Vieweg.
- Perrin. *Cours d'algèbre*, Ellipses.
- Guin, Hausberger. *Algèbre I. Groupes, corps et théorie de Galois*, EDP Sciences.
- Fresnel. *Algèbre des matrices*, Hermann.
- Tauvel. *Algèbre*.
- Combes. *Algèbre et géométrie*.

Prerequisites

This course contains a theoretical and a practical part. For the practical part, (almost) all the computations can be solved by two fundamental operations:

- solving linear systems of equations,
- calculating determinants.

We are going to start the course by two sections of recalls: one about the fundaments of vector spaces and one about determinants.
Linear algebra can be done over any field, not only over real or complex numbers.
Some of the students may have seen the definition of a field in previous courses. For Computer Science, finite fields, and especially the field $\mathbb{F}_2$ of two elements, are particularly important. Let us quickly recall the definition of a field.

Definition 0.1. *A* field K *is a set* K *containing two distinct elements* $0, 1$ *and admitting two maps*

$$\begin{aligned} + : K \times K \to K, &\quad (a,b) \mapsto a+b, &\qquad \text{“addition”} \\ \cdot : K \times K \to K, &\quad (a,b) \mapsto a \cdot b &\qquad \text{“multiplication”}, \end{aligned}$$

such that for all $x, y, z \in K$*, the following assertions are satisfied:*

- neutral element for the addition: $x + 0 = x = 0 + x$*;*
- associativity of the addition: $(x+y)+z = x+(y+z)$*;*
- existence of an inverse for the multiplication: *there exists an element called* $-x$ *such that* $x + (-x) = 0 = (-x) + x$*;*
- commutativity of the addition: $x + y = y + x$.
- neutral element for the multiplication: $x \cdot 1 = x = 1 \cdot x$*;*
- associativity of the multiplication: $(x \cdot y) \cdot z = x \cdot (y \cdot z)$*;*
- existence of an inverse for the multiplication: *if* $x \neq 0$*, there exists an element called* $x^{-1} = \frac{1}{x}$ *such that* $x \cdot x^{-1} = 1 = x^{-1} \cdot x$*;*
- commutativity for the multiplication: $x \cdot y = y \cdot x$.
- ditributivity: $(x+y) \cdot z = x \cdot z + y \cdot z$.

Example 0.2.

- $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ *are fields.*
- *If* p *is a prime number,* $\mathbb{Z}/p\mathbb{Z}$ *is a field.*
- $\mathbb{Z}$ *and* $\mathbb{N}$ *are no fields.*

For the following, let K be a field. If this can help you for understanding, you can take $K = \mathbb{R}$ or $K = \mathbb{C}$.

1 Recalls: Vector spaces, bases, dimension, homomorphisms

Goals:

- Master the notions of vector space and subspace;
- master the notions of basis and dimension;
- master the notions of linear map ((homo)morphism), of kernel, of image;
- know examples and be able to prove simple properties.

Matrix descriptions and solving linear systems of equations by Gauss' row reduction algorithm are assumed known and practiced.

Definition of vector spaces

Definition 1.1. *Let V be a set with $0_V \in V$ an element, and maps*

$$+ : V \times V \to V, \quad (v_1, v_2) \mapsto v_1 + v_2 = v_1 + v_2$$

(called addition*) et*

$$\cdot : K \times V \to V, \quad (a, v) \mapsto a \cdot v = av$$

(called scalar multiplication*).*
*We call $(V, +_V, \cdot_V, 0_V)$ un K-*vector space *if*

(A1) $\forall\, u, v, w \in V : (u +_V v) +_V w = u +_V (v +_V w)$*,*

(A2) $\forall\, v \in V : 0_V +_V v = v = v +_V 0_V$*,*

(A3) $\forall\, v \in V \exists\, w \in V : v +_V w = 0 = w +_V v$ *(we write $-v := w$),*

(A4) $\forall\, u, v \in V : u +_V v = v +_V u$*,*

(for mathematicians: these properties say that $(V, +_V, 0_V)$ is an abelian group) and

(MS1) $\forall\, a \in K, \forall\, u, v \in V : a \cdot_V (u +_V v) = a \cdot_V u +_V a \cdot_V v$*,*

(MS2) $\forall\, a, b \in K, \forall v \in V : (a +_K b) \cdot_V v = a \cdot_V v +_V b \cdot_V v$*,*

(MS3) $\forall\, a, b \in K, \forall v \in V : (a \cdot_K b) \cdot_V v = a \cdot_V (b \cdot_V v)$*,*

(MS4) $\forall\, v \in V : 1 \cdot_V v = v$*.*

For clarity, we have written $+_V$, $\cdot_V$ for the addition and the scalar multiplication in V, and $+_K$, $\cdot_K$ for the addition and the multiplication in K. In the following, we will not do this any more.

Example 1.2. *Let $n \in \mathbb{N}$. The canonical K-vector space of dimension n is K^n, the set of column vectors of size n with coefficients in K. As you know, we can add two elements of K^n in the following way:*

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

This addition satisfies the following properties:

(A1) $$(\begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix} + \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{pmatrix}) + \begin{pmatrix} c_1 \\ c_2 \\ \vdots \\ c_n \end{pmatrix} = \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix} + (\begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{pmatrix} + \begin{pmatrix} c_1 \\ c_2 \\ \vdots \\ c_n \end{pmatrix}).$$

(A2) $$\begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix} + \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix} = \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix} = \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix} + \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}.$$

(A3) $$\begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix} + \begin{pmatrix} -a_1 \\ -a_2 \\ \vdots \\ -a_n \end{pmatrix} = \begin{pmatrix} a_1-a_1 \\ a_2-a_2 \\ \vdots \\ a_n-a_n \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}.$$

(A4) $$\begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix} + \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{pmatrix} = \begin{pmatrix} a_1+b_1 \\ a_2+b_2 \\ \vdots \\ a_n+b_n \end{pmatrix} = \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{pmatrix} + \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix}.$$

Moreover, we have a scalar multiplication: we multiply an element of K^n by an element r of K as follows:

$$r \cdot \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix} = \begin{pmatrix} ra_1 \\ ra_2 \\ \vdots \\ ra_n \end{pmatrix}.$$

The addition and the multiplication are compatible in the following manner:

(MS1) $$\forall\, r \in K, \forall \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix}, \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{pmatrix} \in K^n\text{: } r \cdot (\begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix} + \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{pmatrix}) = r \cdot \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix} + r \cdot \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{pmatrix};$$

(MS2) $$\forall\, r, s \in K, \forall \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix} \in K^n\text{: } (r+s) \cdot \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix} = r \cdot \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix} + s \cdot \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix};$$

(MS3) $$\forall\, r, s \in K, \forall \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix} \in K^n\text{: } r \cdot (s \cdot \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix}) = (r \cdot s) \cdot \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix};$$

(MS4) $$\forall \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix} \in K^n\text{: } 1 \cdot \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix} = \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix}.$$

This shows that K^n is indeed a K-vector space.

The following proposition produces a large number of examples.

Proposition 1.3. *Let E be a set. We introduce the notation*

$$\mathcal{F}(E,K) := \{f \mid f : E \to K \text{ map }\}$$

for the set of maps from E to K. We denote the map $E \to K$ such that all its values are 0 by $0_{\mathcal{F}}$ (concretely: $0_{\mathcal{F}} : E \to K$ defined by the rule $0_{\mathcal{F}}(e) = 0$ for all $e \in E$). We define the addition

$$+_{\mathcal{F}} : \mathcal{F}(E,K) \times \mathcal{F}(E,K) \to \mathcal{F}(E,K), \quad (f,g) \mapsto f +_{\mathcal{F}} g \text{ où } \forall e \in E : (f +_{\mathcal{F}} g)(e) := f(e) + g(e)$$

and the scalar mutliplication

$$\cdot_{\mathcal{F}} : K \times \mathcal{F}(E,K) \to \mathcal{F}(E,K), \quad (x,f) \mapsto x \cdot_{\mathcal{F}} f \text{ où } \forall e \in E : (x \cdot_{\mathcal{F}} f)(e) := x \cdot (f(e)).$$

Then, $(\mathcal{F}(E,K), +_{\mathcal{F}}, \cdot_{\mathcal{F}}, 0_{\mathcal{F}})$ is a K-vector space.

Proof. Exercise. □

Most of the time, we will not write the indices, but only $f + g$, $f \cdot g$, etc.

Example 1.4. *(a) $\{f \in \mathcal{F}(\mathbb{R},\mathbb{R}) \mid f(1) = 0\}$ is a K-vector space.*

(b) $\{f \in \mathcal{F}(\mathbb{R},\mathbb{R}) \mid f(0) = 1\}$ is not a K-vector space.

Lemma 1.5. *Let $(V, +_V, \cdot_V, 0_V)$ be a K-vector space. Then, the following properties are satisfied for all $v \in V$ and all $a \in K$:*

(a) $0 \cdot_V v = 0_V$;

(b) $a \cdot_V 0_V = 0_V$;

(c) $a \cdot_V v = 0_V \Rightarrow a = 0 \vee v = 0_V$;

(d) $(-1) \cdot_V v = -v$.

Proof. (a) $0 \cdot_V v = (0+0) \cdot_V v = 0 \cdot_V v + 0 \cdot_V v$, donc $0 \cdot_V v = 0_V$.
(b) $a \cdot_V 0_V = a \cdot_V (0_V + 0_V) = a \cdot_V 0_V + a \cdot_V 0_V$, donc $a \cdot_V 0_V = 0_V$.
(c) Assume $a \cdot_V v = 0_V$. If $a = 0$, the assertion $a = 0 \vee v = 0_V$ is true. Assume therefore $a \neq 0$. Then a^{-1} has a meaning. Consequently, $v = 1 \cdot_V v = (a^{-1} \cdot a) \cdot_V v = a^{-1} \cdot_V (a \cdot_V v) = a^{-1} \cdot_V 0_V = 0_V$ by (b).
(d) $v +_V (-1) \cdot_V v = 1 \cdot_V v +_V (-1) \cdot_V v = (1 + (-1)) \cdot_V v = 0 \cdot_V v = 0_V$ by (a). □

Instead of $(V, +_V, \cdot_V, 0_V)$ we will simply write V.

Vector subspaces

Definition 1.6. *Let V be a K-vector space. We say that a non-empty subset $W \subseteq V$ is a* vector subspace of *V if*

$$\forall\, w_1, w_2 \in W, \forall a \in K : a \cdot w_1 + w_2 \in W.$$

Notation: $W \leq V$.

Example 1.7.

- *Let V be a K-vector space. The set $\{0\}$ is a vector subspace of V, called the* zero space, *denoted by 0 for simplicity (do not confuse with the element 0).*
- *Let $V = \mathbb{R}^2$ and $W = \{\left(\begin{smallmatrix} a \\ 0 \end{smallmatrix}\right) \mid a \in \mathbb{R}\} \subseteq V$. Then, W is a subspace of V.*
- *Let $V = \mathbb{R}^3$ and $W = \left\{\left(\begin{smallmatrix} a \\ b \\ 2b \end{smallmatrix}\right) \mid a, b \in \mathbb{R}\right\} \subseteq V$. Then, W is a subspace of V.*
- *Let $n, m \in \mathbb{N}_{\geq 1}$. We consider the system of linear equations*

$$\begin{aligned} a_{1,1}x_1 + a_{1,2}x_2 + \cdots + a_{1,n}x_n &= b_1 \\ a_{2,1}x_1 + a_{2,2}x_2 + \cdots + a_{2,n}x_n &= b_2 \\ &\vdots \\ a_{m,1}x_1 + a_{m,2}x_2 + \cdots + a_{m,n}x_n &= b_m \end{aligned}$$

with $b_i, a_{i,j} \in K$ for $1 \leq i \leq m$, $1 \leq j \leq n$.

(a) *Let S be the set of all solutions of the homogeneous system with $x_1, x_2, \ldots, x_n \in K$, i.e.*

$$S = \left\{ \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} \in K^n \mid \forall i \in \{1, 2, \ldots, m\} : \sum_{j=1}^{n} a_{i,j}x_j = 0 \right\}.$$

Then, S is a vector subspace of the standard K-vector space K^n.

(b) *Let $\begin{pmatrix} r_1 \\ r_2 \\ \vdots \\ r_n \end{pmatrix} \in K^n$ be a solution of the system of linear equations, i.e.:*

$$\forall i \in \{1, 2, \ldots, m\} : \sum_{j=1}^{n} a_{i,j}r_j = b_i.$$

Let S be the vector subspace of K^n defined in (a).

Then, the solutions if the system of linear equations are the set

$$\left\{ \begin{pmatrix} r_1 \\ r_2 \\ \vdots \\ r_n \end{pmatrix} + \begin{pmatrix} s_1 \\ s_2 \\ \vdots \\ s_n \end{pmatrix} \mid \begin{pmatrix} s_1 \\ s_2 \\ \vdots \\ s_n \end{pmatrix} \in S \right\}.$$

Here is a general form to obtain and write subspaces.

Definition-Lemma 1.8. *Let V be a K-vector space and $E \subseteq V$ a non-empty subspace. We set*

$$\langle E \rangle := \{\sum_{i=1}^{m} a_i e_i \mid m \in \mathbb{N}, e_1, \ldots, e_m \in E, a_1, \ldots, a_m \in K\}.$$

This is a vector subspace of V, said to be generated by E.
By convention, we set $\langle \emptyset \rangle = 0$, the zero subspace.

Proof. Since $\langle E\rangle$ is non-empty (since E is non-empty), it suffizes to check the definition of subspace. Let therefore $w_1, w_2 \in \langle E\rangle$ and $a \in K$. We can write

$$w_1 = \sum_{i=1}^{m} a_i e_i \text{ et } w_2 = \sum_{i=1}^{m} b_i e_i$$

for $a_i, b_i \in K$ and $e_i \in E$ for all $i = 1, \dots, m$. Thus we have

$$a \cdot w_1 + w_2 = \sum_{i=1}^{m} (aa_i + b_i)e_i,$$

which is indeed an element of $\langle E\rangle$. □

Example 1.9. *The set* $\left\{a \cdot \begin{pmatrix} 1 \\ 1 \\ 2 \end{pmatrix} + b \cdot \begin{pmatrix} 0 \\ 0 \\ 7 \end{pmatrix} \mid a, b \in \mathbb{R}\right\}$ *is a subspace of* $\mathbb{R}^3$.

Sometimes it is useful to characterize the subspace generated by a set in a more theoretical way. To do so, we need the following lemma.

Lemma 1.10. *Let V be a K-vector space and $W_i \le V$ subspaces for $i \in I \neq \emptyset$. Then, $W := \bigcap_{i\in I} W_i$ is a vector subspace of V.*

Proof. Exercise. □

In contrast, $\bigcup_{i\in I} W_i$ is not a subspace in general (as you see it in an exercise)!

Example 1.11. *How to compute the intersection of two subspaces?*

(a) *The easiest case is when the two subspaces are given as the solutions of two systems of linear equations, for example:*

- *V is the subset of $\begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} \in K^n$ such that $\sum_{i=1}^{n} a_{i,j}x_i = 0$ for $j = 1, \dots, \ell$, et*
- *W is the subset of $\begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} \in K^n$ such that $\sum_{i=1}^{n} b_{i,k}x_i = 0$ pour $k = 1, \dots, m$.*

In this case, the subspace $V \cap W$ is given as the set of common solutions for all the equalities.

(b) *Suppose now that the subspaces are given as subspaces of K^n generated by finite sets of vectors: Let $V = \langle E\rangle$ and $W = \langle F\rangle$ où*

$$E = \left\{\begin{pmatrix} e_{1,1} \\ e_{2,1} \\ \vdots \\ e_{n,1} \end{pmatrix}, \dots, \begin{pmatrix} e_{1,m} \\ e_{2,m} \\ \vdots \\ e_{n,m} \end{pmatrix}\right\} \subseteq K^n \text{ and } F = \left\{\begin{pmatrix} f_{1,1} \\ f_{2,1} \\ \vdots \\ f_{n,1} \end{pmatrix}, \dots, \begin{pmatrix} f_{1,p} \\ f_{2,p} \\ \vdots \\ f_{n,p} \end{pmatrix}\right\} \subseteq K^n.$$

Then

$$V \cap W = \{\sum_{i=1}^{m} a_i \begin{pmatrix} e_{1,i} \\ e_{2,i} \\ \vdots \\ e_{n,i} \end{pmatrix} \mid$$

$$\exists\, b_1, \dots, b_p \in K : a_1 \begin{pmatrix} e_{1,1} \\ e_{2,1} \\ \vdots \\ e_{n,1} \end{pmatrix} + \dots + a_m \begin{pmatrix} e_{1,m} \\ e_{2,m} \\ \vdots \\ e_{n,m} \end{pmatrix} - b_1 \begin{pmatrix} f_{1,1} \\ f_{2,1} \\ \vdots \\ f_{n,1} \end{pmatrix} - \dots - b_p \begin{pmatrix} f_{1,p} \\ f_{2,p} \\ \vdots \\ f_{n,p} \end{pmatrix} = 0\}.$$

Here is a concrete example: $E = \left\{ \left(\begin{smallmatrix}1\\1\\2\end{smallmatrix}\right), \left(\begin{smallmatrix}0\\1\\0\end{smallmatrix}\right) \right\} \subseteq K^n$ *and* $F = \left\{ \left(\begin{smallmatrix}1\\0\\1\end{smallmatrix}\right), \left(\begin{smallmatrix}2\\0\\1\end{smallmatrix}\right) \right\} \subseteq K^n$*. We have to solve the system*

$$\left(\begin{smallmatrix}1&0&-1&-2\\1&1&0&0\\2&0&-1&-1\end{smallmatrix}\right)\left(\begin{smallmatrix}x_1\\x_2\\y_1\\y_2\end{smallmatrix}\right) = 0.$$

With operations on the rows, we obtain

$$\ker(\left(\begin{smallmatrix}1&0&-1&-2\\1&1&0&0\\2&0&-1&-1\end{smallmatrix}\right)) = \ker(\left(\begin{smallmatrix}1&0&-1&-2\\0&1&1&2\\0&0&1&3\end{smallmatrix}\right)) = \ker(\left(\begin{smallmatrix}1&0&0&1\\0&1&0&-1\\0&0&1&3\end{smallmatrix}\right)),$$

thus we obtain as solution subspace the line generated by $\left(\begin{smallmatrix}-1\\1\\-3\\1\end{smallmatrix}\right)$*, so the intersection is given by the line*

$$\langle -1 \cdot \left(\begin{smallmatrix}1\\1\\2\end{smallmatrix}\right) + 1 \cdot \left(\begin{smallmatrix}0\\1\\0\end{smallmatrix}\right)\rangle = \langle -3 \cdot \left(\begin{smallmatrix}1\\0\\1\end{smallmatrix}\right) + 1 \cdot \left(\begin{smallmatrix}2\\0\\1\end{smallmatrix}\right)\rangle = \langle \left(\begin{smallmatrix}1\\0\\2\end{smallmatrix}\right)\rangle.$$

Here is the alternative characterization of the subspace generated by a set

Lemma 1.12. *Let V be a K-vector space and $E \subseteq V$ a non-empty subset. Then we have the equality*

$$\langle E \rangle = \bigcap_{W \leq V \text{ subspace s.t. } E \subseteq W} W$$

where the right hand side is the intersection of all the subspaces W of V containing E.

Proof. To prove the equality of two sets, we have to prove the two inclusions.
' $\subseteq$ ': Any subspace W containing E, also contains all the linear combinations of elements of E, hence W contains $\langle E \rangle$. Consequently, $\langle E \rangle$ in the intersection on the right.
' $\supseteq$ ': Since $\langle E \rangle$ belongs to the subspaces in the intersection on the right, it is clear that this intersection is contained in $\langle E \rangle$. □

Definition 1.13. *Let V be a K-vector space and $E \subseteq V$ a subset. We say that V is* generated by E (as vector subspace) *if $V = \langle E \rangle$.*
Put another way, this means that any element of V is written as linear combination of vectors in E.

Definition 1.14. *Let V be a K-vector space and $W_i \leq V$ subspaces of V for $i \in I \neq \emptyset$. We set*

$$\sum_{i \in I} W_i := \langle \bigcup_{i \in I} W_i \rangle,$$

the subspace of V generated by all the elements of all the W_i's. We call it the sum of the W_i's, $i \in I$.
If $I = \{1, 2, \ldots, n\}$, we can write $\sum_{i=1}^n W_i$ explicitly as

$$\sum_{i=1}^n W_i = \{\sum_{i=1}^n w_i \mid w_1 \in W_1, \ldots w_n \in W_n\}.$$

For a general I, this generalizes as:

$$\sum_{i \in I} W_i = \{\sum_{i \in I} w_i \mid \big(\forall\, i \in I : w_i \in W_i\big) \text{ and } w_i \neq 0 \text{ for only finitely many } i \in I\}.$$

We use the notation $\sum_{i \in I}' w_i$ to indicate $w_i \neq 0$ for only finitely many $i \in I$.

Example 1.15. *How to compte/obtain the sum of two subspaces?*
The answer is very easy if the two subspaces are given by generators: If $U = \langle E \rangle$ and $V = \langle F \rangle$ are subspaces of a K-vector space V, then $U + V = \langle E \cup F \rangle$.
(The question of giving a basis for the sum is different... see later.)

When are the $w_i \in W_i$ in the writing $w = \sum'_{i \in I} w_i$ unique?

Definition 1.16. *Let V be a K-vector space and $W_i \leq V$ the subspace of V for $i \in I \neq \emptyset$.*
We say that the sum $W = \sum_{i \in I} W_i$ is direct *if for all $i \in I$ we have*

$$W_i \cap \sum_{j \in I \setminus \{i\}} W_j = 0.$$

Notation for direct sums: $\bigoplus_{i \in I} W_i$.
If $I = \{1, \dots, n\}$, we sometimes write the elements of a direct sum $\bigoplus_{i=1}^n W_i$ as $w_1 \oplus w_2 \oplus \dots \oplus w_n$ (where $w_i \in W_i$ for $i \in I$, of course).

Example 1.17. *In Example 1.11 (b), the sum $V + W$ is not direct since the intersection $V \cap W$ is a line and thus non-zero.*

Proposition 1.18. *Let V be a K-vector space, $W_i \leq V$ subspaces of V for $i \in I \neq \emptyset$ and $W = \sum_{i \in I} W_i$. Then the following assertions are equivalent:*

(i) $W = \bigoplus_{i \in I} W_i$;

(ii) for all $w \in W$ and all $i \in I$ there exists a unique $w_i \in W_i$ such that $w = \sum'_{i \in I} w_i$.

Proof. "(i) ⇒ (ii)": The existence of such $w_i \in W_i$ is clear. Let us thus show the uniqueness

$$w = \sum_{i \in I}{}' w_i = \sum_{i \in I}{}' w'_i$$

with $w_i, w'_i \in W_i$ for all $i \in I$ (remember that the notation $\sum'$ indicates that only finitely many w_i, w'_i are non-zero). This implies for $i \in I$:

$$w_i - w'_i = \sum_{j \in I \setminus \{i\}}{}' (w'_j - w_j) \in W_i \cap \sum_{j \in I \setminus \{i\}} W_j = 0.$$

Thus, $w_i - w'_i = 0$, so $w_i = w'_i$ for all $i \in I$, showing uniqueness.
"(ii) ⇒ (i)": Let $i \in I$ and $w_i \in W_i \cap \sum_{j \in I \setminus \{i\}} W_j$. Then, $w_i = \sum'_{j \in I \setminus \{i\}} w_j$ with $w_j \in W_j$ for all $j \in I$. We can now write 0 in two ways

$$0 = \sum_{i \in I}{}' 0 = -w_i + \sum_{j \in I \setminus \{i\}}{}' w_j.$$

Hence, the uniqueness imples $-w_i = 0$. Therefore, we have shown $W_i \cap \sum_{j \in I \setminus \{i\}} W_j = 0$. □

Bases

Definition 1.19. *Let V be a K-vector space and $E \subseteq V$ a subspace.*
*We say that E is K-*linearly independent *if*

$$\forall\, n \in \mathbb{N}\,\forall\, a_1,\dots,a_n \in K\,\forall\, e_1,\dots,e_n \in E : \big(\sum_{i=1}^{n} a_ie_i = 0 \in V \Rightarrow a_1 = a_2 = \cdots = a_n = 0\big)$$

*(i.e., the only K-linear combination of elements of E representing $0 \in V$ is the one in which all the coefficients are 0). On the other hand, we say that E is K-*linearly dependent.
*We call E a K-*basis of *V if E generates V and E is K-linearly independent.*

Example 1.20. *How to compute whether two vectors are linearly independent? (Same answer than almost always:) Solve a system of linear equations.*
Let the subspace

$$\left\{\begin{pmatrix} e_{1,1} \\ e_{2,1} \\ \vdots \\ e_{n,1} \end{pmatrix}, \dots, \begin{pmatrix} e_{1,m} \\ e_{2,m} \\ \vdots \\ e_{n,m} \end{pmatrix}\right\}$$

of K^n be given. These vectors are linearly independent if and only if the only solution of the system of linear equations

$$\begin{pmatrix} e_{1,1} & e_{1,2} & \cdots & e_{1,m} \\ e_{2,1} & e_{2,2} & \cdots & e_{2,m} \\ \vdots & \vdots & \ddots & \vdots \\ e_{n,1} & e_{n,2} & \cdots & e_{n,m} \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_m \end{pmatrix} = 0$$

is zero.

Example 1.21. *Let $d \in \mathbb{N}_{>0}$. Set $e_1 = \begin{pmatrix} 1 \\ 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, e_2 = \begin{pmatrix} 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \dots, e_d = \begin{pmatrix} 0 \\ 0 \\ 0 \\ \vdots \\ 1 \end{pmatrix}$ et $E = \{e_1, e_2, \dots, e_d\}$.*
Then:

- *E generates K^d:*

  Any vector $v = \begin{pmatrix} a_1 \\ a_2 \\ a_3 \\ \vdots \\ a_d \end{pmatrix}$ is written as K-linear combination: $v = \sum_{i=1}^{d} a_ie_i$.

- *E is K-linearly independent:*

  If we have a K-linear combination $0 = \sum_{i=1}^{d} a_ie_i$, then clearly $a_1 = \cdots = a_d = 0$.

- *E is thus a K-basis of K^d, since E generates K^d and is K-linearly independent. We call it the* canonical basis *of K^d.*

The following theorem characterizes bases.

Theorem 1.22. *Let V be a K-vector space and $E = \{e_1, e_2, \dots, e_n\} \subseteq V$ be a finite subset. Then, the following assertions are equivalent:*

(i) E is a K-basis.

(ii) *E is a minimal set of generators of V, i.e.: E generates V, but for all $e \in E$, the set $E \setminus \{e\}$ does not generate V.*

(iii) *E is a maximal K-linearly independent set, i.e.: E is K-linearly independent, but for all $e \in V \setminus E$, the set $E \cup \{e\}$ is K-linearly dependent.*

(iv) *Any $v \in V$ is written as $v = \sum_{i=1}^{n} a_i e_i$ with unique $a_1, \dots, a_n \in K$.*

Corollary 1.23. *Let V be a K-vector space and $E \subseteq V$ a finite set generating V. Then, V has K-basis contained in E.*

In the appendix of this section, we will show using Zorn's Lemma that any vector space has a basis.

Example 1.24. *(a) Let $V = \left\{ \left(\begin{smallmatrix} a \\ a \\ b \end{smallmatrix}\right) \mid a, b \in \mathbb{R} \right\}$. A basis of V is $\left\{ \left(\begin{smallmatrix} 1 \\ 1 \\ 0 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 \\ 0 \\ 1 \end{smallmatrix}\right) \right\}$.*

(b) Let $V = \langle \left(\begin{smallmatrix} 1 \\ 2 \\ 3 \end{smallmatrix}\right), \left(\begin{smallmatrix} 2 \\ 3 \\ 4 \end{smallmatrix}\right), \left(\begin{smallmatrix} 3 \\ 5 \\ 7 \end{smallmatrix}\right) \rangle \subseteq \mathbb{Q}^3$.

The set $E = \left\{ \left(\begin{smallmatrix} 1 \\ 2 \\ 3 \end{smallmatrix}\right), \left(\begin{smallmatrix} 2 \\ 3 \\ 4 \end{smallmatrix}\right) \right\}$ is a $\mathbb{Q}$-basis of V. Reason:

- *The system of linear equations*

$$a_1 \cdot \left(\begin{smallmatrix} 1 \\ 2 \\ 3 \end{smallmatrix}\right) + a_2 \cdot \left(\begin{smallmatrix} 2 \\ 3 \\ 4 \end{smallmatrix}\right) + a_3 \cdot \left(\begin{smallmatrix} 3 \\ 5 \\ 7 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 0 \\ 0 \\ 0 \end{smallmatrix}\right)$$

  has a non-zero solution (for instance $a_1 = 1$, $a_2 = 1$, $a_3 = -1$). This imples that E generates V since we can express the third generator by the two first.

- *The system of linear equations*

$$a_1 \cdot \left(\begin{smallmatrix} 1 \\ 2 \\ 3 \end{smallmatrix}\right) + a_2 \cdot \left(\begin{smallmatrix} 2 \\ 3 \\ 4 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 0 \\ 0 \\ 0 \end{smallmatrix}\right)$$

  only has $a_1 = a_2 = 0$ as solution. Thus E is $\mathbb{Q}$-linearly independent.

(c) The $\mathbb{R}$-vectore space

$$V = \{f : \mathbb{N} \to \mathbb{R} \mid \exists\, S \subseteq \mathbb{N} \text{ finite } \forall\, n \in \mathbb{N} \setminus S : f(n) = 0\}$$

has $\{e_n \mid n \in \mathbb{N}\}$ avec $e_n(m) = \delta_{n,m}$ (Kronecker delta: $\delta_{n,m} = \begin{cases} 1 & \text{si } n = m, \\ 0 & \text{if } n \neq m. \end{cases}$) as $\mathbb{R}$-basis. This is thus a basis with infinitely many elements.

(d) Similarly to the previous example, the $\mathbb{R}$-vector space

$$V = \{f : \mathbb{R} \to \mathbb{R} \mid \exists\, S \subseteq \mathbb{R} \text{ finite } \forall\, x \in \mathbb{R} \setminus S : f(x) = 0\}$$

has $\{e_x \mid x \in \mathbb{R}\}$ with $e_x(y) = \delta_{x,y}$ as $\mathbb{R}$-basis. This is thus a basis which is not countable.

Example 1.25. *How to compute a basis for a vector space generated by a finite set of vectors? (Same answer than almost always:) Solve a system of linear equations.*
Let V be a K-vector space generated by $\{e_1, e_2, \dots, e_m\}$ (assumed all non-zero). We proceed as follows:

- *Add e_1 to the basis.*

- *If e_2 is linearly independent from e_1 (i.e. e_2 is not a scalar multiple of e_1), add e_2 to the basis and in this case e_1, e_2 are linearly independent (otherwise, do nothing).*

- *If e_3 is linearly independent from the vectors chosen for the basis, add e_3 to the basis and in this case the elements chosen for the basis are linarly independent (otherwise, do nothing).*

- *If e_4 is linearly independent from the vectors already chosen for the basis, add e_4 to the basis and in this case all the chosen elements for the basis are linearly independent (otherwise, do nothing).*

- *etc. until the last vector.*

Here is a concrete example in $\mathbb{R}^4$:

$$e_1 = \begin{pmatrix} 1 \\ 1 \\ 0 \\ 2 \end{pmatrix}, e_2 = \begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \end{pmatrix}, e_3 = \begin{pmatrix} 4 \\ 1 \\ 3 \\ 2 \end{pmatrix}, e_4 = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 1 \end{pmatrix}.$$

- *Add e_1 to the basis.*

- *Add e_2 to the basis since e_2 is clearly not a multiple of e_1 (see, for example, the second coefficient), thus e_1 et e_2 are linearly independent.*

- *Are e_1, e_2, e_3 linearly independent?We consider the system of linear equations given by the matrix*
$$\begin{pmatrix} 1 & 1 & 4 \\ 1 & 0 & 1 \\ 0 & 1 & 3 \\ 2 & 0 & 2 \end{pmatrix}.$$
By transformations on the rows, we obtain the matrix
$$\begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 3 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}.$$
We obtain the solution $\begin{pmatrix} 1 \\ 3 \\ -1 \end{pmatrix}$. So, we do not add e_3 to the basis since e_3 is linearly dependent from e_1, e_2.

- *Are e_1, e_2, e_4 linearly independent? We consider the system of linear equations given by the matrix*
$$\begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \\ 2 & 0 & 1 \end{pmatrix}.$$
By transformations on the rows, we obtain the matrix
$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}.$$
The corresponding system has no non-zero solution. Therfore e_1, e_2, e_4 are linearly independent. This is the basis that we looked for.

Dimension

Corollary 1.26. *Let K be a field and V a K-vector space having a finite K-basis. Then, all the K-bases of V are finite and have the same cardinality.*

This corollary allows us to make a very important definition, that of the dimension of a vector space. The dimension measures the 'size' or the 'number of degrees of freedom' of a vector space.

Definition 1.27. *Let K be a field and V a K-vector space. If V has a finite K-basis of cardinality n, we say that V is of* dimension n. *If V has no finite K-basis, we say that V is of* infinite dimension.
Notation: $\dim_K(V)$.

Example 1.28. *(a) The dimension of the standard K-vector space K^n is equal to n.*

(b) The zero K-vector space $(\{0\}, +, \cdot, 0)$ is of de dimension 0 (and it is the only one).

(c) The $\mathbb{R}$-vector space $\mathcal{F}(\mathbb{N}, \mathbb{R})$ is of infinite dimension.

Lemma 1.29. *Let K be a field, V a K-vector space of dimension n and $W \leq V$ a subspace.*

(a) $\dim_K(W) \leq \dim_K(V)$.

(b) If $\dim_K(W) = \dim_K(V)$, then $W = V$.

The content of the following proposition is that any K-linearly independent set can be completed to become a K-basis.

Proposition 1.30 (Basisergänzungssatz)**.** *Let V be a K-vector space of dimension n, $E \subseteq V$ a finite set such that E generates V and $\{e_1, \dots, e_r\} \subset V$ a subset that is K-linearly independent.*
Then $r \leq n$ and there exist $e_{r+1}, e_{r+2}, \dots, e_n \in E$ such that $\{e_1, \dots, e_n\}$ is a K-basis of V.

The proposition 1.30 can be shown in an abstract manner or in a constructive manner. Assume that we have elements $e_1, \dots, e_r$ that are K-linearly independent. If $r = n$, these elements are a K-basis by Lemma 1.29 (b) and we are done. Assume therefore that $r < n$. We now run through the elements of E until we find $e \in E$ such that $e_1, \dots, e_r, e$ are K-linearly independent. Such an element e has to exist, otherwise the set E would be contained in the subspace generated by $e_1, \dots, e_r$, an could therefore not generate V. We call $e =: e_{r+1}$ and we have a K-linearly independent set of cardinality $r + 1$. It now suffices to continue this process until we arrive at a K-linearly independent set with n elements, which is automatically a K-basis.

Corollary 1.31. *Let V be a K-vector space of finite dimension n and let $W \leq V$ be a vector subspace. Then there exists a vector subspace $U \leq V$ such that $V = U \oplus V$. Moreover, we have the equality $\dim(V) = \dim(W) + \dim(U)$.*
We call U a complement *of W in V. Note that this complement is not unique in general.*

Proof. We choose a K-basis $w_1, \dots, w_r$ of W and we use the proposition 1.30 to obtain vectors $u_1, \dots, u_s \in V$ such that $w_1, \dots, w_r, u_1, \dots, u_s$ form a K-basis of V. Put $U = \langle u_1, \dots, u_s \rangle$. Clearly, we have $V = U + W$ and also $U \cap W = 0$, so $V = U \oplus W$. The assertion concerning dimensions follows. □

Proposition 1.32. *Let V be a K-vector space of finite dimension n. Let $B \subset V$ be a subset of cardinality n. Then, the following assertions are equivalent.*

(i) *B is a K-basis.*

(ii) *B is K-linearly independent.*

(iii) *B generates V.*

Proof. For the equivalence between (i) and (ii) it suffices to observe that a K-linearly independent set of cardinality n is necessarily maximal (thus a K-basis by Theorem 1.22), since if it was not maximal, there would be a maximal K-linearly independent set of cardinality strictly larger than n, thus a K-basis of cardinality different from n which is not possible by Corollary 1.26.
Similarly, for the equivalence between (i) and (iii) it suffices to observe that a set of cardinality n that generates V is necessarily minimal (thus a K-basis by Theorem 1.22), since if it was not minimal, there would be a minimal set of cardinality strictly smaller than n that generates V, thus a K-basis of cardinality different from n. □

Linear maps: homomorphisms of vector spaces

We start with the main idea :
The (homo-)morphisms are maps that respect all the structures.

Definition 1.33. *Let V, W be K-vector spaces. A map*

$$\varphi : V \to W$$

*is called K-*linear *or* (homo-)morphism of K-vector spaces *if*

$$\forall\, v_1, v_2 \in V : \varphi(v_1 +_V v_2) = \varphi(v_1) +_W \varphi(v_2)$$

and

$$\forall\, v \in V, \forall a \in K : \varphi(a \cdot_V v) = a \cdot_W \varphi(v).$$

A bijective homomorphism of K-vector spaces is called an isomorphism. *We often denote the isomorphisms by a tilda: $\varphi : V \xrightarrow{\sim} W$. If there exists an isomorphism $V \to W$, we often simply write $V \cong W$.*

Example 1.34. *(a) We start by the most important example. Let $n \in \mathbb{N}$.*

Let $M = \begin{pmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,n} \\ a_{2,1} & a_{2,2} & \cdots & a_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m,1} & a_{m,2} & \cdots & a_{m,n} \end{pmatrix}$ be a matrix with n columns, m rows and with coefficients in K (we denote the set of these matrices by $\mathrm{Mat}_{m\times n}(K)$; this is also a K-vector space). It defines the K-linear map

$$\varphi_M : K^n \to K^m, \quad v \mapsto Mv$$

where Mv is the usual product for matrices. Explicitely,

$$\varphi_M(v) = Mv = \begin{pmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,n} \\ a_{2,1} & a_{2,2} & \cdots & a_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m,1} & a_{m,2} & \cdots & a_{m,n} \end{pmatrix} \begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{pmatrix} = \begin{pmatrix} \sum_{i=1}^n a_{1,i}v_i \\ \sum_{i=1}^n a_{2,i}v_i \\ \vdots \\ \sum_{i=1}^n a_{m,i}v_i \end{pmatrix}.$$

The K-linearity reads as

$$\forall\, a \in K\, \forall\, v, w \in V : M \circ (a \cdot v + w) = a \cdot (M \circ v) + M \circ w.$$

This equality is very easy to verify (you should have seen it in your Linear Algebra 1 course).

(b) Let $a \in \mathbb{R}$. Then, $\varphi : \mathbb{R} \to \mathbb{R}$, $x \mapsto ax$ is $\mathbb{R}$-linear (this is the special case $n = m = 1$ of (a) if we look at the scalar a as a matrix (a)). On the other hand, if $0 \neq b \in \mathbb{R}$, then $\mathbb{R} \to \mathbb{R}$, $x \mapsto ax + b$ is not $\mathbb{R}$-linear!

(c) Let $n \in \mathbb{N}$. Then, the map $\varphi : \mathcal{F}(\mathbb{N}, \mathbb{R}) \to \mathbb{R}$, $f \mapsto f(n)$ is K-linear.

Definition 1.35. *Let V, W be K-vector spaces and $\varphi : V \to W$ a K-linear map. The* kernel of *φ is defined as*

$$\ker(\varphi) = \{v \in V \mid \varphi(v) = 0\}.$$

Proposition 1.36. *Let V, W be K-vector spaces and $\varphi : V \to W$ a K-linear map.*

(a) $\mathrm{Im}(\varphi)$ is a vector subspace of W.

(b) $\ker(\varphi)$ is a vector subspace of V.

(c) φ is surjective if and only if $\mathrm{Im}(\varphi) = W$.

(d) φ is injective if and only if $\ker(\varphi) = 0$.

(e) If φ is an isomorphism, its inverse is one too (in particular, its inverse is also K-linear).

Definition 1.37. *Let $M \in \mathrm{Mat}_{m \times n}(K)$ be a matrix. We call* rank of columns *of M the dimension of the vector subspace of K^m generates by the columns of M. We use the notation* $\mathrm{rk}(M)$.
Similarly, we define the rank of rows *of M the dimension of the vector subspace of K^n generated by the rows of M. More formally, it is the rank of M^{tr}, the transpose matrix.*

We will see towards the end of the course that for any matrix, the rank of columns is equal to the rank of rows. This explains why we did not mention the word “ columns” in the notation of the rank.
If $\varphi_M : K^n \to K^m$ is the K-linear map associated to M, then

$$\mathrm{rk}(M) = \dim(\mathrm{Im}(\varphi_M))$$

since the image of φ_M is precisely the vector space generated by the columns of M.

Corollary 1.38. *(a) Let $\varphi : V \to X$ be a K-linear map between two K-vector spaces. We assume that V has finite dimension. Then,*

$$\dim(V) = \dim(\ker(\varphi)) + \dim(\operatorname{Im}(\varphi)).$$

(b) Let $M \in \operatorname{Mat}_{m\times n}(K)$ be a matrix. Then, we have

$$n = \dim(\ker(M)) + \operatorname{rk}(M).$$

Proof. (a) Let $W = \ker(\varphi)$. We choose a complement $U \leq V$ such that $V = U \oplus W$ by Corollary 1.31. As $U \cap W = 0$, the map $\varphi|_U : U \to X$ is injective. Moreover, $\varphi(V) = \varphi(U+W) = \varphi(U)$ shows that $\operatorname{Im}(\varphi)$ is equal to $\varphi(U)$. Consequently, $\dim(\operatorname{Im}(\varphi)) = \dim(\varphi(U)) = \dim(U)$, thus the desired equality.
(b) follows directly from (a) by the above considerations. □

Part (b) is very useful for computing the kernel of a matrix: if we know the rank of M, we deduce the dimension of the kernel by the formula

$$\dim(\ker(M)) = n - \operatorname{rk}(M).$$

Gauß' algorithm in terms of matrices

We consider three types of matrices:

Definition 1.39. *For $0 \neq \lambda \in K$ and $1 \leq i, j \leq n$, $i \neq j$, we define the following matrices in $\operatorname{Mat}_{n\times n}(K)$, called* elementary matrices*:*

- *$P_{i,j}$ is equal to the identity id_n except that the i-th and the j-th rows are exchanged (or, equivalently, the i-th and the j-th column are exchanged): $P_{i,j} = \begin{pmatrix} 1 &&&&&&&& \\ & \ddots &&&&&&& \\ && 1 &&&&&& \\ &&& 0 &&& 1 && \\ &&&& 1 &&&& \\ &&&&& 1 &&& \\ &&& 1 &&& 0 && \\ &&&&&&& 1 & \\ &&&&&&&& \ddots \\ &&&&&&&&& 1 \end{pmatrix}$.*

- *$S_i(\lambda)$ is equal to the identity id_n except that the coefficient (i,i) on the diagonal is λ (instead of 1): $S_i(\lambda) = \begin{pmatrix} 1 &&&&& \\ & \ddots &&&& \\ && 1 &&& \\ &&& \lambda && \\ &&&& 1 & \\ &&&&& \ddots \\ &&&&&& 1 \end{pmatrix}$.*

- *$Q_{i,j}(\lambda)$ is equal to the identity id_n except that the coefficient (i,j) is λ (instead of 0): $Q_{i,j}(\lambda) = \begin{pmatrix} 1 &&& \\ & \ddots && \\ && \ddots & \lambda \\ &&& \ddots \\ &&&& 1 \end{pmatrix}$.*

The elementary matrices have a signification for the operations of matrices.

Lemma 1.40. *Let $\lambda \in K$, $i, j, n, m \in \mathbb{N}_{>0}$, $i \neq j$ and $M \in \mathrm{Mat}_{n\times m}(K)$.*

(a) $P_{i,j}M$ is the matrix obtained from M by exchanging the i-th and the j-th row.
$MP_{i,j}$ is the matrix obtained from M by exchanging the i-th and the j-th coulumn.

(b) $S_i(\lambda)M$ is the matrix obtained from M by multiplying the i-th row by λ.
$MS_i(\lambda)$ is the matrix obtained from M by multiplying the i-th column by λ.

(c) $Q_{i,j}(\lambda)M$ is the matrix obtained from M by adding λ times the j-th row to the i-th row.
$MQ_{i,j}(\lambda)$ is the matrix obtained from M by adding λ times the i-th column to the j-th column.

Proof. Easy computations. □

Proposition 1.41. *Let $M \in \mathrm{Mat}_{n\times m}(K)$ be a matrix and let $N \in \mathrm{Mat}_{n\times m}(K)$ be the matrix obtained from M by making operations on the rows (as in Gauß' algorithm).*

(a) Then there exist matrices $C_1, \dots, C_r$ (for some $r \in \mathbb{N}$) chosen among the matrices of Definition 1.39 such that $(C_1 \cdots C_r) \cdot M = N$.

(b) $\ker(M) = \ker(N)$ and thus Gauß' row reduction algorithm can be used in order to compute the kernel of a matrix.

Proof. (a) By Lemma 1.40 any operation on the rows can be done by left multiplication by one of the matrices of Definition 1.39.
(b) All the matrices of Definition 1.39 are invertible, thus do not change the kernel. □

Similarly to (b), any operation on the columns corresponds to right multiplication by one of the matrices of Definition 1.39. Thus, if N is a matrix obtained from a matrix M by doing operations on the columns, there exist matrices $C_1, \dots, C_r$ (for some $r \in \mathbb{N}$) chosen among the matrices of Definition 1.39 such that $M \cdot (C_1 \cdots C_r) = N$. Since the matrices C_i are invertible, we also have

$$\mathrm{im}(M) = \mathrm{im}(N),$$

and in particular the rank of M is equal to the rank of N.

Often we are interested in knowing a matrix C such that $CM = N$ where N is obtained from M by operations on the rows.
In order to obtain this, it suffices to observe that $C \cdot \mathrm{id} = C$, hence applying C is equivalent to doing operations on the corresponding rows of the matrix id. In the following example, we see how this is done in practice.

Example 1.42. *Let $M = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix}$. We write the augmented matrix and do the operations on the* *rows as always, but on the whole matrix.*

$$\begin{pmatrix}1&0&0&1&2&3\\0&1&0&4&5&6\\0&0&1&7&8&9\end{pmatrix} \mapsto \begin{pmatrix}1&0&0&1&2&3\\-4&1&0&0&-3&-6\\-7&0&1&0&-6&-12\end{pmatrix} \mapsto \begin{pmatrix}1&0&0&1&2&3\\-4&1&0&0&-3&-6\\1&-2&1&0&0&0\end{pmatrix}$$

$$\mapsto \begin{pmatrix}1&0&0&1&2&3\\4/3&-1/3&0&0&1&2\\1&-2&1&0&0&0\end{pmatrix} \mapsto \begin{pmatrix}-5/3&2/3&0&1&0&-1\\4/3&-1/3&0&0&1&2\\1&-2&1&0&0&0\end{pmatrix}$$

The left half of the final matrix is the matrix C looked for: $C = \begin{pmatrix}-5/3&2/3&0\\4/3&-1/3&0\\1&-2&1\end{pmatrix}$. The right half is the matrix obtained by the operations on the rows.
We know that we have the following equality (to convince ourselves, we can verify it by a small computation):

$$CM = \begin{pmatrix}-5/3&2/3&0\\4/3&-1/3&0\\1&-2&1\end{pmatrix}\begin{pmatrix}1&2&3\\4&5&6\\7&8&9\end{pmatrix} = \begin{pmatrix}1&0&-1\\0&1&2\\0&0&0\end{pmatrix}.$$

As application of the Gauß's algorithm written in terms of matrices, we obtain that any invertible square matrix M can be written as product of the matrices of Definition 1.39. Indeed, that we can transform M into identity by operations on the rows.

Matrices and representation of linear maps

In Example 1.34 (a) we have seen that matrices give rise to K-linear maps. It is very important and sometimes called *main theorem of linear algebra* that the inverse assertion is also true:
after choice of basis any K-linear map is given by a matrix.

Notation 1.43. *Let V be a K-vector space and $S = \{v_1, \dots, v_n\}$ a K-basis of V. We recall that $v = \sum_{i=1}^n b_i v_i$ with unique $b_1, \dots, b_n \in K$; these are the coordinates of v for the basis S. We use the following notation:*

$$v_S = \begin{pmatrix}b_1\\b_2\\\vdots\\b_n\end{pmatrix} \in K^n.$$

Example 1.44. *(a) Let $n \in \mathbb{N}$ and $e_1 = \begin{pmatrix}1\\0\\0\\\vdots\\0\end{pmatrix}, e_2 = \begin{pmatrix}0\\1\\0\\\vdots\\0\end{pmatrix}, \dots, e_n = \begin{pmatrix}0\\0\\0\\\vdots\\1\end{pmatrix}$.*

Thus $E = \{e_1, e_2, \dots, e_n\}$ is a canonical K-basis of K^n. Then, for all $v = \begin{pmatrix}a_1\\a_2\\a_3\\\vdots\\a_n\end{pmatrix} \in K^n$ we have $v_E = \begin{pmatrix}a_1\\a_2\\a_3\\\vdots\\a_n\end{pmatrix}$.

(b) Let $V = \mathbb{R}^2$ and $S = \{\left(\begin{smallmatrix}1\\1\end{smallmatrix}\right), \left(\begin{smallmatrix}1\\-1\end{smallmatrix}\right)\}$. It is a $\mathbb{R}$-basis of V (since the dimension is 2 and the two vectors are $\mathbb{R}$-linearly independent). Let $v = \left(\begin{smallmatrix}4\\2\end{smallmatrix}\right) \in V$. Then, $v = 3 \cdot \left(\begin{smallmatrix}1\\1\end{smallmatrix}\right) + \left(\begin{smallmatrix}1\\-1\end{smallmatrix}\right)$, so $v_S = \left(\begin{smallmatrix}3\\1\end{smallmatrix}\right)$.

The following proposition says that any K-vector space of dimension n is isomorphic to K^n.

Proposition 1.45. *Let V be a K-vector space of finite dimension n with K-basis $S = \{v_1, \dots, v_n\}$. Then, the map $\varphi = ()_S : V \to K^n$ given by $v \mapsto v_S$ is a K-isomorphism.*

Proof. Let $v, w \in V$ and $a \in K$. We write v and w in coordinates for the basis S: $v = \sum_{i=1}^n b_i v_i$ and $w = \sum_{i=1}^n c_i v_i$. Thus, we have $av + w = \sum_{i=1}^n (ab_i + c_i)v_i$. Written as vectors we thus find:

$$v_S = \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{pmatrix}, \quad w_S = \begin{pmatrix} c_1 \\ c_2 \\ \vdots \\ c_n \end{pmatrix} \text{ et } (av+w)_S = \begin{pmatrix} ab_1+c_1 \\ ab_2+c_2 \\ \vdots \\ ab_n+c_n \end{pmatrix},$$

thus the equality $(a \cdot v + w)_S = a \cdot v_S + w_S$. This shows that the map φ is K-linear. We show that it is bijective.

Injectivity: Let $v \in V$ be such that $v_S = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$, i.e. $v \in \ker(\varphi)$. This means that $v = \sum_{i=1}^n 0 \cdot v_i = 0$. The kernel of φ therefore only contains 0, so, φ is injective.

Surjectivity: Let $\begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix} \in K^n$. We set $v := \sum_{i=1}^n a_i \cdot v_i$. We have $\varphi(v) = \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix}$ and the surjectivity is proven.

□

Theorem 1.46. *Let V, W be two K-vector spaces of finite dimension n and m and $\varphi : V \to W$ a K-linear map. Let $S = \{v_1, \dots, v_n\}$ be a K-basis of V and $T = \{w_1, \dots, w_m\}$ a K-basis of W. For all $1 \le i \le n$, the vector $\varphi(v_i)$ belongs to W. We can thus express it as a K-linear combination of the vectors in the basis T, so:*

$$\varphi(v_i) = \sum_{j=1}^m a_{j,i} w_j.$$

We 'gather' the coefficients $a_{j,i}$ in a matrix:

$$M_{T,S}(\varphi) := \begin{pmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,n} \\ a_{2,1} & a_{2,2} & \cdots & a_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m,1} & a_{m,2} & \cdots & a_{m,n} \end{pmatrix} \in \mathrm{Mat}_{m \times n}(K).$$

Then, for all $v \in V$ we have

$$(\varphi(v))_T = M_{T,S}(\varphi) \circ v_S.$$

This means that the matrix product $M_{T,S}(\varphi) \circ v_S$ gives the coordinates in basis T of the image $\varphi(v)$. Then, the matrix $M_{T,S}(\varphi)$ describes the K-linear map φ in coordinates.

Observe that it is easy to write the matrix $M_{T,S}(\varphi)$: the i-th column of $M_{T,S}(\varphi)$ is $(\varphi(v_i))_T$.

Proof. We do a very simple matrix computation:

$$M_{T,S}(\varphi) \circ (v_i)_S = \begin{pmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,n} \\ a_{2,1} & a_{2,2} & \cdots & a_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m,1} & a_{m,2} & \cdots & a_{m,n} \end{pmatrix} \circ \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} = \begin{pmatrix} a_{1,i} \\ a_{2,i} \\ \vdots \\ a_{m,i} \end{pmatrix} = (\varphi(v_i))_T,$$

where the 1 is in the i-th row of the vector. We have thus obtained the result for the vectors v_i in the basis S.
The general assertion follows by linearity: Let $v = \sum_{i=1}^n b_i v_i$. Then we obtain

$$\begin{aligned} M_{T,S}(\varphi) \circ (\sum_{i=1}^n b_i v_i)_S &= \sum_{i=1}^n b_i \cdot \big(M_{T,S}(\varphi) \circ (v_i)_S\big) \\ &= \sum_{i=1}^n b_i \cdot (\varphi(v_i))_T = (\sum_{i=1}^n b_i \cdot \varphi(v_i))_T = (\varphi(\sum_{i=1}^n b_i \cdot v_i))_T = (\varphi(v))_T. \end{aligned}$$

This shows the theorem. □

Example 1.47. *$\mathbb{C}$ has a $\mathbb{R}$-basis $B = \{1, i\}$. Let $z = x + iy \in \mathbb{C}$ with $x, y \in \mathbb{R}$, thus $z_B = \left(\begin{smallmatrix} x \\ y \end{smallmatrix}\right)$. Let $a = r + is$ with $r, s \in \mathbb{R}$. The map*

$$\varphi : \mathbb{C} \to \mathbb{C}, \quad z \mapsto a \cdot z$$

is $\mathbb{R}$-linear. We describe $M_{B,B}(\varphi)$. The first column is $(a \cdot 1)_B = (r + is)_B = \left(\begin{smallmatrix} r \\ s \end{smallmatrix}\right)$, and the second column is $(a \cdot i)_B = (-s + ir)_B = \left(\begin{smallmatrix} -s \\ r \end{smallmatrix}\right)$, then $M_B(\varphi) = \left(\begin{smallmatrix} r & -s \\ s & r \end{smallmatrix}\right)$.

Definition 1.48. *Let us denote by $\mathrm{Hom}_K(V, W)$ the set of all maps $\varphi : V \to W$ which ate K-linear. In the special case $W = V$, a K-linear map $\varphi : V \to V$ is also called an* endomorphism *of V and we write*

$$\mathrm{End}_K(V) := \mathrm{Hom}_K(V, V).$$

Corollary 1.49. *Let K be a field, V, W two K-vector spaces of finite dimension n and m. Let $S = \{v_1, \ldots, v_n\}$ be a K-basis of V et $T = \{w_1, \ldots, w_m\}$ a K-basis of W.*
Then, the map

$$\mathrm{Hom}_K(V, W) \to \mathrm{Mat}_{m \times n}(K), \quad \varphi \mapsto M_{T,S}(\varphi)$$

is a bijection.

It is important to stress that the bases in the corollary are fixed! The same matrix can express different linear maps if we change the bases.

Proof. **Injectivity:** Suppose that $M_{T,S}(\varphi) = M_{T,S}(\psi)$ for $\varphi, \psi \in \mathrm{Hom}_K(V, W)$. Then for all $v \in V$, we have $(\varphi(v))_T = M_{T,S}(\varphi) \circ v_S = M_{T,S}(\psi) \circ v_S = (\psi(v))_T$. Since the writing in coordinates is unique, we find $\varphi(v) = \psi(v)$ for all $v \in V$, donc $\varphi = \psi$.

Surjectivity: Let $M \in \mathrm{Mat}_{m\times n}(K)$ be a matrix. We define $\varphi \in \mathrm{Hom}_K(V,W)$ by

$$(\varphi(v))_T = M \circ v_S$$

for $v \in V$. It is clear that φ is K-linear. Moreover, we have

$$M_{T,S}(\varphi) \circ v_S = (\varphi(v))_T = M \circ v_S$$

for all $v \in V$. Taking $v = v_i$ such that $(v_i)_S$ is the vector of which the i-th coordinate is 1 and the rest is 0, we obtain that the i-th columns of $M_{T,S}(\varphi)$ and M are the same. This shows that $M = M_{T,S}(\varphi)$.

□

Definition-Lemma 1.50. *Let V be a K-vector space of finite dimension n. Let S_1, S_2 be two K-bases of V. We set*

$$C_{S_2,S_1} := M_{S_2,S_1}(\mathrm{id}_V)$$

and we call it the basis change matrix.

(a) C_{S_2,S_1} is a matrix with n columns and n rows.

(b) For all $v \in V$:

$$v_{S_2} = C_{S_2,S_1} \circ v_{S_1}.$$

In words: the multiplication of the basis change matrices by the vector v expressed in coordinates for the basis S_1, gives the vector v expressed in coordinates for the basis S_2.

(c) C_{S_2,S_1} is invertible with inverse C_{S_1,S_2}.

It is easy to write the matrix C_{S_2,S_1}: its j-th column consists of the coordinates in basis S_2 of the j-th vector of basis S_1.

Proof. (a) This is clear.
(b) $C_{S_2,S_1} \circ v_{S_1} = M_{S_2,S_1}(\mathrm{id}_V) \circ v_{S_1} = (\mathrm{id}_V(v))_{S_2} = v_{S_2}$.
(c) $C_{S_1,S_2} \circ C_{S_2,S_1} \circ v_{S_1} = C_{S_1,S_2} \circ v_{S_2} = v_{S_1}$ for all $v \in V$. This shows that $C_{S_1,S_2} \circ C_{S_2,S_1}$ is identity. The same reasonning holds with the roles of S_1 and S_2 inverted. □

Proposition 1.51. *Let V, W be K-vector spaces of finite dimension, let S_1, S_2 be two K-bases of V, let T_1, T_2 be two K-bases of W, and let $\varphi \in \mathrm{Hom}_K(V,W)$. Then,*

$$M_{T_2,S_2}(\varphi) = C_{T_2,T_1} \circ M_{T_1,S_1}(\varphi) \circ C_{S_1,S_2}.$$

Proof. $C_{T_2,T_1} \circ M_{T_1,S_1}(\varphi) \circ C_{S_1,S_2} \circ v_{S_2} = C_{T_2,T_1} \circ M_{T_1,S_1}(\varphi) v_{S_1} = C_{T_2,T_1} \circ (\varphi(v))_{T_1} = (\varphi(v))_{T_2}$.
□

Proposition 1.52. *Let V, W, Z be K-vector spaces of finite dimension, let S be a K-basis of V, T a K-basis of W and U a K-basis of Z. Let $\varphi \in \mathrm{Hom}_K(V,W)$ and $\psi \in \mathrm{Hom}_K(W,Z)$. Then,*

$$M_{U,T}(\psi) \circ M_{T,S}(\varphi) = M_{U,S}(\psi \circ \varphi).$$

In words: the matrix product corresponds to the composition of maps.

Proof. $M_{U,T}(\psi) \circ M_{T,S}(\varphi) \circ v_S = M_{U,T}(\psi) \circ (\varphi(v))_T = (\psi(\phi(v)))_U = M_{U,T}(\psi \circ \varphi) \circ v_S$. □

Appendix: existence of bases

For lack of time, this section will neither be taught, neither be examined.
In the lecture course "Structures mathématiques" we have introduced the sets from an intuitive and non-rigurous point of view. A strict treatment can only take place in a logic course at a more advanced stage (such a course is not offered at the UL for the moment – you can consult books for more details).
In set theory, there is an important axiom: the 'axiom of choix'.[1] In set theory one shows 'Zorn's Lemma' which says that the axiom of choice is equivalent to the following assertion.

Axiom 1.53 (Zorn's Lemma)**.** *Let S be a non-empty set and $\leq$ a partial order on S.*[2] *We make the following hypothesis: Any subset $T \subseteq S$ which is totally ordered*[3] *has an upper bound.*[4]
Then, S has a maximal element.[5]

To show how to apply Zorn's Lemma, we prove that ant vector space has a basis. If you have seen this assertion in your Linear Algebra 1 lecture course, then it was for finite-dimensional vector spaces because the general case is in fact equivalent to the axiom of choice (an thus to Zorn's Lemma).

Proposition 1.54. *Let K be a field and $V \neq \{0\}$ a K-vector space. Then, V has a K-basis.*

Proof. We recall some notions of linear algebra. A finite subset $G \subseteq V$ is called *K-linearly independent* if the only linear combination $0 = \sum_{g \in G} a_g g$ with $a_g \in K$ is that where $a_g = 0$ for all $g \in G$. More generally, a non-necessarily finite subset $G \subseteq V$ is called *K-linearly independent* if any finite subset $H \subseteq G$ is K-linearly independent. A subset $G \subseteq V$ is called a *K-basis* if it is K-linearly independet and generates V.[6]
We want to use Zorn's Lemma 1.53. Let

$$S := \{G \subseteq V \text{ subset} \mid G \text{ is } K\text{-linearly independent } \}.$$

The set S is non-empty since $G = \{v\}$ is K-linearly independent for all $0 \neq v \in V$. The inclusion of sets '$\subseteq$' defines an order relation on S (it is obvious – see Algebra 1).
We verify that the hypothesis of Zorn's Lemma is satisfied: Let $T \subseteq S$ be a totally ordered subset. We have to produce an upper bound $E \in S$ for T. We set $E := \bigcup_{G \in T} G$. It is clear that $G \subseteq E$ for all $G \in T$. One has to show that $E \in S$, thus that E is K-linearly independent. Let $H \subseteq E$ be a subset of cardinality n. We show by induction on n that there exists $G \in T$ such that $H \subseteq G$. The assertion is clear for $n = 1$. Assume it proven for $n - 1$ and write $H = H' \sqcup \{h\}$. The exist $G', G \in T$ such

[1] Axiom of choice: Let X be a set of which the elements are non-empty sets. Then there exists a function f defined on X which to any $M \in X$ associates an element of M. Such a function is called "function of choice".

[2] e recall that by definition the three following points are satisfied:

- $s \leq s$ for all $s \in S$.
- If $s \leq t$ and $t \leq s$ for $s, t \in S$, then $s = t$.
- If $s \leq t$ and $t \leq u$ for $s, t, u \in S$, then $s \leq u$.

[3] T is totally ordered if T is ordered and for all pair $s, t \in T$ we have $s \leq t$ or $t \leq s$.

[4] $g \in S$ is an upper bound for T if $t \leq g$ for all $t \in T$.

[5] $m \in S$ is maximal if for all $s \in S$ such that $m \leq s$ we have $m = s$.

[6] i.e.: any element $v \in V$ writes as $v = \sum_{i=1}^{n} a_i g_i$ with $n \in \mathbb{N}$, $a_1, \ldots, a_n \in K$ et $g_1, \ldots, g_n \in G$.

that $H' \subseteq G'$ (by induction hypothesis because the cardinality of H' is $n-1$) and $h \in G$ (by the case $n = 1$). By the fact that T is totally ordered, we have $G \subseteq G'$ or $G' \subseteq G$. In both cases we obtain that H is a subset of G or of G'. Since H is a finite subset of a set which is K-linearly independent, H is too. Thus, E is K-linearly independent.

Zorn's Lemma gives us a maximal element $B \in S$. We show that B is a K-basis of V. As element of S, B is K-linearly independent. One has to show that B generates V. Suppose that this is not the case and let us take $v \in V$ which cannot be written as a K-linear combination of the elements in B. Then the set $G := B \cup \{v\}$ is also K-linearly independent, since any K-linear combination $0 = av + \sum_{i=1}^{n} a_i b_i$ with $n \in \mathbb{N}$, $a, a_1, \dots, a_n \in K$ and $b_1, \dots, b_n \in B$ with $a \neq 0$ would lead to the contradiction $v = \sum_{i=1}^{n} \frac{-a_i}{a} b_i$ (note that $a = 0$ corresponds to a K-linear combination in B which is K-linearly independent). But, $B \subsetneq G \in S$ contradicts maximality of B. □

2 Recalls: Determinants

Goals:

- Master the definition and the fundamental properties of the determinants;
- be able to compute determinants;
- know examples and be able to prove simple properties.

Définition et premières propriétés

The determinants have been introduced the previous semester. Here we recall them form another viewpoint: we start from the computation rules. Actually, our first proposition can be used as a definition; it is Weierstraß' axiomatic (see the book of Fischer).

In this section we allow that K is a commutative ring (but you can still take $K = \mathbb{R}$ or $K = \mathbb{C}$ without loss of information).

If $M = \begin{pmatrix} m_{1,1} & m_{1,2} & \cdots & m_{1,n} \\ m_{2,1} & m_{2,2} & \cdots & m_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ m_{n,1} & m_{n,2} & \cdots & m_{n,n} \end{pmatrix}$ is a matrix, we denote by $m_i = \begin{pmatrix} m_{i,1} & m_{i,2} & \cdots & m_{i,n} \end{pmatrix}$ its i-th row, i.e. $M = \begin{pmatrix} m_1 \\ m_2 \\ \vdots \\ m_n \end{pmatrix}$.

Proposition 2.1. *Let $n \in \mathbb{N}_{>0}$. The* determinant *is a map*

$$\det : \mathrm{Mat}_{n\times n}(K) \to K, \quad M \mapsto \det(M)$$

such that

D1 $\det$ *is K*-linear *in each row, that is, for all $1 \le i \le n$, if $m_i = r + \lambda s$ with $\lambda \in K$, $r = \begin{pmatrix} r_1 & r_2 & \cdots & r_n \end{pmatrix}$ and $s = \begin{pmatrix} s_1 & s_2 & \cdots & s_n \end{pmatrix}$, then*

$$\det \begin{pmatrix} m_1 \\ \vdots \\ m_{i-1} \\ m_i \\ m_{i+1} \\ \vdots \\ m_n \end{pmatrix} = \det \begin{pmatrix} m_1 \\ \vdots \\ m_{i-1} \\ r+\lambda s \\ m_{i+1} \\ \vdots \\ m_n \end{pmatrix} = \det \begin{pmatrix} m_1 \\ \vdots \\ m_{i-1} \\ r \\ m_{i+1} \\ \vdots \\ m_n \end{pmatrix} + \lambda \cdot \det \begin{pmatrix} m_1 \\ \vdots \\ m_{i-1} \\ s \\ m_{i+1} \\ \vdots \\ m_n \end{pmatrix}.$$

D2 $\det$ *is* alternating*, that is, if two of the rows of M are equal, then* $\det(M) = 0$.

D3 $\det$ *is* normalized*, that is,* $\det(\mathrm{id}_n) = 1$ *where* id_n *is the identity.*

Proof. This has been proven in the course of linear algebra in the previous semester. □

We often use the notation

$$\begin{vmatrix} m_{1,1} & m_{1,2} & \cdots & m_{1,n} \\ m_{2,1} & m_{2,2} & \cdots & m_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ m_{n,1} & m_{n,2} & \cdots & m_{n,n} \end{vmatrix} := \det \begin{pmatrix} m_{1,1} & m_{1,2} & \cdots & m_{1,n} \\ m_{2,1} & m_{2,2} & \cdots & m_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ m_{n,1} & m_{n,2} & \cdots & m_{n,n} \end{pmatrix}.$$

Proposition 2.2. *The following properties are satisfied.*

D4 *For all $\lambda \in K$, we have* $\det(\lambda \cdot M) = \lambda^n \det(M)$.

D5 *If a row is equal to* 0*, then* $\det(M) = 0$.

D6 *If $\tilde{M}$ is obtained from M by swapping two rows, then* $\det(M) = -\det(\tilde{M})$.

D7 *Let $\lambda \in A$ and $i \neq j$. If $\tilde{M}$ is obtained from M by adding λ times the j-th row to the i-th row, then* $\det(M) = \det(\tilde{M})$.

Proof. **D4** This follows from the linearity (D1).
D5 This follows from the linearity (D1).

D6 Let us say that the i-th and the j-the row are swapped. Thus $M = \begin{pmatrix} m_1 \\ \vdots \\ m_i \\ \vdots \\ m_j \\ \vdots \\ m_n \end{pmatrix}$ and $\tilde{M} = \begin{pmatrix} m_1 \\ \vdots \\ m_j \\ \vdots \\ m_i \\ \vdots \\ m_n \end{pmatrix}$.

$$\begin{aligned} \det(M) + \det(\tilde{M}) &= \det \begin{pmatrix} m_1 \\ \vdots \\ m_i \\ \vdots \\ m_j \\ \vdots \\ m_n \end{pmatrix} + \det \begin{pmatrix} m_1 \\ \vdots \\ m_j \\ \vdots \\ m_i \\ \vdots \\ m_n \end{pmatrix} \\ &\overset{\text{D2}}{=} \det \begin{pmatrix} m_1 \\ \vdots \\ m_j \\ \vdots \\ m_j \\ \vdots \\ m_n \end{pmatrix} + \det \begin{pmatrix} m_1 \\ \vdots \\ m_i \\ \vdots \\ m_j \\ \vdots \\ m_n \end{pmatrix} + \det \begin{pmatrix} m_1 \\ \vdots \\ m_j \\ \vdots \\ m_i \\ \vdots \\ m_n \end{pmatrix} + \det \begin{pmatrix} m_1 \\ \vdots \\ m_i \\ \vdots \\ m_i \\ \vdots \\ m_n \end{pmatrix} \\ &\overset{\text{D1}}{=} \det \begin{pmatrix} m_1 \\ \vdots \\ m_i{+}m_j \\ \vdots \\ m_j \\ \vdots \\ m_n \end{pmatrix} + \det \begin{pmatrix} m_1 \\ \vdots \\ m_i{+}m_j \\ \vdots \\ m_i \\ \vdots \\ m_n \end{pmatrix} = \det \begin{pmatrix} m_1 \\ \vdots \\ m_i{+}m_j \\ \vdots \\ m_i{+}m_j \\ \vdots \\ m_n \end{pmatrix} \overset{\text{D2}}{=} 0. \end{aligned}$$

D7 We have

$$\det(\tilde{M}) = \det\begin{pmatrix} m_1 \\ \vdots \\ m_i+\lambda m_j \\ \vdots \\ m_j \\ \vdots \\ m_n \end{pmatrix} \overset{\text{D1}}{=} \det\begin{pmatrix} m_1 \\ \vdots \\ m_i \\ \vdots \\ m_j \\ \vdots \\ m_n \end{pmatrix} + \lambda \cdot \det\begin{pmatrix} m_1 \\ \vdots \\ m_j \\ \vdots \\ m_j \\ \vdots \\ m_n \end{pmatrix} \overset{\text{D2}}{=} \det(M) + \lambda \cdot 0 = \det(M).$$

□

Proposition 2.3. *The following properties are satisfied.*

D8 *If M is of (upper) triangular form*

$$\begin{pmatrix} \lambda_1 & m_{1,2} & m_{1,3} & \cdots & m_{1,n} \\ 0 & \lambda_2 & m_{2,3} & \cdots & m_{2,n} \\ 0 & 0 & \lambda_3 & \cdots & m_{3,n} \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & \lambda_n \end{pmatrix},$$

then $\det(M) = \prod_{i=1}^{n} \lambda_i$.

D9 *If M is a bloc matrix $\left(\begin{smallmatrix} A & B \\ 0 & C \end{smallmatrix}\right)$ with square matrices A and C, then* $\det(M) = \det(A) \cdot \det(C)$.

Proof. Left to the reader. □

Leibniz' Formula

Lemma 2.4. *For $1 \leq i \leq n$, let $e_i := \left(\begin{smallmatrix} 0 & \cdots & 0 & 1 & 0 & \cdots & 0 \end{smallmatrix}\right)$ where the 1 is at the i-th position. Let $\sigma : \{1, \dots, n\} \to \{1, \dots, n\}$ be a map. Let $M = \begin{pmatrix} e_{\sigma(1)} \\ e_{\sigma(2)} \\ \vdots \\ e_{\sigma(n)} \end{pmatrix}$. Then*

$$\det(M) = \begin{cases} 0 & \text{if } \sigma \text{ is not bijective,} \\ \operatorname{sgn}(\sigma) & \text{if } \sigma \text{ is bijective } (\sigma \in S_n). \end{cases}$$

Proof. If σ is not bijective, then the matrix has twice the same row, thus the determinant is 0. If σ is bijective, then σ is a product of transpositions $\sigma = \tau_r \circ \cdots \circ \tau_1$ (see Algebra 1). Thus $\operatorname{sgn}(\sigma) = (-1)^r$. Let us start by $\sigma = \mathrm{id}$. In this case the determinant is 1 and thus equal to $\operatorname{sgn}(\sigma)$. We continue by induction and we suppose thus (induction hypothesis) that the result is true for $r - 1$ transpositions (with $r \geq 1$). Let M' be the matrix that corresponds to $\sigma' = \tau_{r-1} \circ \cdots \circ \tau_1$; its determinant is $(-1)^{r-1} = \operatorname{sgn}(\sigma')$ by induction hypothesis. The matrix M is obtained from M' by swapping two rows, thus $\det(M) = -\det(M') = -(-1)^{r-1} = (-1)^r$. □

Proposition 2.5 (Leibniz' Formula)**.** *Let $M = \begin{pmatrix} m_{1,1} & m_{1,2} & \cdots & m_{1,n} \\ m_{2,1} & m_{2,2} & \cdots & m_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ m_{n,1} & m_{n,2} & \cdots & m_{n,n} \end{pmatrix} \in \mathrm{Mat}_{n \times n}(K)$. Then,*

$$\det(M) = \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) \cdot m_{1,\sigma(1)} \cdot m_{2,\sigma(2)} \cdot \ldots \cdot m_{n,\sigma(n)}.$$

Proof. The linearity of rows (D1) gives us

$$\begin{aligned}\det(M) &= \sum_{i_1=1}^{n} m_{1,i_1} \begin{vmatrix} e_{i_1} \\ m_2 \\ m_3 \\ \vdots \\ m_n \end{vmatrix} = \sum_{i_1=1}^{n} \sum_{i_2=1}^{n} m_{1,i_1} m_{2,i_2} \begin{vmatrix} e_{i_1} \\ e_{i_2} \\ m_3 \\ \vdots \\ m_n \end{vmatrix} \\ &= \cdots = \sum_{i_1=1}^{n} \sum_{i_2=1}^{n} \cdots \sum_{i_n=1}^{n} m_{1,i_1} m_{2,i_2} \cdots m_{n,i_n} \begin{vmatrix} e_{i_1} \\ e_{i_2} \\ e_{i_3} \\ \vdots \\ e_{i_n} \end{vmatrix} \\ &= \sum_{\sigma \in S_n} m_{1,\sigma(1)} m_{2,\sigma(2)} \cdots m_{n,\sigma(n)} \cdot \operatorname{sgn}(\sigma),\end{aligned}$$

where the last equality results from Lemma 2.4. Note that the determinant of the matrix $\begin{pmatrix} e_{i_1} \\ e_{i_2} \\ e_{i_3} \\ \vdots \\ e_{i_n} \end{pmatrix}$ is non-zero only if the i_j's are all different; this allows us to identify it with the permutation $\sigma(j) = i_j$. That the determinant is unique is clear because it is a function of the coefficients of the matrix. □

Corollary 2.6. *Let* $M \in \mathrm{Mat}_{n\times n}(K)$. *We denote by* M^{tr} *the transposed matrix. Then,* $\det(M) = \det(M^{\mathrm{tr}})$.

Proof. We use Leibniz' Formula 2.5. Note first that $\operatorname{sgn}(\sigma) = \operatorname{sgn}(\sigma^{-1})$ for all σ in S_n since sgn is a homomorphism of groups, $1^{-1} = 1$ et $(-1)^{-1} = -1$. Write now

$$\begin{aligned} m_{1,\sigma(1)} m_{2,\sigma(2)} \cdots m_{n,\sigma(n)} &= m_{\sigma^{-1}(\sigma(1)),\sigma(1)} m_{\sigma^{-1}(\sigma(2)),\sigma(2)} \cdots m_{\sigma^{-1}(\sigma(n)),\sigma(n)} \\ &= m_{\sigma^{-1}(1),1} m_{\sigma^{-1}(2),2} \cdots m_{\sigma^{-1}(n),n},\end{aligned}$$

where for the last equality we have only written the product in another order since the elements $\sigma(1), \sigma(2), \ldots, \sigma(n)$ run through $1, 2, \ldots, n$ (only in another order).
We thus have

$$\begin{aligned}\det(M) &= \sum_{\sigma\in S_n} \operatorname{sgn}(\sigma) m_{1,\sigma(1)} m_{2,\sigma(2)} \cdots m_{n,\sigma(n)} \\ &= \sum_{\sigma\in S_n} \operatorname{sgn}(\sigma^{-1}) m_{\sigma^{-1}(1),1} m_{\sigma^{-1}(2),2} \cdots m_{\sigma^{-1}(n),n} \\ &= \sum_{\sigma\in S_n} \operatorname{sgn}(\sigma^{-1}) m^{\mathrm{tr}}_{1,\sigma^{-1}(1)} m^{\mathrm{tr}}_{2,\sigma^{-1}(2)} \cdots m^{\mathrm{tr}}_{n,\sigma^{-1}(n)} \\ &= \sum_{\sigma\in S_n} \operatorname{sgn}(\sigma) m^{\mathrm{tr}}_{1,\sigma(1)} m^{\mathrm{tr}}_{2,\sigma(2)} \cdots m^{\mathrm{tr}}_{n,\sigma(n)} \\ &= \det(M^{\mathrm{tr}}),\end{aligned}$$

where we have used the bijection $S_n \to S_n$ given by $\sigma \mapsto \sigma^{-1}$; it is thus makes no change if the sum runs through $\sigma \in S_n$ or through the inverses. □

Corollary 2.7. *The rules* **D1** *to* **D9** *are also true for the columns instead of the rows.*

Proof. By taking the transpose of a matrix, the rows become columns, but by Corollary 2.6, the determinant does not change. □

Laplace expansion

Definition 2.8. *Let* $n \in \mathbb{N}_{>0}$ *and* $M = \begin{pmatrix} m_{1,1} & m_{1,2} & \cdots & m_{1,n} \\ m_{2,1} & m_{2,2} & \cdots & m_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ m_{n,1} & m_{n,2} & \cdots & m_{n,n} \end{pmatrix} \in \mathrm{Mat}_{n\times n}(K)$. *For* $1 \le i, j \le n$ *we define the matrices*

$$M_{i,j} = \begin{pmatrix} m_{1,1} & \cdots & m_{1,j-1} & 0 & m_{1,j+1} & \cdots & m_{1,n} \\ \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ m_{i-1,1} & \cdots & m_{i-1,j-1} & 0 & m_{i-1,j+1} & \cdots & m_{i-1,n} \\ 0 & \cdots & 0 & 1 & 0 & \cdots & 0 \\ m_{i+1,1} & \cdots & m_{i+1,j-1} & 0 & m_{i+1,j+1} & \cdots & m_{i+1,n} \\ \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ m_{n,1} & \cdots & m_{n,j-1} & 0 & m_{n,j+1} & \cdots & m_{n,n} \end{pmatrix} \in \mathrm{Mat}_{n\times n}(A)$$

and

$$M'_{i,j} = \begin{pmatrix} m_{1,1} & \cdots & m_{1,j-1} & m_{1,j+1} & \cdots & m_{1,n} \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ m_{i-1,1} & \cdots & m_{i-1,j-1} & m_{i-1,j+1} & \cdots & m_{i-1,n} \\ m_{i+1,1} & \cdots & m_{i+1,j-1} & m_{i+1,j+1} & \cdots & m_{i+1,n} \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ m_{n,1} & \cdots & m_{n,j-1} & m_{n,j+1} & \cdots & m_{n,n} \end{pmatrix} \in \mathrm{Mat}_{n-1\times n-1}(A).$$

Moreover, let $\tilde{M}_{i,j}$ *be the matrix obtained from* M *by replacing the* j*-th column by* $\begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$*, where the* 1 *is at the* i*-th position.*
The determinants $\det(M'_{i,j})$ *are called the* minors *of* M.

Lemma 2.9. *Let* $n \in \mathbb{N}_{>0}$ *and* $M \in \mathrm{Mat}_{n\times n}(K)$. *For all* $1 \le i, j \le n$*, we have*

(a) $\det(M_{i,j}) = (-1)^{i+j} \cdot \det(M'_{i,j})$*,*

(b) $\det(\tilde{M}_{i,j}) = \det(M_{i,j})$.

Proof. (a) By swapping i rows, the row with the zeros is the first one. By swapping j columns, we obtain the matrix

$$\begin{pmatrix} 1 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ 0 & m_{1,1} & \cdots & m_{1,j-1} & m_{1,j+1} & \cdots & m_{1,n} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & m_{i-1,1} & \cdots & m_{i-1,j-1} & m_{i-1,j+1} & \cdots & m_{i-1,n} \\ 0 & m_{i+1,1} & \cdots & m_{i+1,j-1} & m_{i+1,j+1} & \cdots & m_{i+1,n} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & m_{n,1} & \cdots & m_{n,j-1} & m_{n,j+1} & \cdots & m_{n,n} \end{pmatrix} \in \mathrm{Mat}_{n\times n}(A)$$

of which the determinant is $\det(M'_{i,j})$ (because of **D9**), which proves the result.
(b) Adding $-m_{i,k}$ times the j-th column to the k-th column of $\tilde{M}_{i,j}$ makes the coefficient (i,k) equal to 0 for $k \neq i$ without changing the determinant (Corollary 2.7). □

Proposition 2.10 (Laplace expansion for the rows)**.** *Let* $n \in \mathbb{N}_{>0}$. *For all* $1 \le i \le n$*, we have the equality*

$$\det(M) = \sum_{j=1}^{n} (-1)^{i+j} m_{i,j} \det(M'_{i,j})$$

Proof. By the axiom **D2** (linearity in the rows), we have

$$\det(M) = \sum_{j=1}^{n} m_{i,j} \begin{vmatrix} m_1 \\ \vdots \\ m_{i-1} \\ e_i \\ m_{i+1} \\ \vdots \\ m_n \end{vmatrix} = \sum_{j=1}^{n} m_{i,j} \det(M_{i,j}) = \sum_{j=1}^{n} (-1)^{i+j} m_{i,j} \det(M'_{i,j}).$$

□

Corollary 2.11 (Laplace expansion for the columns). *For all $n \in \mathbb{N}_{>0}$ and all $1 \leq j \leq n$, we have the formula*

$$\det(M) := \sum_{i=1}^{n} (-1)^{i+j} m_{i,j} \det(M'_{i,j}).$$

Proof. It suffices to apply Proposition 2.10 to the transposed matrix and to remember (Corollary 2.6) that the determinant of the transposed matrix is the same. □

Note that the formulas of Laplace can be written as

$$\det(M) = \sum_{j=1}^{n} m_{i,j} \det(M_{i,j}) = \sum_{i=1}^{n} m_{i,j} \det(M_{i,j}).$$

Adjoint matrices

Definition 2.12. *The* adjoint matrix $\mathrm{adj}(M) = M^{\#} = (m^{\#}_{i,j})$ *of the matrix $M \in \mathrm{Mat}_{n\times n}(A)$ is defined by* $m^{\#}_{i,j} := \det(M_{j,i}) = (-1)^{i+j} \det(M'_{j,i})$.

Proposition 2.13. *For all matrix $M \in \mathrm{Mat}_{n\times n}(K)$, we have the equality*

$$M^{\#} \cdot M = M \cdot M^{\#} = \det(M) \cdot \mathrm{id}_n.$$

Proof. Let $N = (n_{i,j}) := M \cdot M^{\#}$. We compute $n_{i,j}$:

$$n_{i,j} = \sum_{k=1}^{n} m^{\#}_{i,k} m_{k,j} = \sum_{k=1}^{n} \det(M_{k,i}) m_{k,j}.$$

If $i = j$, we find $n_{i,i} = \det(M)$ by Laplace's formula. But we don't need to use this formula and we continue in generality by using $\det(M_{k,i}) = \det(\tilde{M}_{k,i})$ by Lemma 2.9 (b). The linearity in the i-th column shows that $\sum_{k=1}^{n} \det(\tilde{M}_{k,i}) m_{k,j}$ is the determinant of the matrix of which the i-th column is replaced by the j-th column. If $i = j$, this matrix is M, so $m_{i,i} = \det(M)$. If $i \neq j$, this determinant (and thus $n_{i,j}$) is 0 because two of the columns are equal.
The proof for $M^{\#} \cdot M$ is similar. □

Corollary 2.14. *Let $M \in \mathrm{Mat}_{n\times n}(K)$.*

(a) If $\det(M)$ is invertible in K (for K a field this means $\det(M) \neq 0$), then M is invertible and the inverse matrix M^{-1} is equal to $\frac{1}{\det(M)} M^{\#}$.

(b) If M is invertible, then $M^{-1}\det(M) = M^{\#}$.

Proof. Proposition 2.13. □

We finish this recall by the following fundamental result.

Proposition 2.15. *Let $M, N \in \mathrm{Mat}_{n\times n}(K)$.*

(a) $\det(M \cdot N) = \det(M) \cdot \det(N)$.

(b) The following statements are equivalent:

  (i) M is invertible;

  (ii) $\det(M)$ is invertible.

In this case: $\det(M^{-1}) = \frac{1}{\det(M)}$.

Proof. (a) was proved in the lecture Linear Algebra 1.
(b) is obvious because of Proposition 2.13. □

3 Eigenvalues

Goals:

- Master the definition and fundamental properties of eigenvalues and eigenvectors;
- be able to compute eigenspaces;
- know examples and be able to prove simple properties.

Example 3.1. *(a) Consider $M = \left(\begin{smallmatrix} 3 & 0 \\ 0 & 2 \end{smallmatrix}\right) \in \mathrm{Mat}_{2\times 2}(\mathbb{R})$. We have:*

- $\left(\begin{smallmatrix} 3 & 0 \\ 0 & 2 \end{smallmatrix}\right)\left(\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right) = 3 \cdot \left(\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right)$ *and*
- $\left(\begin{smallmatrix} 3 & 0 \\ 0 & 2 \end{smallmatrix}\right)\left(\begin{smallmatrix} 0 \\ 1 \end{smallmatrix}\right) = 2 \cdot \left(\begin{smallmatrix} 0 \\ 1 \end{smallmatrix}\right)$.

(b) Consider $M = \left(\begin{smallmatrix} 3 & 1 \\ 0 & 2 \end{smallmatrix}\right) \in \mathrm{Mat}_{2\times 2}(\mathbb{R})$. We have:

- $\left(\begin{smallmatrix} 3 & 1 \\ 0 & 2 \end{smallmatrix}\right)\left(\begin{smallmatrix} a \\ 0 \end{smallmatrix}\right) = 3 \cdot \left(\begin{smallmatrix} a \\ 0 \end{smallmatrix}\right)$ *for all $a \in \mathbb{R}$.*
- $\left(\begin{smallmatrix} 3 & 1 \\ 0 & 2 \end{smallmatrix}\right)\left(\begin{smallmatrix} a \\ b \end{smallmatrix}\right) = \left(\begin{smallmatrix} 3a+b \\ 2b \end{smallmatrix}\right) = 2 \cdot \left(\begin{smallmatrix} a \\ b \end{smallmatrix}\right) \Leftrightarrow a = -b$. *Thus for all $a \in \mathbb{R}$, we have* $\left(\begin{smallmatrix} 3 & 1 \\ 0 & 2 \end{smallmatrix}\right)\left(\begin{smallmatrix} a \\ -a \end{smallmatrix}\right) = 2 \cdot \left(\begin{smallmatrix} a \\ -a \end{smallmatrix}\right)$.

(c) Consider $M = \left(\begin{smallmatrix} 5 & 1 \\ -4 & 10 \end{smallmatrix}\right) \in \mathrm{Mat}_{2\times 2}(\mathbb{R})$. We have:

- $\left(\begin{smallmatrix} 5 & 1 \\ -4 & 10 \end{smallmatrix}\right)\left(\begin{smallmatrix} 1 \\ 4 \end{smallmatrix}\right) = 9\left(\begin{smallmatrix} 1 \\ 4 \end{smallmatrix}\right)$ *and*
- $\left(\begin{smallmatrix} 5 & 1 \\ -4 & 10 \end{smallmatrix}\right)\left(\begin{smallmatrix} 1 \\ 1 \end{smallmatrix}\right) = 6\left(\begin{smallmatrix} 1 \\ 1 \end{smallmatrix}\right)$.

(d) Consider $M = \left(\begin{smallmatrix} 2 & 1 \\ 0 & 2 \end{smallmatrix}\right) \in \mathrm{Mat}_{2\times 2}(\mathbb{R})$. We have:

- $\left(\begin{smallmatrix} 2 & 1 \\ 0 & 2 \end{smallmatrix}\right)\left(\begin{smallmatrix} a \\ 0 \end{smallmatrix}\right) = 2 \cdot \left(\begin{smallmatrix} a \\ 0 \end{smallmatrix}\right)$ *for all $a \in \mathbb{R}$.*

- *Let* $\lambda \in \mathbb{R}$. *We look at* $\left(\begin{smallmatrix} 2 & 1 \\ 0 & 2 \end{smallmatrix}\right)\left(\begin{smallmatrix} a \\ b \end{smallmatrix}\right) = \left(\begin{smallmatrix} 2a+b \\ 2b \end{smallmatrix}\right) = \lambda \cdot \left(\begin{smallmatrix} a \\ b \end{smallmatrix}\right) \Leftrightarrow (2a + b = \lambda a \wedge 2b = \lambda b) \Leftrightarrow (b = 0 \wedge (\lambda = 2 \vee a = 0)) \vee (\lambda = 2 \wedge b = 0) \Leftrightarrow b = 0 \wedge (\lambda = 2 \vee a = 0)$.

  Thus, the only solutions of $M\left(\begin{smallmatrix} a \\ b \end{smallmatrix}\right) = \lambda \cdot \left(\begin{smallmatrix} a \\ b \end{smallmatrix}\right)$ *with a vector* $\left(\begin{smallmatrix} a \\ b \end{smallmatrix}\right) \neq \left(\begin{smallmatrix} 0 \\ 0 \end{smallmatrix}\right)$ *are of the form* $M\left(\begin{smallmatrix} a \\ 0 \end{smallmatrix}\right) = 2 \cdot \left(\begin{smallmatrix} a \\ 0 \end{smallmatrix}\right)$ *with* $a \in \mathbb{R}$.
- *Consider* $M = \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right) \in \mathrm{Mat}_{2\times 2}(\mathbb{R})$. *We look at* $\left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)\left(\begin{smallmatrix} a \\ b \end{smallmatrix}\right) = \left(\begin{smallmatrix} b \\ -a \end{smallmatrix}\right)$. *This vector is equal to* $\lambda \cdot \left(\begin{smallmatrix} a \\ b \end{smallmatrix}\right)$ *if and only if* $b = \lambda \cdot a$ *and* $a = -\lambda \cdot b$. *This gives* $a = -\lambda^2 \cdot a$. *Thus there is no* $\lambda \in \mathbb{R}$ *with this property if* $\left(\begin{smallmatrix} a \\ b \end{smallmatrix}\right) \neq \left(\begin{smallmatrix} 0 \\ 0 \end{smallmatrix}\right)$.

We will study these phenomena in general. Let K be a commutative (as always) field and V a K-vector space. We recall that a K-linear application $\varphi : V \to V$ is also called *endomorphism* and that we denote $\mathrm{End}_K(V) := \mathrm{Hom}_K(V, V)$.

Definition 3.2. *Let V be a K-vector space of finite dimension n and $\varphi \in \mathrm{End}_K(V)$.*

- $\lambda \in K$ *is called* eigenvalue *of* φ *if there exists* $0 \neq v \in V$ *such that* $\varphi(v) = \lambda v$ *(or equivalently :* $\ker(\varphi - \lambda \cdot \mathrm{id}_V) \neq 0$*).*
- *We set* $E_\varphi(\lambda) := \ker(\varphi - \lambda \cdot \mathrm{id}_V)$. *Being the kernel of a K-linear application,* $E_\varphi(\lambda)$ *is a K-subspace of V. If λ is an eigenvalue of φ, we call* $E_\varphi(\lambda)$ the eigenspace for λ.
- *Any* $0 \neq v \in E_\varphi(\lambda)$ *is called* eigenvector for the eigenvalue λ.
- *We denote* $\mathrm{Spec}(\varphi) = \{\lambda \in K \mid \lambda \text{ est valeur propre de } \varphi\}$.
- *Let* $M \in \mathrm{Mat}_{n\times n}(K)$. *We know that the application*

$$\varphi_M : K^n \to K^n, \quad \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} \mapsto M \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix}$$

  is K-linear, thus $\varphi_M \in \mathrm{End}_K(K^n)$. *In this case, we often speak of eigenvalue/eigenvector of M (in stead of φ_M).*

Proposition 3.3. *The eigenspaces* $E_\varphi(\lambda)$ *and* $E_M(\lambda)$ *are vector subspaces.*

Proof. This clear since the eigenspaces are defined as kernels of a matrix/linear endomorphism, and we know that kernels are vector subspaces. □

We reconsider the previous example.

Example 3.4.

(a) Let $M = \left(\begin{smallmatrix} 3 & 0 \\ 0 & 2 \end{smallmatrix}\right) \in \mathrm{Mat}_{2\times 2}(\mathbb{R})$.

- $\mathrm{Spec}(M) = \{2, 3\}$*;*
- $E_M(2) = \langle \left(\begin{smallmatrix} 0 \\ 1 \end{smallmatrix}\right) \rangle$*;*
- $E_M(3) = \langle \left(\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right) \rangle$.
- *The matrix M is diagonal and the canonical basis* $\left(\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 \\ 1 \end{smallmatrix}\right)$ *consists in eigenvectors of M.*

(b) Let $M = \left(\begin{smallmatrix} 3 & 1 \\ 0 & 2 \end{smallmatrix}\right) \in \mathrm{Mat}_{2\times 2}(\mathbb{R})$.

- $\mathrm{Spec}(M) = \{2, 3\}$;
- $E_M(2) = \langle \left(\begin{smallmatrix} 1 \\ -1 \end{smallmatrix}\right) \rangle$;
- $E_M(3) = \langle \left(\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right) \rangle$.
- *The matrix* M *is not diagonale, but* K^2 *has basis* $\left(\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 \\ -1 \end{smallmatrix}\right)$ *whose elements are eigenvectors of* M.
- *Let us define the matrix whose columns are the above base vectors* $C := \left(\begin{smallmatrix} 1 & 1 \\ 0 & -1 \end{smallmatrix}\right)$. *This matrix is invertible (since the columns form a basis) and we have*

  $$C^{-1}MC = \left(\begin{smallmatrix} 3 & 0 \\ 0 & 2 \end{smallmatrix}\right),$$

  a diagonal matrix with eigenvalues on the diagonal! Note that we do not need to compute with matrices, the product of matrices is just a reformulation of the statements seen before.

(c) Let $M = \left(\begin{smallmatrix} 5 & 1 \\ -4 & 10 \end{smallmatrix}\right) \in \mathrm{Mat}_{2\times 2}(\mathbb{R})$.

- $\mathrm{Spec}(M) = \{6, 9\}$;
- $E_M(6) = \langle \left(\begin{smallmatrix} 1 \\ 1 \end{smallmatrix}\right) \rangle$;
- $E_M(9) = \langle \left(\begin{smallmatrix} 1 \\ 4 \end{smallmatrix}\right) \rangle$;
- *The eigenvectors* $\left(\begin{smallmatrix} 1 \\ 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 \\ 4 \end{smallmatrix}\right)$ *form a basis of* K^2 *and thus the matrix* $C := \left(\begin{smallmatrix} 1 & 1 \\ 1 & 4 \end{smallmatrix}\right)$ *whose columns are these base vectors is invertible and*

  $$C^{-1}MC = \left(\begin{smallmatrix} 6 & 0 \\ 0 & 9 \end{smallmatrix}\right),$$

  again a diagonal matrix with the eigenvalues on the diagonal!

(d) Let $M = \left(\begin{smallmatrix} 2 & 1 \\ 0 & 2 \end{smallmatrix}\right) \in \mathrm{Mat}_{2\times 2}(\mathbb{R})$.

- $\mathrm{Spec}(M) = \{2\}$;
- $E_M(2) = \langle \left(\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right) \rangle$;
- K^2 *has no basis consisting of eigenvectors of* M, *thus we cannot adapt the procedure of the previous examples in this case.*

(e) Let $M = \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right) \in \mathrm{Mat}_{2\times 2}(\mathbb{R})$.

- $\mathrm{Spec}(M) = \emptyset$;
- *The matrix* M *has no eigenvalues in* $\mathbb{R}$.

Example 3.5. *Let* $K = \mathbb{R}$ *and* $V = \mathcal{C}^\infty(\mathbb{R})$ *be the* $\mathbb{R}$*-vector space of smooth functions* $f : \mathbb{R} \to \mathbb{R}$. *Let* $D : V \to V$ *be the derivation* $f \mapsto Df = \frac{df}{dx} = f'$. *It is an* $\mathbb{R}$*-linear application, whence* $D \in \mathrm{End}_{\mathbb{R}}(V)$.
Let us consider $f(x) = \exp(rx)$ *with* $r \in \mathbb{R}$. *From Analysis, we know that* $D(f) = r \cdot \exp(rx) = r \cdot f$. *Thus* $(x \mapsto \exp(rx)) \in \mathrm{End}_{\mathbb{R}}(V)$ *is an eigenvector for the eigenvalue* r.
We thus find $\mathrm{Spec}(D) = \mathbb{R}$.

In some examples we have met matrices M such that there is an invertible matrix C with the property that $C^{-1}MC$ is a diagonal matrix. But we have also seen examples where we could not find such a matrix C.

Definition 3.6. *(a) A matrix M is said to be* diagonalizable *if there exists an invertible matrix C such that $C^{-1}MC$ is diagonal.*

(b) Let V be a K-vector space of finite dimension n and $\varphi \in \mathrm{End}_K(V)$. We say that φ is diagonalizable *if V admits a K-basis consisting of eigenvectors of φ.*

This definition precisely expresses the idea of diagonalization mentioned before, as the following lemma tells us. Its proof indicates how to find the matrix C (which is not unique, in general).

Lemma 3.7. *Let $\varphi \in \mathrm{End}_K(V)$ and $\mathrm{Spec}(\varphi) = \{\lambda_1, \dots, \lambda_r\}$. The following statements are equivalent:*

(i) φ is diagonalizable.

(ii) There is a basis S of V such that

$$M_{S,S}(\varphi) = \begin{pmatrix} \lambda_1 & & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & \ddots & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & \lambda_1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & \lambda_2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \ddots & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & \lambda_2 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & \ddots & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & \ddots & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \lambda_r & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \ddots & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \lambda_r \end{pmatrix}.$$

Proof. "(i) ⇒ (ii)": By definition, there exists a K-basis of V consisting of eigenvectors. We sort them according to the eigenvalues:

$$S = \{v_{1,1}, \dots, v_{1,e_1}, v_{2,1}, \dots, v_{2,e_2}, \dots, \dots, \dots, v_{r,1}, \dots, v_{r,e_r}\}$$

where for all $1 \le i \le r$ the vectors $v_{i,1}, \dots, v_{i,e_i}$ are eigenvectors for the eigenvalue λ_i. The form of the matrix $M_{S,S}(\varphi)$ is clear.
"(ii) ⇒ (i)": The basis S consists of eigenvectors, hence φ is diagonalizable by definition. □

Proposition 3.8. *Let $M \in \mathrm{Mat}_{n\times n}(K)$ and φ_M be the K-linear application $K^n \to K^n$ given by $\begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} \mapsto M \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix}$. The following statements are equivalent.*

(i) φ_M is diagonalizable.

(ii) There exists $C \in \mathrm{Mat}_{n\times n}(K)$ invertible such that $C^{-1}MC$ is a diagonal matrix; thus M is diagonalizable.

Proof. "(i) $\Rightarrow$ (ii)": Let S be the K-basis of K^n which exists in view of diagonalizability of φ_M. It suffices to take C to be the matrix whose columns are the elements of basis S.
"(ii) $\Rightarrow$ (i)": Let e_i be the i-th standard vector. It is an eigenvector for the matrix $C^{-1}MC$, say with eigenvalue λ_i. The equality $C^{-1}MCe_i = \lambda_i \cdot e_i$ gives $MCe_i = \lambda_i \cdot Ce_i$, i.e. Ce_i is an eigenvector for the matrix M of same eigenvalue. But, Ce_i is nothing but the i-th column of C. Thus, the columns of C form a basis of K^n consisting of eigenvectors. □

The question that we are now interested in, is the following: how can we decide whether φ (or M) is diagonalizable and, if this is the case, how can we find the matrix C? In fact, it is useful to consider two "sub-questions" individually:

- How can we compute $\mathrm{Spec}(\varphi)$?
- For $\lambda \in \mathrm{Spec}(\varphi)$, how can we compute the eigenspace $E_\varphi(\lambda)$?

We will answer the first question in the following section. For the moment, we consider the second question. Let us start by $E_M(\lambda)$. This is $E_M(\lambda) = \ker(M - \lambda \cdot \mathrm{id}_n)$. This computation is done using Gauss' reduction.

Example 3.9. *(a) For the matrix $M = \left(\begin{smallmatrix} 5 & 1 \\ -4 & 10 \end{smallmatrix}\right) \in \mathrm{Mat}_{2\times 2}(\mathbb{R})$ and the eigenvalue 9 we have to compute the kernel of $\left(\begin{smallmatrix} 5 & 1 \\ -4 & 10 \end{smallmatrix}\right) - 9 \cdot \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right) = \left(\begin{smallmatrix} -4 & 1 \\ -4 & 1 \end{smallmatrix}\right)$. Recall that in order to compute the kernel of a matrix, one is only allowed to do operations on the rows (and not on the columns since these mix the variables). We thus have*

$$\ker(\left(\begin{smallmatrix} -4 & 1 \\ -4 & 1 \end{smallmatrix}\right)) = \ker(\left(\begin{smallmatrix} -4 & 1 \\ 0 & 0 \end{smallmatrix}\right)) = \langle \left(\begin{smallmatrix} 1 \\ 4 \end{smallmatrix}\right) \rangle.$$

For the eigenvalue 6 we do a similar computation:

$$\ker(\left(\begin{smallmatrix} 5 & 1 \\ -4 & 10 \end{smallmatrix}\right) - 6 \cdot \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)) = \ker(\left(\begin{smallmatrix} -1 & 1 \\ -4 & 4 \end{smallmatrix}\right)) = \ker(\left(\begin{smallmatrix} -1 & 1 \\ 0 & 0 \end{smallmatrix}\right)) = \langle \left(\begin{smallmatrix} 1 \\ 1 \end{smallmatrix}\right) \rangle.$$

(b) The matrix $M = \left(\begin{smallmatrix} 2 & 1 & 1 \\ 3 & 2 & 3 \\ -3 & -1 & -2 \end{smallmatrix}\right) \in \mathrm{Mat}_{3\times 3}(\mathbb{R})$ has eigenvalues $-1, 1, 2$.

For the eigenvalue 1, we compute the kernel

$$\begin{aligned} \ker\left(\left(\begin{smallmatrix} 2 & 1 & 1 \\ 3 & 2 & 3 \\ -3 & -1 & -2 \end{smallmatrix}\right) - 1 \cdot \left(\begin{smallmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{smallmatrix}\right) \right) &= \ker\left(\left(\begin{smallmatrix} 1 & 1 & 1 \\ 3 & 1 & 3 \\ -3 & -1 & -3 \end{smallmatrix}\right) \right) \\ &= \ker\left(\left(\begin{smallmatrix} 1 & 1 & 1 \\ 0 & -2 & 0 \\ 0 & 0 & 0 \end{smallmatrix}\right) \right) = \ker\left(\left(\begin{smallmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{smallmatrix}\right) \right) = \langle \left(\begin{smallmatrix} 1 \\ 0 \\ -1 \end{smallmatrix}\right) \rangle \end{aligned}$$

For the eigenvalue -1, we compute the kernel

$$\begin{aligned} \ker\left(\left(\begin{smallmatrix} 2 & 1 & 1 \\ 3 & 2 & 3 \\ -3 & -1 & -2 \end{smallmatrix}\right) + 1 \cdot \left(\begin{smallmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{smallmatrix}\right) \right) &= \ker\left(\left(\begin{smallmatrix} 3 & 1 & 1 \\ 3 & 3 & 3 \\ -3 & -1 & -1 \end{smallmatrix}\right) \right) \\ &= \ker\left(\left(\begin{smallmatrix} 3 & 1 & 1 \\ 0 & 2 & 2 \\ 0 & 0 & 0 \end{smallmatrix}\right) \right) = \ker\left(\left(\begin{smallmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 0 \end{smallmatrix}\right) \right) = \langle \left(\begin{smallmatrix} 0 \\ 1 \\ -1 \end{smallmatrix}\right) \rangle \end{aligned}$$

For the eigenvalue 2, we compute the kernel

$$\ker\left(\left(\begin{smallmatrix} 2 & 1 & 1 \\ 3 & 2 & 3 \\ -3 & -1 & -2 \end{smallmatrix}\right) - 2 \cdot \left(\begin{smallmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{smallmatrix}\right) \right) = \ker\left(\left(\begin{smallmatrix} 0 & 1 & 1 \\ 3 & 0 & 3 \\ -3 & -1 & -4 \end{smallmatrix}\right) \right) = \ker\left(\left(\begin{smallmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 0 \end{smallmatrix}\right) \right) = \langle \left(\begin{smallmatrix} 1 \\ 1 \\ -1 \end{smallmatrix}\right) \rangle$$

We write these vectors in the matrix $C = \left(\begin{smallmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ -1 & -1 & -1 \end{smallmatrix}\right)$ *in order to have*

$$C^{-1} \cdot M \cdot C = \left(\begin{smallmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 2 \end{smallmatrix}\right).$$

This explains how to find the eigenspaces in examples. If one wishes to compute the eigenspace $E_\varphi(\lambda) = \ker(\varphi - \lambda \cdot \mathrm{id}_V)$ in a more abstract way, one has to choose a K-basis S of V and represent φ by the matrix $M = M_{S,S}(\varphi)$. In the basis S, $E_\varphi(\lambda)$ is the kernel $\ker(M - \lambda \cdot \mathrm{id}_n)$, and we have already seen how to compute this one.

Let us finally give a more abstract, but useful reformulation of the diagonalizablility. We first need a preliminary.

Lemma 3.10. *Let* $\varphi \in \mathrm{End}_K(V)$ *and* $\lambda_1, \dots, \lambda_r$ *be two by two distinct. Then,* $\sum_{i=1}^r E_\varphi(\lambda_i) = \bigoplus_{i=1}^r E_\varphi(\lambda_i)$.

Proof. We proceed by induction on $r \geq 1$. The case $r = 1$ is trivial. We assume the result true for $r - 1 \geq 1$ and we show it for r. We have to show that for all $1 \leq i \leq r$ we have

$$0 = E_\varphi(\lambda_i) \cap \sum_{j=1, j\neq i}^{r} E_\varphi(\lambda_j) = E_\varphi(\lambda_i) \cap \bigoplus_{j=1, j\neq i}^{r} E_\varphi(\lambda_j),$$

where the second equality follows from the induction hypothese (the sum has $r - 1$ factors). Let $v \in E_\varphi(\lambda_i) \cap \bigoplus_{j=1,j\neq i}^r E_\varphi(\lambda_j)$. Then, $v = \sum_{j=1,j\neq i}^r v_j$ avec $v_j \in E_\varphi(\lambda_j)$. We have

$$\varphi(v) = \lambda_i \cdot v = \sum_{j=1,j\neq i}^{r} \lambda_i \cdot v_j = \varphi(\sum_{j=1,j\neq i}^{r} v_j) = \sum_{j=1,j\neq i}^{r} \varphi(v_j) = \sum_{j=1,j\neq i}^{r} \lambda_j \cdot v_j,$$

thus

$$0 = \sum_{j=1,j\neq i}^{r} (\lambda_j - \lambda_i) \cdot v_j.$$

Since the sum is direct and $\lambda_j - \lambda_i \neq 0$ for all $i \neq j$, we conclude that $v_j = 0$ for all $1 \leq j \leq r$, $j \neq i$, so that $v = 0$. □

Proposition 3.11. *Let* $\varphi \in \mathrm{End}_K(V)$. *The following statements are equivalent:*

(i) φ *is diagonalizable.*

(ii) $V = \bigoplus_{\lambda \in \mathrm{Spec}(\varphi)} E_\varphi(\lambda)$.

Proof. "(i) ⇒ (ii)": We have the inclusion $\sum_{\lambda\in\mathrm{Spec}(\varphi)} E_\varphi(\lambda) \subseteq V$. By Lemma 3.10, the sum is direct, therefore we have the inclusion $\bigoplus_{\lambda\in\mathrm{Spec}(\varphi)} E_\varphi(\lambda) \subseteq V$. Since φ is diagonalizable, there exists a K-basis of V consisting of eigenvectors for φ. Thus, any element of this basis already belongs to $\bigoplus_{\lambda\in\mathrm{Spec}(\varphi)} E_\varphi(\lambda)$, whence the equality $\bigoplus_{\lambda\in\mathrm{Spec}(\varphi)} E_\varphi(\lambda) = V$.
"(ii) ⇒ (i)": For all $\lambda \in \mathrm{Spec}(\varphi)$ let S_λ be a K-basis of the eigenspace $E_\varphi(\lambda)$. Thus $S = \bigcup_{\lambda\in\mathrm{Spec}(\varphi)} S_\lambda$ is a K-basis of V consisting of eigenvectors, showing that φ is diagonalizable. □

4 Excursion: euclidean division and gcd of polynomials

Goals:

- Master the euclidean division and Euclide's algorithm;
- be able to compute the euclidean division, the gcd and a Bezout identity using Euclide's algorithm.

We assume that notions of polynomials are known from highschool or other lecture courses. We denote by $K[X]$ the set of all polynomials with coefficients in K, where X denotes the variable. A polynomial can hence be written as finite sum $\sum_{i=0}^{d} a_i X^i$ with $a_0, \dots, a_d \in K$. We can of course choose any other symbol for the variable, e.g. x, T, $\Box$; in this case, we write $\sum_{i=0}^{d} a_i x^i$, $\sum_{i=0}^{d} a_i T^i$, $\sum_{i=0}^{d} a_i \Box^i$, $K[x]$, $K[T]$, $K[\Box]$, etc.
The degree of a polynomial f will be denoted $\deg(f)$ with the convention $\deg(0) = -\infty$. Recall that for any $f, g \in K[X]$ we have $\deg(fg) = \deg(f) + \deg(g)$ and $\deg(f+g) \leq \max\{\deg(f), \deg(g)\}$.

Definition 4.1. *A polynomial $f = \sum_{i=0}^{d} a_i X^i$ of degree d is called* unitary *if $a_d = 1$.*
A polynomial $f \in K[X]$ of degree ≥ 1 is called irreducible *if it cannot be written as product $f = gh$ with $g, h \in K[X]$ of degree ≥ 1.*

It is a fact that the only irreducible polynomials in $\mathbb{C}[X]$ are the polynomials of degree 1. (One says that $\mathbb{C}$ is *algebraically closed*.) Any irreducible polynomial in $\mathbb{R}[X]$ is either of degree 1 (and trivially, any polynomial of degree 1 is irreducible), or of degree 2 (there exist irreducible polynomials of degree 2, such as $X^2 + 1$, but also reducible polynomials, such as $X^2 - 1 = (X-1)(X+1)$; more precisely, a polynomial of degree 2 is irreducible if and only if its discriminant is negative).

Definition 4.2. *A polynomial $f \in K[X]$ is called* divisor *of a polynomial $g \in K[X]$ if there exists $q \in K[X]$ such that $g = qf$. We use the notation notation $f \mid g$.*

If f divides g, we clearly have $\deg(f) \leq \deg(g)$.
For everything that will be done on polynomials in this lecture course, the euclidean division plays a central role. We now prove its existence.

Theorem 4.3 (Euclidean division)**.** *Let $g = \sum_{i=0}^{d} b_i X^i \in K[X]$ be a polynomial of degree $d \geq 0$. Then, for any polynomial $f \in K[X]$ there exist unique polynomials $q, r \in K[X]$ such that*

$$f = qg + r \quad \text{and} \quad \deg(r) < d.$$

We call r the rest *of the division.*

Proof. Let $f(X) = \sum_{i=0}^{n} a_i X^i \in K[X]$ of degree n.
Existence: We prove the existence by induction on n. If $n < d$, we set $q = 0$ and $r = f$ and we are done. Let us therefore assume $n \geq d$ and that the existence is already known for all polynomials of degree strictly smaller than n. We set

$$f_1(X) := f(X) - a_n \cdot b_d^{-1} X^{n-d} g(X).$$

This is a polynomial of degree at most $n-1$ since we annihilated the coefficient in front of X^n. Then, by induction hypothesis, there are $q_1, r_1 \in K[X]$ such that $f_1 = q_1 g + r_1$ and $\deg(r_1) < d$. Thus

$$f(X) = f_1(X) + a_n b_d^{-1} g(X) X^{n-d} = q(X)g(X) + r_1(X)$$

where $q(X) := q_1(X) + a_n b_d^{-1} X^{n-d}$ and we have shown the existence.
Uniqueness: Assume that $f = qg + r = q_1 g + r_1$ with $q, q_1, r, r_1 \in K[X]$ and $\deg(r), \deg(r_1) < d$. Then $g(q - q_1) = r_1 - r$. If $q = q_1$, then $r = r_1$ and we are done. If $q \neq q_1$, then $\deg(q - q_1) \geq 0$ and we find $\deg(r_1 - r) = \deg(g(q - q_1)) \geq \deg(g) = d$. This is a contradiction, thus $q \neq q_1$ cannot appear. □

In the exercises, you will do euclidean divisions.

Corollary 4.4. *Let $f \in K[X]$ be a polynomial of degree $\deg(f) \geq 1$ and let $a \in K$. Then, the following statements are equivalent:*

(i) $f(a) = 0$

(ii) $(X - a) \mid f$

Proof. (i) $\Rightarrow$ (ii): Assume that $f(a) = 0$ and compute the euclidean division of $f(X)$ by $X - a$:

$$f(X) = q(X)(X - a) + r$$

for $r \in K$ (a polynomial of degree < 1). Evaluating this equality in a, gives $0 = f(a) = q(a)(a - a) + r = r$, and thus the rest is zero.
(ii) $\Rightarrow$ (i): Assume that $X - a$ divides $f(X)$. Then we have $f(X) = q(X) \cdot (X - a)$ for some polynomial $q \in K[X]$. Evaluating this in a gives $f(a) = q(a) \cdot (a - a) = 0$. □

Proposition 4.5. *Let $f, g \in K[X]$ be two polynomials such that $f \neq 0$. Then there exists a unique unitary polynomial $d \in K[X]$, called* greatest common divisor $\mathrm{pgcd}(f, g)$*, such that*

- *$d \mid f$ and $d \mid g$ (*common divisor*) and*
- *for all $e \in K[X]$ we have $((e \mid f$ and $e \mid g) \Rightarrow e \mid d)$ (*greatest *in the sense that any other common divisor divides d).*

Moreover, there exist polynomials $a, b \in K[X]$ such that we have a Bezout relation

$$d = af + bg.$$

Proof. We show that Euclide's algorithm gives the result.

- Preparation: We set
$$\begin{cases} f_0 = f,\ f_1 = g & \text{if } \deg(f) \geq \deg(g), \\ f_0 = g,\ f_1 = f & \text{otherwise.} \end{cases}$$
We also set $B_0 = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$.

- If $f_1 = 0$, we **stop** and set $d := f_0$.
  If $f_1 \neq 0$, we do the euclidean division
  $$f_0 = f_1 q_1 + f_2 \quad \text{where } q_1, f_2 \in A \text{ such that}(f_2 = 0 \text{ or } \deg(f_2) < \deg(f_1)).$$
  We set $A_1 := \left(\begin{smallmatrix} -q_1 & 1 \\ 1 & 0 \end{smallmatrix}\right)$, $B_1 := A_1 B_0$.
  We have $\begin{pmatrix} f_2 \\ f_1 \end{pmatrix} = A_1 \begin{pmatrix} f_1 \\ f_0 \end{pmatrix} = B_1 \begin{pmatrix} f_1 \\ f_0 \end{pmatrix}$.
- If $f_2 = 0$, we **stop** and we set $d := f_1$.
  If $f_2 \neq 0$, we do the euclidean division
  $$f_1 = f_2 q_2 + f_3 \quad \text{where } q_2, f_3 \in A \text{ such that } (f_3 = 0 \text{ or } \deg(f_3) < \deg(f_2)).$$
  We set $A_2 := \left(\begin{smallmatrix} -q_2 & 1 \\ 1 & 0 \end{smallmatrix}\right)$, $B_2 := A_2 B_1$.
  We have $\begin{pmatrix} f_3 \\ f_2 \end{pmatrix} = A_2 \begin{pmatrix} f_2 \\ f_1 \end{pmatrix} = B_2 \begin{pmatrix} f_1 \\ f_0 \end{pmatrix}$.
- If $f_3 = 0$, we **stop** and set $d := f_2$.
  If $f_3 \neq 0$, we do the euclidean division
  $$f_2 = f_3 q_3 + f_4 \quad \text{where } q_3, f_4 \in A \text{ such that } (f_4 = 0 \text{ or } \deg(f_4) < \deg(f_3)).$$
  We set $A_3 := \left(\begin{smallmatrix} -q_3 & 1 \\ 1 & 0 \end{smallmatrix}\right)$, $B_3 := A_3 B_2$.
  We have $\begin{pmatrix} f_4 \\ f_3 \end{pmatrix} = A_3 \begin{pmatrix} f_3 \\ f_2 \end{pmatrix} = B_3 \begin{pmatrix} f_1 \\ f_0 \end{pmatrix}$.
- $\cdots$
- If $f_n = 0$, we **stop** and set $d := f_{n-1}$.
  If $f_n \neq 0$, we do the euclidean division
  $$f_{n-1} = f_n q_n + f_{n+1} \quad \text{where } q_n, f_{n+1} \in A \text{ such that } (f_{n+1} = 0 \text{ or } \deg(f_{n+1}) < \deg(f_n)).$$
  We set $A_n := \left(\begin{smallmatrix} -q_n & 1 \\ 1 & 0 \end{smallmatrix}\right)$, $B_n := A_n B_{n-1}$.
  We have $\begin{pmatrix} f_{n+1} \\ f_n \end{pmatrix} = A_n \begin{pmatrix} f_n \\ f_{n-1} \end{pmatrix} = B_n \begin{pmatrix} f_1 \\ f_0 \end{pmatrix}$.
- $\cdots$

It is clear that the above algorithm (it is Euclide’s algorithm!) stops since

$$\deg(f_n) < \deg(f_{n-1}) < \cdots < \deg(f_2) < \deg(f_1)$$

are natural numbers or $-\infty$.
Let us assume that the algorithm stops with $f_n = 0$. Then, $d = f_{n-1}$. By construction we have:

$$\begin{pmatrix} f_n \\ f_{n-1} \end{pmatrix} = \left(\begin{smallmatrix} 0 \\ d \end{smallmatrix}\right) = B_{n-1} \begin{pmatrix} f_1 \\ f_0 \end{pmatrix} = \left(\begin{smallmatrix} \alpha & \beta \\ r & s \end{smallmatrix}\right) \begin{pmatrix} f_1 \\ f_0 \end{pmatrix} = \begin{pmatrix} \alpha f_1 + \beta f_0 \\ r f_1 + s f_0 \end{pmatrix},$$

showing

$$d = rf_1 + sf_0. \tag{4.1}$$

Note that the determinant of A_i is -1 for all i, hence $\det(B_{n-1}) = (-1)^{n-1}$. Thus the matrix $C := (-1)^{n-1} \left(\begin{smallmatrix} s & -\beta \\ -r & \alpha \end{smallmatrix}\right)$ is the inverse of B_{n-1}. Therefore

$$\begin{pmatrix} f_1 \\ f_0 \end{pmatrix} = CB_{n-1} \begin{pmatrix} f_1 \\ f_0 \end{pmatrix} = C \begin{pmatrix} 0 \\ d \end{pmatrix} = \begin{pmatrix} d(-1)^n\beta \\ d(-1)^{n-1}\alpha \end{pmatrix},$$

showing $d \mid f_1$ and $d \mid f_0$. This shows that d is a common divisor of f_0 and f_1. If e is any common divisor of f_0 and f_1, then by Equation (4.1) e divisdes d. Finally, one divides d, r, s by the leading coefficient of d to make d unitary.

If we have d_1, d_2 unitary gcds, then d_1 divides d_2 and d_2 divides d_1. As both are unitary, it follows that $d_1 = d_2$,proving the uniqueness. □

In the exercises, you will train to compute the gcd of two polynomials. We do not require to use matrices in order to find Bezout's relation; it will simply suffice to " go up" through the equalities in order to get it.

5 Characteristic polynmial

Goals:

- Master the definition of characteristic polynomial;
- know its meaning for the computation of eigenvalues;
- be able to compute characteristic polynomials;
- know examples and be able to prove simple properties.

In Section 3 we have seen how to compute the eigenspace for a given eigenvalue. Here we will answer the question: **How to find the eigenvalues?**

Let us start with the main idea. Let $\lambda \in K$ and M a square matrix. Recall

$$E_M(\lambda) = \ker(\lambda \cdot \mathrm{id} - M).$$

We have the following equivalences:

(i) λ is an eigenvalue for M.

(ii) $E_M(\lambda) \neq 0$.

(iii) The matrix $\lambda \cdot \mathrm{id} - M$ is not invertible.

(iv) $\det(\lambda \cdot \mathrm{id} - M) = 0$.

The main idea is to consider λ as a variable X. Then the determinant of $X \cdot \mathrm{id} - M$ becomes a polynomial in $K[X]$. It is the *characteristic polynomial*. By the above equivalences, its roots are precisely the eigenvalues of M.

Definition 5.1. • *Let* $M \in \mathrm{Mat}_{n\times n}(K)$ *be a matrix. The* characteristic polynomial of M *is defined by*

$$\mathrm{charpoly}_M(X) := \det\big(X \cdot \mathrm{id}_n - M\big) \in K[X].$$

- *Let* V *be a* K*-vector space of finite dimension and* $\varphi \in \mathrm{End}_K(V)$ *and* S *a* K*-basis of* V*. The* characteristic polynomial of φ *is defined by*

$$\mathrm{charpoly}_{\phi}(X) := \mathrm{charpoly}_{M_{S,S}(\varphi)}(X).$$

Remark 5.2. *Information for 'experts': Note that the definition of characteristic polynomials uses the determinants in the ring* $K[X]$*. That is the reason why we presented the determinants in a more general way in the recall. Alternatively, one can also work in the field of rational functions over* K*, i.e. the field whose elements are fractions of polynomials with coefficients in* K*.*

Lemma 5.3. *Let* $M \in \mathrm{Mat}_{n\times n}(K)$*.*

(a) $\mathrm{charpoly}_M(X)$ *is a unitary polynomial of degree* n*.*

(b) $\mathrm{charpoly}_M(X)$ *is conjugation invariant, i.e., for all* $N \in \mathrm{GL}_n(K)$ *we have the equality*

$$\mathrm{charpoly}_M(X) = \mathrm{charpoly}_M\, N^{-1}MN(X).$$

Proof. (a) This is proved by induction on n. The case $n = 1$ is clear because the matrix is $(X - m_{1,1})$, hence its determinant is $X - m_{1,1}$.
For the induction step, recall the notation $M'_{i,j}$ for the matrix obtained by M when deleting the i-th row and the j-th column. Assume the result is proved for $n - 1$. By Laplace expansion, we have

$$\mathrm{charpoly}_M(X) = (X - m_{1,1})\,\mathrm{charpoly}_{M'_{1,1}}(X) - \sum_{i=2}^{n}(-1)^i m_{i,1}\cdot\det\big(X\cdot\mathrm{id} - M\big)'_{i,1}.$$

By hypothesis induction, $\mathrm{charpoly}_{M_{1,1}}(X)$ is a unitary polynomial of degree $n-1$, hence $(X - m_{1,1})\,\mathrm{charpoly}_{M_{1,1}}(X)$ is unitary of degree n. In the matrix $\big(X\cdot\mathrm{id} - M\big)'_{i,1}$ with $i \neq 1$, the variable X only appears $n-2$ times. Thus in the characteristic polynomial, it can only appear to the $n-2$-th power at most. Consequently, $\mathrm{charpoly}_M(X)$ is unitary.
(b) We use the multiplicativity of the determinant for the ring $K[X]$ (Proposition 2.15).

$$\begin{aligned}\mathrm{charpoly}_{N^{-1}MN}(X) &= \det(X\cdot\mathrm{id}_n - N^{-1}MN) = \det(N^{-1}(X\cdot\mathrm{id}_n - M)N)\\ &= \det(N)^{-1}\det(X\cdot\mathrm{id}_n - M)\det(N) = \det(X\cdot\mathrm{id}_n - M) = \mathrm{charpoly}_M(X).\end{aligned}$$

□

Corollary 5.4. *Let* V *be a* K*-vector space of finite dimension* n*.*

(a) $\mathrm{charpoly}_\varphi(X)$ *is a unitary polynomial of degree* n*.*

(b) $\mathrm{charpoly}_\varphi(X)$ *is independent from the choice of the basis of* V *which appears in its definition.*

Proof. (a) Lemma 5.3 (a).
(b) Let S and T be two basis of V. The statement follows from Lemma 5.3 (b) and the equality $M_{T,T}(\varphi) = C_{S,T}^{-1} \circ M_{S,S}(\varphi) \circ C_{S,T}$. □

We reconsider the examples of Section 3.

Example 5.5. *(a) Let* $M = \begin{pmatrix} 3 & 0 \\ 0 & 2 \end{pmatrix} \in \mathrm{Mat}_{2\times 2}(\mathbb{R})$. *We find*

$$\mathrm{charpoly}_M(X) = (X-3)(X-2).$$

(It is important to know the factorization in irreducible polynomials of the characteristic polynomial. Thus it is useless to write it as $X^2 - 5X + 6$*.)*

(b) Let $M = \begin{pmatrix} 3 & 1 \\ 0 & 2 \end{pmatrix} \in \mathrm{Mat}_{2\times 2}(\mathbb{R})$. *We find once again*

$$\mathrm{charpoly}_M(X) = (X-3)(X-2).$$

(c) Let $M = \begin{pmatrix} 5 & 1 \\ -4 & 10 \end{pmatrix} \in \mathrm{Mat}_{2\times 2}(\mathbb{R})$. *We find*

$$\mathrm{charpoly}_M(X) = (X-5)(X-10) + 4 = (X-6)(X-9).$$

Note that in order to simplify the computation, Lemma 5.3 (b) allows us to use the conjugate matrix $\begin{pmatrix} 1 & 1 \\ 1 & 4 \end{pmatrix}^{-1} \begin{pmatrix} 5 & 1 \\ -4 & 10 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & 4 \end{pmatrix} = \begin{pmatrix} 6 & 0 \\ 0 & 9 \end{pmatrix}$ *for the computation of the characteristic polynomial, thus one can immediately write the factorization in linear factors (in general, this will not be possible).*

(d) Let $M = \begin{pmatrix} 2 & 1 \\ 0 & 2 \end{pmatrix} \in \mathrm{Mat}_{2\times 2}(\mathbb{R})$. *We find*

$$\mathrm{charpoly}_M(X) = (X-2)^2,$$

a polynomial with a double root.

(e) Let $M = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \in \mathrm{Mat}_{2\times 2}(\mathbb{R})$. *We find*

$$\mathrm{charpoly}_M(X) = X^2 + 1,$$

a polynomial that does not factor in linear factors in $\mathbb{R}[X]$.

(f) Let $M = \left(\begin{smallmatrix} 2 & 1 & 1 \\ 3 & 2 & 3 \\ -3 & -1 & -2 \end{smallmatrix}\right) \in \mathrm{Mat}_{3\times 3}(\mathbb{R})$. *For the characteristic polynomial, we compute the determinant*

$$\begin{aligned} \left|\begin{smallmatrix} X-2 & -1 & -1 \\ -3 & X-2 & -3 \\ 3 & 1 & X+2 \end{smallmatrix}\right| &= (X-2) \cdot \left|\begin{smallmatrix} X-2 & -3 \\ 1 & X+2 \end{smallmatrix}\right| + 3 \cdot \left|\begin{smallmatrix} -1 & -1 \\ 1 & X+2 \end{smallmatrix}\right| + 3 \cdot \left|\begin{smallmatrix} -1 & -1 \\ X-2 & -3 \end{smallmatrix}\right| \\ &= (X-2)\big((X-2)(X+2)+3\big) + 3 \cdot \big(-(X+2)+1\big) + 3 \cdot \big(3 + (X-2)\big) \\ &= (X-2)(X^2-1) = (X-2)(X-1)(X+1) \end{aligned}$$

Proposition 5.6. *(a) For $M \in \mathrm{Mat}_{n\times n}(K)$ we have*

$$\mathrm{Spec}(M) = \{a \in K \mid \mathrm{charpoly}_M(a) = 0\} = \{a \in K \mid \ (X-a) \mid \mathrm{charpoly}_M(X)\}.$$

(b) For $\varphi \in \mathrm{End}_K(V)$ with a K-vector space V of finite dimension, we have

$$\mathrm{Spec}(\varphi) = \{a \in K \mid \mathrm{charpoly}_\varphi(a) = 0\} = \{a \in K \mid \ (X-a) \mid \mathrm{charpoly}_\varphi(X)\}.$$

Proof. It suffices to prove (a). The first equality follows from (with $a \in K$):

$$a \in \mathrm{Spec}(M) \Leftrightarrow \ker(a \cdot \mathrm{id}_n - M) \neq 0 \Leftrightarrow \underbrace{\det(a \cdot \mathrm{id}_n - M)}_{=\mathrm{charpoly}_M(a)} = 0 \Leftrightarrow \mathrm{charpoly}_M(a) = 0.$$

The second equality is just the fact that $a \in K$ is a root of a polynomial f if and only if $(X-a)|f$ (Corollary 4.4). □

We have thus identified the eigenvalues with the roots of the characteristic polynomial. This answers our question in the beginning: **In order to compute the eigenvalues of a matrix, compute its characteristic polynomial and find its roots**.

But the characteristic polynomial has another important property that was discovered by Cayley and Hamilton. We first need to introduce some terminology.

Definition 5.7. *(a) Let $M \in \mathrm{Mat}_{n\times n}(K)$ be a matrix. If $f(X) = \sum_{i=0}^d a_i X^i \in K[X]$ is a polynomial, then we set $f(M) := \sum_{i=0}^d a_i M^i \in \mathrm{Mat}_{n\times n}(K)$. Note: $M^0 = \mathrm{id}_n$.*

(b) Let $\varphi \in \mathrm{End}_K(V)$ be an endomorphism of a K-vector space V. If $f(X) = \sum_{i=0}^d a_i X^i \in K[X]$ is a polynomial, then we set $f(\varphi) := \sum_{i=0}^d a_i \varphi^i$, which is still an endomorphism in $\mathrm{End}_K(V)$. Be careful: $\varphi^i = \underbrace{\varphi \circ \varphi \circ \cdots \circ \varphi}_{i \text{ times}}$ et $\varphi^0 = \mathrm{id}_V$.

Definition-Lemma 5.8 (For mathematicians only). *(a) The application "evaluation"*

$$\mathrm{ev}_M : K[X] \to \mathrm{Mat}_{n\times n}(K), \quad f(X) \mapsto f(M)$$

is a ring homomorphism (even a homomorphism of K-algebras).

(b) The application "evaluation"

$$\mathrm{ev}_\varphi : K[X] \to \mathrm{End}_K(V), \quad f(X) \mapsto f(\varphi)$$

is a ring homomorphism (even a homomorphism of K-algebras).

Proof. Easy computations. □

Theorem 5.9 (Cayley-Hamilton). *Let $M \in \mathrm{Mat}_{n\times n}(K)$. Then,*

$$\mathrm{charpoly}_M(M) = 0_n \in \mathrm{Mat}_{n\times n}(K).$$

Proof. The trick is to use adjoint matrices. In $\mathrm{Mat}_{n\times n}(K[X])$ we have

$$(X\cdot \mathrm{id}_n - M)^{\#}\cdot(X\cdot\mathrm{id}_n - M) = \det(X\cdot\mathrm{id}_n - M)\cdot\mathrm{id}_n \overset{\text{déf}}{=} \mathrm{charpoly}_M(X)\cdot\mathrm{id}_n. \tag{5.2}$$

The idea of the proof is very simple: if one replaces X by M in (5.2), one obtains 0, since on the left hand side we have the factor $(M\cdot\mathrm{id}_n - M) = M - M = 0$. The problem is that in $\mathrm{Mat}_{n\times n}(K[X])$, X appears in the coefficients of the matrices, and we are certainly not allowed to replace a coefficient of a matrix by a matrix. What we do is to write a matrix whose coefficients are polynomials as polynomial whose coefficients are matrices:

$$\begin{pmatrix} \sum_{k=0}^d a_{1,1,k}X^k & \cdots & \sum_{k=0}^d a_{1,n,k}X^k \\ \vdots & \ddots & \vdots \\ \sum_{k=0}^d a_{n,1,k}X^k & \cdots & \sum_{k=0}^d a_{n,n,k}X^k \end{pmatrix} = \sum_{k=0}^d \begin{pmatrix} a_{1,1,k} & \cdots & a_{1,n,k} \\ \vdots & \ddots & \vdots \\ a_{n,1,k} & \cdots & a_{n,n,k} \end{pmatrix}\cdot X^k\cdot\mathrm{id}_n.$$

Having done this, one would have to show that the evaluation of this polynomial with matrix coefficients in a matrix gives rise to a ring homomorphism. Unfortunately, the matrix ring is not commutative, hence the developed theory does not apply. The proof that we give avoids this problem by doing a comparison of the coefficients instead of an evaluation, but is based on the same idea.

The definition of adjoint matrix shows that the largest power of X that can appear in a coefficient of the matrix $(X\cdot\mathrm{id}_n - M)^{\#}$ is $n-1$. As indicated above, we can hence write this matrix as polynomial of degree $n-1$ with coefficients in $\mathrm{Mat}_{n\times n}(K)$:

$$(X\cdot\mathrm{id}_n - M)^{\#} = \sum_{i=0}^{n-1} B_i X^i \quad \text{with} \quad B_i \in \mathrm{Mat}_{n\times n}(K).$$

We write $\mathrm{charpoly}_M(X) = \sum_{i=0}^n a_i X^i$ (où $a_n = 1$) and consider Equation (5.2) in $\mathrm{Mat}_{n\times n}(K)$:

$$\begin{aligned}\mathrm{charpoly}_M(X)\cdot\mathrm{id}_n &= \sum_{i=0}^n a_i\cdot\mathrm{id}_n\cdot X^i = \big(\sum_{i=0}^{n-1} B_i X^i\big)(X\cdot\mathrm{id}_n - M)\\ &= \sum_{i=0}^{n-1}(B_iX^{i+1} - B_iMX^i) = -B_0M + \sum_{i=1}^{n-1}(B_{i-1} - B_iM)X^i + B_{n-1}X^n.\end{aligned}$$

We compare the coefficients (still matrices!) to obtain

$$a_0\cdot\mathrm{id}_n = -B_0M, \quad a_i\cdot\mathrm{id}_n = B_{i-1} - B_iM \text{ for } 1\le i\le n-1 \quad \text{and} \quad B_{n-1} = \mathrm{id}_n.$$

This comparision of coefficients allows us to continue with our calculations in $\mathrm{Mat}_{n\times n}(K)$ in order to obtain $\mathrm{charpoly}_M(M) = 0_n$ as follows:

$$\begin{aligned}&\mathrm{charpoly}_M(M)\cdot\mathrm{id}_n = \sum_{i=0}^n a_i\cdot M^i = -B_0M + \sum_{i=1}^{n-1}(B_{i-1} - B_iM)M^i + B_{n-1}M^n\\ &= -B_0M + B_0M - B_1M^2 + B_1M^2 - B_2M^3 + B_2M^3 - \cdots - B_{n-1}M^n + B_{n-1}M^n = 0_n.\end{aligned}$$

□

The theorem of Cayley-Hamilton is still true if one replaces the matrix M by an endomorphism $\varphi \in \mathrm{End}_K(V)$.

Theorem 5.10 (Cayley-Hamilton for endomorphisms)**.** *Let V be a K-vector space of finite dimension and $\varphi \in \mathrm{End}_K(\varphi)$. Then,* $\mathrm{charpoly}_\varphi(\varphi) = 0 \in \mathrm{End}_K(V)$.

Proof. By definition we have, $\mathrm{charpoly}_\varphi(X) = \mathrm{charpoly}_{M_{S,S}(\varphi)}(X)$ and by Theorem 5.9

$$0 = \mathrm{charpoly}_{M_{S,S}(\varphi)}(M_{S,S}(\varphi)) = M_{S,S}(\mathrm{charpoly}_{M_{S,S}(\varphi)}(\varphi)) = M_{S,S}(\mathrm{charpoly}_\varphi(\varphi)),$$

thus $\mathrm{charpoly}_\varphi(\varphi) = 0$. This computation is based on $M_{S,S}(\varphi^i) = \big(M_{S,S}(\varphi)\big)^i$ (see exercises) □

6 Minimal polynomial

Goals:

- Master the definition of minimal polynomial;
- know its meaning for the computation of eigenvalues;
- know how to compute minimal polynomials;
- know examples and be able to prove simple properties.

Beside the characteristic polynomial, we will also introduce the *minimal polynomial*.

Definition-Lemma 6.1. *Let $M \in \mathrm{Mat}_{n\times n}(K)$ be a matrix.*

(a) There exists a unique unitary polynomial $\mathrm{mipo}_M(X) \in K[X]$ of minimal degree with the property $\mathrm{mipo}_M(M) = 0_n$. This polynomial is called the minimal polynomial of M.

(b) Any polynomial $f \in K[X]$ with the property $f(M) = 0_n$ is a multiple of $\mathrm{mipo}_M(X)$.

(c) For any invertible matrix $N \in \mathrm{Mat}_{n\times n}(K)$, we have $\mathrm{mipo}_{N^{-1}MN}(X) = \mathrm{mipo}_M(X)$.

(d) Let $\varphi \in \mathrm{End}_K(V)$ for a K-vector space V of finite dimension with K-basis S. We set

$$\mathrm{mipo}_\varphi(X) := \mathrm{mipo}_{M_{S,S}(\varphi)}(X)$$

and call it minimal polynomial of φ. *This polynomial is independent from the choice of the basis S.*

Proof. (a,b) By Theorem of Cayley-Hamilton 5.9 there exists a polynomial $0 \neq f \in K[X]$ that annihilates M. Let us now consider the set of such polynomials

$$E = \{f \in K[X] \mid f \neq 0 \text{ and } f(M) = 0\}.$$

We choose unitary $g \in E$ of minimal degree among the elements of E.

We will use the euclidean division to show the uniqueness and (b). Let $f \in E$. We thus have $q, r \in K[X]$ such that $r = 0$ or $\deg(r) < \deg(g)$ and

$$f = qg + r,$$

which implies

$$0 = f(M) = q(M)g(M) + r(M) = q(M) \cdot 0 + r(M) = r(M).$$

Consequently, let $r = 0$, let $r \in E$. This last possibility is excluded as the degree of r is strictly smaller that the degree of g which is minimal. The fact that $r = 0$ means $f = qg$, thus any other polynomial of E is a multiple of g. This also implies the uniqueness: if f has the same degree than g and is also unitary, then $f = g$.
(c) It suffices to note $(N^{-1}MN)^i = N^{-1}M^iN$, hence for all $f \in K[X]$

$$f(N^{-1}MN) = N^{-1}f(M)N = 0_n \Leftrightarrow f(M) = 0_n.$$

(d) The independence of the basis choice is a consequence of (c) and the equality $M_{T,T}(\varphi) = C_{S,T}^{-1} \circ M_{S,S}(\varphi) \circ C_{S,T}$ for any other basis T. □

Proposition 6.2. *Let V be a K-vector space of finite dimension and $\varphi \in \mathrm{End}_K(V)$. Then,* $\mathrm{Spec}(\varphi) = \{a \in K \mid \ (X - a) \mid \mathrm{mipo}_\varphi(X)\} = \{a \in K \mid \mathrm{mipo}_\varphi(a) = 0\}$.

Clearly, the same statement holds for matrices $M \in \mathrm{Mat}_{n \times n}(K)$. Compare this proposition to Proposition 5.6.

Proof. The second equality is clear (same argument as in the proof of Proposition 5.6). To see the first equality, first assume that $(X - a) \nmid \mathrm{mipo}_\varphi(X)$. From this we deduce that the gcd of $(X - a)$ and $\mathrm{mipo}_\varphi(X)$ is 1, which allows us (by Euclide/Bézout algorithm) to find $b, c \in K[X]$ such that $1 = b(X)(X - a) + c(X)\,\mathrm{mipo}_\varphi(X)$. Let now $v \in V$ t.q. $\varphi(v) = av$. We have

$$v = \mathrm{id}_V v = b(\varphi)(\varphi(v) - av) + c(\varphi)\,\mathrm{mipo}_\varphi(\varphi)v = 0 + 0 = 0,$$

hence $a \notin \mathrm{Spec}(\varphi)$.
Assume now that $(X - a) \mid \mathrm{mipo}_\varphi(X)$ which allows us to write $\mathrm{mipo}_\varphi(X) = (X - a)g(X)$ for some $g \in K[X]$. Since the degree of g is strictly smaller than the degree of $\mathrm{mipo}_\varphi(X)$, there has to be a $v \in V$ such that $w := g(\varphi)v \neq 0$ (otherwise, the minimal polynomial $\mathrm{mipo}_\varphi(X)$ would be a divisor of $g(X)$ which is impossible). We thus have

$$(\varphi - a)w = \mathrm{mipo}_\varphi(\varphi)v = 0,$$

hence $a \in \mathrm{Spec}(\varphi)$. □

It is useful to observe that Propositions 5.6 and 6.2 state that $\mathrm{charpoly}_\varphi(X)$ and $\mathrm{mipo}_\varphi(X)$ have the same factors of degree 1. Moreover, the characteristic polynomial $\mathrm{charpoly}_\varphi(X)$ is always a multiple of the minimal polynomial $\mathrm{mipo}_\varphi(X)$, by the theorem of Cayley-Hamilton, as we will now see.

Corollary 6.3. *Let $M \in \mathrm{Mat}_{n\times n}(K)$. Then, the minimal polynomial $\mathrm{mipo}_M(X)$ is a divisor of the characteristic polynomial $\mathrm{charpoly}_M(X)$. We also have the same statement for $\varphi \in \mathrm{End}_K(V)$.*

Proof. By the Theorem of Cayley-Hamilton 5.9 $\mathrm{charpoly}_M(M) = 0_n$, and hence $\mathrm{mipo}_M(X)$ divides $\mathrm{charpoly}_M(X)$ by Lemma 6.1. □

Example 6.4. *Here are key examples to understand the difference between minimal and characteristic polynomial:*

- *The following three matrices have the same characteristic polynomial, $(X-1)^2$:*

  $$M_1 := \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right), \quad M_2 := \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right), \quad M_3 := \left(\begin{smallmatrix} 1 & 691 \\ 0 & 1 \end{smallmatrix}\right).$$

  The minimal polynomial of M_1 is $X-1$. Since $M_2 - 1 \cdot \mathrm{id}_2 = \left(\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right) \neq 0_2$ and $M_3 - 1 \cdot \mathrm{id}_2 = \left(\begin{smallmatrix} 0 & 691 \\ 0 & 0 \end{smallmatrix}\right) \neq 0_2$, the minimal polynomial is $(X-1)^2$ in both cases. Note that we used the fact that the only non-constant normalized divisors of $(X-1)^2$ are $X-1$ and $(X-1)^2$, therefore the minimal polynomial has to be one of them.

- *The same arguments give the minimal polynomials of the following matrices (but, note that there is one more possibility):*

  $$M_4 := \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, M_5 := \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, M_6 := \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}.$$

Example 6.5. *Let us treat a more complicated example. Let*

$$M = \begin{pmatrix} 4 & 3 & -3 & 7 \\ 7 & 0 & -3 & 7 \\ 6 & -1 & -2 & 6 \\ -1 & -4 & 4 & -4 \end{pmatrix}.$$

There are (at least) two ways to proceed:

(I) Compute the characteristic polynomial and deduce the minimal polynomial .

A computation shows:

$$\mathrm{charpoly}_M(X) = X^4 + 2X^3 - 11X^2 - 12X + 36 = (X+3)^2 \cdot (X-2)^2.$$

We know that the linear factors in the minimal polynomial are the same as in the characteristic one. We thus know that

$$\mathrm{mipo}_M(X) = (X+3)^a \cdot (X-2)^b$$

for $1 \leq a, b \leq 2$.

We compute the minima polynomial trying out the possibilities.

- *We start with the possibility of the lowest degree:*

  $$M_{-3} := M + 3 \cdot \mathrm{id} = \begin{pmatrix} 7 & 3 & -3 & 7 \\ 7 & 3 & -3 & 7 \\ 6 & -1 & 1 & 6 \\ -1 & -4 & 4 & -1 \end{pmatrix}, \quad M_2 := M - 2 \cdot \mathrm{id} = \begin{pmatrix} 2 & 3 & -3 & 7 \\ 7 & -2 & -3 & 7 \\ 6 & -1 & -4 & 6 \\ -1 & -4 & 4 & -6 \end{pmatrix}$$

  and we compute

  $$M_{-3} \cdot M_2 = \begin{pmatrix} 10 & -10 & 10 & 10 \\ 10 & -10 & 10 & 10 \\ 5 & -5 & 5 & 5 \\ -5 & 5 & -5 & -5 \end{pmatrix} \neq 0.$$

  Thus $(X-3)(X+2)$ is not the minimal polynomial.

- *We increase the powers, one by one*

  We compute

$$M_{-3}^2 \cdot M_2 = \begin{pmatrix} 50 & -50 & 50 & 50 \\ 50 & -50 & 50 & 50 \\ 25 & -25 & 25 & 25 \\ -25 & 25 & -25 & -25 \end{pmatrix} \neq 0.$$

  Thus the minimal polynomial is not $(X-3)^2(X+2)$.

  We continue and compute

$$M_{-3} \cdot M_2^2 = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}.$$

  We thus finished and found that

$$\mathrm{mipo}_M(X) = (X+3) \cdot (X-2)^2 = X^3 - X^2 - 8X + 12.$$

(II) *If one does not know the characteristic polynomial and if one does not want to compute it, one can proceed differently. This will lead us to the standard answer:* In order to compute the minimal polynomial, we have to solve systems of linear equations.

We proceed by induction on the (potentiel) degree d *of the minimal polynomial.*

$d = 1$ *If the degree is* 1*, the matrix would be diagonal. This is obviously not the case.*

$d = 2$ *We compute*

$$M^2 = \begin{pmatrix} 12 & -13 & 13 & 3 \\ 3 & -4 & 13 & 3 \\ -1 & -4 & 13 & -1 \\ -4 & 9 & -9 & 5 \end{pmatrix}.$$

Now, we have to consider the system of linear equations:

$$0 = a_2 M^2 + a_1 M + a_0 =$$

$$a_2 \cdot \begin{pmatrix} 12 & -13 & 13 & 3 \\ 3 & -4 & 13 & 3 \\ -1 & -4 & 13 & -1 \\ -4 & 9 & -9 & 5 \end{pmatrix} + a_1 \cdot \begin{pmatrix} 4 & 3 & -3 & 7 \\ 7 & 0 & -3 & 7 \\ 6 & -1 & -2 & 6 \\ -1 & -4 & 4 & -4 \end{pmatrix} + a_0 \cdot \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

These are 16 linear equations. In practice, one can write the coefficients in a big matrix. The first row contains the coefficients $(1,1)$ *of the three matrices, the second row contains the coefficients* $(1,2)$*, etc., until row 16 which contains the coefficients* $(4,4)$*:*

$$\begin{pmatrix} 12 & 4 & 1 \\ -13 & 3 & 0 \\ 13 & -3 & 0 \\ 3 & 7 & 0 \\ 3 & 7 & 0 \\ -4 & 0 & 1 \\ 13 & -3 & 0 \\ 3 & 7 & 0 \\ -1 & 6 & 0 \\ -4 & -1 & 0 \\ 13 & -2 & 1 \\ -1 & 6 & 0 \\ -4 & -1 & 0 \\ 9 & -4 & 0 \\ -9 & 4 & 0 \\ 5 & -4 & 1 \end{pmatrix}.$$

We find that this system does not have a non-zero solution since the rank of the matrix is 3.

$d = 3$ *We compute*

$$M^3 = \begin{pmatrix} 32 & 11 & -11 & 59 \\ 59 & -16 & -11 & 59 \\ 47 & -12 & -15 & 47 \\ -12 & -23 & 23 & -39 \end{pmatrix}.$$

Now, we have to consider the system of linear equations:

$$0 = a_3M^3 + a_2M^2 + a_1M + a_0 =$$
$$a_3 \cdot \begin{pmatrix} 32 & 11 & -11 & 59 \\ 59 & -16 & -11 & 59 \\ 47 & -12 & -15 & 47 \\ -12 & -23 & 23 & -39 \end{pmatrix} + a_2 \cdot \begin{pmatrix} 12 & -13 & 13 & 3 \\ 3 & -4 & 13 & 3 \\ -1 & -4 & 13 & -1 \\ -4 & 9 & -9 & 5 \end{pmatrix} + a_1 \cdot \begin{pmatrix} 4 & 3 & -3 & 7 \\ 7 & 0 & -3 & 7 \\ 6 & -1 & -2 & 6 \\ -1 & -4 & 4 & -4 \end{pmatrix} + a_0 \cdot \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

These are 16 equations. We write the matrix with the coefficients (note that it suffices to add the first column). We also provide a generator of the kernel (obtained by Gauß' algorithm (in general)):

$$\begin{pmatrix} 32 & 12 & 4 & 1 \\ 11 & -13 & 3 & 0 \\ -11 & 13 & -3 & 0 \\ 59 & 3 & 7 & 0 \\ 59 & 3 & 7 & 0 \\ -16 & -4 & 0 & 1 \\ -11 & 13 & -3 & 0 \\ 59 & 3 & 7 & 0 \\ 47 & -1 & 6 & 0 \\ -12 & -4 & -1 & 0 \\ -15 & 13 & -2 & 1 \\ 47 & -1 & 6 & 0 \\ -12 & -4 & -1 & 0 \\ -23 & 9 & -4 & 0 \\ 23 & -9 & 4 & 0 \\ -39 & 5 & -4 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ -1 \\ -8 \\ 12 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}.$$

We see that the result is the polynomial $X^3 - X^2 - 8X + 12$, the same as in (I).

7 Diagonalization and spectral decompostion

Goals:

- Know and master the spectral decomposition;
- be able to decide whether a matrix/endomorphism is diagonalizable; if so, be able to compute the diagonal form and a matrix of basis change;
- be able to compute the spectral decompostion of a matrix/endomorphism;
- know examples and be able to prove simple properties.

A diagonal form is certainly the simplest form that one can wish a matrix to have. But we already saw that matrices do not have this form in general. The *spectral decompostion* and the *Jordan form* are simple forms that one can always obtain. In the most advantageous cases, these forms are diagonal. Let V be a K-vector space (of dimension n) and $\varphi \in \mathrm{End}_K(V)$ be an endomorphism. We first do a fundamental, but simple, observation concerning block matrices.

Lemma 7.1. *(a) Let $W \leq V$ be a subspace such that $\varphi(W) \subseteq (W)$. Let S_1 be a basis of W that we extend to a basis S of V. Then,*

$$M_{S,S}(\varphi) = \begin{pmatrix} \boxed{M_1} & \boxed{???} \\ \boxed{0} & \boxed{???} \end{pmatrix}$$

with $M_1 = M_{S_1,S_1}(\varphi|_W)$.

(b) Let $V = W_1 \oplus W_2$ be such that $\varphi(W_i) \subseteq W_i$ for $i = 1, 2$. Let S_i be a K-basis of W_i for $i = 1, 2$; hence, $S = S_1 \cup S_2$ is a K-basis of V. Then,

$$M_{S,S}(\varphi) = \begin{pmatrix} \boxed{M_1} & \boxed{0} \\ \boxed{0} & \boxed{M_2} \end{pmatrix}$$

with $M_1 = M_{S_1,S_1}(\varphi|_{W_1})$ and $M_2 = M_{S_2,S_2}(\varphi|_{W_2})$.

Proof. It suffices to apply the rules to write the matrix $M_{S,S}(\varphi)$. □

We will continue by a lemma.

Lemma 7.2. *Let $\varphi \in \mathrm{End}_K(V)$.*

(a) Let $f \in K[X]$ and $W := \ker(f(\varphi))$. Then, W is a subspace of V that is stable under φ, i.e. for all $w \in W$ we have $\varphi(w) \in W$. This allows us to restrict φ à W; we will denote the restricted map by $\varphi|_W : W \to W$.

(b) Let $f, g \in K[X]$ be two coprime polynomials, i.e.: $\mathrm{pgcd}(f(X), g(X)) = 1$. Then,

$$\underbrace{\ker(f(\varphi) \cdot g(\varphi))}_{=:W} = \underbrace{\ker(f(\varphi))}_{=:W_1} \oplus \underbrace{\ker(g(\varphi))}_{=:W_2}.$$

Before the proof, a brief word about the notation: $f(\varphi)$ is a K-linear application $V \to V$, then one can apply it to a vector $v \in V$. Our notation for this is: $f(\varphi)(v)$ or $f(\varphi)v$. Note the different roles of the two pairs of parenthesis in the first expression. One could also write $(f(\varphi))(v)$, but I find this notation a bit cumbersome.

Proof. (a) The kernel of any K-linear application is a subspace. Write $f(X) = \sum_{i=0}^{d} a_i X^i$. Let then $w \in W$, i.e. $f(\varphi)w = \sum_{i=0}^{d} a_i \varphi^i(w) = 0$. We compute

$$f(\varphi)(\varphi(w)) = \sum_{i=0}^{d} a_i \varphi^i(\varphi(w)) = \sum_{i=0}^{d} a_i \varphi^{i+1}(w) = \varphi\big(\sum_{i=0}^{d} a_i \varphi^i(w)\big) = \varphi(0) = 0.$$

(b) It is clear that $W_1 \subseteq W$ and $W_2 \subseteq W$, whence $W_1 + W_2 \subseteq W$. We have to prove that

- $W_1 \cap W_2 = 0$ (the zero K-vector space) and
- $W_1 + W_2 = W$.

Since $K[X]$ is a euclidean ring, we can use Euclide's algorithm (Bézout) to obtain two other polynomials $a, b \in K[X]$ such that $1 = a(X)f(X) + b(X)g(X)$. First consider $w \in W_1 \cap W_2$. Then

$$w = \mathrm{id}_V(w) = a(\varphi)f(\varphi)w + b(\varphi)g(\varphi)w = 0 + 0 = 0,$$

which proves the first point. For the second, let $w \in W$. The equation that we used reads

$$w = w_2 + w_1 \text{ with } w_2 := a(\varphi)f(\varphi)w \text{ and } w_1 := b(\varphi)g(\varphi)w.$$

But, we have

$$f(\varphi)(w_1) = b(\varphi)f(\varphi)g(\varphi)w = b(\varphi)0 = 0 \Rightarrow w_1 \in W_1$$

and

$$g(\varphi)(w_2) = a(\varphi)f(\varphi)g(\varphi)w = a(\varphi)0 = 0 \Rightarrow w_2 \in W_2,$$

which concludes the proof. □

Theorem 7.3 (Spectral decomposition). *Let $\varphi \in \mathrm{End}_K(V)$ be an endomorphism with minimal polynomial $\mathrm{mipo}_\varphi(X) = f_1^{e_1}(X) \cdot f_2^{e_2}(X) \cdot \ldots \cdot f_r^{e_r}(X)$ where the polynomials $f_i(X)$ are irreducible (they are therefore prime elements in the principal ring $K[X]$) and coprime, i.e. $\mathrm{pgcd}(f_i, f_j) = 1$ for all $1 \leq i < j \leq n$ (if one chooses the f_i's monic, then the condition is equivalent to saying that the polynomials are all distinct). Set $W_i := \ker(f_i^{e_i}(\varphi))$. Then the following statements hold.*

(a) $V = \bigoplus_{i=1}^r W_i$.

(b) If one chooses a basis S_i of the subspace W_i for $1 \leq i \leq r$, then $S = S_1 \cup S_2 \cup \cdots \cup S_r$ is a basis of W for which we have:

$$M_{S,S}(\varphi) = \begin{pmatrix} \boxed{M_1} & \boxed{0} & \boxed{0} & \cdots & \boxed{0} \\ \boxed{0} & \boxed{M_2} & \boxed{0} & \cdots & \boxed{0} \\ \vdots & & \ddots & \ddots & \vdots \\ \boxed{0} & \cdots & \boxed{0} & \boxed{M_{r-1}} & \boxed{0} \\ \boxed{0} & \cdots & \boxed{0} & \boxed{0} & \boxed{M_r} \end{pmatrix}$$

with $M_i := M_{S_i,S_i}(\varphi|_{W_i})$ for $1 \leq i \leq r$.

Proof. (a) follows from Lemma 7.2 (b) by induction.
(b) is clear: Write the matrix with these rules in order to obtain this form. Note that the blocks outside the diagonal are zero since $\varphi(W_i) \subseteq W_i$. □

The most important case is when $f_i(X) = X - a_i$ with $a_i \neq a_j$ for $i \neq j$ (which implies that the f_i are irreducible and distinct). The spectral decomposition is in fact only a (decisive!) step towards Jordan reduction. In the next proposition we will also see its importance for diagonalization. For the moment we illustrate the effect of the spectral decomposition by an example. Before this, it can be useful to recall how one applies the results for linear applications φ to matrices.

Remark 7.4. *Let $M \in \mathrm{Mat}_{n\times n}(K)$. One can apply the spectral decompostion to M as follwos. For the canonical basis $B := (\begin{pmatrix} 1 \\ 0 \\ 0 \\ \vdots \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \\ \vdots \\ 0 \\ 0 \end{pmatrix}, \ldots, \begin{pmatrix} 0 \\ 0 \\ 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix})$ the matrix M describes a K-linear application $\varphi = \varphi_M$ and one has $M = M_{B,B}(\varphi)$.*
The spectral decomposition gives us a basis S. Let $C := M_{B,S}(\mathrm{id})$ be the matrix of basis change between S and the canonical basis. Then, we have

$$M_{S,S}(\varphi) = C^{-1}MC.$$

To be still concreter, let us recall how to write the matrix C. If $S = (v_1, \dots, v_n)$ and the vecors v_i are given in coordinates for the standard basis, then the i-th column of C is just the vector v_i.

Then, the spectral decomposition can be used to compute a similar matrix (by definition, two matrices A, B are similar *if one is the conjugate of the other: there exists an invertible matrix C such that $B = C^{-1}AC$) à M having the nice form of the theorem.*

Example 7.5. *(a) Let $M := \begin{pmatrix} 1 & 2 & 3 \\ 0 & 1 & 4 \\ 0 & 0 & 5 \end{pmatrix}$ with coefficients in $\mathbb{R}$. The characteristic polynomial is $(X-1)^2(X-5)$. It is clear that* $\ker(M - 5 \cdot \mathrm{id}_3)$ *is of dimension 1; i.e. 5 is an eigenvalue of multiplicity 1 (by definition: its eigenspace is of dimension 1). Without computation, it is clear that* $\dim \ker((M - \mathrm{id}_3)^2) = 3 - 1 = 2$.

Theorem 7.3 implies the existence of a matrix C such that

$$C^{-1} \cdot M \cdot C = \begin{pmatrix} 1 & x & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 5 \end{pmatrix}$$

for some $x \in \mathbb{R}$ that needs to be determined.

In fact, one easily sees that $x \neq 0$, since in this case, the minimal polynomial would be $(X-1)(X-5)$ which is false (also see Proposition 7.7).

Let us compute such a matrix C. For this, we have to compute a basis of the kernel of the matrix

$$(M - \mathrm{id}_3)^2 = \begin{pmatrix} 0 & 2 & 3 \\ 0 & 0 & 4 \\ 0 & 0 & 4 \end{pmatrix} \begin{pmatrix} 0 & 2 & 3 \\ 0 & 0 & 4 \\ 0 & 0 & 4 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 20 \\ 0 & 0 & 16 \\ 0 & 0 & 16 \end{pmatrix}.$$

We can thus simply take $\begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}$.

We also have to compute the kernel of the matrix

$$M - 5 \cdot \mathrm{id}_3 = \begin{pmatrix} -4 & 2 & 3 \\ 0 & -4 & 4 \\ 0 & 0 & 0 \end{pmatrix}.$$

To compute this kernel, we add $\frac{1}{2}$ times the second row to the first and obtain $\begin{pmatrix} -4 & 0 & 5 \\ 0 & -4 & 4 \\ 0 & 0 & 0 \end{pmatrix}$.

The kernel is thus generated by the vector $\begin{pmatrix} 5 \\ 4 \\ 4 \end{pmatrix}$.

The desired matrix C is therefore $\begin{pmatrix}1&0&5\\0&1&4\\0&0&4\end{pmatrix}$. To convince ourselves of the exactness of the computation, we verify it

$$C^{-1}MC = \begin{pmatrix}1&0&-5/4\\0&1&-1\\0&0&1/4\end{pmatrix}\begin{pmatrix}1&2&3\\0&1&4\\0&0&5\end{pmatrix}\begin{pmatrix}1&0&5\\0&1&4\\0&0&4\end{pmatrix} = \begin{pmatrix}1&2&0\\0&1&0\\0&0&5\end{pmatrix}.$$

The theorem on Jordan reduction will tell us (later) that we can choose another matrix C such that the 2 appearing in the matrix is replaced by a 1.

(b) *Let $M := \begin{pmatrix}2&-1&3\\-2&1&-4\\1&1&0\end{pmatrix}$ with coefficients in $\mathbb{R}$. Firstly we compute its characteristic polynomial:*

$$\mathrm{charpoly}_M(X) = \det(\begin{pmatrix}X-2&1&-3\\2&X-1&4\\-1&-1&X\end{pmatrix})$$

$$= (X-2)(X-1)X-4+6-3(X-1)+4(X-2)-2X = X^3-3X^2+X-3 = (X-3)(X^2+1).$$

For this computation we used Sarrus' rule. To obtain the factorization, we can try small integers to find a zero (here 3). The other factor X^2+1 comes from the division of X^3-3X^2+X-3 by $(X-3)$. Note that X^2+1 is irreducible in $\mathbb{R}[X]$ (but not in $\mathbb{C}[X]$).

Let us start with the computation of

$$E_M(3) = \ker(M - 3\cdot \mathrm{id}_n) = \ker(\begin{pmatrix}-1&-1&3\\-2&-2&-4\\1&1&-3\end{pmatrix}).$$

Now one would have to do operations on the rows to obtain the echelon form of the matrix in order to deduce the kernel. But we are lucky, we can just 'see' a vector in the kernel, namely $\begin{pmatrix}1\\-1\\0\end{pmatrix}$.

This vector then generates $E_M(3)$ (the dimension cannot be 2 since in this case $(X-3)^2$ would be a divisor of the characteristic polynomial).

Let us now compute

$$\ker(M^2+M^0) = \ker(\begin{pmatrix}10&0&10\\-10&-0&-10\\0&0&0\end{pmatrix}).$$

This kernel is clearly of dimension 2 generated by $\begin{pmatrix}1\\0\\-1\end{pmatrix}, \begin{pmatrix}0\\1\\0\end{pmatrix}$.

Thus we can write the desired matrix: $C = \begin{pmatrix} 1 & 1 & 0 \\ -1 & 0 & 1 \\ 0 & -1 & 0 \end{pmatrix}$.

We verify our computation:

$$C^{-1}MC = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 0 & -1 \\ 1 & 1 & 1 \end{pmatrix} \begin{pmatrix} 2 & -1 & 3 \\ -2 & 1 & -4 \\ 1 & 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 & 0 \\ -1 & 0 & 1 \\ 0 & -1 & 0 \end{pmatrix} = \begin{pmatrix} 3 & 0 & 0 \\ 0 & -1 & -1 \\ 0 & 2 & 1 \end{pmatrix}.$$

Before giving another characterization of the diagonalizability we recall easy properties of diagonal matrices in a lemma.

Lemma 7.6. *Let $D \in \mathrm{Mat}_{n\times n}(K)$ be a diagonal matrix with $\lambda_1, \lambda_2, \dots, \lambda_n$ on the diagonal.*

(a) $\mathrm{Spec}(D) = \{\lambda_i \mid i = 1, \dots, n\}$.

Note that $\#\,\mathrm{Spec}(D) < n$ if and only if there exist $1 \le i < j \le n$ such that $\lambda_i = \lambda_j$.

(b) $\mathrm{mipo}_D(X) = \prod_{\lambda\in\mathrm{Spec}(D)}(X - \lambda)$.

Proof. These statements are clear. □

The form of the minimal polynomial in the lemma, allows us to give another characterization of the diagonalizability:

Proposition 7.7. *Let V be K-vector space of finite dimension and $\varphi \in \mathrm{End}_K(V)$. The following statements are equivalent:*

(i) φ *is diagonalizable.*

(ii) $\mathrm{mipo}_\varphi(X) = \prod_{a\in\mathrm{Spec}(\varphi)}(X - a)$.

The same statements are also true for matrices $M \in \mathrm{Mat}_{n\times n}(K)$.

Proof. We write $\mathrm{Spec}(\varphi) = \{a_1, \dots, a_r\}$.
"(i) ⇒ (ii)": We choose a basis S such that $M := M_{S,S}(\varphi)$ is diagonal (see Proposition 3.11). A very easy computation shows that $\prod_{i=1}^r (M - a_i) = 0_n$. Then, $\mathrm{mipo}_\varphi(X)$ is a divisor of $\prod_{i=1}^r (X - a_i)$. But Proposition 6.2 shows that for all i one has $(X - a_i) \mid \mathrm{mipo}_\varphi(X)$. Therefore, $\mathrm{mipo}_\varphi(X) = \prod_{i=1}^r (X - a_i)$ (the two polynomials are unitary).
"(ii) ⇒ (i)": We apply the spectral decomposition 7.3 and it suffices to note that the matrices M_i are diagonal since $W_i = E_\varphi(a_i)$ is the eigenspace for the eigenvalue a_i. □

Example 7.8. *Consider the matrix* $M := \begin{pmatrix} 1 & 0 & 2 \\ 0 & 1 & 3 \\ 0 & 0 & 4 \end{pmatrix}$ *with coefficients in $\mathbb{R}$. Its minimal polynomial is $(X-1)(X-4)$, thus, it is diagonalizable.*
(To obtain the minimal polynomial it suffices to see that the eigenspace for the eigenvalue 1 is of dimension 2.)

8 Jordan reduction

Goals:

- Know and master the Jordan reduction;
- be able to decide on different possibilities for the Jordan reduction knowing the minimal and characteristic polynomial;
- be able to compute Jordan's reduction of a matrix/endomorphism as well as of a basis change if the characteristic polynomial factorizes into linear factors;
- know examples and be able to prove simple properties.

In Proposition 3.11 we have seen that diagonalizable matrices are similar to diagonal matrices. The advantage of a diagonal matrix for computations is evident. Unfortunately, not all matrices are diagonalizable. NOur goal is now to choose a basis S of V in such a way that $M_{S,S}(\varphi)$ has a "simple, nice and elegant" form and is close to be diagonal.
We also saw that the spectral decomposition 7.3 gives us a diagonal form "in blocks". Our goal for Jordan's reduction will be to make these blocks have the simplest possible form.
We present *Jordan's reduction* (the *Jordan normal form*) from an algorithmic point of view. The proofs can be shortened a bit if one works without coordinates, but in this case, the computation of the reduction is not clear.
For the sequel, let V be a K-vector space of dimension n and $\varphi \in \mathrm{End}_K(V)$ an endomorphism.

Definition 8.1. *Let $v \in V$. We set*

$$\langle v \rangle_\varphi := \langle \varphi^i(v) \mid i \in \mathbb{N} \rangle,$$

the subspace of V generated by $v, \varphi(v), \varphi^2(v), \dots$.

Remark 8.2. *The following statements are clear and will be used without being mentioned explicitely.*

(a) $\langle v \rangle_\varphi$ is stable under φ, i.e., $\varphi(\langle v \rangle_\varphi) \subseteq \langle v \rangle_\varphi$.

(b) If $W \subseteq V$ is a vector subspace that is stable under φ and if $v \in W$, then $\langle v \rangle_\varphi \subseteq W$.

Lemma 8.3. *The minimal polynomial of the matrix in $\mathrm{Mat}_{n\times n}(K)$*

$$\begin{pmatrix} a & 1 & 0 & 0 & \dots & 0 \\ 0 & a & 1 & 0 & \dots & 0 \\ 0 & 0 & \ddots & \ddots & \ddots & \vdots \\ \vdots & \vdots & \ddots & \ddots & 1 & 0 \\ 0 & 0 & \dots & 0 & a & 1 \\ 0 & 0 & \dots & 0 & 0 & a \end{pmatrix}$$

is equal to $(X-a)^n$.

Proof. Exercise. □

This matrix appears very naturally, as we will now see.

Lemma 8.4. *Let $a \in K$, $e \in \mathbb{N}_{>0}$ and $v \in V$ such that*

$$(\varphi - a \cdot \mathrm{id})^e(v) = 0 \quad \text{and} \quad (\varphi - a \cdot \mathrm{id})^{e-1}(v) \neq 0.$$

We set:

$$\begin{aligned} v_e &:= v, \\ v_{e-1} &:= (\varphi - a \cdot \mathrm{id})(v), \\ &\dots \\ v_2 &:= (\varphi - a \cdot \mathrm{id})^{e-2}(v), \\ v_1 &:= (\varphi - a \cdot \mathrm{id})^{e-1}(v). \end{aligned}$$

(a) We have:

$$\begin{aligned} \varphi(v_1) &= av_1, \\ \varphi(v_2) &= v_1 + av_2, \\ \varphi(v_3) &= v_2 + av_3, \\ &\dots, \\ \varphi(v_e) &= v_{e-1} + av_e. \end{aligned}$$

(b) $\langle v \rangle_\varphi = \langle v_1, \dots, v_e \rangle$, the subspace of V generated by $v_1, \dots, v_e$.

(c) The minimal polynomial of φ acting on $\langle v \rangle_\varphi$ is equal to $(X - a)^e$.

(d) The vectors $v_1, \dots, v_e$ are K-linearly independent and consequently form a basis S of $\langle v \rangle_\varphi$.

(e) $M_{S,S}(\varphi|_{\langle v \rangle_\varphi}) = \begin{pmatrix} a & 1 & 0 & 0 & \dots & 0 \\ 0 & a & 1 & 0 & \dots & 0 \\ 0 & 0 & \ddots & \ddots & \ddots & \vdots \\ \vdots & \vdots & \ddots & \ddots & 1 & 0 \\ 0 & 0 & \dots & 0 & a & 1 \\ 0 & 0 & \dots & 0 & 0 & a \end{pmatrix}.$

Proof. (a) This is a very easy computation:

$$\begin{aligned} (\varphi - a \cdot \mathrm{id})v_1 &= (\varphi - a \cdot \mathrm{id})^e v = 0 && \Rightarrow \varphi(v_1) = av_1. \\ (\varphi - a \cdot \mathrm{id})v_2 &= v_1 && \Rightarrow \varphi(v_2) = v_1 + av_2. \\ &\dots \\ (\varphi - a \cdot \mathrm{id})v_e &= v_{e-1} && \Rightarrow \varphi(v_e) = v_{e-1} + av_e. \end{aligned}$$

(b) The equations in (a) show that $\langle v_1, \dots, v_e \rangle$ is stable under φ. As $v = v_e \in \langle v \rangle_\varphi$, we obtain the inclusion $\langle v \rangle_\varphi \subseteq \langle v_1, \dots, v_e \rangle$. The inverse inclusion can be seen by definition:

$$v_{e-i} = (\varphi - a \cdot \mathrm{id})^i(v) = \sum_{k=0}^{i} \tbinom{i}{k} a^{i-k} \varphi^k(v). \tag{8.3}$$

(c) The polynomial $(X-a)^e$ annihilates v and thus $\langle v \rangle_\varphi$. As $(X-a)^{e-1}$ does not annihilate v, the minimal polynomial of $\varphi|_{\langle v \rangle_\varphi}$ is $(X-a)^e$.
(d) Assume that we have a non-trivial linear combination of the form

$$0 = \sum_{i=0}^{j} \alpha_i v_{e-i}$$

for $\alpha_j \neq 0$ and $0 \leq j \leq e-1$. By Equation (8.3), we obtain

$$0 = \sum_{i=0}^{j} \alpha_i \sum_{k=0}^{i} \tbinom{i}{k} a^{i-k} \varphi^k(v) = \sum_{k=0}^{j-1} \big(\sum_{i=k}^{j} \alpha_i \tbinom{i}{k} a^{i-k} \big) \varphi^k(v) + \alpha_j \varphi^j(v).$$

We thus have a non-zero polynomial of degree $j \leq e-1$ that annihilates v and thus $\langle v \rangle_\varphi$. This is a contradiction with (c).
(e) Part (a) precisely gives the information to write the matrix. □

We will now specify what we mean by “the Jordan form”.

Definition 8.5. *A matrix $M \in \mathrm{Mat}_{n \times n}(K)$ is said to have “the Jordan form” if M is diagonal in blocks and each block has the form of Lemma 8.4(e).*
More precisely, M has the Jordan form if

$$M = \begin{pmatrix} \boxed{M_1} & \boxed{0} & \boxed{0} & \dots & \boxed{0} \\ \boxed{0} & \boxed{M_2} & \boxed{0} & \dots & \boxed{0} \\ \vdots & & \ddots & \ddots & \vdots \\ \boxed{0} & \dots & \boxed{0} & \boxed{M_{r-1}} & \boxed{0} \\ \boxed{0} & \dots & \boxed{0} & \boxed{0} & \boxed{M_r} \end{pmatrix}$$

(diagonal matrix in blocks), where, for all $1 \leq i \leq r$,

$$M_i = \begin{pmatrix} a_i & 1 & 0 & 0 & \dots & 0 \\ 0 & a_i & 1 & 0 & \dots & 0 \\ 0 & 0 & \ddots & \ddots & \ddots & \vdots \\ \vdots & \vdots & \ddots & \ddots & 1 & 0 \\ 0 & 0 & \dots & 0 & a_i & 1 \\ 0 & 0 & \dots & 0 & 0 & a_i \end{pmatrix}.$$

(We do not ask that the a_i’s are two-by-two distinct here. But we can bring together the blocks having the same a_i; this will be the case in Theorem 8.8.)

The procedure to find an invertible matrix C such that $C^{-1}MC$ has the Jordan form is called Jordan reduction. *We also call* Jordan reduction *the procedure (to present) to find a basis S such that $M_{S,S}(\varphi)$ has the Jordan form (for an endomorphism φ). It may also happen that we call the obtained matrix* Jordan reduction of M or of φ.

Example 8.6. *We reconsider the matrices of Example 6.4.*

- *The matrices $M_1 := \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$, $M_2 := \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ have the Jordan form, but not $M_3 := \left(\begin{smallmatrix} 1 & 691 \\ 0 & 1 \end{smallmatrix}\right)$ (its Jordan reduction is M_2).*

- *The matrices*

$$M_4 := \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, M_5 := \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, M_6 := \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$$

  also have the Jordan form.

- *The/one Jordan reduction of the matrix $\begin{pmatrix} 1 & 2 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 5 \end{pmatrix}$ obtained in Example 7.5(a) by the spectral decomposition is $\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 5 \end{pmatrix}$ (explained later).*

Be careful: with our definitions, there exist matrices that do not have a Jordan reduction (except if one works over $\mathbb{C}$, but not over $\mathbb{R}$); we can weaken the requirements to have a Jordan reduction for any matrix; we will not continue this in this lecture course for time reasons. In the exercises, you will see some steps to the general case.

We now present the algorithm of Jordan's reduction. For this we set:

- $\varphi_a := \varphi - a \cdot \mathrm{id}$,

- $V_i = \ker(\varphi_a^i)$

For the moment, we make the hypothesis

$$\mathrm{mipo}_{\varphi}(X) = (X - a)^e.$$

From this we obtain

$$V = V_e \supset V_{e-1} \supset V_{e-2} \supset \cdots \supset V_1 = E_{\varphi}(a) \supset V_0 = 0.$$

We can imagine the vector space V as being in a rectangular box:

$$\begin{array}{r||cccccccc}
V_e \setminus V_{e-1} & \blacksquare & & & & & & & \blacksquare \\
V_{e-1} \setminus V_{e-2} & & \blacksquare & \blacksquare & \blacksquare & & & & \\
V_{e-2} \setminus V_{e-3} & \blacksquare & & \blacksquare & \blacksquare & \blacksquare & & & \\
\vdots & & & & & & & & \\
V_2 \setminus V_1 & & \blacksquare & \blacksquare & & \blacksquare & \blacksquare & & \blacksquare \\
V_1 & \blacksquare & \blacksquare & \blacksquare & \blacksquare & \blacksquare & \blacksquare & \blacksquare & \blacksquare
\end{array}$$

Each black block represents a non-zero vector, and the set of all the vectors in the diagram is linearly independent. In the algorithm, we want to order the rectangular box. For the moment, we put the black blocks in an arbitrary way to indicate that we do not yet have many information about its vectors (there is no deep meaning in the image). The fact that there are two blocks in the first row means that $\dim V_e - \dim V_{e-1} = 2$, etc. We can observe that the number of blocks does not decrease when moving from the top to the bottom.

(1.) We choose a vector $x_1 \in V_e \setminus V_{e-1}$. Then we have the non-zero vectors $\varphi_a(x_1) \in V_{e-1}$, $\varphi_a^2(x_1) \in V_{e-2}$, and more generally, $\varphi_a^i(x_1) \in V_{e-i}$ pour $i = 0, \dots, e-1$. We modify the image:

$$\begin{array}{r||cccccccc}
V_e \setminus V_{e-1} & x_1 & & & & & & & \blacksquare \\
V_{e-1} \setminus V_{e-2} & \varphi_a(x_1) & & \blacksquare & \blacksquare & & & & \\
V_{e-2} \setminus V_{e-3} & \varphi_a^2(x_1) & & \blacksquare & \blacksquare & \blacksquare & & & \\
\vdots & & & & & & & & \\
V_2 \setminus V_1 & \varphi_a^{e-2}(x_1) & \blacksquare & & & \blacksquare & \blacksquare & & \blacksquare \\
V_1 & \varphi_a^{e-1}(x_1) & \blacksquare & \blacksquare & \blacksquare & \blacksquare & \blacksquare & \blacksquare & \blacksquare
\end{array}$$

The first column hence contains a basis of $\langle x_1 \rangle_\varphi$.

If $\langle x_1 \rangle_\varphi = V$ (if no black block remains), we are done. Otherwise, we continue.

(2.) Now we compute the integer k such that $\langle x_1 \rangle_\varphi + V_k = V$, but $\langle x_1 \rangle_\varphi + V_{k-1} \neq V$. In our example, $k = e$.

We choose a vector x_2 in $V_k \setminus (\langle x_1 \rangle_\varphi + V_{k-1})$. We thus have the non-zero vectors $\varphi_a^i(x_2) \in V_{k-i}$ for $i = 0, \dots, k-1$. We change the image:

$$\begin{array}{r||cccccccc}
V_e \setminus V_{e-1} & x_1 & x_2 & & & & & & \\
V_{e-1} \setminus V_{e-2} & \varphi_a(x_1) & \varphi_a(x_2) & \blacksquare & & & & & \\
V_{e-2} \setminus V_{e-3} & \varphi_a^2(x_1) & \varphi_a^2(x_2) & \blacksquare & & \blacksquare & & & \\
\vdots & & & & & & & & \\
V_2 \setminus V_1 & \varphi_a^{e-2}(x_1) & \varphi_a^{e-2}(x_2) & & \blacksquare & \blacksquare & & \blacksquare & \\
V_1 & \varphi_a^{e-1}(x_1) & \varphi_a^{e-1}(x_2) & \blacksquare & \blacksquare & \blacksquare & \blacksquare & \blacksquare & \blacksquare
\end{array}$$

The second column hence contains a basis of $\langle x_2 \rangle_\varphi$. Lemma 8.7 tells us that the sum $\langle x_1 \rangle_\varphi + \langle x_2 \rangle_\varphi$ is direct.

If $\langle x_1 \rangle_\varphi \oplus \langle x_2 \rangle_\varphi = V$ (if no black block relains), we are done. Otherwise, we continue.

(3.) Now we compute the integer k such that $\langle x_1\rangle_\varphi \oplus \langle x_2\rangle_\varphi + V_k = V$, but $\langle x_1\rangle_\varphi \oplus \langle x_2\rangle_\varphi + V_{k-1} \neq V$. In our example, $k = e-1$.

We choose a vector x_3 in $V_k \setminus (\langle x_1\rangle_\varphi \oplus \langle x_2\rangle_\varphi + V_{k-1})$. We thus have the non-zero vectors $\varphi_a^i(x_3) \in V_{k-i}$ for $i = 0, \dots, k-1$. We change the image:

$$\begin{array}{r||cccccccc}
V_e \setminus V_{e-1} & x_1 & x_2 & & & & & & \\
V_{e-1} \setminus V_{e-2} & \varphi_a(x_1) & \varphi_a(x_2) & x_3 & & & & & \\
V_{e-2} \setminus V_{e-3} & \varphi_a^2(x_1) & \varphi_a^2(x_2) & \varphi_a(x_3) & & \blacksquare & & & \\
\vdots & & & & & & & & \\
V_2 \setminus V_1 & \varphi_a^{e-2}(x_1) & \varphi_a^{e-2}(x_2) & \varphi_a^{e-3}(x_3) & & \blacksquare & & \blacksquare & \\
V_1 & \varphi_a^{e-1}(x_1) & \varphi_a^{e-1}(x_2) & \varphi_a^{e-2}(x_3) & \blacksquare & \blacksquare & \blacksquare & \blacksquare & \blacksquare
\end{array}$$

The third column thus contains a basis of $\langle x_3\rangle_\varphi$. Lemma 8.7 tells us that the sum $\langle x_1\rangle_\varphi \oplus \langle x_2\rangle_\varphi + \langle x_3\rangle_\varphi$ is direct.

If $\langle x_1\rangle_\varphi \oplus \langle x_2\rangle_\varphi \oplus \langle x_3\rangle_\varphi = V$ (if no black block relains), we are done. Otherwise, we continue.

(...) We continue like this until no black block remains. In our example, we obtain the image:

$$\begin{array}{r||cccccccc}
V_e \setminus V_{e-1} & x_1 & x_2 & & & & & & \\
V_{e-1} \setminus V_{e-2} & \varphi_a(x_1) & \varphi_a(x_2) & x_3 & & & & & \\
V_{e-2} \setminus V_{e-3} & \varphi_a^2(x_1) & \varphi_a^2(x_2) & \varphi_a(x_3) & x_4 & & & & \\
\vdots & & & & & & & & \\
V_2 \setminus V_1 & \varphi_a^{e-2}(x_1) & \varphi_a^{e-2}(x_2) & \varphi_a^{e-3}(x_3) & \varphi_a^{e-4}(x_4) & x_5 & & & \\
V_1 & \varphi_a^{e-1}(x_1) & \varphi_a^{e-1}(x_2) & \varphi_a^{e-2}(x_3) & \varphi_a^{e-3}(x_4) & \varphi_a(x_5) & x_6 & x_7 & x_8
\end{array}$$

Each column contains a basis of $\langle x_i\rangle_\varphi$ and corresponds to a block. More precisely, we put the vectors that are contained in a box into a basis S, beginning in the left-bottom corner, then we go up through the first colums, then we start at the bottom of the second column and goes up, then the third column from bottom to top, etc. Then, $M_{S,S}(\varphi)$ will be a block matrix. Each block has a on the main diagonal and 1 on the diagonal above the main diagonal. Each column corresponds to a block, and the size of the block is given by the height of the column. In our example, we thus have 8 blocks, two of size e, one of size $e-1$, one of size $e-2$, one of size 2 and three of size 1.

In order to justify the algorithm, we still need to prove the following lemma.

Lemma 8.7. *Let $L = \langle x_1\rangle_\varphi \oplus \langle x_2\rangle_\varphi \oplus \cdots \oplus \langle x_i\rangle_\varphi$ constructed in the previous algorithm. By the algorithm, we have in particular*

$$\dim_K \langle x_1\rangle_\varphi \geq \dim_K \langle x_2\rangle_\varphi \geq \cdots \geq \dim_K \langle x_i\rangle_\varphi.$$

(The dimension is here equal to the height of the corresponding column.)
Let k be the integer such that $L + V_k = V$ and $L + V_{k-1} \neq V$. We have $V_k \nsubseteq L + V_{k-1}$.
By the algorithm, we also have $k \leq \dim_K \langle x_i\rangle_\varphi$.
If $y \in V_k \setminus (L + V_{k-1})$ is any vector, then the sum $L + \langle y\rangle_\varphi$ is direct.

Proof. If $V_k \subseteq L + V_{k-1}$, then $V_k + L = V_{k-1} + L$ (as $V_{k-1} \subseteq V_k$). This implies the first statement: $V_k \nsubseteq L + V_{k-1}$.
Let us now show that the sum $L + \langle y \rangle_\varphi$ is direct, i.e., $L \cap \langle y \rangle_\varphi = 0$. Let $w \in L \cap \langle y \rangle_\varphi$. We suppose $w \neq 0$. Let j be the maximum such that $w \in V_{k-j}$. We have $0 \le j \le k-1$. Consequently, we can write $w = \sum_{q=0}^{k-1-j} c_q \varphi_a^{q+j}(y)$ for $c_q \in K$ with $c_0 \neq 0$. Hence

$$w = \varphi_a^j\big(c_0 y + \sum_{q=1}^{k-j-1} c_q \varphi_a^q(y)\big).$$

By construction of L, we can write

$$w = \varphi_a^j(\ell)$$

for $\ell \in L$. This is the case since $L \cap V_{k-j}$ is generated by $\varphi_a^{e_m}(x_m)$ for $1 \le m \le i$ and $j \le e_m = \dim_K \langle x_m \rangle_\varphi - (k-j)$.
Thus we obtain

$$0 = \varphi_a^j\big(c_0 y - \ell + \sum_{q=1}^{k-j-1} c_q \varphi_a^q(y)\big).$$

This implies

$$z := c_0 y - \ell + \sum_{q=1}^{k-j-1} c_q \varphi_a^q(y) \in V_j \subseteq V_{k-1}.$$

Using that $\sum_{q=1}^{k-j-1} c_q \varphi_a^q(y) \in V_{k-1}$, we finally obtain

$$y = \frac{1}{c_0}\ell + \frac{1}{c_0} z + \frac{1}{c_0} \sum_{q=1}^{k-j-1} c_q \varphi_a^q(y) \in L + V_{k-1},$$

a contradiction. Therefore $w = 0$. □

Combining the spectral decomposition with the algorithm above, we finally obtain the theorem about Jordan's reduction.

Theorem 8.8 (Jordan's reduction)**.** *Assume that the minimal polynomial of φ is equal to*

$$\mathrm{mipo}_\varphi(X) = \prod_{i=1}^{r} (X - a_i)^{e_i}$$

with different $a_i \in K$ and $e_i > 0$ (this is always the case if K is "algebraically closed" (see Algebra 3), e.g. $K = \mathbb{C}$).

Then, φ has a Jordan reduction.

We can precisely describe the Jordan reduction, as follows. Computing $V_i := \ker\big((\varphi - a_i \cdot \mathrm{id})^{e_i}\big)$, we obtain the spectral decomposition *(see Theorem 7.3), i.e.:*

$$V = \bigoplus_{i=1}^{r} V_i \quad \text{and} \quad \varphi(V_i) \subseteq V_i \text{ for all } 1 \le i \le r.$$

For all $1 \leq i \leq r$, we apply the above algorithm to construct $x_{i,1}, \dots, x_{i,s_i} \in V_i$ such that

$$V_i = \langle x_{i,1} \rangle_\varphi \oplus \cdots \oplus \langle x_{i,s_i} \rangle_\varphi \quad \text{et} \quad \varphi(\langle x_{i,j} \rangle_\varphi) \subseteq \langle x_{i,j} \rangle_\varphi.$$

Let $e_{i,j}$ the minimal positive integer such that $(\varphi - a_i \cdot \mathrm{id})^{e_{i,j}}(x_{i,j}) = 0$ for all $1 \leq i \leq r$ and $1 \leq j \leq s_i$.

For each space $\langle x_{i,j} \rangle_\varphi$ we choose the basis $S_{i,j}$ as in Lemma 8.4. We put

$$S := S_{1,1} \cup S_{1,2} \cup \cdots \cup S_{1,s_1} \cup S_{2,1} \cup S_{2,2} \cup \cdots \cup S_{2,s_2} \cup \ldots \ldots \cdots \cup S_{r,s_r}.$$

Then, S is a K-basis of V such that

$$M_{S,S}(\varphi) = \begin{pmatrix} \boxed{M_1} & \boxed{0} & \boxed{0} & \dots & \boxed{0} \\ \boxed{0} & \boxed{M_2} & \boxed{0} & \dots & \boxed{0} \\ \vdots & & \ddots & \ddots & \vdots \\ \boxed{0} & \dots & \boxed{0} & \boxed{M_{r-1}} & \boxed{0} \\ \boxed{0} & \dots & \boxed{0} & \boxed{0} & \boxed{M_r} \end{pmatrix}$$

(diagonal block matrix), where, for all $1 \leq i \leq r$,

$$M_i = \begin{pmatrix} \boxed{N_{i,1}} & \boxed{0} & \boxed{0} & \dots & \boxed{0} \\ \boxed{0} & \boxed{N_{i,2}} & \boxed{0} & \dots & \boxed{0} \\ \vdots & & \ddots & \ddots & \vdots \\ \boxed{0} & \dots & \boxed{0} & \boxed{N_{i,s_i-1}} & \boxed{0} \\ \boxed{0} & \dots & \boxed{0} & \boxed{0} & \boxed{N_{i,s_i}} \end{pmatrix}$$

(diagonal block matrix), where, for all $1 \leq j \leq s_i$,

$$N_{i,j} = \begin{pmatrix} a_i & 1 & 0 & 0 & \dots & 0 \\ 0 & a_i & 1 & 0 & \dots & 0 \\ 0 & 0 & \ddots & \ddots & \ddots & \vdots \\ \vdots & \vdots & \ddots & \ddots & 1 & 0 \\ 0 & 0 & \dots & 0 & a_i & 1 \\ 0 & 0 & \dots & 0 & 0 & a_i \end{pmatrix},$$

which is of size $e_{i,j}$. The $N_{i,j}$'s are called the Jordan blocks *(for the eigenvalue a_i).*

Remark 8.9. *Explicitely, the basis S is the following:*

$$\begin{array}{ccccc}
(\varphi - a_1 \cdot \mathrm{id})^{e_{1,1}-1}(x_{1,1}), & (\varphi - a_1 \cdot \mathrm{id})^{e_{1,1}-2}(x_{1,1}), & \dots & (\varphi - a_1 \cdot \mathrm{id})(x_{1,1}), & x_{1,1}, \\
(\varphi - a_1 \cdot \mathrm{id})^{e_{1,2}-1}(x_{1,2}), & (\varphi - a_1 \cdot \mathrm{id})^{e_{1,2}-2}(x_{1,2}), & \dots & (\varphi - a_1 \cdot \mathrm{id})(x_{1,2}), & x_{1,2}, \\
\vdots & \vdots & \vdots & \vdots & \vdots \\
(\varphi - a_1 \cdot \mathrm{id})^{e_{1,s_1}-1}(x_{1,s_1}), & (\varphi - a_1 \cdot \mathrm{id})^{e_{1,s_1}-2}(x_{1,s_1}), & \dots & (\varphi - a_1 \cdot \mathrm{id})(x_{1,s_1}), & x_{1,s_1}, \\
(\varphi - a_2 \cdot \mathrm{id})^{e_{2,1}-1}(x_{2,1}), & (\varphi - a_2 \cdot \mathrm{id})^{e_{2,1}-2}(x_{2,1}), & \dots & (\varphi - a_2 \cdot \mathrm{id})(x_{2,1}), & x_{2,1}, \\
(\varphi - a_2 \cdot \mathrm{id})^{e_{2,2}-1}(x_{2,2}), & (\varphi - a_2 \cdot \mathrm{id})^{e_{2,2}-2}(x_{2,2}), & \dots & (\varphi - a_2 \cdot \mathrm{id})(x_{2,2}), & x_{2,2}, \\
\vdots & \vdots & \vdots & \vdots & \vdots \\
(\varphi - a_2 \cdot \mathrm{id})^{e_{2,s_2}-1}(x_{2,s_2}), & (\varphi - a_2 \cdot \mathrm{id})^{e_{2,s_2}-2}(x_{2,s_2}), & \dots & (\varphi - a_2 \cdot \mathrm{id})(x_{2,s_2}), & x_{2,s_2}, \\
(\varphi - a_3 \cdot \mathrm{id})^{e_{3,1}-1}(x_{3,1}), & (\varphi - a_3 \cdot \mathrm{id})^{e_{3,1}-2}(x_{3,1}), & \dots & (\varphi - a_3 \cdot \mathrm{id})(x_{3,1}), & x_{3,1}, \\
\vdots & \vdots & \vdots & \vdots & \vdots \\
\vdots & \vdots & \vdots & \vdots & \vdots \\
(\varphi - a_r \cdot \mathrm{id})^{e_{r,s_r}-1}(x_{r,s_r}), & (\varphi - a_r \cdot \mathrm{id})^{e_{r,s_r}-2}(x_{r,s_r}), & \dots & (\varphi - a_r \cdot \mathrm{id})(x_{r,s_r}), & x_{r,s_r}
\end{array}.$$

Note that the Jordan reduction is not unique in general (we can for instance permute the blocks). Thus, to be precise, we would rather speak of a Jordan reduction, which we will sometimes do. If S is a basis such that $M_{S,S}(\varphi)$ has the form of the theorem, we will say that $M_{S,S}(\varphi)$ is *the/a Jordan reduction* or that it has *the/a Jordan form*.

To apply Theorem 8.8 to matrices, take a look (once again) at Remark 7.4.

Example 8.10. *(a) The/a Jordan reduction of the matrix* $\begin{pmatrix} 1 & 2 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 5 \end{pmatrix}$ *obtained by the spectral decomposition in Example 7.5(a) is* $\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 5 \end{pmatrix}$ *for the following reason.*

The matrix satisfies the hypothesis of Theorem 8.8, thus it has a Jordan reduction. As it is not diagonalizable, there can only be one block with 1 *on the diagonal, but the characteristic polynomial shows that* 1 *has to appear twice on the diagonal. Therefore, there is no other possibility.*

(b) Consider the matrix $M := \begin{pmatrix} 1 & 1 & 0 \\ -1 & 3 & 0 \\ -1 & 1 & 2 \end{pmatrix}$ *with coefficients in* $\mathbb{R}$.

A computation shows that $\mathrm{charpoly}_M(X) = (X-2)^3$. *Then,* $r = 1$ *in the notations of Theorem 8.8 and, hence, the Jordan reduction has to be among the following three matrices:*

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

We easily find that $\mathrm{mipo}_M(X) = (X-2)^2$*. From this we can already deduce that the Jordan reduction is* $\begin{pmatrix} 2 & 1 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 2 \end{pmatrix}$.

The question becomes unpleasant if one asks to compute a matrix C *such that* $C^{-1}MC = \begin{pmatrix} 2 & 1 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 2 \end{pmatrix}$*. But this is not so hard. We follow the algorithm on Jordan's reduction:*

- *We have* $M - 2\mathrm{id}_3 = \begin{pmatrix} -1 & 1 & 0 \\ -1 & 1 & 0 \\ -1 & 1 & 0 \end{pmatrix}$.
- *Then,* $\ker(M - 2\mathrm{id}_3) = \langle \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix} \rangle$.
- *We have that* $\mathrm{mipo}_M(X) = (X-2)^2$ *(which is easily verified:* $(M - 2 \cdot \mathrm{id}_3)^2 = 0_3$*). According to the algorithm, we choose*

  $$x_1 \in \ker((M - 2\mathrm{id}_3)^2) \setminus \ker(M - 2\mathrm{id}_3) = \mathbb{R}^3 \setminus \langle \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix} \rangle,$$

  for instance $x_1 = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$.
- *We start writing our basis* S*. The first vector of the basis is, according to the algorithm,*

  $$v_1 := (M - 2\mathrm{id}_3)x_1 = \begin{pmatrix} -1 & 1 & 0 \\ -1 & 1 & 0 \\ -1 & 1 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} -1 \\ -1 \\ -1 \end{pmatrix}$$

  and the second one is just $v_2 := x_1$.
- *In the second step, we have to choose a vector*

  $$y \in \ker(M - 2\mathrm{id}_3) \setminus \langle v_1, v_2 \rangle = \langle \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix} \rangle \setminus \langle \begin{pmatrix} -1 \\ -1 \\ -1 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} \rangle.$$

  We choose $y = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}$ *and we immediately set* $v_3 = y$.
- *It suffices to write the vectors* v_1, v_2, v_3 *as columns of a matrix:*

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

Theorem 8.8 tells us that

$$C^{-1}MC = \begin{pmatrix} 0 & -1 & 0 \\ 1 & -1 & 0 \\ 0 & -1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 & 0 \\ -1 & 3 & 0 \\ -1 & 1 & 2 \end{pmatrix} \begin{pmatrix} -1 & 1 & 0 \\ -1 & 0 & 0 \\ -1 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 1 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 2 \end{pmatrix},$$

which can be verified.

Remark 8.11. *In some examples and exercises you saw/see that the knowledge of the minimal polynomial already gives us many information about the Jordan reduction.*
More precisely, if a is an eigenvalue of φ and $(X-a)^e$ is the biggest power of $X-a$ dividing the minimal polynomial $\mathrm{mipo}_\varphi(X)$, then the size of the largest Jordan block with a on the diagonal is e.
In general, we do not obtain the entire Jordan reduction following this method; if, for instance, $(X-a)^{e+2}$ is the biggest power of $X-a$ dividing $\mathrm{charpoly}_\varphi(X)$, then, we have two possibilities: (1) there are two Jordan blocks for the eigenvalue a of size e and 2; or (2) there are three Jordan blocks for a of size e, 1 and 1.

Example 8.12. *We do an example. Let*

$$M = \begin{pmatrix} -2 & -1 & -5 & -3 & 6 & -4 \\ -1 & 2 & -1 & -1 & 1 & 0 \\ 2 & 1 & 4 & 2 & -2 & 1 \\ 4 & 2 & 4 & 6 & -5 & 2 \\ 0 & 1 & -1 & 1 & 3 & -1 \\ 1 & -1 & 1 & 0 & -1 & 5 \end{pmatrix}.$$

Its characteristic polynomial is

$$\mathrm{charpoly}_M(X) = X^6 - 18X^5 + 135X^4 - 540X^3 + 1215X^2 - 1458X + 729 = (X-3)^6.$$

Let us first compute

$$M_3 := M + 3\mathrm{id} = \begin{pmatrix} -5 & -1 & -5 & -3 & 6 & -4 \\ -1 & -1 & -1 & -1 & 1 & 0 \\ 2 & 1 & 1 & 2 & -2 & 1 \\ 4 & 2 & 4 & 3 & -5 & 2 \\ 0 & 1 & -1 & 1 & 0 & -1 \\ 1 & -1 & 1 & 0 & -1 & 2 \end{pmatrix},$$

then

$$M_3^2 = \begin{pmatrix} 0 & 5 & -1 & 3 & -2 & -5 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & -1 & 1 & -1 & 0 & 1 \\ 0 & -3 & 1 & -2 & 1 & 3 \\ 0 & 1 & 1 & 0 & -1 & -1 \\ 0 & -2 & 0 & -1 & 1 & 2 \end{pmatrix}, \quad M_3^3 = \begin{pmatrix} 0 & 3 & 3 & 0 & -3 & -3 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & -1 & -1 & 0 & 1 & 1 \\ 0 & -2 & -2 & 0 & 2 & 2 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & -1 & -1 & 0 & 1 & 1 \end{pmatrix}, \quad M_3^4 = 0.$$

We thus have

$$\mathrm{mipo}_M(X) = (X-3)^4$$

and

$$V_4 = \ker(M_3^4) = \mathbb{R}^6 \supsetneq V_3 \supsetneq V_2 \supsetneq V_1 = E_M(3) \supsetneq 0.$$

We first compute

$$V_3 = \ker(M_3^3) = \ker \begin{pmatrix} 0 & 1 & 1 & 0 & -1 & -1 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix} = \langle \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ -1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ -1 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} \rangle.$$

In fact, it is not necessary for the algorithm to give an entire basis of V_3, it suffices to find a vector that does not belong to the kernel. It is very easy. We will take $x_1 = \left(\begin{smallmatrix} 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{smallmatrix}\right)$ and we compute

$$x_1 = \left(\begin{smallmatrix} 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{smallmatrix}\right), M_3x_1 = \left(\begin{smallmatrix} -1 \\ -1 \\ 1 \\ 2 \\ 1 \\ -1 \end{smallmatrix}\right), M_3^2x_1 = \left(\begin{smallmatrix} 5 \\ 0 \\ -1 \\ -3 \\ 1 \\ -2 \end{smallmatrix}\right), M_3^3x_1 = \left(\begin{smallmatrix} 3 \\ 0 \\ -1 \\ -2 \\ 0 \\ -1 \end{smallmatrix}\right).$$

We thus already have a Jordan block of size 4. Thus there is either a block of size 2, or two blocks of size 1. We now compute

$$V_2 = \ker(M_3^2) = \ker \begin{pmatrix} 0 & 1 & 1 & 0 & -1 & -1 \\ 0 & 0 & -6 & 3 & 3 & 0 \\ 0 & 0 & 2 & -1 & -1 & 0 \\ 0 & 0 & 4 & -2 & -2 & 0 \\ 0 & 0 & 2 & -1 & -1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix} = \ker \begin{pmatrix} 0 & 1 & 1 & 0 & -1 & -1 \\ 0 & 0 & 1 & -1/2 & -1/2 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

$$= \ker \begin{pmatrix} 0 & 1 & 0 & 1/2 & -1/2 & -1 \\ 0 & 0 & 1 & -1/2 & -1/2 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix} = \langle \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 1/2 \\ 1/2 \\ 0 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ -1/2 \\ 1/2 \\ 1 \\ 0 \\ 0 \end{pmatrix} \rangle.$$

Finally, we compute the eigenspace for the eigenvalue 3*:*

$$V_1 = \ker(M_3) = \ker \begin{pmatrix} -5 & -1 & -5 & -3 & 6 & -4 \\ -1 & -1 & -1 & -1 & 1 & 0 \\ 2 & 1 & 1 & 2 & -2 & 1 \\ 4 & 2 & 4 & 3 & -5 & 2 \\ 0 & 1 & -1 & 1 & 0 & -1 \\ 1 & -1 & 1 & 0 & -1 & 2 \end{pmatrix} = \ker \begin{pmatrix} 1 & -1 & 1 & 0 & -1 & 2 \\ 0 & 1 & -1 & 1 & 0 & -1 \\ 0 & -6 & 0 & -3 & 1 & 6 \\ 0 & -2 & 0 & -1 & 0 & 2 \\ 0 & 3 & -1 & 2 & 0 & -3 \\ 0 & 6 & 0 & 3 & -1 & -6 \end{pmatrix}$$

$$= \ker \begin{pmatrix} 1 & 0 & 0 & 1 & -1 & 1 \\ 0 & 1 & -1 & 1 & 0 & -1 \\ 0 & 0 & -6 & 3 & 1 & 0 \\ 0 & 0 & -2 & 1 & 0 & 0 \\ 0 & 0 & 2 & -1 & 0 & 0 \\ 0 & 0 & 6 & -3 & -1 & 0 \end{pmatrix} = \ker \begin{pmatrix} 1 & 0 & 0 & 1 & -1 & 1 \\ 0 & 1 & -1 & 1 & 0 & -1 \\ 0 & 0 & 1 & -1/2 & 0 & 0 \\ 0 & 0 & -6 & 3 & 1 & 0 \\ 0 & 0 & 2 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

$$= \ker \begin{pmatrix} 1 & 0 & 0 & 1 & -1 & 1 \\ 0 & 1 & 0 & 1/2 & 0 & -1 \\ 0 & 0 & 1 & -1/2 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix} = \ker \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1/2 & 0 & -1 \\ 0 & 0 & 1 & -1/2 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix} = \langle \begin{pmatrix} -1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}, \begin{pmatrix} -1 \\ -1/2 \\ 1/2 \\ 1 \\ 0 \\ 0 \end{pmatrix} \rangle.$$

Thus there are 2 *eigenvectors, hence two blocks in total. Thus the second block is of size* 2*. We have to find a vector in* V_2 *which is not in* $V_1 + \langle x_1, M_3x_1, M_3^2x_1, M_3^3x_1 \rangle$*, thus an element of*

$$\langle \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 1/2 \\ 1/2 \\ 0 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ -1/2 \\ 1/2 \\ 1 \\ 0 \\ 0 \end{pmatrix} \rangle \setminus \langle \begin{pmatrix} -1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}, \begin{pmatrix} -1 \\ -1/2 \\ 1/2 \\ 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} -1 \\ -1 \\ 1 \\ 2 \\ 1 \\ -1 \end{pmatrix}, \begin{pmatrix} 5 \\ 0 \\ -1 \\ -3 \\ 1 \\ -2 \end{pmatrix}, \begin{pmatrix} 3 \\ 0 \\ -1 \\ -2 \\ 0 \\ -1 \end{pmatrix} \rangle.$$

To find such an element, we test if the vectors (one by one) of the basis of V_2 *are linearly independent form the space on the right. We are lucky that it already works out for* $x_2 := \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$ *(as one can see from a standard computation). We thus calculate*

$$x_2 = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \quad M_3x_2 = \begin{pmatrix} -5 \\ -1 \\ 2 \\ 4 \\ 0 \\ 1 \end{pmatrix}.$$

We can now write the matrix

$$C := \begin{pmatrix} 3 & 5 & -1 & 0 & -5 & 1 \\ 0 & 0 & -1 & 1 & -1 & 0 \\ -1 & -1 & 1 & 0 & 2 & 0 \\ -2 & -3 & 2 & 0 & 4 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 \\ -1 & -2 & -1 & 0 & 1 & 0 \end{pmatrix}$$

and a computation verifies

$$C^{-1}MC = \begin{pmatrix} 3 & 1 & 0 & 0 & 0 & 0 \\ 0 & 3 & 1 & 0 & 0 & 0 \\ 0 & 0 & 3 & 1 & 0 & 0 \\ 0 & 0 & 0 & 3 & 0 & 0 \\ 0 & 0 & 0 & 0 & 3 & 1 \\ 0 & 0 & 0 & 0 & 0 & 3 \end{pmatrix}.$$

Remark 8.13. *Here are some remarks that are easy to prove and can sometimes be useful for computations. Suppose* $\mathrm{mipo}_M(X) = (X-a)^e$.

(a) The size of the largest Jordan block is e.

(b) Each Jordan block contains an eigenspace of dimension 1 *for the eigenvalue* a.

(c) The number of Jordan blocks is equal to the dimension of the eigenspace for the eigenvalue a.

9 Hermitian spaces

Goals:

- Know the definitions of euclidian and hermitian spaces;
- know fundamental properties of euclidian and hermitian spaces;
- be able to compute orthonormal basis using the method of Gram-Schmidt;
- know examples and be able to prove simple properties.

We will start by a motivation of some of the topics that will follow.
Let $M \in \mathrm{Mat}_{n\times n}(K)$ be a matrix. Consider the application:

$$\langle\ ,\ \rangle_M : K^n \times K^n \to K, \quad \langle \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix}, \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{pmatrix} \rangle_M := (a_1 \ \ a_2 \ \ \cdots \ \ a_n) M \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{pmatrix}.$$

We thus have the equality

$$\langle x, y \rangle_M = x^{\mathrm{tr}} M y.$$

If M is the identity, then

$$\langle \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix}, \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{pmatrix} \rangle = (a_1 \ \ a_2 \ \ \cdots \ \ a_n) \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{pmatrix} = \sum_{i=1}^{n} a_i b_i.$$

This is the well-known canonical scalar product. This gives moreover (if $K = \mathbb{R}$)

$$\langle \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix}, \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix} \rangle = a_1^2 + a_2^2 + \cdots + a_n^2 > 0$$

for all $\begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix} \neq 0$.

Let us treat another example: $M = \left(\begin{smallmatrix} 1 & 2 \\ 3 & 4 \end{smallmatrix}\right)$. Then

$$\langle \left(\begin{smallmatrix} a_1 \\ a_2 \end{smallmatrix}\right), \begin{pmatrix} b_1 \\ b_2 \end{pmatrix} \rangle = (a_1 \ \ a_2) \left(\begin{smallmatrix} 1 & 2 \\ 3 & 4 \end{smallmatrix}\right) \begin{pmatrix} b_1 \\ b_2 \end{pmatrix} = a_1 b_1 + 2a_1 b_2 + 3a_2 b_1 + 4a_2 b_2.$$

In general, we immediately observe the following properties:

(a) *Linearity in the first variable:* For all $y \in K^n$, the application

$$\langle \cdot, y \rangle_M : K^n \to K, \quad x \mapsto \langle x, y \rangle_M$$

is K-linear, i.e., for all $x_1, x_2 \in K^n$ and all $a \in K$, we have

$$\langle x_1 + a x_2, y \rangle_M = \langle x_1, y \rangle_M + a \langle x_2, y \rangle_M.$$

(b) *Linéarité dans la deuxière variable:* For all $x \in K^n$, the application

$$\langle x, \cdot \rangle_M : K^n \to K, \quad y \mapsto \langle x, y \rangle_M$$

is K-linear, i.e. for all $y_1, y_2 \in K^n$ and all $a \in K$, we have

$$\langle x, y_1 + a y_2 \rangle_M = \langle x, y_1 \rangle_M + a \langle x, y_2 \rangle_M.$$

Question: When do we have that $\langle \ , \ \rangle_M$ is symmetric, i.e., $\langle x, y \rangle_M = \langle y, x \rangle_M$ for all $x, y \in K^n$?
To see the answer to this question, choose $x = e_i$ as the i-th canonical vector and $y = e_j$. Then

$$\langle e_i, e_j \rangle_M = e_i^{\mathrm{tr}} M e_j = e_i (j\text{-th column of } M) = i\text{-th coeff. of } (j\text{-th column of } M) = m_{i,j}.$$

Hence, $\langle e_i, e_j \rangle_M = \langle e_j, e_i \rangle_M$ implies $m_{i,j} = m_{j,i}$ for all $1 \leq i, j \leq n$, in other words, M is symmetric $M = M^{\mathrm{tr}}$.
Conversely, let us start from a symmetric matrix $M = M^{\mathrm{tr}}$. We do a small, but elegant computation:

$$\langle x, y \rangle_M = x^{\mathrm{tr}} M y = (x^{\mathrm{tr}} M y)^{\mathrm{tr}} = y^{\mathrm{tr}} M^{\mathrm{tr}} (x^{\mathrm{tr}})^{\mathrm{tr}} = y^{\mathrm{tr}} M x = \langle y, x \rangle_M,$$

where we used that $x^{\mathrm{tr}} M y$ is a matrix of size 1, hence equal to its transpose, as well as the following lemma:

Lemma 9.1. *Let $M \in \mathrm{Mat}_{n,m}(K)$ and $N \in \mathrm{Mat}_{m,\ell}(K)$ be matrices. Then*

$$(M \cdot N)^{\mathrm{tr}} = N^{\mathrm{tr}} \cdot M^{\mathrm{tr}}.$$

Proof. Exercise. □

We thus obtained the equivalence:

$$\langle\ ,\ \rangle_M \text{ is symmetric} \Longleftrightarrow M \text{ is symmetric: } M = M^{\mathrm{tr}}.$$

Question: For $K = \mathbb{R}$, when do we have $\langle x, x\rangle_M \geq 0$ for all $x \in \mathbb{R}^n$?
We have seen that it is the case if M is the identity and $\langle\ ,\ \rangle$ is hence the canonical scalar product. We will come back to this question later.
For the moment, let us move to $K = \mathbb{C}$. We denote $\overline{z} = x - iy$ the complex conjugate $z = x + iy \in \mathbb{C}$ with $x = \mathrm{Re}(z)$ and $y = \mathrm{Im}(z)$.
For complex numbers, it is not true that $\sum_{i=1}^n z_i^2$ is greater than or equal to 0, in fact, this is even not a question that one may ask since z_i^2 is in general not a real number, hence asking if it is greater than zero is meaningless. On the other hand, the absolute value $z_i\overline{z_i} = |z_i|^2$ is always real and non-negative. Thus it is useful to change the definition in the case $K = \mathbb{C}$:

$$\langle\ ,\ \rangle_M : \mathbb{C}^n \times \mathbb{C}^n \to \mathbb{C}, \quad \langle x, y\rangle_M := x^{\mathrm{tr}} M \overline{y}$$

where $\overline{y}$ is the vector obtained when applying complex conjugation on all coefficients. Note that the definition is the same as the one given before if $K = \mathbb{R}$ since complex conjugation does not have an effect on real numbers.
With M being the identity, this gives

$$\langle \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix}, \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{pmatrix} \rangle = (a_1 \ \ a_2 \ \ \cdots \ \ a_n) \begin{pmatrix} \overline{b_1} \\ \overline{b_2} \\ \vdots \\ \overline{b_n} \end{pmatrix} = \sum_{i=1}^n a_i \overline{b_i}.$$

This is once more the well-known canonical scalar product. Moreover, we obtain

$$\langle \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix}, \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix} \rangle = |a_1|^2 + |a_2|^2 + \cdots + |a_n|^2 > 0$$

for all $\begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix} \neq 0$.
Let us look the following properties:

(a) *Linearity in the first variable:* Unchanged!

(b) *Sesqui-linearity in the second variable:* For all $x \in \mathbb{C}^n$, the application

$$\langle x, \cdot\rangle_M : K^n \to K, \quad y \mapsto \langle x, y\rangle_M$$

is sesqui-linear, i.e., for all $y_1, y_2 \in K^n$ and all $a \in K$, we have

$$\langle x, y_1 + ay_2\rangle_M = \langle x, y_1\rangle_M + \overline{a}\langle x, y_2\rangle_M.$$

By the same computations as above, we obtain the equivalence:

$$\langle x,y\rangle_M = \overline{\langle y,x\rangle_M} \text{ for all } x,y\in\mathbb{C}^n \Longleftrightarrow M=\overline{M^{\mathrm{tr}}}.$$

A matrix M such that $M=\overline{M^{\mathrm{tr}}}$ is called *hermitian*.
For the sequel of this section we set $K=\mathbb{R}$ or $K=\mathbb{C}$.

Definition 9.2. *Let V be a K-vector space. An application*

$$\langle\cdot,\cdot\rangle : V\times V\to K,\quad (v,w)\mapsto\langle v,w\rangle$$

is called herlitian form *if for all $v,v_1,v_2,w,w_1,w_2\in V$ and for all $a,b\in K$ we have*

- $\langle av_1+v_2,w\rangle = a\langle v_1,w\rangle+\langle v_2,w\rangle$ *(linearity in the first variable),*
- $\langle v,bw_1+w_2\rangle=\overline{b}\langle v,w_1\rangle+\langle v,w_2\rangle$ *(*sesqui-linearity *in the second variable) and*
- $\langle v,w\rangle=\overline{\langle w,v\rangle}$.

A hermitian form $\langle\cdot,\cdot\rangle$ is said to be positive *if*

- $\forall\, v\in V:\langle v,v\rangle\geq 0$. *(Note that $\langle v,v\rangle=\overline{\langle v,v\rangle}$, whence $\langle v,v\rangle\in\mathbb{R}$.)*

It is said to be positive definite *if*

- $\forall\, 0\neq v\in V:\langle v,v\rangle>0$.

A hermitian positive definite form is also called a scalar product.
We call hermitian space *any tuple $(V,\langle\cdot,\cdot\rangle)$ where $\langle\cdot,\cdot\rangle$ is a positive definite hermitian form.*

Remark 9.3. *Note that for $K=\mathbb{R}$ the last two conditions of the definition of a hermitian form read*

- $\langle v,bw_1+w_2\rangle=b\langle v,w_1\rangle+\langle v,w_2\rangle$ *(linearity in the second variable) and*
- $\forall\, v\in V\;\forall\, w\in W:\langle v,w\rangle=\langle w,v\rangle$.

We refer this to as a bilinear symmetric *form.*
In the literature, if $K=\mathbb{R}$, one rather uses the name euclidian space *in stead of hermitian space (which is often reserved for $K=\mathbb{C}$). Here, to simplify the terminology, we will always speak of hermitian spaces, even if $K=\mathbb{R}$.*

We have already seen the canonical scalar products for $\mathbb{R}^n$ and $\mathbb{C}^n$. Similar definitions can also be made in spaces of functions (of finite dimension):

Example 9.4. *(a) The canonical scalar product $\langle\ ,\ \rangle_M$ for M the identity is indeed a scalar product if $K=\mathbb{R}$ or $K=\mathbb{C}$.*

(b) Let $\mathcal{C}=\{f:[0,1]\to\mathbb{R}\mid f$ is continuoud $\}$ be the set of all continuous functions from $[0,1]$ to $\mathbb{R}$. It is an $\mathbb{R}$-vector space for $+$ and $\cdot$ defined pointwise. The application

$$\langle\cdot,\cdot\rangle:\mathcal{C}\times\mathcal{C}\to\mathbb{R},\quad\langle f,g\rangle=\int_0^1 f(x)g(x)dx$$

is a hermitian positive definite form.

(c) Let $\mathcal{C} = \{f : [0,1] \to \mathbb{C} \mid f$ is continuous $\}$ be the set of all continuous functions from $[0,1]$ to $\mathbb{C}$. It is a $\mathbb{C}$-vector space for $+$ and $\cdot$ defined pointwise. The application

$$\langle \cdot, \cdot \rangle : \mathcal{C} \times \mathcal{C} \to \mathbb{C}, \quad \langle f, g \rangle = \int_0^1 f(x)\overline{g(x)}dx$$

is a hermitian positive definite form.

Definition 9.5. *Let $(V, \langle \cdot, \cdot \rangle)$ be a hermitian K-space.*
We say that $v, w \in V$ are orthogonal $v \perp w$ *if $\langle v, w \rangle = 0$. Note: $v \perp w \Leftrightarrow w \perp v$.*
Let $W \leq V$ be a subspace. We say that $v \in V$ and W are orthogonal $v \perp W$ *if $v \perp w$ for all $w \in W$. Note: $v \perp W \Leftrightarrow W \perp v$ (with evident defintions).*
Let $U \leq V$ be another subspace. We say that U and W are orthogonal $U \perp W$ *if $U \perp w$ for all $w \in W$. Note: $U \perp W \Leftrightarrow W \perp U$.*
The orthogonal complement of W *is defined as*

$$W^{\perp} = \{v \in V \mid v \perp W\}.$$

The norm ("length") *of $v \in V$ is defined as $|v| := \sqrt{\langle v, v \rangle}$ and $|v - w|$ is said to be the* distance *between v and w.*

Proposition 9.6. *Let $(V, \langle \cdot, \cdot \rangle)$ be a hermitian K-space.*

(a) For all $v \in V$ we have $|v| \geq 0$ and $|v| = 0 \Leftrightarrow v = 0$.

(b) For all $v \in V$ and all $a \in K$ we have: $\underbrace{|a \cdot v|}_{|\cdot| \text{ in } V} = \underbrace{|a|}_{|\cdot| \text{ in } K} \cdot \underbrace{|v|}_{|\cdot| \text{ in } V}$.

*(c) For all $v, w \in V$ we have $\underbrace{|\langle v, w \rangle|}_{|\cdot| \text{ in } K} \leq \underbrace{|v|}_{|\cdot| \text{ in } V} \cdot \underbrace{|w|}_{|\cdot| \text{ in } V}$ (*Cauchy-Schwarz inequality *).*

*(d) For all $v, w \in V$ we have $\underbrace{|v + w|}_{|\cdot| \text{ in } V} \leq \underbrace{|v|}_{|\cdot| \text{ in } V} + \underbrace{|w|}_{|\cdot| \text{ in } V}$ (*triangular inequality*).*

Proof. (a) Defintion.
(b) $|a \cdot v|^2 = \langle a \cdot v, a \cdot v \rangle = a \cdot \overline{a} \cdot \langle v, v \rangle = |a|^2 \cdot |v|^2$.
(c) 1st case: $w = 0$. Then, $\langle v, w \rangle = \langle v, 0 \cdot w \rangle = 0\langle v, w \rangle = 0$, whence $|\langle v, w \rangle| = 0 = |v| \cdot |w|$.
2nd case: $w \neq 0$. Let $c := \frac{\langle v,w \rangle}{|w|^2}$. Then

$$\begin{aligned} 0 &\leq |w|^2 \cdot \langle v - c \cdot w, v - c \cdot w \rangle \\ &= |w|^2 \cdot \langle v, v \rangle - |w|^2 \cdot c \cdot \langle w, v \rangle - |w|^2 \cdot \overline{c} \cdot \langle v, w \rangle + |w|^2 \cdot c \cdot \overline{c} \cdot \langle w, w \rangle \\ &= |w|^2 \cdot |v|^2 - \underbrace{\langle v, w \rangle \cdot \langle w, v \rangle}_{=|\langle v,w \rangle|} - \underbrace{\overline{\langle v, w \rangle} \cdot \langle v, w \rangle + \langle v, w \rangle \cdot \overline{\langle v, w \rangle}}_{=0}. \end{aligned}$$

(d)

$$\begin{aligned}|v+w|^2 &= \langle v+w, v+w\rangle \\ &= \langle v,v\rangle + \langle v,w\rangle + \langle w,v\rangle + \langle w,w\rangle \\ &= |v|^2 + |w|^2 + \langle v,w\rangle + \overline{\langle v,w\rangle} \\ &= |v|^2 + |w|^2 + 2\cdot \mathrm{Re}(\langle v,w\rangle) \\ &\leq |v|^2 + |w|^2 + 2\cdot |\langle v,w\rangle| \\ &\leq |v|^2 + |w|^2 + 2\cdot |v|\cdot|w| \\ &= (|v|+|w|)^2.\end{aligned}$$

□

Proposition 9.7 (Pythagoras). *If $v \perp w$, then $|v+w|^2 = |v|^2 + |w|^2$.*

Proof. $|v+w|^2 = \langle v+w, v+w\rangle = \langle v,v\rangle + \langle w,w\rangle = |v|^2+|w|^2$. □

Note that any hermitian positive definite form is non-degenerate: if $\langle v,w\rangle = 0$ for all $w \in W$, then in particular $\langle v,v\rangle = |v|^2 = 0$, whence $v = 0$. The same argument also shows that $w = 0$ si $\langle v,w\rangle = 0$ for all $v \in V$.

Definition 9.8. *Let $(V, \langle\cdot,\cdot\rangle)$ be a hermitian K-space and $S = \{s_i \mid i \in I\}$ (with I a set, e.g., $S = \{s_1,\dots,s_n\}$ if $I = \{1,2,\dots,n\}$).*
We say that S is an orthogonal system *if*

- *$\langle s_i, s_i\rangle > 0$ for all $i \in I$ and*
- *$\langle s_i, s_j\rangle = 0$ for all $i,j \in I$, $i \neq j$.*

We say that S is an orthonormal system *if $\langle s_i, s_j\rangle = \delta_{i,j}$ pour tout $i,j \in I$.*
If S is a basis of V which is an orthogonal/orthonormal system, we speak of an orthogonal/orthonormal basis.

Example 9.9. *The canonical basis of $\mathbb{R}^n$ (or of $\mathbb{C}^n$) is an orthonormal basis for the canonical scalar product of Example 9.4.*

Proposition 9.10 (Gram-Schmidt Orthonormalization). *Let $(V, \langle\cdot,\cdot\rangle)$ be a hermitian K-space and $s_1, s_2, \dots, s_n \in V$ K-linearly independent vectors.*
The method of Gram-Schmidt *(see proof) computes the vectors $t_1, t_2, \dots, t_n \in V$ such that*

- *$\langle t_i, t_j\rangle = \delta_{i,j}$ for all $1 \leq i,j \leq n$ and*
- *$\langle s_1, s_2, \dots, s_r\rangle = \langle t_1, t_2, \dots, t_r\rangle$ for all $1 \leq r \leq n$ (in words: the subspaces of V generated by $s_1, s_2, \dots, s_r$ and by $t_1, t_2, \dots, t_r$ are equal for all $1 \leq r \leq n$).*

Proof. We present the method of Gram-Schmidt.
It is an induction on $r = 1, 2, \dots, n$; hence there are n steps.
$\underline{r=1.}$ $t_1 := \frac{s_1}{|s_1|}$.

$\underline{r \Rightarrow r+1.}$ By induction hypothesis we already have $t_1, \dots, t_r$ such that $\langle t_i, t_j \rangle = \delta_{i,j}$ for all $1 \leq i, j \leq r$ and $\langle s_1, s_2, \dots, s_r \rangle = \langle t_1, t_2, \dots, t_r \rangle$.
We have to find t_{r+1}. First we define

$$w_{r+1} := s_{r+1} - \sum_{i=1}^{r} \langle s_{r+1}, t_i \rangle t_i.$$

This vector satisfies for all $1 \leq j \leq r$

$$\begin{aligned}
\langle w_{r+1}, t_j \rangle &= \langle s_{r+1} - \sum_{i=1}^{r} \langle s_{r+1}, t_i \rangle t_i, t_j \rangle \\
&= \langle s_{r+1}, t_j \rangle - \sum_{i=1}^{r} \langle \langle s_{r+1}, t_i \rangle t_i, t_j \rangle \\
&= \langle s_{r+1}, t_j \rangle - \langle \langle s_{r+1}, t_j \rangle t_j, t_j \rangle \\
&= \langle s_{r+1}, t_j \rangle - \langle s_{r+1}, t_j \rangle \cdot \langle t_j, t_j \rangle \\
&= 0
\end{aligned}$$

Since $\langle s_1, s_2, \dots, s_r \rangle = \langle t_1, t_2, \dots, t_r \rangle$, we have $w_{r+1} \notin \langle t_1, t_2, \dots, t_r \rangle$, hence, in particular, $w_{r+1} \neq 0$. This allows us to define

$$t_{r+1} := \frac{w_{r+1}}{|w_{r+1}|}.$$

This vector clearly satisfies $\langle t_{r+1}, t_i \rangle = \delta_{r+1,i}$ for all $1 \leq i \leq r+1$ and $\langle s_1, s_2, \dots, s_r, s_{r+1} \rangle = \langle t_1, t_2, \dots, t_r, t_{r+1} \rangle$. □

Example 9.11. *We apply the method of Gram-Schmidt to the following vectors:*

$$s_1 = \begin{pmatrix} 1 \\ 1 \\ 0 \\ 1 \\ 0 \\ 1 \end{pmatrix}, s_2 = \begin{pmatrix} 1 \\ 3 \\ -2 \\ 3 \\ -2 \\ 5 \end{pmatrix}, s_3 = \begin{pmatrix} -1 \\ 5 \\ 2 \\ -3 \\ -6 \\ 3 \end{pmatrix}$$

sur $\mathbb{R}^6$ avec le produit scalaire canonique.

(1) *Let us compute the length of s_1:*

$$|s_1| = \sqrt{4} = 2.$$

Thus

$$t_1 = \frac{1}{2} s_1 = \begin{pmatrix} 1/2 \\ 1/2 \\ 0 \\ 1/2 \\ 0 \\ 1/2 \end{pmatrix}.$$

(2) *Let us now compute*

$$\langle s_2, t_1 \rangle = \langle \begin{pmatrix} 1 \\ 3 \\ -2 \\ 3 \\ -2 \\ 5 \end{pmatrix}, \begin{pmatrix} 1/2 \\ 1/2 \\ 0 \\ 1/2 \\ 0 \\ 1/2 \end{pmatrix} \rangle = 6.$$

Thus

$$w_2 := s_2 - \langle s_2, t_1 \rangle t_1 = \begin{pmatrix} 1 \\ 3 \\ -2 \\ 3 \\ -2 \\ 5 \end{pmatrix} - 6 \begin{pmatrix} 1/2 \\ 1/2 \\ 0 \\ 1/2 \\ 0 \\ 1/2 \end{pmatrix} = \begin{pmatrix} -2 \\ 0 \\ -2 \\ 0 \\ -2 \\ 2 \end{pmatrix}.$$

The length of w_2 is

$$|w_2| = \sqrt{16} = 4.$$

Donc

$$t_2 = \frac{1}{4} w_2 = \begin{pmatrix} -1/2 \\ 0 \\ -1/2 \\ 0 \\ -1/2 \\ 1/2 \end{pmatrix}.$$

(3) *Now compute*

$$\langle s_3, t_1 \rangle = \langle \begin{pmatrix} -1 \\ 5 \\ 2 \\ -3 \\ -6 \\ 3 \end{pmatrix}, \begin{pmatrix} 1/2 \\ 1/2 \\ 0 \\ 1/2 \\ 0 \\ 1/2 \end{pmatrix} \rangle = 2$$

and

$$\langle s_3, t_2 \rangle = \langle \begin{pmatrix} -1 \\ 5 \\ 2 \\ -3 \\ -6 \\ 3 \end{pmatrix}, \begin{pmatrix} -1/2 \\ 0 \\ -1/2 \\ 0 \\ -1/2 \\ 1/2 \end{pmatrix} \rangle = 4.$$

Thus

$$w_3 := s_3 - \langle s_3, t_1 \rangle t_1 - \langle s_3, t_2 \rangle t_2 = \begin{pmatrix} -1 \\ 5 \\ 2 \\ -3 \\ -6 \\ 3 \end{pmatrix} - 2 \begin{pmatrix} 1/2 \\ 1/2 \\ 0 \\ 1/2 \\ 0 \\ 1/2 \end{pmatrix} - 4 \begin{pmatrix} -1/2 \\ 0 \\ -1/2 \\ 0 \\ -1/2 \\ 1/2 \end{pmatrix} = \begin{pmatrix} 0 \\ 4 \\ 4 \\ -4 \\ -4 \\ 0 \end{pmatrix}.$$

The length of w_3 is

$$|w_3| = \sqrt{64} = 8.$$

Thus

$$t_3 = \frac{1}{8} w_3 = \begin{pmatrix} 0 \\ 1/2 \\ 1/2 \\ -1/2 \\ -1/2 \\ 0 \end{pmatrix}.$$

Corollary 9.12. *Let $(V, \langle \cdot, \cdot \rangle)$ be a hermitian K-space of finite dimension (or even countable). Then, V has an orthonormal K-basis.*

Proof. Direct consequence of Gram-Schmidt 9.10. □

Corollary 9.13. *Let $(V, \langle \cdot, \cdot \rangle)$ be a hermitian K-space and $W \leq V$ be a subspace of finite dimension. Let $s_1, \ldots, s_n \in W$ be an orthonormal K-basis of W (which exists in view of Corollary 9.12). We define*

$$\pi_W : V \to W, \quad v \mapsto \sum_{i=1}^{n} \langle v, s_i \rangle s_i.$$

This application is called the orthogonal projection on W.

(a) π_W *is* K*-linear and satisfies* $\pi_W \circ \pi_W = \pi_W$.

(b) $V = W \oplus W^{\perp}$.

(c) For all $v \in V$*, we have*

$$|\pi_W(v)|^2 = \sum_{i=1}^{n} |\langle v, s_i \rangle|^2 \leq |v|^2.$$

This is Bessel's inequality.

(d) For all $v \in V$*,* $\pi_W(v)$ *can be characterized as the unique* $w \in W$ *such that* $|v - w|$ *is minimal. The application* π_W *is therefore independent from the choice of the basis.*

Proof. (a) Simple computations.
(b) Let $v \in V$. We write $v = \pi_W(v) + (v - \pi_W(v))$. We clearly have $\pi_W(v) \in W$. Let us show that $v - \pi_W(v) \in W^{\perp}$; for this it suffices to prove that $\langle v - \pi_W(v), s_j \rangle = 0$ for all $1 \leq j \leq n$:

$$\langle v - \pi_W(v), s_j \rangle = \langle v, s_j \rangle - \langle \sum_{i=1}^{n} \langle v, s_i \rangle s_i, s_j \rangle = \langle v, s_j \rangle - \sum_{i=1}^{n} \langle v, s_i \rangle \cdot \langle s_i, s_j \rangle = \langle v, s_j \rangle - \langle v, s_j \rangle = 0.$$

This gives us $V = W + W^{\perp}$, thus it suffices to show that the sum is direct. Let $w \in W \cap W^{\perp}$. In particular, $w \perp w$, i.e., $\langle w, w \rangle = |w|^2 = 0$, whence $w = 0$.
(c) We have just seen that $\pi_W(v) \perp (v - \pi_W(v))$, hence by Pythagoras 9.7 we have

$$|v|^2 = |\pi_W(v)|^2 + |v - \pi_W(v)|^2,$$

whence $|\pi_W(v)|^2 \leq |v|^2$. This already proves the inequality. Let us now prove the equality:

$$|\pi_W(v)|^2 = \langle \pi_W(v), \pi_W(v) \rangle = \sum_{j=1}^{n} \sum_{k=1}^{n} \langle v, s_j \rangle \overline{\langle v, s_k \rangle} \langle s_j, s_k \rangle = \sum_{j=1}^{n} |\langle v, s_j \rangle|^2.$$

(d) We use again Pythagoras 9.7 to obtain for $w \in W$

$$|v - w|^2 = |\underbrace{(v - \pi_W(v))}_{\in W^{\perp}} + \underbrace{(\pi_W(v) - w)}_{\in W}|^2 = \underbrace{|v - \pi_W(v)|^2}_{\text{indépendant de } w} + |\pi_W(v) - w|^2.$$

Thus $|v - w|$ is minimal if and only if $|\pi_W(v) - w| = 0$, i.e. if and only if $w = \pi_W(v)$. □

10 Normal, adjoint, self-adjoint operators and isometries

Goals:

- Master the concepts of normal, adjoint and self-adjoint operators;
- master the notion of isometry and the notions of unitary and orthogonal matrix;
- know the fundamental properties of normal and self-adjoint operators and of isometries;

- be able to decide whether these notions are satisfied;
- know examples and be able to prove simple properties.

We continue with $K \in \{\mathbb{R}, \mathbb{C}\}$. In this section, we are interested in the question when in a hermitian space, a linear application is “ compatible” with the scalar product; more precisely, we would like to compare

$$\langle Mv, w\rangle, \langle Mv, Mw\rangle, \langle v, Mw\rangle, \text{ and } \langle v, w\rangle$$

where M is a matrix and v, w are vectors.
This will lead us to symmetric, hermitian, orthogonal, unitary matrices and isometries. We will prove later that any symmetric matrix with real coefficients is diagonalizable, and generalizations of this.
We make/recall the following definitions:

Definition 10.1. *(a) We call* symmetric matrix *or* self-adjoint matrix *any matrix $M \in \mathrm{Mat}_{n\times n}(\mathbb{R})$ such that $M^{\mathrm{tr}} = M$.*

(b) We call hermitian matrix *or* self-adjoint matrix *any matrix $M \in \mathrm{Mat}_{n\times n}(\mathbb{C})$ such that $M^{\mathrm{tr}} = \overline{M}$.*

Note that a symmetric matrix is nothing but a hermitian matrix with real coefficients.

(c) We call orthogonal matrix *or* isometry *any matrix $M \in \mathrm{Mat}_{n\times n}(\mathbb{R})$ such that $M^{\mathrm{tr}}M = \mathrm{id}$.*

(d) We call unitary matrix *or* isometry *any matrix $M \in \mathrm{Mat}_{n\times n}(\mathbb{C})$ such that $M^{\mathrm{tr}}\overline{M} = \mathrm{id}$.*

Note that an orthogonal matrix is nothing but a unitary matrix with real coefficients.

Definition 10.2. *We define the following matrix groups where the multiplication law is the composition of matrices:*

(a) $\mathrm{GL}_n(K) = \{M \in \mathrm{Mat}_{n\times n}(K) \mid \det(M) \neq 0\}$*, the* general linear group *over K,*

(b) $\mathrm{SL}_n(K) = \{M \in \mathrm{Mat}_{n\times n}(K) \mid \det(M) = 1\}$*, the* special linear group *over K,*

(c) $O_n = \{M \in \mathrm{GL}_n(\mathbb{R}) \mid M^{\mathrm{tr}}M = \mathrm{id}\}$*, the* orthogonal group*;*

(d) $\mathrm{SO}_n = \{M \in \mathrm{SL}_n(\mathbb{R}) \mid M^{\mathrm{tr}}M = \mathrm{id}\}$*, the* special orthogonal group,

(e) $U_n = \{M \in \mathrm{GL}_n(\mathbb{C}) \mid M^{\mathrm{tr}}\overline{M} = \mathrm{id}\}$*, the* unitary group,

(f) $\mathrm{SU}_n = \{M \in \mathrm{SL}_n(\mathbb{C}) \mid M^{\mathrm{tr}}\overline{M} = \mathrm{id}\}$*, the* special unitary group.

Lemma 10.3. *Let $M \in \mathrm{Mat}_{n\times n}(K)$ be a square matrix.*

(a) The following statements are equivalent:

(i) M is self-adjoint.

(ii) For all $v, w \in K^n$ we have: $v^{\mathrm{tr}}M^{\mathrm{tr}}\overline{w} = v^{\mathrm{tr}}\overline{M}\overline{w}$.
Note that in terms of scalar product, this statement can be rewritten as follows: $\langle Mv, w\rangle = \langle v, Mw\rangle$.

(b) The following statements are equivalent:

(i) M is an isometry.

(ii) For all $v, w \in K^n$ we have: $v^{\mathrm{tr}} M^{\mathrm{tr}} \overline{M} \overline{w} = v^{\mathrm{tr}} \overline{w}$.
Note that in terms of scalar product, this statement can be rewritten as follows: $\langle Mv, Mw \rangle = \langle v, w \rangle$.

Proof. We have proved part (a) in the beginning of section 9. The proof of part (b) is obtained using exactly the same arguments. More precisely, it is immediate in view of the formula $e_i^{\mathrm{tr}} M e_j = m_{i,j}$ for any square matrix $M = (m_{i,j})$. □

It is very easy to provide examples of symmetric or hermitian matrices (choose arbitrary real coefficients on the diagonal, write arbitrary real coefficients (or complew, depending on the situation) in the part below the main diagonal, fill the part above the main diagonal with the corresponding values).

Lemma 10.4. *Let $M \in \mathrm{Mat}_{n \times n}(K)$ be a square matrix. The following statements are equivalent:*

(i) M is an isometry (i.e. unitary or orthogonal);

(ii) the columns of M form an orthonormal basis of K^n (for the canonical scalar product);

(iii) the rows of M form an orthonormal basis of K^n (for the canonical scalar product).

Proof. By the definition of the multiplication of two matrices, statement (ii) is precisely the equality $M^{\mathrm{tr}} \overline{M} = \mathrm{id}$, hence (i). Statement (iii) is statement (ii) fot the matrix M^{tr}. Thus the equivalence between (iii) and (i) is the same as the equivalence

$$M^{\mathrm{tr}} \overline{M} = \mathrm{id} \Leftrightarrow M \overline{M^{\mathrm{tr}}} = \mathrm{id}.$$

Since in groups inverses are unique, the equality on the left hand side is equivalent to $\overline{M} M^{\mathrm{tr}} = \mathrm{id}$, and it suffices to apply complex conjugation to obtain the equality in the right hand side. □

Lemma 10.5. *We have*

$$O_2 = \{ \begin{pmatrix} \cos(\alpha) & -\sin(\alpha) \\ \sin(\alpha) & \cos(\alpha) \end{pmatrix} \in \mathrm{GL}_2(\mathbb{R}) \mid 0 \le \alpha < 2\pi \} \cup \{ \begin{pmatrix} \cos(\alpha) & \sin(\alpha) \\ \sin(\alpha) & -\cos(\alpha) \end{pmatrix} \in \mathrm{GL}_2(\mathbb{R}) \mid 0 \le \alpha < 2\pi \}.$$

Proof. First note that the $M = \begin{pmatrix} \cos(\alpha) & -\sin(\alpha) \\ \sin(\alpha) & \cos(\alpha) \end{pmatrix}$ is orthogonal:

$$M^{\mathrm{tr}} M = \begin{pmatrix} \cos(\alpha) & \sin(\alpha) \\ -\sin(\alpha) & \cos(\alpha) \end{pmatrix} \begin{pmatrix} \cos(\alpha) & -\sin(\alpha) \\ \sin(\alpha) & \cos(\alpha) \end{pmatrix} = \begin{pmatrix} \cos^2(\alpha)+\sin^2(\alpha) & 0 \\ 0 & \cos^2(\alpha)+\sin^2(\alpha) \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

The computation for the matrix $\begin{pmatrix} \cos(\alpha) & \sin(\alpha) \\ \sin(\alpha) & -\cos(\alpha) \end{pmatrix}$ is similar.
Let now $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ be an orthogonal matrix, i.e.

$$M^{\mathrm{tr}} M = \begin{pmatrix} a & c \\ b & d \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a^2+c^2 & ab+cd \\ ab+cd & b^2+d^2 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

From the equalities $a^2 + c^2 = 1$ and $b^2 + d^2 = 1$, we obtain $0 \le \alpha, \beta < 2\pi$ such that

$$a = \cos(\alpha), c = \sin(\alpha), d = \cos(\beta), b = \sin(\beta).$$

The equality $ab + cd = 0$ hence gives

$$0 = \cos(\alpha)\sin(\beta) + \sin(\alpha)\cos(\beta) = \sin(\alpha + \beta).$$

From this we conclude

$$\alpha + \beta = m\pi$$

for some $m \in \mathbb{Z}$. If m is even, we find:

$$\cos(\beta) = \cos(m - \alpha) = \cos(m)\cos(\alpha) + \sin(m)\sin(\alpha) = \cos(\alpha)$$

and

$$\sin(\beta) = \sin(m - \alpha) = \sin(m)\cos(\alpha) - \cos(m)\sin(\alpha) = -\sin(\alpha)$$

which gives

$$\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) = \left(\begin{smallmatrix} \cos(\alpha) & -\sin(\alpha) \\ \sin(\alpha) & \cos(\alpha) \end{smallmatrix}\right).$$

If m is odd, we find:

$$\cos(\beta) = \cos(m - \alpha) = \cos(m)\cos(\alpha) + \sin(m)\sin(\alpha) = -\cos(\alpha)$$

and

$$\sin(\beta) = \sin(m - \alpha) = \sin(m)\cos(\alpha) - \cos(m)\sin(\alpha) = +\sin(\alpha)$$

which gives

$$\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) = \left(\begin{smallmatrix} \cos(\alpha) & \sin(\alpha) \\ \sin(\alpha) & -\cos(\alpha) \end{smallmatrix}\right),$$

as desired. □

We now change the view point: in stead of matrices, we consider linear applications between hermitian spaces.

Proposition 10.6. *Let V and W be two hermitian K-spaces of dimensions n and m and let $\varphi : V \to W$ be a K-linear application.*

(a) There exists a unique K-linear application $\varphi^{\mathrm{ad}} : W \to V$ such that for all $v \in V$ and all $w \in W$

$$\langle \varphi(v), w \rangle = \langle v, \varphi^{\mathrm{ad}}(w) \rangle.$$

Note that the scalar product on the left is the one from W, and the scalar product on the right is the one from V.

The application φ^{ad} is called the adjoint of φ.

(b) Let S be an orthonormal K-basis of V and T be an orthonormal K-basis of W. Then

$$M_{S,T}(\varphi^{\mathrm{ad}}) = \overline{M_{T,S}(\varphi)^{\mathrm{tr}}}$$

(the matrix obtained from the transpose by complex conjugation).

If M is a matrix, we denote M^{ad} the matrix $\overline{M}^{\mathrm{tr}} = \overline{M^{\mathrm{tr}}}$ and call it the adjoint matrix. *Thus $M_{S,T}(\varphi^{\mathrm{ad}})$ is the adjoint matrix of $M_{T,S}(\varphi)$.*

Proof. Let $S = s_1, \dots, s_n$ and $T = t_1, \dots, t_m$ be the two orthonormal basis. Let

$$M_{T,S}(\varphi) = (a_{i,j})_{1 \le i \le m, 1 \le j \le n},$$

i.e. $\varphi(s_i) = \sum_{k=1}^m a_{k,i} t_k$. We will take (b) as definition of φ^{ad}: it is the K-linear application represented by $\overline{M_{T,S}(\varphi)^{\mathrm{tr}}}$. Concertely, we have $\varphi^{\mathrm{ad}}(t_j) = \sum_{k=1}^n \overline{a_{j,k}} s_k$.
We first verify:

$$\begin{aligned} \langle \varphi(s_i), t_j \rangle &= \langle \sum_{k=1}^m a_{k,i} t_k, t_j \rangle = \sum_{k=1}^m a_{k,i} \langle t_k, t_j \rangle &&= a_{j,i} \\ \langle s_i, \varphi^{\mathrm{ad}}(t_j) \rangle &= \langle s_i, \sum_{k=1}^n \overline{a_{j,k}} s_k \rangle = \sum_{k=1}^m a_{j,k} \langle s_i, s_k \rangle &&= a_{j,i} \end{aligned}$$

We can now obtain (a) by linearity: let $v = \sum_{i=1}^n b_i s_i$ and $w = \sum_{j=1}^m c_j t_j$; we have

$$\begin{aligned} \langle \varphi(v), w \rangle &= \langle \varphi(\sum_{i=1}^n b_i s_i), \sum_{j=1}^m c_j t_j \rangle \\ &= \langle \sum_{i=1}^n b_i \varphi(s_i), \sum_{j=1}^m c_j t_j \rangle \\ &= \sum_{i=1}^n b_i \sum_{j=1}^m \overline{c_j} \langle \varphi(s_i), t_j \rangle \\ &= \sum_{i=1}^n b_i \sum_{j=1}^m \overline{c_j} \langle s_i, \varphi^{\mathrm{ad}}(t_j) \rangle \\ &= \langle \sum_{i=1}^n b_i s_i, \sum_{j=1}^m c_j \varphi^{\mathrm{ad}}(t_j) \rangle \\ &= \langle \sum_{i=1}^n b_i s_i, \varphi^{\mathrm{ad}}(\sum_{j=1}^m c_j t_j) \rangle \\ &= \langle v, \varphi^{\mathrm{ad}}(w) \rangle. \end{aligned}$$

For the uniqueness of φ^{ad}, write $\varphi^{\mathrm{ad}}(t_j) = \sum_{k=1}^n d_{k,j} s_k$, and compute

$$a_{j,i} = \langle \varphi(s_i), t_j \rangle = \langle s_i, \varphi^{\mathrm{ad}}(t_j) \rangle = \langle s_i, \sum_{k=1}^n d_{k,j} s_k \rangle = \sum_{k=1}^n \overline{d_{k,j}} \langle s_i, s_k \rangle = \overline{d_{i,j}}.$$

We thus obtain $d_{i,j} = \overline{a_{j,i}}$, the uniqueness. □

Note that if $K = \mathbb{R}$, the adjoint of a matirx M is the transpose.

Proposition 10.7. *Let U, V, W be hermitian K-spcaes of finite dimensions and $U \xrightarrow{\varphi,\psi} V \xrightarrow{\eta} W$ be K-linear applications. Then:*

(a) $\mathrm{id}_V^{\mathrm{ad}} = \mathrm{id}_V$,

(b) $(\varphi+\psi)^{\mathrm{ad}} = \varphi^{\mathrm{ad}} + \psi^{\mathrm{ad}}$,

(c) $\forall\, x \in K : (x\varphi)^{\mathrm{ad}} = \overline{x}\varphi^{\mathrm{ad}}$,

(d) $(\eta \circ \varphi)^{\mathrm{ad}} = \varphi^{\mathrm{ad}} \circ \eta^{\mathrm{ad}}$ *and*

(e) $(\varphi^{\mathrm{ad}})^{\mathrm{ad}} = \varphi$.

The same statements hold for matrices.

Proof. The statements for matrices are easily verified. The only point where one needs to be careful is $(M \circ N)^{\mathrm{tr}} = N^{\mathrm{tr}} \circ M^{\mathrm{tr}}$, it is Lemma 9.1. □

Definition 10.8. *Let V be a hermitian K-space of finite dimension and let $\varphi : V \to V$ be a K-endomorphism.*
We say that φ is self-adjoint *if $\varphi = \varphi^{\mathrm{ad}}$.*

In view of Proposition 10.6, we thus have

$$\varphi \text{ is self-adjoint } \Leftrightarrow M_{S,S}(\varphi) \text{ is self-adjoint,}$$

for an orthonormal basis S of V.
For the proof of the next proposition, we need a small lemma.

Lemma 10.9. *Let $(V, \langle,\rangle)$ be a hermitian space. Then, if $v \perp V$ for $v \in V$, then $v = 0$.*

Proof. If $v \perp V$, we have in particular, $v \perp v$, whence $0 = \langle v, v\rangle = |v|^2$ which implies $v = 0$. □

Proposition 10.10. *Let V be a hermitian K-space of finite dimension and let $\varphi : V \to V$ be a K-endomorphism.*

(a) The following statements are equivalent.

(i) φ is self-adjoint ($\varphi = \varphi^{\mathrm{ad}}$).

(ii) $\langle v, w\rangle_\varphi := \langle \varphi(v), w\rangle$ for $v \in V$ and $w \in V$ is a hermitian form.

(b) If φ is self-adjoint then: $\varphi = 0 \Leftrightarrow \forall\, v \in V$: $\langle v, v\rangle_\varphi = 0$.

Proof. (a) It is always true (even if φ is not self-adjoint) that $\langle \cdot, \cdot\rangle_\varphi$ is linear in the first variable and sesquilinear in the second. One therefore has to check the third property in the definition of hermitian forms 9.2. Let $v, w \in V$. First we do the computation

$$\overline{\langle v, w\rangle_\varphi} = \overline{\langle \varphi(v), w\rangle} = \overline{\langle v, \varphi^{\mathrm{ad}}(w)\rangle} = \langle \varphi^{\mathrm{ad}}(w), v\rangle = \langle w, v\rangle_{\varphi^{\mathrm{ad}}}.$$

We thus have

$$\begin{aligned}
&\forall\, v, w \in V : \overline{\langle v, w\rangle_\varphi} = \langle w, v\rangle_\varphi \\
\Leftrightarrow &\forall\, v, w \in V : \langle \varphi^{\mathrm{ad}}(w), v\rangle = \langle \varphi(w), v\rangle \\
\Leftrightarrow &\forall\, v, w \in V : \langle (\varphi^{\mathrm{ad}} - \varphi)(w), v\rangle = 0 \\
\Leftrightarrow &\forall\, w \in V : (\varphi^{\mathrm{ad}} - \varphi)(w) \perp V = 0 \\
\Leftrightarrow &\forall\, w \in V : (\varphi^{\mathrm{ad}} - \varphi)(w) = 0 \\
\Leftrightarrow &\varphi^{\mathrm{ad}} = \varphi
\end{aligned}$$

by Lemma 10.9.
(b) If $\varphi = 0$, it follows trivially that

$$\langle v, v\rangle_\varphi = \langle \varphi(v), v\rangle = \langle 0, v\rangle = 0.$$

Suppose now that $\langle v, v\rangle_\varphi = 0$ for all $v \in V$. Let $v, w \in V$ and $a \in K$. We compute

$$\begin{aligned} 0 &= \langle v + aw, v + aw\rangle_\varphi \\ &= \langle \varphi(v + aw), v + aw\rangle \\ &= \underbrace{\langle \varphi(v), v\rangle}_{=0} + \langle \varphi(v), aw\rangle + \langle \varphi(aw), v\rangle + \underbrace{\langle \varphi(aw), aw\rangle}_{=0} \\ &= \overline{a}\langle \varphi(v), w\rangle + a\langle \varphi(w), v\rangle \\ &= \overline{a}\langle \varphi(v), w\rangle + a\langle w, \varphi(v)\rangle \\ &= \overline{a}\langle \varphi(v), w\rangle + a\overline{\langle \varphi(v), w\rangle} \\ &= 2 \cdot \mathrm{Re}(\overline{a}\langle \varphi(v), w\rangle). \end{aligned}$$

With $a = 1$, we obtain $0 = \mathrm{Re}(\langle \varphi(v), w\rangle)$, and with $a = i$ we find $0 = \mathrm{Im}(\langle \varphi(v), w\rangle)$. Consequently, we have for all $v, w \in V$

$$0 = \langle \varphi(v), w\rangle.$$

For all $v \in V$, we thus find $\varphi(v) \perp V$, whence the desired result $\varphi(v) = 0$ by Lemma 10.9. □

If one applies the previous proposition with φ_M for a square matrix M, we find back the result of the discussion in the beginning if section 9. Then:

(a) $M = M^{\mathrm{ad}} \Leftrightarrow M$ is self-adjoint $\Leftrightarrow (v, w) \mapsto v^{\mathrm{tr}}Aw$ is a hermitian form.

(b) If M is self-adjoint, then: $M = 0 \;\Leftrightarrow\; \forall\, v \in K^n : v^{\mathrm{tr}}Mv = 0$.

We now introduce the applications that preserve lengths: the “ isometries”.

Definition 10.11. *Let V be a hermitian space. We call* isometry *any $\varphi \in \mathrm{End}_K(V)$ such that for all $v \in V$*

$$|\varphi(v)| = |v|.$$

Lemma 10.12. *Let V be a hermitian space and let $\varphi \in \mathrm{End}_K(V)$. The following statements are equivalent:*

(i) φ is an isometry.

(ii) $\varphi^{\mathrm{ad}} \circ \varphi = \mathrm{id}_V$ (in particular, φ is an isomorphism).

(iii) For all $v, w \in W$: $\langle \varphi(v), \varphi(w)\rangle = \langle v, w\rangle$.

Proof. “(i) ⇒ (ii)”: We have for all $v \in V$:

$$\langle v, v\rangle = \langle \varphi(v), \varphi(v)\rangle = \langle v, \varphi^{\mathrm{ad}}(\varphi(v))\rangle,$$

hence

$$\langle v, (\varphi^{\mathrm{ad}} \circ \varphi - \mathrm{id}_V)(v)\rangle = 0 \text{ et, alors, } \langle(\varphi^{\mathrm{ad}} \circ \varphi - \mathrm{id}_V)(v), v\rangle = 0.$$

Note that $\varphi^{\mathrm{ad}} \circ \varphi - \mathrm{id}_V$ is self-adjoint, thus Proposition 10.10(b) implies that $\varphi^{\mathrm{ad}} \circ \varphi - \mathrm{id}_V = 0$, whence $\varphi^{\mathrm{ad}} \circ \varphi - \mathrm{id}_V$.

"(ii) ⇒ (iii)": Let $v, w \in V$, then

$$\langle\varphi(v), \varphi(w)\rangle = \langle v, \varphi^{\mathrm{ad}}(\varphi(w))\rangle = \langle v, w\rangle.$$

"(iii) ⇒ (i)": Let $v \in V$. Then,

$$|\varphi(v)|^2 = \langle\varphi(v), \varphi(v)\rangle = \langle v, v\rangle = |v|^2.$$

□

By this lemma, we have

$$\varphi \text{ is an isometry } \Leftrightarrow M_{S,S}(\varphi) \text{ is an isometry (i.e. orthogonal or unitary)}$$

for an orthonormal basis S of V.

Until now we always considered two types of endomorphisms/matrices: self-adjoint and isometries. We would like to treat some of their properties in parallel. We thus look for a common generalization. Normal operators are such a generalization. We first give the definition in a " metric"way

Definition 10.13. *Let V be a hermitian space. We call* normal operator *any $\varphi \in \mathrm{End}_K(V)$ such that for all $v \in V$*

$$|\varphi(v)| = |\varphi^{\mathrm{ad}}(v)|.$$

Example 10.14.

- *If φ is self-adjoint, we have $\varphi^{\mathrm{ad}} = \varphi$, whence, φ is normal.*
- *If φ is an isometry, we have that φ is an isometry and $\varphi^{\mathrm{ad}} = \varphi^{-1}$. As $|\varphi(v)| = |v|$ we find $|\varphi^{\mathrm{ad}}(v)| = |\varphi^{-1}(v)| = |v|$, whence, φ is normal.*

Proposition 10.15. *Let V be a hermitian space and let $\varphi \in \mathrm{End}_K(V)$. The following statements are equivalent:*

(i) *φ is normal.*

(ii) $\varphi^{\mathrm{ad}} \circ \varphi = \varphi \circ \varphi^{\mathrm{ad}}$.

Proof. First we compute

$$\begin{aligned} |\varphi(v)|^2 - |\varphi^{\mathrm{ad}}(v)|^2 &= \langle\varphi(v), \varphi(v)\rangle - \langle\varphi^{\mathrm{ad}}(v), \varphi^{\mathrm{ad}}(v)\rangle \\ &= \langle\varphi(v), (\varphi^{\mathrm{ad}})^{\mathrm{ad}}(v)\rangle - \langle\varphi^{\mathrm{ad}}(v), \varphi^{\mathrm{ad}}(v)\rangle \\ &= \langle\varphi^{\mathrm{ad}} \circ \varphi(v), v\rangle - \langle\varphi \circ \varphi^{\mathrm{ad}}(v), v\rangle \\ &= \langle(\varphi^{\mathrm{ad}} \circ \varphi - \varphi \circ \varphi^{\mathrm{ad}})(v), v\rangle. \end{aligned}$$

Note that $\varphi \circ \varphi^{\mathrm{ad}} - \varphi^{\mathrm{ad}} \circ \varphi$ is self-adjoint. Consequently, (Propositon 10.10(b)) we have

$$\big(\forall\, v \in V : |\varphi(v)|^2 = |\varphi^{\mathrm{ad}}(v)|^2\big) \Leftrightarrow \varphi^{\mathrm{ad}} \circ \varphi = \varphi \circ \varphi^{\mathrm{ad}}.$$

□

In terms of matrices, we thus have:

$$\varphi \text{ is normal } \Longleftrightarrow \overline{M}^{\text{tr}} M = M \overline{M}^{\text{tr}} \overset{\text{définition}}{\Longleftrightarrow} M \text{ is normal}$$

where $M = M_{S,S}(\varphi)$ for an orthonormal basis S of V.

Lemma 10.16. *Let V be a hermitian space and let $\varphi \in \mathrm{End}_K(V)$ be normal. Let $a \in \mathrm{Spec}(\varphi)$ be an eigenvalue of φ.*

(a) $E_\varphi(a) = E_{\varphi^{\mathrm{ad}}}(\overline{a})$.

(b) If φ is self-adjoint, then $a \in \mathbb{R}$.

(c) If φ is an isometry, then $|a| = 1$

Proof. (a) We first prove that $\ker(\varphi) = \ker(\varphi^{\mathrm{ad}})$ for any normal operator. Let $v \in V$, then,

$$v \in \ker(\varphi) \Leftrightarrow \varphi(v) = 0 \Leftrightarrow |\varphi(v)| = 0 \overset{\text{déf. normalité}}{\Leftrightarrow} |\varphi^{\mathrm{ad}}(v)| = 0 \Leftrightarrow \varphi^{\mathrm{ad}}(v) = 0 \Leftrightarrow v \in \ker(\varphi^{\mathrm{ad}}).$$

Now put $\psi := \varphi - a \cdot \mathrm{id}_V$. This is also a normal operator:

$$\begin{aligned}\psi \circ \psi^{\mathrm{ad}} &= (\varphi - a \cdot \mathrm{id}_V) \circ (\varphi - a \cdot \mathrm{id}_V)^{\mathrm{ad}} = (\varphi - a \cdot \mathrm{id}_V) \circ (\varphi^{\mathrm{ad}} - \overline{a} \cdot \mathrm{id}_V) = \varphi \circ \varphi^{\mathrm{ad}} - a \cdot \varphi^{\mathrm{ad}} - \overline{a} \cdot \varphi + a \cdot \overline{a} \cdot \mathrm{id}_V \\ &= \varphi^{\mathrm{ad}} \circ \varphi - a \cdot \varphi^{\mathrm{ad}} - \overline{a} \cdot \varphi + a \cdot \overline{a} \cdot \mathrm{id}_V = (\varphi - a \cdot \mathrm{id}_V)^{\mathrm{ad}} \circ (\varphi - a \cdot \mathrm{id}_V) = \psi^{\mathrm{ad}} \circ \psi.\end{aligned}$$

The previous computation gives us

$$E_\varphi(a) = \ker(\varphi - a \cdot \mathrm{id}_V) = \ker(\psi) = \ker(\psi^{\mathrm{ad}}) = \ker(\varphi^{\mathrm{ad}} - \overline{a} \cdot \mathrm{id}_V) = E_{\varphi^{\mathrm{ad}}}(\overline{a}).$$

(b) For all $v \in E_\varphi(a)$ we have $v \in E_\varphi(\overline{a})$, hence $a \cdot v = \varphi(v) = \varphi^{\mathrm{ad}}(v) = \overline{a} \cdot v$, that is, $a = \overline{a}$ and consequently $a \in \mathbb{R}$.
(c) For all $v \in E_\varphi(a)$ we have $v = \varphi^{-1}(\varphi(v)) = \varphi^{-1}(a \cdot v) = a \cdot \varphi^{-1}(v) = a \cdot \overline{a} \cdot v = |a|^2 \cdot v$, whence $|a|^2 = 1$. □

Example 10.17. *This example gives us an idea of the spectral theorem.*

(a) Firstly we continue the analysis of O_2 of Lemma 10.5.

(1) Let $M = \begin{pmatrix} \cos(\alpha) & -\sin(\alpha) \\ \sin(\alpha) & \cos(\alpha) \end{pmatrix}$. Its characteristic polynomial is

$$(X - \cos(\alpha))^2 + \sin^2(\alpha) = X^2 - 2\cos(\alpha)X + 1$$

whose discriminant is $4\cos^2(\alpha) - 4 \leq 0$ with equality if and only if $|\cos(\alpha)| = 1$, if and only if $\alpha \in \pi\mathbb{Z}$.

Consequently, if $\alpha \notin \pi\mathbb{Z}$, then M has no eigenvalue and is therefore not diagonalizable. This is also geometrically clear since M represents the rotation by angle α that does not fix any vector unless the angle is a multiple of π.

If α is an even multiple of π, then $M = \mathrm{id}$. If α is an odd multiple of π, then $M = -\mathrm{id}$.

(2) Let $M = \left(\begin{smallmatrix} \cos(\alpha) & \sin(\alpha) \\ \sin(\alpha) & -\cos(\alpha) \end{smallmatrix}\right)$. Its characteristic polynomial is

$$X^2 - \cos^2(\alpha) - \sin^2(\alpha) = X^2 - 1 = (X-1)(X+1).$$

The matirx M is thus diagonalizable with eigenvalues -1 and 1.

Geometrically, it is a reflexion by one axis (eigenvector for eigenvalue 1).

(b) Let $M \in \mathrm{Mat}_{3\times 3}(\mathbb{R})$ be an orthogonal matrix. Its characteristic polynomial is monic of degree 3 and has therefore a real root λ_1. By Lemma 10.16, this root is either 1 or -1. There is thus an eigenvector v_1 for the eigenvalue λ_1. We can normalize it such that $|v_1| = 1$.

By Gram-Schmidt, we can find vectors v_2, v_3 such that v_1, v_2, v_3 form an orthonormal basis of $\mathbb{R}^3$. Moreover, since M is an isometry, for $i = 1, 2$, we have

$$0 = \langle v_i, v_1 \rangle = \langle Mv_i, Mv_1 \rangle = \lambda_1 \langle Mv_i, v_1 \rangle.$$

This means that M sends the subspace $W \leq \mathbb{R}^3$ generated by v_2, v_3 into itself.

If one writes the vectors v_1, v_2, v_3 as columns in a matrix C (which is orthogonal!), we thus obtain

$$C^{\mathrm{tr}} M C = \begin{pmatrix} \lambda_1 & 0 & 0 \\ 0 & a & b \\ 0 & c & d \end{pmatrix}.$$

The matrix $A := \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ is orthogonal and belongs to O_2.

If $\det(A) = \det(M)/\lambda_1 = 1$, we have that $A = \left(\begin{smallmatrix} \cos(\alpha) & -\sin(\alpha) \\ \sin(\alpha) & \cos(\alpha) \end{smallmatrix}\right)$ for some $0 \leq \alpha < 2\pi$. If $\det(A) = -1$, we can find a basis w_2, w_3 of W consisting of normalized eigenvectors: $|w_i| = 1$ for $i = 2, 3$ for the eigenvalues $1, -1$. Consequently, v_1, w_2, w_3 is an orthonormal basis of $\mathbb{R}^3$. If D is the (orthogonal!) matrix whose columns are these vectors, we finally have

$$D^{\mathrm{tr}} M D = \begin{pmatrix} \lambda_1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix}$$

for $\lambda_2 \in \{1, -1\}$.

11 Spectral Theorem

Goals:

- Know the spectral theorems;
- be able to compute the diagonalization of normal complex matrices, adjoint matrices;
- be able to compute the normal form of orthonormal matrices;
- know examples and be able to prove simple properties.

Let V be a hermitian space and let $U, W \leq V$ be two vector subspaces. We write $U \obot W$ for $U + W$ if the sum is direct ($U \oplus W$) and the two subspaces are orthogonal ($U \perp W$).

Lemma 11.1. *Let V be a hermitian space and $\varphi \in \operatorname{End}_K(V)$ normal. Then, for all distinct $a_1, \dots, a_n \in \operatorname{Spec}(\varphi)$, we have*

$$E_\varphi(a_1) + E_\varphi(a_2) + \cdots + E_\varphi(a_n) = E_\varphi(a_1) \obot E_\varphi(a_2) \obot \cdots \obot E_\varphi(a_n).$$

Proof. In Lemma 3.10 wa have already seen that the sum of eigenspaces is direct. Let $0 \neq v \in E_\varphi(a_i)$ and $0 \neq w \in E_\varphi(a_j)$ with $i \neq j$ (i.e. $w \in E_{\varphi^{\mathrm{ad}}}(\overline{a_j})$ by Lemma 10.16). We have

$$\langle \varphi(v), w \rangle = \langle a_i v, w \rangle = a_i \langle v, w \rangle,$$

but also

$$\langle \varphi(v), w \rangle = \langle v, \varphi^{\mathrm{ad}}(w) \rangle = \langle v, \overline{a_j} w \rangle = a_j \langle v, w \rangle,$$

whence $\langle v, w \rangle = 0$. □

We first prove the spectral theorem for normal operators with complex coefficients. The reason for this is that in this case we have the following theorem.

Theorem 11.2 (Fundamental Theorem of Algebra)**.** *Any polynomial $f \in \mathbb{C}[X]$ of degree ≥ 1 has a zero.*

Proof. Analysis Course. □

Theorem 11.3 (Spectral Theorem for normal operators)**.** *Let V be a hermitian $\mathbb{C}$-space of finite dimension and $\varphi \in \operatorname{End}_K(V)$. The following statements are equivalent:*

(i) *φ is normal.*

(ii) *$V = \obot_{a \in \operatorname{Spec}(\varphi)} E_\varphi(a)$ (in particular, φ is diagonalizable).*

(iii) *V has an orthonormal basis consisting of eigenvectors for φ.*

Proof. "(i) ⇒ (ii)": We have already seen that $W := \bigoplus_{a \in \operatorname{Spec}(\varphi)} E_\varphi(a)$ is a subspace of V and we know that the sum is orthogonal by Lemma 11.1. Corollary 9.13(b) yields the existence of on orthogonal complement $V = W \oplus W^\perp$. The aim is to show $W^\perp = 0$.
Lemma 10.16 implies that $W = \bigoplus_{a \in \operatorname{Spec}(\varphi)} E_{\varphi^{\mathrm{ad}}}(\overline{a})$, whence $\varphi^{\mathrm{ad}}(W) \subseteq W$. Let now $v \in W^\perp$. Then for all $w \in W$,

$$\langle \varphi(v), w \rangle = \langle v, \varphi^{\mathrm{ad}}(w) \rangle = 0,$$

showing that $\varphi(v) \in W^\perp$. Hence we can restrict φ to $W^\perp$. Let $f = \operatorname{charpoly}_{\varphi|_{W^\perp}} \in \mathbb{C}[X]$ be a characteristic polynomial. Assume that $W^\perp \neq 0$, so that $\deg(f) \geq 1$. By the Fundamental Theorem of Algebra 11.2, this polynomial has a zero $z \in \mathbb{C}$. Since $\operatorname{charpoly}_{\varphi|_{W^\perp}} \mid \operatorname{charpoly}_\varphi$, we find $z \in \operatorname{Spec}(\varphi)$, whence $W^\perp \cap W \neq 0$, leading to a contradiction. Therefore, $W^\perp = 0$, as desired.
"(ii) ⇒ (iii)": It suffices to choose an orthonormal basis of each $E_\varphi(a)$ and take the union; we will then automatically have an orthonormal basis of V because the eigenspaces are orthogonal.

"(iii) ⇒ (i)": Let $S = s_1, \dots, s_n$ be an orthonormal basis of V consisting of eigenvectors. Let a_i be the eigenvalue associated to s_i (we do not require that the a_i's are two by two distinct). Thus we have $\varphi(s_i) = a_i \cdot s_i$. Let $1 \leq j \leq n$. We have

$$\langle s_j, \varphi^{\mathrm{ad}}(s_i) - \overline{a_i} s_i \rangle = \langle s_j, \varphi^{\mathrm{ad}}(s_i) \rangle - \langle s_j, \overline{a_i} s_i \rangle = \langle \varphi(s_j), s_i \rangle - a_i \langle s_j, s_i \rangle = (a_j - a_i) \langle s_j, s_i \rangle = 0.$$

Therefore $(\varphi^{\mathrm{ad}}(s_i) - \overline{a_i} s_i) \perp V$, whence $\varphi^{\mathrm{ad}}(s_i) = \overline{a_i} \cdot s_i$. The computation

$$\begin{aligned} \varphi(\varphi^{\mathrm{ad}}(s_i)) &= \varphi(\overline{a_i} \cdot s_i) = \overline{a_i} \cdot \varphi(s_i) = \overline{a_i} \cdot a_i \cdot s_i \\ \varphi^{\mathrm{ad}}(\varphi(s_i)) &= \varphi^{\mathrm{ad}}(a_i \cdot s_i) = a_i \cdot \varphi^{\mathrm{ad}}(s_i) = a_i \cdot \overline{a_i} \cdot s_i, \end{aligned}$$

implies $\varphi \circ \varphi^{\mathrm{ad}} = \varphi^{\mathrm{ad}} \circ \varphi$, the normality of φ. □

Let us now provide the translation in terms of matrices of the spectral theorem 11.3.

Corollary 11.4. *Let $M \in \mathrm{Mat}_{n \times n}(\mathbb{C})$ be a matrix. Then the following statements are equivalent:*

(i) M is normal, i.e. $\overline{M}^{\mathrm{tr}} \cdot M = M \cdot \overline{M}^{\mathrm{tr}}$.

(ii) There exists a unitary *matrix $C \in \mathrm{Mat}_{n \times n}(\mathbb{C})$ such that $\overline{C}^{\mathrm{tr}} \cdot M \cdot C$ is a diagonal matrix.*

Proof. "(i) ⇒ (ii)": Let $\varphi = \varphi_M$ be the endomorphism of $\mathbb{C}^n$ such that $M_{S,S}(\varphi) = M$ where S is the canonical basis (which is orthonormal for the canonical scalar product!). By Proposition 10.6 we have $\overline{M}^{\mathrm{tr}} = M_{S,S}(\varphi^{\mathrm{ad}})$. Therefore the hypothesis that M is normal translates the fact that φ is normal. We use Theorem 11.3 to obtain an orthonormal basis T of eigenvectors. Thus $C_{S,T}^{-1} \cdot M_{S,S}(\varphi) \cdot C_{S,T} = M_{T,T}(\varphi)$ is a diagonal matrix. Recall now that the columns of $C := C_{S,T}$ are the vectors of basis T. Since T is orthonormal for the canonical scalar product, we have $C \cdot \overline{C}^{\mathrm{tr}} = \mathrm{id}_n$ and the statement is proven.

"(ii) ⇒ (i)": Let $\overline{C}^{\mathrm{tr}} \cdot M \cdot C = \mathrm{diag}(a_1, \dots, a_n)$, be the diagonal matrix having $a_1, \dots, a_n$ on the diagonal. First notice that

$$\overline{(\overline{C}^{\mathrm{tr}} \cdot MC)}^{\mathrm{tr}} = \overline{C}^{\mathrm{tr}} \cdot \overline{M}^{\mathrm{tr}} \cdot C = \mathrm{diag}(\overline{a_1}, \dots, \overline{a_n}).$$

Since diagonal matrices commute, we find

$$\begin{aligned} \overline{(\overline{C}^{\mathrm{tr}} \cdot MC)}^{\mathrm{tr}} \cdot (\overline{C}^{\mathrm{tr}} \cdot MC) &= \overline{C}^{\mathrm{tr}} \cdot \overline{M}^{\mathrm{tr}} \cdot C \cdot \overline{C}^{\mathrm{tr}} \cdot MC = \overline{C}^{\mathrm{tr}} \cdot \overline{M}^{\mathrm{tr}} \cdot MC \\ &= (\overline{C}^{\mathrm{tr}} \cdot MC) \cdot \overline{(\overline{C}^{\mathrm{tr}} \cdot MC)}^{\mathrm{tr}} = \overline{C}^{\mathrm{tr}} \cdot M \cdot C \cdot \overline{C}^{\mathrm{tr}} \overline{M}^{\mathrm{tr}} \cdot C = \overline{C}^{\mathrm{tr}} \cdot M \cdot \overline{M}^{\mathrm{tr}} \cdot C, \end{aligned}$$

thus $\overline{M}^{\mathrm{tr}} \cdot M = M \cdot \overline{M}^{\mathrm{tr}}$. □

Lemma 11.5. *Let $M \in \mathrm{Mat}_{n \times n}(\mathbb{R})$ be a matrix which we consider on $\mathbb{C}$.*

(a) For all $\mu \in \mathbb{C}$ and all $v \in \mathbb{C}^n$ we have the equivalence: $v \in E_M(\mu) \Longleftrightarrow \overline{v} \in E_M(\overline{\mu})$.

(b) For $\mu \in \mathbb{C}$ we have the equivalence: $\mu \in \mathrm{Spec}(M) \Longleftrightarrow \overline{\mu} \in \mathrm{Spec}(M)$.

(c) For $\mu \in \mathbb{R}$, the eigenspace $E_M(\mu) \subseteq \mathbb{C}^n$ has a basis in $\mathbb{R}^n$.

*(d) Let $\mu \in \mathrm{Spec}(M)$ such that $\mu \in \mathbb{C} \setminus \mathbb{R}$ and let $v \in E_M(\mu)$ such that $|v| = 1$.
Set $x := \frac{1}{\sqrt{2}}(v + \overline{v}), y := \frac{1}{i\sqrt{2}}(v - \overline{v}) \in E_M(\mu) \oplus E_M(\overline{\mu})$.
Then $|x| = 1$, $|y| = 1$, $x \perp y$, $Mx = \mathrm{Re}(\mu) \cdot x - \mathrm{Im}(\mu) \cdot y$ and $My = \mathrm{Re}(\mu) \cdot y + \mathrm{Im}(\mu) \cdot x$.*

Proof. (a) We observe: $Mv = \mu \cdot v \Longleftrightarrow \overline{Mv} = M\overline{v} = \overline{\mu \cdot v} = \overline{\mu} \cdot \overline{v}$ which implies the result. (b) is a direct consequence of (a).

(c) It suffices to show that $E_M(\mu)$ admits a system of generators in $\mathbb{R}^n$. Let $v_1, \dots, v_r \in \mathbb{C}^n$ be a $\mathbb{C}$-basis of $E_M(\mu)$. Set $x_j = \mathrm{Re}(v_j)$ and $y_j = \mathrm{Im}(v_j)$ for $j = 1, \dots, r$. These vectors belong to $E_M(\mu)$ since so does $\overline{v_j}$ for all j. Since $v_j = x_j + iy_j$, the vectors $x_1, \dots, x_r, y_1, \dots, y_r$ generate $E_M(\mu)$.

(d) First observe that $v \perp \overline{v}$ since $E_M(\mu) \perp E_M(\overline{\mu})$ as $\mu \neq \overline{\mu}$. We have

$$|x|^2 = \langle x, x\rangle = (\frac{1}{\sqrt{2}})^2 \langle v + \overline{v}, v + \overline{v}\rangle = \frac{1}{2}\big(\langle v, v\rangle + \langle \overline{v}, \overline{v}\rangle + \langle v, \overline{v}\rangle + \langle \overline{v}, v\rangle\big) = 1.$$

The calculation of $|y|$ is similar:

$$|y|^2 = \langle y, y\rangle = (\frac{1}{\sqrt{2}})^2 \langle v - \overline{v}, v - \overline{v}\rangle = \frac{1}{2}\big(\langle v, v\rangle + \langle \overline{v}, \overline{v}\rangle - \langle v, \overline{v}\rangle - \langle \overline{v}, v\rangle\big) = 1.$$

We also have:

$$\langle x, y\rangle = \frac{i}{2}\langle v + \overline{v}, v - \overline{v}\rangle = \frac{i}{2}\big(\langle v, v\rangle - \langle \overline{v}, \overline{v}\rangle + \langle \overline{v}, v\rangle - \langle v, \overline{v}\rangle\big) = 0.$$

Let us now compute the action of M:

$$\begin{aligned}
Mx &= \frac{1}{\sqrt{2}}(Mv + M\overline{v}) = \frac{1}{\sqrt{2}}(\mu v + \overline{\mu v}) = \frac{1}{2\sqrt{2}}\big((\mu + \overline{\mu})(v + \overline{v}) + (\mu - \overline{\mu})(v - \overline{v})\big)\\
&= \frac{1}{2}(\mu + \overline{\mu})x - \frac{1}{2i}(\mu - \overline{\mu})y = \mathrm{Re}(\mu) \cdot x - \mathrm{Im}(\mu) \cdot y\\
My &= \frac{1}{i\sqrt{2}}(Mv - M\overline{v}) = \frac{1}{\sqrt{2}i}(\mu v - \overline{\mu v}) = \frac{1}{2i\sqrt{2}}\big((\mu + \overline{\mu})(v - \overline{v}) + (\mu - \overline{\mu})(v + \overline{v})\big)\\
&= \frac{1}{2}(\mu + \overline{\mu})y + \frac{1}{2i}(\mu - \overline{\mu})x = \mathrm{Re}(\mu) \cdot y + \mathrm{Im}(\mu) \cdot x.
\end{aligned}$$

□

Corollary 11.6. *Let $M \in \mathrm{Mat}_{n\times n}(\mathbb{R})$ be a normal matrix, i.e. $M^{\mathrm{tr}} \cdot M = M \cdot M^{\mathrm{tr}}$.
Let $\lambda_1, \dots, \lambda_r, \mu_1, \dots,$
$\mu_s, \overline{\mu_1}, \dots, \overline{\mu_s}$ for $n = r + 2s$ and $\lambda_1, \dots, \lambda_r \in \mathbb{R}$ and $\mu_1, \dots, \mu_s \in \mathbb{C} \setminus \mathbb{R}$ be the diagonal coefficients of the matrix of Corollary 11.4. We set $\alpha_i = \mathrm{Re}(\mu_i)$ and $\beta_i = \mathrm{Im}(\mu_i)$ for $1 \leq i \leq s$.*

Then, there exists an orthogonal *matrix* $C \in \mathrm{Mat}_{n\times n}(\mathbb{R})$ *such that*

$$C^{\mathrm{tr}} \cdot M \cdot C = \begin{pmatrix} \lambda_1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & \lambda_2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\ 0 & \dots & 0 & \lambda_r & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & \dots & \dots & 0 & \alpha_1 & \beta_1 & 0 & 0 & 0 & 0 \\ 0 & \dots & \dots & 0 & -\beta_1 & \alpha_1 & 0 & 0 & 0 & 0 \\ 0 & \dots & \dots & 0 & 0 & 0 & \ddots & \ddots & 0 & 0 \\ 0 & \dots & \dots & 0 & 0 & 0 & \ddots & \ddots & 0 & 0 \\ 0 & \dots & \dots & 0 & 0 & 0 & 0 & 0 & \alpha_s & \beta_s \\ 0 & \dots & \dots & 0 & 0 & 0 & 0 & 0 & -\beta_s & \alpha_s \end{pmatrix}.$$

Proof. In view of Corollary 11.4 and Lemma 11.5, we have an orthonormal basis

$$w_1, w_2, \dots, w_r, v_1, \overline{v_1}, v_2, \overline{v_2}, \dots v_s, \overline{v_s}$$

of $\mathbb{C}^n$ consisting of eigenvectors for the eigenvalues

$$\lambda_1, \lambda_2, \dots, \lambda_r, \mu_1, \overline{\mu_1}, \mu_2, \overline{\mu_2}, \dots, \mu_s, \overline{\mu_s}$$

where $n = r + 2s$ and the property $w_i \in \mathbb{R}^n$ for $1 \le i \le r$ is satisfied. As in the lemma, set $x_j = \frac{1}{\sqrt{2}}(v_j + \overline{v_j})$ et $y_j = \frac{1}{i\sqrt{2}}(v_j - \overline{v_j})$.
Then, $w_1, w_2, \dots, w_r, x_1, y_1, x_2, y_2, \dots, x_s, y_s$ form an orthonormal basis of $\mathbb{R}^n$. If this orthonormal basis is written in the columns of C (which is then orthogonal), then $C^{-1}MC$ has the desired form. This follows from the computations in Lemma 11.5. □

Remark 11.7. *Let* $M \in \mathrm{Mat}_{n\times n}(K)$ *for* $K \in \{\mathbb{R}, \mathbb{C}\}$. *To compute the matrix* C *of corollaries 11.4 and 11.6, we can use the techniques that we already studied. We proceed as follows:*

(1) Compute the characteristic polynomial.

(2) Compute the eigenvalues in $\mathbb{C}$ *(as roots of the characteristic polynomial).*

(3) If $M \in \mathrm{Mat}_{n\times n}(\mathbb{C})$*, for all* $a \in \mathrm{Spec}(M)$*, compute a* $\mathbb{C}$*-basis of* $E_M(a)$.

(4) If $M \in \mathrm{Mat}_{n\times n}(\mathbb{R})$*, for all* $a \in \mathrm{Spec}(M)$ *real, compute an* $\mathbb{R}$*-basis of* $E_M(a)$*, and for all* $a \in \mathrm{Spec}(M)$ *not real, compute a* $\mathbb{C}$*-basis of* $E_M(a)$.

(5) Using Gram-Schmidt, compute an orthonormal basis of $E_M(a)$ *(on* $\mathbb{R}$ *if the original basis is on* $\mathbb{R}$*) for all* $a \in \mathrm{Spec}(M)$.

Note that if $a \in \mathbb{C} \setminus \mathbb{R}$ *and* $M \in \mathrm{Mat}_{n\times n}(\mathbb{R})$*, then we obtain an orthonormal basis of* $E_M(\overline{a})$ *by applying complex conjugation to the orthonormal basis of* $E_M(a)$.

(6) If $M \in \mathrm{Mat}_{n\times n}(\mathbb{C})$*, write the vectors of the orthonormal bases as columns of the matrix* C.

(7) If $M \in \mathrm{Mat}_{n\times n}(\mathbb{R})$, arrange the eigenvalues of M (seen as matrix with complex coefficients) as follows: first the real eigenvalues $\lambda_1, \dots, \lambda_r$, then $\mu_1, \dots, \mu_s, \overline{\mu_1}, \dots, \overline{\mu_s} \in \mathbb{C} \setminus \mathbb{R}$.

For each vector v of the orthonormal basis of a proper space $E_M(\mu_i)$ for all $i = 1, \dots, s$, compute the vectors x, y as in Corollary 11.6 and obtain an orthonormal basis with real coefficients of $E_M(\mu_i) \oplus E_M(\overline{\mu_i})$.

Write the vectors of the real orthonormal basis of $E_M(\lambda_i)$ for $i = 1, \dots, r$ and of $E_M(\mu_i) \oplus E_M(\overline{\mu_i})$ as columns of the matrix C.

Example 11.8. *Let us treat a concrete example for a symmetric matrix. Let*

$$M = \begin{pmatrix} 14 & 38 & -40 \\ 38 & 71 & 20 \\ -40 & 20 & 5 \end{pmatrix}.$$

Its characteristic polynomial is $(X+45)(X-45)(X-90)$.
Let us compute the eigenspaces:

$$E_M(-45) = \ker \begin{pmatrix} 59 & 38 & -40 \\ 38 & 116 & 20 \\ -40 & 20 & 50 \end{pmatrix} = \langle \begin{pmatrix} 2 \\ -1 \\ 2 \end{pmatrix} \rangle,$$

$$E_M(45) = \ker \begin{pmatrix} -31 & 38 & -40 \\ 38 & 26 & 20 \\ -40 & 20 & -40 \end{pmatrix} = \langle \begin{pmatrix} 4 \\ -2 \\ -5 \end{pmatrix} \rangle$$

and

$$E_M(90) = \ker \begin{pmatrix} -76 & 38 & -40 \\ 38 & -19 & 20 \\ -40 & 20 & -85 \end{pmatrix} = \langle \begin{pmatrix} 1 \\ 2 \\ 0 \end{pmatrix} \rangle.$$

These vectors are already orthogonal by Lemma 11.1. One can easily verify it. Thus, it suffices to normalize them and to write them as columns of a matrix:

$$C = \begin{pmatrix} \frac{2}{3} & \frac{4}{3\sqrt{5}} & \frac{1}{\sqrt{5}} \\ \frac{-1}{3} & \frac{-2}{3\sqrt{5}} & \frac{2}{\sqrt{5}} \\ \frac{2}{3} & \frac{-\sqrt{5}}{3} & 0 \end{pmatrix}.$$

By construction, C is orthogonal, which can also be checked by a direct computation. We obtain by construction (to check by computation):

$$C^{\mathrm{tr}} M C = \begin{pmatrix} -45 & 0 & 0 \\ 0 & 45 & 0 \\ 0 & 0 & 90 \end{pmatrix}.$$

We can now state a stronger result if φ is self-adjoint.

Corollary 11.9. *Let $K \in \{\mathbb{R}, \mathbb{C}\}$. Let $M \in \mathrm{Mat}_{n\times n}(K)$ be a matrix. Then the following statements are equivalent:*

(i) M *is self-adjoint (symmetric/hermitian).*

(ii) There exists an isometry (unitary/orthogonal matrix) $C \in \mathrm{Mat}_{n\times n}(K)$ *such that* $\overline{C}^{\mathrm{tr}} \cdot M \cdot C = \mathrm{diag}(a_1, \dots, a_n)$ *with* $a_1, \dots, a_n \in \mathbb{R}$.

Proof. "(i) ⇒ (ii)": Since M is self-adjoint, it is normal. We can thus apply Corollary 11.6. Moreover, we obtain $r = n$ and $s = 0$ in the notation of the corollary, since $\mathrm{Spec}(M) \subset \mathbb{R}$ by Lemma 10.16.
"(ii) ⇒ (i)": Let $\overline{C}^{\mathrm{tr}} \cdot M \cdot C = \mathrm{diag}(a_1, \dots, a_n)$, the diagonal matrix with $a_1, \dots, a_n \in \mathbb{R}$ on the diagonal. Taking the adjoint on both sides, we have $\overline{C}^{\mathrm{tr}} \cdot M \cdot C = \overline{C}^{\mathrm{tr}} \cdot \overline{M}^{\mathrm{tr}} \cdot C$ since the diagonal matrix is invariant. Therefore, $M = \overline{M}^{\mathrm{tr}}$. □

Corollary 11.10. *Let* $K \in \{\mathbb{R}, \mathbb{C}\}$. *Let* V *be a hermitian* K*-space of finite dimension and* $\varphi \in \mathrm{End}_K(V)$. *Then the following statements are equivalent:*

(i) φ *is self-adjoint.*

(ii) $V = \bigoplus_{a \in \mathrm{Spec}(\varphi)} E_\varphi(a)$ *(in particular,* φ *is diagonalizable) and* $\mathrm{Spec}(\varphi) \subset \mathbb{R}$.

(iii) V *has an orthonormal basis consisting of eigenvectors for the real eigenvalues of* φ.

Proof. We will deduce this theorem from Corollary 11.9. For this, let S be an orthonormal basis of V. Then, φ is normal/self-adjoint if and only if $M := M_{S,S}(\varphi)$ is normal/self-adjoint (this comes from Proposition 10.6).
"(i) ⇒ (ii)": It suffices to apply Corollary 11.9 to the matrix M.
"(ii) ⇒ (iii)": It suffices once again to choose an orthonormal basis in each eigenspace.
"(iii) ⇒ (i)": Let T be the orthonormal basis in the hypothesis. Let C be the matrix whose columns are the vectors of the basis T. Then, $\overline{C}^{\mathrm{tr}} \cdot M_{S,S}(\varphi) \cdot C$ is diagonal with real coefficients, hence Corollary 11.9 tells us that $M_{S,S}(\varphi)$ is self-adjoint, then φ l'est aussi. □

Corollary 11.11. *(a) Let* $M \in \mathrm{Mat}_{n\times n}(\mathbb{C})$ *be an isometry. Then there exists a* unitary *matrix* $C \in \mathrm{Mat}_{n\times n}(\mathbb{C})$ *such that* $\overline{C}^{\mathrm{tr}} MC$ *is diagonal and all the coefficients on the diagonal have absolute value* 1.

(b) Let $M \in \mathrm{Mat}_{n\times n}(\mathbb{R})$ *be an isometry. Then there exists an* orthogonal *matrix* $C \in \mathrm{Mat}_{n\times n}(\mathbb{R})$ *such that*

$$C^{\mathrm{tr}} \cdot M \cdot C = \begin{pmatrix} \lambda_1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & \lambda_2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\ 0 & \dots & 0 & \lambda_r & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & \dots & \dots & 0 & \cos(\alpha_1) & \sin(\alpha_1) & 0 & 0 & 0 & 0 \\ 0 & \dots & \dots & 0 & -\sin(\alpha_1) & \cos(\alpha_1) & 0 & 0 & 0 & 0 \\ 0 & \dots & \dots & 0 & 0 & 0 & \ddots & \ddots & 0 & 0 \\ 0 & \dots & \dots & 0 & 0 & 0 & \ddots & \ddots & 0 & 0 \\ 0 & \dots & \dots & 0 & 0 & 0 & 0 & 0 & \cos(\alpha_s) & \sin(\alpha_s) \\ 0 & \dots & \dots & 0 & 0 & 0 & 0 & 0 & -\sin(\alpha_s) & \cos(\alpha_s) \end{pmatrix}$$

where $\lambda_1, \dots, \lambda_r \in \{-1, 1\}$.

Proof. (a) This is an immediate consequence of Corollary 11.4 and of Lemma 10.16.
(b) This follows from Corollary 11.6 and from Lemma 10.16 since for $z \in \mathbb{C}$ with absolute value 1 we have $\mathrm{Re}(z) = \cos(\alpha)$ and $\mathrm{Im}(z) = \sin(\alpha)$ if one writes $z = \exp(i\alpha)$. □

Part (b) is a generalization of Example 10.17.

Corollary 11.12. *Let $K \in \{\mathbb{R}, \mathbb{C}\}$. Let V be a hermitian K-space of finite dimension and let $\varphi \in \mathrm{End}_K(V)$ be an isometry.*

(i) If $K = \mathbb{C}$, then there exists an orthonormal $\mathbb{C}$-basis S of V such that $M_{S,S}(\varphi)$ is diagonal and all the coefficients on the diagonal have absolute value 1.

(ii) If $K = \mathbb{R}$, then there exists an orthonormal $\mathbb{C}$-basis S of V such that $M_{S,S}(\varphi)$ is as in part (b) of Corollary 11.11.

Proof. Its the translation of Corollary 11.11 in the case of endomorphisms. □

Definition 11.13. *(a) Let V be a hermitian K-space of finite dimension and let $\varphi \in \mathrm{End}_K(V)$ autoadjoint. One says that φ is* positive (positive definite) *if the hermitian form $\langle , \rangle_\varphi$ of Proposition 10.10 is positive (positive definite).*

(b) Let $M \in \mathrm{Mat}_{n\times n}(K)$ be an autoadjoint (symmetric (if $K = \mathbb{R}$) or hermitian (if $K = \mathbb{C}$)) matrix. One says that M is positive (positive definite) *if the hermitian form $\langle v, w \rangle_M := v^{\mathrm{tr}} M \overline{w}$ is positive (positive definite).*

Lemma 11.14. *Let V be a hermitian K-space of finite dimension with orthonormal basis S and let $\varphi \in \mathrm{End}_K(V)$ be self-adjoint. Then:*

(a) φ is positive (positive definite) $\Longleftrightarrow$ $M_{S,S}(\varphi)$ is positive (positive definite).

(b) φ is positive $\Longleftrightarrow$ $\mathrm{Spec}(\varphi) \subseteq \mathbb{R}_{\geq 0}$.

(c) φ is positive definite $\Longleftrightarrow$ $\mathrm{Spec}(\varphi) \subseteq \mathbb{R}_{>0}$.

Proof. Exercise. □

Lemma 11.15. *Let $M \in \mathrm{Mat}_{n\times n}(K)$ be a positive and self-adjoint matrix (symmetric (if $K = \mathbb{R}$) or hermitian (if $K = \mathbb{C}$)). Then there exists a positive matrix $N \in \mathrm{Mat}_{n\times n}(K)$ such that $N^2 = M$ and $NM = MN$. Moreover, M is positive definite if and only if N is.*

Proof. Exercise. □

Theorem 11.16 (Décomposition polaire)**.** *Let V be a hermitian K-space of finite dimension and let $\varphi \in \mathrm{End}_K(V)$ be an isomorphism (i.e. an invertible endomorphism).*
Then there exists a unique autoadjoint and positive $\psi \in \mathrm{End}_K(V)$ and a unique isomerty $\chi \in \mathrm{End}_K(V)$ such that $\varphi = \chi \circ \psi$.

Proof. Existence: By one of the exercises, φ^{ad} is also an isomorphism. Define the isomorphism $\theta := \varphi^{\mathrm{ad}} \circ \varphi$. It is self-adjoint:

$$\theta^{\mathrm{ad}} = (\varphi^{\mathrm{ad}} \circ \varphi)^{\mathrm{ad}} = \varphi^{\mathrm{ad}} \circ (\varphi^{\mathrm{ad}})^{\mathrm{ad}} = \varphi^{\mathrm{ad}} \circ \varphi = \theta,$$

hence $\mathrm{Spec}(\theta) \subseteq \mathbb{R}$ by Lemma 10.16. Let us now show that it is positive definite:

$$\langle v, v\rangle_\theta = \langle \theta(v), v\rangle = \langle \varphi^{\mathrm{ad}}(\varphi(v)), v\rangle = \langle \varphi(v), \varphi(v)\rangle = |\varphi(v)|^2 > 0$$

for all $0 \neq v \in V$. Therefore, by Lemma 11.15 there exists positive definite $\psi \in \mathrm{End}_K(V)$ such that $\psi^2 = \theta$. Put $\chi := \varphi \circ \psi^{-1}$. To finish the proof of existence it suffices to prove that χ is an isomerty:

$$\begin{aligned}\chi^{-1} = \psi \circ \varphi^{-1} = \psi^{-1} \circ \psi^2 \circ \varphi^{-1} &= \psi^{-1} \circ \theta \circ \varphi^{-1} \\ &= \psi^{-1} \circ \varphi^{\mathrm{ad}} \circ \varphi \circ \varphi^{-1} = \psi^{-1} \circ \varphi^{\mathrm{ad}} = (\varphi \circ \psi^{-1})^{\mathrm{ad}} = \chi^{\mathrm{ad}}\end{aligned}$$

where we used $(\psi^{-1})^{\mathrm{ad}} = (\psi^{\mathrm{ad}})^{-1} = \psi^{-1}$ as ψ is self-adjoint.
Uniqueness: Assume that $\varphi = \chi_1 \circ \psi_1 = \chi_2 \circ \psi_2$ for isometries χ_1, χ_2 and self-adjoint positive definite isomorphisms ψ_1, ψ_2. We obtain

$$\chi_2^{-1} \circ \chi_1 = \psi_2 \circ \psi_1^{-1} =: \beta.$$

On the left hand side we have an isometry and on the right hand side a self-adjoint positive definite endomorphism. Thus there exists an orthonormal basis S such that $M_{S,S}(\beta)$ is diagonal, and the coefficients on the diagonal are positive reals (since β is positive self-adjoint) and of absolute value 1 (since β is an isometry). It is therefore the identity, $\beta = \mathrm{id}$, whence $\chi_1 = \chi_2$ et $\psi_1 = \psi_2$. □

12 Quadrics

Goals:

- Be able to do simultaneous operations on rows and columns;
- know the link with elementary matrices;
- be able to compute a diagonal matrix using simultaneous operations on rows and columns;
- know the definition of quadrics;
- know the definition of equivalence of quadrics;
- know the classification of quadrics;
- be able to compute the type in the classification for a given quadric;
- know examples and be able to prove simple properties.

Simultanoeus operations on rows and columns

We go back to the study of elementary operations (Gauß algorithm) on rows and columns (see Definition 1.39 and the following), except that we now do simultaneous operations on the rows and columns, i.e. any operation that is done on the rows has to be done on the columns too. For instance, if we add the third row to the fifth, then we also have to add the third column to the fifth column. The advantage is that a symmetric matrix will stay symmetric. Along with Lemma 1.40, we have the following lemma.

Lemma 12.1. *Let $\lambda \in K$, $i, j, n \in \mathbb{N}_{>0}$, $i \neq j$ and $M \in \mathrm{Mat}_{n\times n}(K)$.*

(a) $P_{i,j}^{\mathrm{tr}} M P_{i,j}$ is the matrix that is obtained from M by interchanging the i-th row with j-th row and the i-th column with the j-th column.

(b) $S_i(\lambda)^{\mathrm{tr}} M S_i(\lambda)$ is the matrix that is obtained from M by multiplying the i-th row and the i-th column by λ. In particular, the coefficient at (i, i) is multiplied by λ^2.

(c) $Q_{i,j}(\lambda)^{\mathrm{tr}} M Q_{i,j}(\lambda)$ is the matrix that is obtained from M by adding λ times the i-th row to the j-th row, and λ times the i-th column to the j-th column.

Proof. Il suffices to use Lemma 1.40. □

Example 12.2. *Let $M = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 4 & 5 \\ 3 & 5 & 6 \end{pmatrix}$. It is a symmetric matrix. We write the augmented matrix and we do the operations on the rows and columns (only on the right half). We need the left half only if we want a real matrix C such that CMC^{tr} (Be careful: in the above considerations, we had the transpose at the left, here it is at the right) coincides with the matrix obtained by transforming the rows and columns simultaneously.*

$$\begin{pmatrix} 1 & 0 & 0 & 1 & 2 & 3 \\ 0 & 1 & 0 & 2 & 4 & 5 \\ 0 & 0 & 1 & 3 & 5 & 6 \end{pmatrix} \mapsto \begin{pmatrix} 1 & 0 & 0 & 1 & 2 & 3 \\ -2 & 1 & 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 3 & 5 & 6 \end{pmatrix} \mapsto \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 3 \\ -2 & 1 & 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 3 & -1 & 6 \end{pmatrix}$$

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

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

$$\mapsto \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 0 \\ -3 & 0 & 1 & 0 & -3 & -1 \\ -1 & 1 & -1/3 & 0 & 0 & 1/3 \end{pmatrix} \mapsto \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 0 \\ -3 & 0 & 1 & 0 & -3 & 0 \\ -1 & 1 & -1/3 & 0 & 0 & 1/3 \end{pmatrix}$$

$$\mapsto \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 0 \\ -\sqrt{3} & 0 & 1/\sqrt{3} & 0 & -\sqrt{3} & 0 \\ -\sqrt{3} & \sqrt{3} & -1/\sqrt{3} & 0 & 0 & 1/\sqrt{3} \end{pmatrix} \mapsto \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 0 \\ -\sqrt{3} & 0 & 1/\sqrt{3} & 0 & -1 & 0 \\ -\sqrt{3} & \sqrt{3} & -1/\sqrt{3} & 0 & 0 & 1 \end{pmatrix}$$

Note that the -1 in the middle of the right half cannot be transformed into 1 since one can only multiply/divide by squares. Let C be the left half of the final matrix: $C = \begin{pmatrix} 1 & 0 & 0 \\ -\sqrt{3} & 0 & 1/\sqrt{3} \\ -\sqrt{3} & \sqrt{3} & -1/\sqrt{3} \end{pmatrix}$. The right half is the matrix obtained by simultaneous operations on the rows and columns. By Lemma 12.1, we have the following equality (to convince yourself, you can verify it by a short computaion):

$$CMC^{\text{tr}} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Writing $D = C^{\text{tr}}$, we have the transpose at the left: $D^{\text{tr}}MD = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$.

We will now generalize what we have seen in the example.

Proposition 12.3. *Let K be a field such that $1 + 1 \neq 0$ and let $M \in \text{Mat}_{n\times n}(K)$ be a symmetric matrix. Then there is a matrix $C \in \text{GL}_n(K)$ such that $C^{\text{tr}}MC$ is a diagonal matrix.*

Proof. The proof is done by induction on n. The case $n = 1$ is trivial (there is nothing to do). Assume the proposition is proven for matrices of size $n - 1$.

Let $M = \begin{pmatrix} m_{1,1} & m_{1,2} & \dots & m_{1,n} \\ m_{2,1} & m_{2,2} & \dots & m_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ m_{n,1} & m_{n,2} & \dots & m_{n,n} \end{pmatrix}$. If M is the zero matrix, there is nothing to do. Let us therefore suppose that M is non-zero. We will use simultaneous operations on the rows and columns. We proceed in two steps.

(1) Transform the matrix so that $m_{1,1} \neq 0$.

Case 1: there exists i such that $m_{i,i} \neq 0$: In this case, we interchange the i-th and the first row and the i-th and the first column.

Case 2: $m_{i,i} = 0$ for all $i = 1, \dots, n$: Since M is not the zero matrix, there is $i \neq j$ such that $m_{i,j} \neq 0$. We add the i-th to the j-th row and the i-th to the j-th column. This gives $m_{i,j} + m_{j,i} = 2m_{i,j}$ at position (j, j) and we are thus back to Case 1.

(2) By (1), we have $m_{1,1} \neq 0$. For all $i = 2, \dots, n$, we add $-m_{1,i}/m_{1,1}$ times the first row to the i-th row and $-m_{1,i}/m_{1,1}$ times the first column to the i-th column.

We obtain a matrix of the form $\begin{pmatrix} m_{1,1} & 0 & \dots & 0 \\ 0 & m_{2,2} & \dots & m_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & m_{n,2} & \dots & m_{n,n} \end{pmatrix}$.

The induction hypothesis applied to the remaining block of size $n - 1$ finishes the proof. □

Corollary 12.4. *The rank of a matrix is invariant under simultaneous operations on the rows and columns.*

Proof. Assume that N is obtained from M by simultaneous operations on the rows and columns. By Proposition 12.3 we have $C^{\mathrm{tr}}MC = N$ for an invertible matrix C. Since C^{tr} is also invertible (for instance, since $0 \neq \det(C) = \det(C^{\mathrm{tr}})$), we have $\mathrm{rk}(N) = \mathrm{rk}(C^{\mathrm{tr}}MC) = \dim(\mathrm{im}(C^{\mathrm{tr}}MC)) = \dim(\mathrm{im}(C^{\mathrm{tr}}M)) = \dim(C^{\mathrm{tr}}(\mathrm{im}(M)) = \dim(\mathrm{im}(M)) = \mathrm{rk}(M)$. □

Quadrics

In the whole section, let K be a field such that $1 + 1 \neq 0$, for instance $K = \mathbb{R}$ or $K = \mathbb{C}$. First recall that $K[X_1, X_2, \ldots, X_n]$ denotes the ring of polynomials in variables $X_1, X_2, \ldots, X_n$ with coefficients in K. An element of $K[X_1, X_2, \ldots, X_n]$ is of the form

$$\sum_{i_1=0}^{d_1} \sum_{i_2=0}^{d_2} \cdots \sum_{i_n=0}^{d_n} a_{i_1,i_2,\ldots,i_n} X_1^{i_1} X_2^{i_2} \ldots X_n^{i_n}.$$

In the sequel, we will only consider quadratic polynomials.

Definition 12.5. *We call* quadratic polynomial (in n variables and with coefficients in K) *any element of* $K[X_1, X_2, \ldots, X_n]$ *of the form*

$$q(X_1, X_2, \ldots, X_n) = \sum_{1 \leq i \leq j \leq n} a_{i,j} X_i X_j + \sum_{i=1}^{n} a_{0,i} X_i + a_{0,0}.$$

Example 12.6. *(a) Let $n = 1$. Let X be the variable. Any quadratic polynomial is of the form*

$$a_{1,1}X^2 + a_{0,1}X + a_{0,0} = a_2X^2 + a_1X + a_0$$

where we relabelled the coefficients in a standard way.

(b) Let $n = 2$. Let X, Y be the variables. Any quadratic polynomial is of the form

$$a_{1,1}X^2 + a_{1,2}XY + a_{2,2}Y^2 + a_{0,1}X + a_{0,2}Y + a_{0,0}.$$

In particular, we have the following example:

(1) $\frac{X^2}{a^2} + \frac{Y^2}{b^2} - 1$

(2) $\frac{X^2}{a^2} - \frac{Y^2}{b^2} - 1$

(3) $\frac{X^2}{a^2} - Y$

Lemma 12.7. *Let $n \in \mathbb{N}$ and let $A \in \mathrm{Mat}_{(n+1)\times(n+1)}(K)$ be a symmetric matrix. Its coefficients will be called $a_{i,j}$ for $0 \leq i, j \leq n$ (note that the numeration starts at 0!). Let $\tilde{X}$ be the vector containing the variables preceded by 1:*

$$A = \begin{pmatrix} a_{0,0} & a_{0,1} & \cdots & a_{0,n} \\ a_{0,1} & a_{1,1} & \cdots & a_{1,n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{0,n} & a_{1,n} & \cdots & a_{n,n} \end{pmatrix}, \quad \tilde{X} = \begin{pmatrix} 1 \\ X_1 \\ \vdots \\ X_n \end{pmatrix}.$$

Then the polynomial

$$q_A(X_1,\dots,X_n)=\tilde{X}^{\mathrm{tr}}A\tilde{X}=2\sum_{1\le i<j\le n}a_{i,j}X_iX_j+\sum_{i=1}^{n}a_{i,i}X_i^2+2\sum_{i=1}^{n}a_{0,i}X_i+a_{0,0}$$

is quadratic and any quadratic polynomial arises from a unique symmetric matrix A by this formula.

Proof. Clear. □

As in the preceding lemma, for $x=\begin{pmatrix}x_1\\ \vdots\\ x_n\end{pmatrix}\in K^n$, we denote $\tilde{x}=\begin{pmatrix}1\\ x_1\\ \vdots\\ x_n\end{pmatrix}$, the vector x preceded by 1.

Definition 12.8. *We call* quadric (in dimension n) *any set*

$$Q_A:=Q_A(K):=\{x\in K^n\mid \tilde{x}^{\mathrm{tr}}A\tilde{x}=0\}$$

where A is a symmetric matrix $\mathrm{Mat}_{(n+1)\times(n+1)}(K)$.

Example 12.9. *Consider $n=2$.*

(1) Let $A=\begin{pmatrix}-1&0&0\\0&\frac{1}{a^2}&0\\0&0&\frac{1}{b^2}\end{pmatrix}$. We have $Q_A=\{x\in\mathbb{R}^2\mid \frac{X^2}{a^2}+\frac{Y^2}{b^2}-1=0\}$. Geometrically, it defines an ellipse.

(2) Let $A=\begin{pmatrix}-1&0&0\\0&\frac{1}{a^2}&0\\0&0&\frac{-1}{b^2}\end{pmatrix}$. We have $Q_A=\{x\in\mathbb{R}^2\mid \frac{X^2}{a^2}-\frac{Y^2}{b^2}-1=0\}$. Geometrically, it defines a hyperbola.

(3) Let $A=\begin{pmatrix}0&0&\frac{-1}{2}\\0&\frac{1}{a^2}&0\\\frac{-1}{2}&0&0\end{pmatrix}$. We have $Q_A=\{x\in\mathbb{R}^2\mid \frac{X^2}{a^2}-Y=0\}$. Geometrically, it defines a parabola.

We also define an augmented matrix: let $C=(c_{i,j})\in\mathrm{Mat}_{n\times n}(K)$ be a matrix and $y\in K^n$ a vector. We set:

$$\widetilde{C_y}=\begin{pmatrix}1&0&\dots&0\\y_1&c_{1,1}&\dots&c_{1,n}\\\vdots&\vdots&\ddots&\vdots\\y_n&c_{n,1}&\dots&c_{n,n}\end{pmatrix}.$$

Lemma 12.10. *Let $A\in\mathrm{Mat}_{(n+1)\times(n+1)}(K)$ be a symmetric matrix and Q_A the associated quadric. Let $\varphi:K^n\to K^n$ be an* affinity, *i.e. an application of the form*

$$\varphi(v)=Bv+By$$

where $B \in \mathrm{GL}_n(K)$ and $y \in K^n$. Let $\tilde{C} := \widetilde{(B^{-1})}_{-y} = \begin{pmatrix} 1 & 0 & \dots & 0 \\ -y_1 & c_{1,1} & \dots & c_{1,n} \\ \vdots & \vdots & \ddots & \vdots \\ -y_n & c_{n,1} & \dots & c_{n,n} \end{pmatrix}$.
Then $\varphi(Q_A) = Q_{\tilde{C}^{\mathrm{tr}}A\tilde{C}}$. The image of a quadric by an affinity is therefore also a quadric.

Proof. The claim follows from the equality

$$\tilde{C}\widetilde{\varphi(x)} = \tilde{C}(\widetilde{Bx+By}) = (\widetilde{-y+x+y}) = \tilde{x}.$$

We therefore obtain the equality

$$\tilde{x}^{\mathrm{tr}}A\tilde{x} = (\tilde{C}\widetilde{\varphi(x)})^{\mathrm{tr}}A(\tilde{C}\widetilde{\varphi(x)}) = \widetilde{\varphi(x)}^{\mathrm{tr}}\left(\tilde{C}^{\mathrm{tr}}A\tilde{C}\right)\widetilde{\varphi(x)},$$

which proves the result. □

Definition 12.11. *Let $q_1(X_1,\dots,X_n)$ et $q_2(X_1,\dots,X_n)$ be quadratic polynomials arising from the symmetric matrices $A, B \in \mathrm{Mat}_{(n+1)\times(n+1)}(K)$, i.e. $q_1 = q_A$, $q_2 = q_B$.*
We say that $q_1(X_1,\dots,X_n)$ et $q_2(X_1,\dots,X_n)$ are equivalent *if there exists $C \in \mathrm{GL}_n(K)$, $y \in K^n$ and $0 \neq x \in K$ such that $\widetilde{C_y}^{\mathrm{tr}} A \widetilde{C_y} = xB$.*

Thus, by Lemma 12.10 we have that $q_A(X_1,\dots,X_n)$ and $q_B(X_1,\dots,X_n)$ are equivalent if and only if there exists an affinity $\varphi : K^n \to K^n$ such that $\varphi(Q_A) = Q_B$.
Our next goal is to characterize the quadrics up to equivalence. For this, we need the following definition.

Definition 12.12. *We call* system of representatives of $K^\times$ modulo squares *any set $R \in K \setminus \{0\}$ verifying that for all $x \in K^\times$ there is a unique $r \in R$ and $y \in K$ such that $x = r \cdot y^2$.*

Example 12.13. *(a) If $K = \mathbb{C}$, then $R = \{1\}$ is a system of representatives of $\mathbb{C}^\times$ modulo squares. Indeed, any element of $\mathbb{C}$ is a square.*

(b) If $K = \mathbb{R}$, then $R = \{-1, 1\}$ is a system of representatives of $\mathbb{R}^\times$ modulo squares. Indeed, any positive element of $\mathbb{R}$ is a square, and any negative element is minus a square.

(c) We call squarefree *any integer $m \in \mathbb{Z}$ that is not divisible by any square of a prime number. Let $R = \{m \in \mathbb{Z} \mid m \text{ is squarefree }\}$.*

If $K = \mathbb{Q}$, then R is a system of representatives $\mathbb{Q}^\times$ modulo squares. Indeed, one can write

$$\frac{a}{b} = ab\frac{1}{b^2} = m\left(\frac{q}{b}\right)^2$$

where $ab = mq^2$ for squarefree $m \in \mathbb{Z}$. Moreover, if $m = m'\left(\frac{r}{s}\right)^2$ and m, m' are squarefree, then $m' \mid m$; similarly, $m \mid m'$; since m and m' have the same sign, we obtain $m = m'$, proving uniqueness.

In the theorem of the classification of quadrics, we will use the following notations: For $n \in \mathbb{N}$, the coefficients of the symmetric matrices $A \in \mathrm{Mat}_{(n+1)\times(n+1)}(K)$ will be labelled as follows:

$$A = \begin{pmatrix} a_{0,0} & a_{0,1} & \dots & a_{0,n} \\ a_{0,1} & a_{1,1} & \dots & a_{1,n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{0,n} & a_{1,n} & \dots & a_{n,n} \end{pmatrix}.$$

Let A_n denote the block of size $n \times n$ of A in the bottom-right corner:

$$A_n = \begin{pmatrix} a_{1,1} & \dots & a_{1,n} \\ \vdots & \ddots & \vdots \\ a_{1,n} & \dots & a_{n,n} \end{pmatrix}.$$

Lemma 12.14. *Let $A \in \mathrm{Mat}_{(n+1)\times(n+1)}(K)$ be symmetric, $C \in \mathrm{GL}_n(K)$ and $y \in K^n$. Then*

$$\left(\widetilde{C_y}^{\mathrm{tr}} A \widetilde{C_y}\right)_n = C^{\mathrm{tr}} A_n C.$$

In particular, the rank of A_n is equal to the rank of $\left(\widetilde{C_y}^{\mathrm{tr}} A \widetilde{C_y}\right)_n$. Thus, the rank of A_n is invariant under equivalence of quadratic polynomials.

Proof. The facts that the first column of $\widetilde{C_y}^{\mathrm{tr}}$ is the vector $\begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$ and that the first row of $\widetilde{C_y}$ is the vector $\begin{pmatrix} 1 & 0 & \dots & 0 \end{pmatrix}$ show the result. □

Theorem 12.15 (Classification of quadrics)**.** *Let R be a system of representatives of$K^\times$ modulo squares. Let $q_A(X_1, \dots, X_n)$ be the quadratic polynomial associated to the symmetric matrix $A \in \mathrm{Mat}_{(n+1)\times(n+1)}(K)$. Let r be the rank of the matrix A_n.*
We have the three following cases:

(I) If $\mathrm{rk}(A) = r$, then there exist $a_2, a_3, \dots, a_r \in R$ such that $q_A(X_1, \dots, X_n)$ is equivalent to $X_1^2 + a_2X_2^2 + a_3X_3^2 + \dots + a_rX_r^2$.

(II) If $\mathrm{rk}(A) = r + 1$, then there exist $a_1, a_2, \dots, a_r \in R$ such that $q_A(X_1, \dots, X_n)$ is equivalent to $a_1X_1^2 + a_2X_2^2 + \dots + a_rX_r^2 + 1$.

(III) If $\mathrm{rk}(A) = r + 2$, then $r \le n - 1$ and there exist $a_1, a_2, \dots, a_r \in R$ such that $q_A(X_1, \dots, X_n)$ is equivalent to $a_1X_1^2 + a_2X_2^2 + \dots + a_rX_r^2 + 2X_{r+1}$.

Proof. In order to obtain these special forms, we are allowed to only use these simultaneous operations on the rows and columns that correspond to the matrices $\widetilde{C_y}$ with C being one of the matrices of Definition 1.39 and $y \in K^n$ any vector.
We proceed in more steps:

(1) In view of Lemma 12.14, Proposition 12.3 shows that using matrices $\widetilde{C_0}$, the matrix A can be transformed into

$$B = \begin{pmatrix} b_{0,0} & b_{0,1} & \dots & b_{0,r} & b_{0,r+1} & \dots & b_{0,n} \\ b_{0,1} & b_{1,1} & 0 & 0 & 0 & \dots & 0 \\ \vdots & 0 & \ddots & 0 & 0 & \ddots & 0 \\ b_{0,r} & 0 & \dots & b_{r,r} & 0 & \dots & 0 \\ b_{0,r+1} & 0 & \dots & 0 & 0 & \dots & 0 \\ \vdots & \vdots & & \vdots & \vdots & \ddots & \vdots \\ b_{0,n} & 0 & \dots & 0 & 0 & \dots & 0 \end{pmatrix}$$

for $b_{i,i} \neq 0$ for $1 \leq i \leq r$ in such a way that q_A and q_B are equivalent.

(2) Note that adding the i-the row (for $i > 1$) to the first corresponds to the matrix $\widetilde{\mathrm{id}_{e_i}}^{\mathrm{tr}}$ where e_{i-1} is the i-th canonical vector. We can thus transform our matrix to obtain

$$B = \begin{pmatrix} b_{0,0} & 0 & \dots & 0 & b_{0,r+1} & \dots & b_{0,n} \\ 0 & b_{1,1} & 0 & 0 & 0 & \dots & 0 \\ \vdots & 0 & \ddots & 0 & 0 & \ddots & 0 \\ 0 & 0 & \dots & b_{r,r} & 0 & \dots & 0 \\ b_{0,r+1} & 0 & \dots & 0 & 0 & \dots & 0 \\ \vdots & \vdots & & \vdots & \vdots & \ddots & \vdots \\ b_{0,n} & 0 & \dots & 0 & 0 & \dots & 0 \end{pmatrix}.$$

(3) It is here where case distinctions have to be made.

(I) Assume $b_{0,0} = b_{0,r+1} = b_{0,r+2} = \cdots = b_{0,n} = 0$. In this case the rank of B (which is equal to the rank of A) is equal to$r$. We could furthermore divide by $b_{1,1}$ (because of the element $0 \neq x \in K$ in the definition of equivalence) to obtain

$$B = \begin{pmatrix} 0 & 0 & \dots & \dots & 0 & 0 & \dots & 0 \\ 0 & 1 & 0 & \dots & 0 & 0 & \dots & 0 \\ \vdots & 0 & b_{2,2} & \ddots & \vdots & 0 & \ddots & 0 \\ 0 & 0 & 0 & \ddots & 0 & 0 & \dots & 0 \\ 0 & 0 & \dots & 0 & b_{r,r} & 0 & \dots & 0 \\ 0 & 0 & \dots & \dots & 0 & 0 & \dots & 0 \\ \vdots & \vdots & \ddots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 0 & 0 & 0 & \dots & 0 \end{pmatrix}.$$

Finally, multiplying the i-th column and the i-th row for $2 \leq i \leq r$ by a suitable element a in K (that is, multiplying $b_{i,i}$ by a^2) we can choose $b_{i,i}$ in R. Now, q_B is precisely of the form (I) in the statement.

(II) Assume $b_{0,r+1} = b_{0,r+2} = \cdots = b_{0,n} = 0$, but $b_{0,0} \neq 0$. In this case, the rank of B (which is equal to the rank of A) is equal to $r + 1$. After division by $b_{0,0}$, we obtain

$$B = \begin{pmatrix} 1 & 0 & \dots & \dots & 0 & 0 & \dots & 0 \\ 0 & b_{1,1} & 0 & \dots & 0 & 0 & \dots & 0 \\ \vdots & 0 & b_{2,2} & \ddots & \vdots & 0 & \ddots & 0 \\ 0 & 0 & 0 & \ddots & 0 & 0 & \dots & 0 \\ 0 & 0 & \dots & 0 & b_{r,r} & 0 & \dots & 0 \\ 0 & 0 & \dots & \dots & 0 & 0 & \dots & 0 \\ \vdots & \vdots & \ddots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 0 & 0 & 0 & \dots & 0 \end{pmatrix}.$$

As in (I), we can achieve $b_{i,i} \in R$ for $1 \leq i \leq r$. Now, q_B is precisely of the form (II) in the statement.

(III) Assume there exists $r + 1 \leq i \leq n$ such that $b_{0,i} \neq 0$. Interchanging simultaneously rows and columns, we can first obtain $b_{0,r+1} \neq 0$. Dividing the matrix by $b_{0,r+1}$, we can thus put this coefficient to be 1. Adding $-b_{0,j}$ times the $(r+1)$-th row to the j-th for $r+2 \leq j \leq n$ (which corresponds to the matrix $(\widetilde{Q_{r,j-1}})_0^{\mathrm{tr}}$) we manage to annihilate $b_{0,j}$ for those j. We thus have the matrix

$$B = \begin{pmatrix} 0 & 0 & \dots & 0 & 0 & 1 & 0 & \dots & 0 \\ 0 & b_{1,1} & 0 & 0 & 0 & 0 & \dots & \dots & 0 \\ \vdots & 0 & b_{2,2} & 0 & \dots & 0 & \ddots & \ddots & 0 \\ 0 & 0 & 0 & \ddots & 0 & 0 & 0 & \dots & 0 \\ 0 & 0 & 0 & 0 & b_{r,r} & 0 & 0 & \dots & 0 \\ 1 & 0 & 0 & \dots & 0 & 0 & 0 & \dots & 0 \\ 0 & 0 & \dots & \dots & 0 & 0 & 0 & \dots & 0 \\ \vdots & \vdots & \ddots & \ddots & \vdots & \vdots & 0 & \ddots & \vdots \\ 0 & 0 & \dots & \dots & 0 & 0 & 0 & \dots & 0 \end{pmatrix}.$$

We see that the rank of B is equal to $r + 2$. As in (I) and (II), we can achieve $b_{i,i} \in R$ for $1 \leq i \leq r$. Now, q_B est precisely of the form (III) in the statement.

This finishes the proof. □

Corollary 12.16. *Let $K = \mathbb{C}$. Let $q(X_1, \dots, X_n) \in \mathbb{C}[X_1, \dots, X_n]$ be a non-zero quadratic polynomial. Then it is equivalent to a unique polynomial among the $3n - 1$ polynomials listed below:*

(I) $X_1^2 + \cdots + X_r^2$ for $1 \leq r \leq n$;

(II) $X_1^2 + \cdots + X_r^2 + 1$ for $1 \leq r \leq n$;

(III) $X_1^2 + \cdots + X_r^2 + 2X_{r+1}$ for $1 \leq r \leq n - 1$.

Proof. We know that $R = \{1\}$ is a system of representatives of $\mathbb{C}^\times$ modulo squares. Hence Theorem 12.15 implies that q is equivalent to one of the listed polynomials. The uniqueness follows from the fact that in this case, the rank together with the type ((I), (II), (III)) is enough to uniquely characterize the polynomial. □

Our next goal is an explicit classification of real quadrics. For this, we have to show the following theorem of Sylvester. First, we need a lemma.

Lemma 12.17. *Let $A \in \mathrm{Mat}_{n\times n}(\mathbb{R})$ be a symmetric matrix and let $\langle v, w\rangle_A := \langle Av, w\rangle$ the symmetric form defined by A on $\mathbb{R}^n$.*

(a) There exist subspaces $V_+, V_-, V_0 \leq \mathbb{R}^n$ such that

- $\mathbb{R}^n = V_+ \bigoplus V_- \bigoplus V_0$,
- *for all $0 \neq v \in V_+$, we have $\langle v, v\rangle_A > 0$,*
- *for all $0 \neq v \in V_-$, we have $\langle v, v\rangle_A < 0$ et*
- *for all $0 \neq v \in V_0$, we have $\langle v, v\rangle_A = 0$.*

(b) If V_+, V_-, V_0 are subspaces having the properties in (a), then

- $\dim V_+$ *is the number of positive eigenvalues of A,*
- $\dim V_-$ *is the number of negative eigenvalues of A et*
- $\dim V_0$ *is the number of 0 eigenvalues of A.*

We have to count the eigenvalues with multiplicity, i.e. the number of times the eigenvalue appears on the diagonal after diagonalization.

Proof. By the spectral theorem, we have an orthonormal basis

$$v_1, \dots, v_s, v_{s+1}, \dots, v_r, v_{r+1}, \dots, v_n$$

of $\mathbb{R}^n$ such that v_i for $1 \leq i \leq s$ are eigenvectors for a positive eigenvalue, v_i for $s+1 \leq i \leq r$ are eigenvectors for a negative eigenvalue and v_i for $s+1 \leq i \leq r$ are eigenvectors for the 0 eigenvalue. We take V_+ to be the subspace generated by $v_1, \dots, v_s$ and V_i the subspace generated by $v_{s+1}, \dots, v_r$ and V_0 the subspace generated by $v_{r+1}, \dots, v_n$. It is clear that all the properties of (a) and (b) are satisfied for these spaces.
Let now V_+', V_-', V_0' be other spaces having the properties of (a). We show that $V_+ \cap (V_-' \oplus V_0') = 0$: if $0 \neq v = w_- + w_0$ for $w_- \in V_-'$ and $w_0 \in V_0'$ were a vector in the intersection, we would have $\langle v, v\rangle_A > 0$ on one side and $\langle w_- + w_0, w_- + w_0\rangle_A = \langle w_-, w_-\rangle_A + \langle w_0, w_0\rangle_A \leq 0$ on the other side. This shows that $V_+ \oplus V_-' \oplus V_0'$ is a subspace of $\mathbb{R}^n$, hence $\dim V_+ \leq \dim V_+'$. By symmetry, we also have $\dim V_+' \leq \dim V_+$, and thus equality. The arguments for the two other equalities are similar. □

Theorem 12.18 (Sylvester). *Let $A \in \mathrm{Mat}_{n\times n}(\mathbb{R})$ be a symmetric matrix and let $C \in \mathrm{GL}_n(\mathbb{R})$. Then, A and $C^{\mathrm{tr}}AC$ have the same number of positive eigenvalues. The same statement holds for negative eigenvalues.*

Proof. We use the notation of Lemma 12.17 for the bilinear form $\langle , \rangle_A$. Consider $C^{-1}V_+$. If $0 \neq v \in C^{-1}V_+$ (hence $Cv \in V_+$), then

$$0 < \langle Cv, Cv\rangle_A = \langle ACv, Cv\rangle = \langle C^{\mathrm{tr}}ACv, v\rangle = \langle v, v\rangle_{C^{\mathrm{tr}}AC}.$$

Moreover, if $w \in C^{-1}V_-$, then

$$0 = \langle Cv, Cw\rangle_A = \langle ACv, Cw\rangle = \langle C^{\mathrm{tr}}ACv, w\rangle = \langle v, w\rangle_{C^{\mathrm{tr}}AC},$$

and thus $C^{-1}V_+ \mathbin{\perp\!\!\!\!\bigcirc} C^{-1}V_-$. By similar arguments, we obtain that $C^{-1}V_+$, $C^{-1}V_-$, $C^{-1}V_0$ are subspaces that satisfy the properties in (a) of Lemma 12.17 for the bilinear form $\langle , \rangle_{C^{\mathrm{tr}}AC}$. Hence the dimension of V_+ (which is the number of positive eigenvalues of A) is equal to the number of positive eigenvalues of $C^{\mathrm{tr}}AC$. The argument for negative eigenvalues is the same. □

Corollary 12.19. *Let $K = \mathbb{C}$. Let $q(X_1, \dots, X_n) \in \mathbb{C}[X_1, \dots, X_n]$ be a non-zero quadratic polynomial. Then it is equivalent to a unique polynomial among the $\frac{3n^2+5n}{2} - 1$ polynomials listed below:*

(I) $X_1^2 + \cdots + X_s^2 - X_{s+1}^2 - \cdots - X_r^2$ *for* $1 \leq s \leq r \leq n$*;*

(II) $X_1^2 + \cdots + X_s^2 - X_{s+1}^2 - \cdots - X_r^2 + 1$ *for* $0 \leq s \leq r \leq n$*,* $1 \leq r$*;*

(III) $X_1^2 + \cdots + X_s^2 - X_{s+1}^2 - \cdots - X_r^2 + 2X_{r+1}$ *for* $0 \leq s \leq r \leq n-1$*,* $1 \leq r$*.*

Proof. We know that $R = \{-1, 1\}$ is a system of representatives of $\mathbb{R}^\times$ modulo squares. Therefore Theorem 12.15 implies that q is equivalent to one of the listed polynomials.. The uniqueness follows from the fact that the difference between the big matrix and the rank of the block of size n in the bottom-right corner determines the type ((I), (II), (III)). Thus it suffices to know the number of positive eigenvalues (and negative ones) in view of Sylvester's Theorem 12.18.
The number of polynomials of type (I) of rank r is equal to r (the sign in front of X_1 is always $+$), hence there exist $1 + 2 + \cdots + n = \frac{n(n+1)}{2}$ polynomials of type (I). The number of polynomials of type (II) of rank r is equal to $r + 1$ (the sign in front of X_1 can be 1 or -1), hence there exist $2+3+\cdots+(n+1) = \frac{(n+1)(n+2)}{2} - 1$ polynomials of type (II). Similarly, the number of polynomials of type (III) of rank r is equal to $r + 1$, but r is bounded by $n - 1$, hence there exist $2 + 3 + \cdots + n = \frac{n(n+1)}{2} - 1$ polynomials of type (III). We thus obtain

$$\frac{n(n+1)}{2} + \frac{(n+1)(n+2)}{2} - 1 + \frac{n(n+1)}{2} - 1 = \frac{3n^2+5n}{2} - 1,$$

the desired number. □

13 Duality

Goals:

- Master the concepts of dual space and dual application;
- know the relation to transpose matrices;

- know the definition and fundamental properties of bilinear forms;
- know the relation to the rank of rows and columns of matrices;
- know examples and be able to prove simple properties.

In this section, we introduce a theory of duality, that is valid for any field K (not only for $\mathbb{R}$ and $\mathbb{C}$). The main results of this section are

- the interpretation of transpose matrices as matrices representing "dual" applications;
- the rank of the columns of a matrix is equal to the rank of the rows; this is sometimes useful for computations.

We start with the interpretation of transpose matrices as matrices representing dual applications. For this, we first introduce the dual vector spacel V^* of a vector space V.

Lemma 13.1. *Let V, W be two K-vector spaces.*

(a) The set of K-linear applications

$$\mathrm{Hom}_K(V,W) := \{f : V \to W \mid f \text{ is } K\text{-linear }\}$$

is a K-vector space for the addition

$$(f+g)(v) := f(v) + g(v) \text{ for } f, g \in \mathrm{Hom}_K(V,W) \text{ and } v \in V$$

and the scalar multiplication

$$(x.f)(v) := x.(f(v)) = f(x.v) \text{ for } f \in \mathrm{Hom}_K(V,W),\ x \in K \text{ and } v \in V.$$

(b) Let S be a K-basis of V and $f : S \to W$ be an application. Then, there exists a unique $F \in \mathrm{Hom}_K(V,W)$ such that $F|_S = f$, namely $F(\sum_{s\in S} a_s s) = \sum_{s\in S} a_s f(s)$.

Proof. Simple computations. □

Definition 13.2. *Let V be a K-vector space. The K-vector space (see Lemma 13.1(a))*

$$V^* := \mathrm{Hom}_K(V,K)$$

is called the dual space of V.

Proposition 13.3. *Let V be a K-vector space of finite dimension n.*

(a) Let $S = \{s_1, \dots, s_n\}$ be a K-basis of V. For all $1 \le i \le n$, let s_i^* be the unique (by Lemma 13.1(b)) element in V^* such that for all $1 \le j \le n$ we have $s_i^*(s_j) = \delta_{i,j} = \begin{cases} 1 & \text{if } i = j, \\ 0 & \text{if } i \neq j. \end{cases}$

Then, $S^* := \{s_1^*, \dots, s_n^*\}$ is a K-basis of V^*, called the dual basis.

(b) If V has finite K-dimension, then $\dim_K(V^*) = \dim_K(V)$.

Proof. (a) Linear independence: Let $0 = \sum_{i=1}^{n} a_i s_i^*$ with $a_1, \dots, a_n \in K$. Then, for all $1 \le j \le n$ we have

$$0 = \sum_{i=1}^{n} a_i s_i^*(s_j) = \sum_{i=1}^{n} a_i \delta_{i,j} = a_j.$$

Generating: Let $f \in V^*$. For $1 \le j \le n$, set $a_j := f(s_j)$ and $g := \sum_{i=1}^{n} a_i s_i^* \in V^*$. We have

$$g(s_j) = \sum_{i=1}^{n} a_i s_i^*(s_j) = a_j = f(s_j)$$

for all $1 \le j \le n$, thus $f = g$.
(b) The dimension of V is the cardinality of any basis of V. By (a), the dual basis has the same cardinality as any basis of V, thus the dimension of V^* equals the dimension of V. □

Definition-Lemma 13.4. *Let V, W be two K-vector spaces and $\varphi : V \to W$ be a K-linear application. Then, the application*

$$\varphi^* : W^* \to V^*, \quad f \mapsto \varphi^*(f) = f \circ \varphi$$

is K-linear. It is called the dual application of φ.

Proof. Firstly we note that $\varphi \circ f$ is K-linear; but, this follows from the fact that the composition of two linear applications is linear. Let $f, g \in W^*$ and $x \in K$. We conclude the proof by the computation

$$\begin{aligned}\varphi^*(x \cdot f + g)(v) &= ((x \cdot f + g) \circ \varphi)(v) = (x \cdot f + g)(\varphi(v)) \\ &= xf(\varphi(v)) + g(\varphi(v)) = (x\varphi^*(f) + \varphi^*(g))(v).\end{aligned}$$

for any $v \in V$, whence $\varphi^*(x \cdot f + g) = x\varphi^*(f) + \varphi^*(g)$. □

Proposition 13.5. *Let V, W be two K-vector spaces and $\varphi : V \to W$ be a K-linear application. Let moreover $S = \{s_1, \dots, s_n\}$ be a K-basis of V and $T = \{t_1, \dots, t_m\}$ a K-basis of W. Then,*

$$\big(M_{T,S}(\varphi)\big)^{\mathrm{tr}} = M_{S^*,T^*}(\varphi^*).$$

Thus, the matrix representing φ^* for the dual bases is the transpose of the matrix representing φ.

Proof. We write

$$M_{T,S}(\varphi) = \begin{pmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,n} \\ a_{2,1} & a_{2,2} & \cdots & a_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m,1} & a_{m,2} & \cdots & a_{m,n} \end{pmatrix} \text{ and } M_{S^*,T^*}(\varphi^*) = \begin{pmatrix} b_{1,1} & b_{1,2} & \cdots & b_{1,m} \\ b_{2,1} & b_{2,2} & \cdots & b_{2,m} \\ \vdots & \vdots & \ddots & \vdots \\ b_{n,1} & b_{n,2} & \cdots & b_{n,m} \end{pmatrix}.$$

This means

$$\varphi(s_j) = \sum_{i=1}^{m} a_{i,j} t_i \text{ and } \varphi^*(t_k^*) = \sum_{i=1}^{n} b_{i,k} s_i^*$$

for all $1 \leq j \leq n$ and $1 \leq k \leq m$. Thus, on the one hand

$$(\varphi^*(t_k^*))(s_j) = t_k^*(\varphi(s_j)) = t_k^*(\sum_{i=1}^{m} a_{i,j} t_i) = \sum_{i=1}^{m} a_{i,j} t_k^*(t_i) = a_{k,j}$$

and on the other hand

$$(\varphi^*(t_k^*))(s_j) = \sum_{i=1}^{n} b_{i,k} s_i^*(s_j) = b_{j,k},$$

whence $a_{k,j} = b_{j,k}$, as desired. □

The dual space gives rise to a natural bilinear form, as we will see in Example 13.8(b); first we make the necessary definitions.

Definition 13.6. *Let V, W be two K-vector spaces. One calls* bilinear form *any application*

$$\langle \cdot, \cdot \rangle : V \times W \to K$$

such that

- $\forall\, a \in K\ \forall\, v_1, v_2 \in V\ \forall\, w \in W : \langle av_1 + v_2, w\rangle = a\langle v_1, w\rangle + \langle v_2, w\rangle$ *(linearity in the first variable) and*
- $\forall\, b \in K\ \forall\, v \in V\ \forall\, w_1, w_2 \in W : \langle v, bw_1 + w_2\rangle = b\langle v, w_1\rangle + \langle v, w_2\rangle$ *(linearity in the second variable).*

Let $\langle \cdot, \cdot \rangle : V \times W \to K$ be a bilinear form. For a subspace $V_1 \leq V$, we call

$$V_1^{\perp} := \{w \in W \mid \forall v \in V_1 : \langle v, w\rangle = 0\} \leq W$$

the orthogonal complement of V_1 in W.
For a subspace $W_1 \leq W$, we call

$$W_1^{\perp} := \{v \in V \mid \forall w \in W_1 : \langle v, w\rangle = 0\} \leq V$$

the orthogonal complement of W_1 in V.
We say that the bilinear form is non-degenerate *if*

- $\forall\, 0 \neq v \in V\ \exists\, w \in W : \langle v, w\rangle \neq 0$ *and*
- $\forall\, 0 \neq w \in W\ \exists\, v \in V : \langle v, w\rangle \neq 0$.

In the sequel, we will write $\langle v, W_1\rangle = 0$ for $\forall\, w \in W_1 : \langle v, w\rangle = 0$ (and vice-versa).

Lemma 13.7. *Let V, W be two K-vector spaces and $\langle \cdot, \cdot \rangle : V \times W \to K$ be a bilinear form.*

(a) For any subspace $V_1 \leq V$, the orthogonal complement of V_1 in W is a subspace of W and for any subspace $W_1 \leq W$, the orthogonal complement of W_1 in V is a subspace of V.

(b) Let $W_1 \leq W_2 \leq W$ be two subspaces. Then, $W_2^{\perp} \leq W_1^{\perp}$.

Also: $V_2^{\perp} \leq V_1^{\perp}$ for any subspaces $V_1 \leq V_2 \leq V$.

(c) The bilinear form is non-degenerate if and only if $W^\perp = 0$ and $V^\perp = 0$.

Proof. (a) Let $V_1 \leq V$ be a subspace. Let $w_1, w_2 \in V_1^\perp$, i.e., $\langle v, w_i\rangle = 0$ for $i = 1, 2$ and all $v \in V_1$. Thus, for all $a \in K$ we have the equality

$$\langle v, aw_1 + w_2\rangle = a\langle v, w_1\rangle + \langle v, w_2\rangle = 0,$$

whence $aw_1 + w_2 \in V_1^\perp$. The argument for $W_1^\perp$ is the same.
(b) Let $v \in W_2^\perp$. By definition $\langle v, W_2\rangle = 0$, hence in particular $\langle v, W_1\rangle = 0$, i.e. $v \in W_1^\perp$. The second statement follows by the same argument.
(c) This is another way of writing the definition. □

Example 13.8. *(a) The application*

$$\langle\cdot,\cdot\rangle : K^n \times K^n \to K, \quad \langle \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix}, \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{pmatrix} \rangle = \begin{pmatrix} a_1 & a_2 & \dots & a_n \end{pmatrix} \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{pmatrix} = \sum_{i=1}^n a_i b_i$$

is bilinear and non-degenerate.

(b) Let V be a K-vector space of finite dimension. The application

$$\langle\cdot,\cdot\rangle : V^* \times V \to K, \quad \langle f, v\rangle := f(v)$$

is bilinear and non-degenerate.

Let $S = \{s_1, \dots, s_n\}$ be a K-basis of V and S^* the dual basis. Let $f = \sum_{i=1}^n a_i s_i^* \in V^*$ and $v = \sum_{i=1}^n b_i s_i \in V$. Then

$$\langle f, v\rangle = \langle \sum_{i=1}^n a_i s_i^*, \sum_{j=1}^n b_j s_j\rangle = \sum_{i=1}^n \sum_{j=1}^n a_i b_j \langle s_i^*, s_j\rangle = \sum_{i=1}^n \sum_{j=1}^n a_i b_j s_i^*(s_j)$$

$$= \sum_{i=1}^n a_i b_i = \begin{pmatrix} a_1 & a_2 & \dots & a_n \end{pmatrix} \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{pmatrix}.$$

We have found the bilinearity of (a).

Proposition 13.9. *Let V, W be two K-vector spaces of finite dimensions and $\langle\cdot,\cdot\rangle : V \times W \to K$ be a non-degenerate bilinear form.*

(a) The applications

$$\varphi : V \to W^*, \quad v \mapsto \varphi(v) =: \varphi_v \text{ with } \varphi_v(w) := \langle v, w\rangle,$$

and

$$\psi : W \to V^*, \quad w \mapsto \psi(w) =: \psi_w \text{ with } \psi_w(v) := \langle v, w\rangle$$

are K-linear isomorphisms.

(b) $\dim_K(V) = \dim_K(W)$.

Proof. The K-linearity of φ and ψ is clear. We show the injectivity of φ. For this, let $v \in \ker(\varphi)$, i.e., $\varphi_v(w) = \langle v, w\rangle = 0$ for all $w \in W$. The non-degeneracy of the bilinear form implies that $v = 0$, which proves the injectivity. From this we deduce $\dim_K(V) \leq \dim_K(W^*) = \dim_K(W)$.
The same arguments applies to ψ give that ψ is injective and thus $\dim_K(W) \leq \dim_K(V^*) = \dim_K(V)$, d'où $\dim_K(V) = \dim_K(W)$. Consequently, φ and ψ are isomorphisms (because the dimension of the image is equal to the dimension of the target space which are thus equal). □

Corollary 13.10. *Let V, W be two K-vector spaces of finite dimensions.*

(a) Then, the application

$$\psi : V \to (V^*)^*, \quad v \mapsto \psi_v = \mathrm{ev}_v : V^* \to K \text{ where } \psi_v(f) = \mathrm{ev}_v(f) = f(v) \text{ for } f \in V^*$$

is a K-linear isomorphism.

(b) Let $\alpha : V \to W$ be a K-linear application. Then, the diagram

$$\begin{tikzcd} V \arrow[r, "\alpha"] \arrow[d, "\psi_1"] & W \arrow[d, "\psi_2"'] \\ (V^*)^* \arrow[r, "(\alpha^*)^*"] & (W^*)^*. \end{tikzcd}$$

is commutative, where ψ_1 and ψ_2 are the isomorphisms from (a), i.e. $\psi_2 \circ \alpha = (\alpha^*)^* \circ \psi_1$.

(c) Let $t_1, \ldots, t_n$ be a K-basis of V^*. Then, there exists a K-basis $s_1, \ldots, s_n$ of V such that $t_i(s_j) = \delta_{i,j}$ for all $1 \leq i, j \leq n$.

Proof. (a) The bilinear form $V^* \times V \to K$, given by $\langle f, v\rangle \mapsto f(v)$ from Example 13.8(b) is non-degenerate. The application ψ is the ψ of Proposition 13.9.
(b) Let $v \in V$. On the one hand, we have $(\alpha^*)^*(\psi_1(v)) = (\alpha^*)^*(\mathrm{ev}_v) = \mathrm{ev}_v \circ \alpha^*$ and on the other hand $\psi_2(\alpha(v)) = \mathrm{ev}_{\alpha(v)}$ with notations from (a). To see that both are equal, let $f \in W^*$. We have

$$\mathrm{ev}_v(\alpha^*(f)) = \mathrm{ev}_v(f \circ \alpha) = f(\alpha(v)) \text{ and } \mathrm{ev}_{\alpha(v)}(f) = f(\alpha(v)),$$

thus the desired equality.
(c) Let $t_1^*, \ldots, t_n^* \in (V^*)^*$ be the dual basis, i.e. $t_j^*(t_i) = \delta_{i,j}$ for all $1 \leq i, j \leq n$. Since ψ from (a) is an isomorphism, there exist $s_1, \ldots, s_n$ (automatically a K-basis of V because it is the image of a basis by an isomorphism) such that $\psi(s_j) = \mathrm{ev}_{s_j} = t_j^*$, thus $t_j^*(f) = f(s_j)$ for all $f \in V^*$. In particular, we have $t_j^*(t_i) = t_i(s_j) = \delta_{i,j}$. □

Proposition 13.11. *Let V, W be two K-vector spaces of finite dimensions and $\langle \cdot, \cdot \rangle : V \times W \to K$ a non-degenerate bilinear form.*

(a) Let $S = \{s_1, \ldots, s_n\}$ be a K-basis of V. Then, there exists a K-basis $T = \{t_1, \ldots, t_n\}$ of W such that $\langle s_i, t_j\rangle = \delta_{i,j}$ for all $1 \leq i, j \leq n$.

(b) For any subspace $V_1 \leq V$ *we have* $(V_1^{\perp})^{\perp} = V_1$.

Also: for any subspace $W_1 \leq W$ *we have* $(W_1^{\perp})^{\perp} = W_1$.

(c) For any subspace $V_1 \leq V$ *we have* $\dim_K(V_1^{\perp}) = \dim_K(V) - \dim_K(V_1)$.

Also: for any subspace $W_1 \leq W$ *we have* $\dim_K(W_1^{\perp}) = \dim_K(W) - \dim_K(W_1)$.

Proof. (a) We consider the K-isomorphism $\varphi : V \to W^*$ of Proposition 13.9 and we set $f_i := \varphi(s_i) = \varphi_{s_i}$ for all $1 \leq i \leq n$. Corollary 13.10 allows us to choose a K-basis $t_1, \dots, t_n$ of W such that $f_i(t_j) = \delta_{i,j}$ for all $1 \leq i, j \leq n$. Finally, we have $\langle s_i, t_j \rangle = \varphi_{s_i}(t_j) = f_i(t_j) = \delta_{i,j}$, as desired.
(b,c) We choose a K-basis $s_1, \dots, s_d$ of V_1 that we extend to a K-basis

$$s_1, \dots, s_d, s_{d+1}, \dots, s_n$$

of V by Proposition 1.30. Using (a), we obtain a K-basis $t_1, \dots, t_n$ of W such that $\langle s_i, t_j \rangle = \delta_{i,j}$ for all $1 \leq i, j \leq n$.
We first show that $V_1^{\perp} = \langle t_{d+1}, \dots, t_n \rangle$. The inclusion "$\supseteq$" is clear. Let therefore $w = \sum_{i=1}^{n} a_i t_i \in V_1^{\perp}$, i.e. $\langle V_1, w \rangle = 0$, thus for all $1 \leq j \leq d$ we have

$$0 = \langle s_j, w \rangle = \langle s_j, \sum_{i=1}^{n} a_i t_i \rangle = \sum_{i=1}^{n} a_i \langle s_j, t_i \rangle = a_j,$$

and therefore $w \in \langle t_{d+1}, \dots, t_n \rangle$. Consequently, $\dim_K(V_1^{\perp}) = n - d = \dim_K(V) - \dim_K(V_1)$.
The same argument used for $V_1^{\perp}$ shows that $\langle s_1, \dots, s_d \rangle$ is a K-basis of $(V_1^{\perp})^{\perp}$ which is therefore equal to V_1. □

Corollary 13.12. *Let* V, W *be two* K*-vector subspaces and* $\varphi : V \to W$ *a* K*-linear application. We have the equalites*

(1) $\operatorname{im}(\varphi)^{\perp} = \ker(\varphi^*)$ *(where* $\perp$ *comes from the natural bilinear form* $W^* \times W \to K$*),*

(2) $\ker(\varphi)^{\perp} = \operatorname{im}(\varphi^*)$ *(where* $\perp$ *comes from the natural bilinear form* $V^* \times V \to K$*),*

(3) $\dim_K(\operatorname{im}(\varphi)) = \dim_K(\operatorname{im}(\varphi^*))$ *and*

(4) $\dim_K(\ker(\varphi)) = \dim_K(\ker(\varphi^*))$.

Proof. We firstly show (1). Let $f \in W^*$. Then

$$f \in \operatorname{im}(\varphi)^{\perp} \Leftrightarrow \forall\, v \in V : 0 = \langle f, \varphi(v) \rangle = f(\varphi(v)) \Leftrightarrow f \circ \varphi = 0 \Leftrightarrow f \in \ker(\varphi^*),$$

whence (1).
We slightly adapt the arguments in order to obtain (2) as follows. Let $v \in V$. Then

$$\begin{aligned} v \in \operatorname{im}(\varphi^*)^{\perp} \Leftrightarrow \forall\, f \in W^* : 0 = \langle \varphi^*(f), v \rangle = \langle f \circ \varphi, v \rangle = f(\varphi(v)) = \langle f, \varphi(v) \rangle \\ \Leftrightarrow \varphi(v) \in W^{\perp} \Leftrightarrow \varphi(v) = 0 \Leftrightarrow v \in \ker(\varphi), \end{aligned}$$

whence $\operatorname{im}(\varphi^*)^{\perp} = \ker(\varphi)$. Applying Proposition 13.11 we obtain $\operatorname{im}(\varphi^*) = \ker(\varphi)^{\perp}$; this is (2).

By Corollary 1.38, we have $\dim_K(V) = \dim_K(\mathrm{im}(\varphi)) + \dim_K(\ker(\varphi))$. Proposition 13.11 gives us

$$\dim_K(\mathrm{im}(\varphi)) = \dim_K(V) - \dim_K(\ker(\varphi)) = \dim_K(\ker(\varphi)^{\perp}) = \dim_K(\mathrm{im}(\varphi^*)),$$

whence (3). The argument to obtain (4) is similar:

$$\dim_K(\ker(\varphi)) = \dim_K(V) - \dim_K(\mathrm{im}(\varphi)) = \dim_K(\mathrm{im}(\varphi)^{\perp}) = \dim_K(\ker(\varphi^*)),$$

which achieves the proof. □

Definition 13.13. *Let $M \in \mathrm{Mat}_{m\times n}(K)$ be a matrix.*
The rank of columns *of M is defined as the dimension of the subspace of K^m generated by the columns of M (seen as elements of K^m).*
The rank of rows *of M is defined as the dimension of the subspace of K^n generated by the rows of M (seen as elements of K^n).*

Corollary 13.14. *Let $M \in \mathrm{Mat}_{m\times n}(K)$. Then, the rank of columns of M is equal to the rank of rows of M. We simply talk of the* rank *de M.*

Proof. The rank of M is the dimension of the image of φ_M, the K-linear application $K^n \to K^m$ associated to M (which sends $v \in K^n$ to $Mv \in K^m$). The matrix representing φ_M^* for the dual basis is M^{tr}. Thus the corollary immediately follows from Corollary 13.12 since the rank of columns of M^{tr} is equal to the rank of rows of M. □

Example 13.15. *Consider the matrix* $\begin{pmatrix} 3 & 5 & 1 \\ 1 & 2 & 3 \\ 4 & 7 & 4 \end{pmatrix}$. *We are interested in its rank (of columns). It is obvious that the third row is the sum of the two first rows (which are linearly independent). Thus the rank of M is 2. It seems more difficult to "see" a non-trivial combination of the columns, but we know that there is one.*

We finish this section with useful properties.

Proposition 13.16. *Let V, W be two K-vector subspaces of finite dimensions and $\langle\cdot,\cdot\rangle : V \times W \to K$ be a non-degenerate bilinear form. Let $W_1 \leq W$ and $W_2 \leq W$ be subspaces. Then, we have*

(a) $(W_1 \cap W_2)^{\perp} = W_1^{\perp} + W_2^{\perp}$ *and*

(b) $(W_1 + W_2)^{\perp} = W_1^{\perp} \cap W_2^{\perp}$.

Also with V in stead of W.

Proof. (a) "⊇": Since $W_1 \cap W_2 \leq W_i$ is a subspace for $i = 1, 2$, we have $W_i^{\perp} \leq (W_1 \cap W_2)^{\perp}$, thus $W_1^{\perp} + W_2^{\perp} \leq (W_1 \cap W_2)^{\perp}$ because $(W_1 \cap W_2)^{\perp}$ is a subspace.
(b) "⊆": For $i = 1, 2$ we have $W_i \leq W_1 + W_2$, thus we obtain $(W_1 + W_2)^{\perp} \leq W_i^{\perp}$ which implies $(W_1 + W_2)^{\perp} \leq W_1^{\perp} \cap W_2^{\perp}$.
(a) "⊆": Combining the proven inclusions, we have

$$W_1 \cap W_2 = ((W_1 \cap W_2)^{\perp})^{\perp} \leq (W_1^{\perp} + W_2^{\perp})^{\perp} \leq (W_1^{\perp})^{\perp} \cap (W_2^{\perp})^{\perp} = W_1 \cap W_2,$$

thus we have equality everywhere and, in particular, $(W_1 \cap W_2)^{\perp} = W_1^{\perp} + W_2^{\perp}$.
(b) It suffices to use (a) with $W_1^{\perp}$ and $W_2^{\perp}$ in stead of W_1 and W_2 to obtain $(W_1^{\perp} \cap W_2^{\perp})^{\perp} = (W_1^{\perp})^{\perp} + (W_2^{\perp})^{\perp}$ and thus $W_1^{\perp} \cap W_2^{\perp} = (W_1 + W_2)^{\perp}$. □

14 Quotients

Goals:

- Know and master the definition of quotient of vector spaces;
- know the isomorphism theorems and other important results;
- be able to compute in quotients of vector spaces;
- know examples and be able to prove simple properties.

Definition 14.1. *Let V be a K-vector space and $W \leq V$ a subspace.*
Any set of the form

$$v + W = \{v + w \mid w \in W\}$$

with $v \in V$ is called affine subspace.
Two subspaces $v_1 + W$ and $v_2 + W$ are called parallel. *They are thus both parallel to W.*

In order to understand the sequel, it is useful to recall the definition of congruences modulo n, i.e. the set $\mathbb{Z}/n\mathbb{Z}$ (for $n \in \mathbb{N}_{\geq 1}$), learned in the lecture course *Structures mathématiques*. To underline the analogy, we can write $V = \mathbb{Z}$ and $W = n\mathbb{Z} = \{nm \mid m \in \mathbb{Z}\}$.
We recall that the set

$$a + n\mathbb{Z} = \{a + mn \mid m \in \mathbb{Z}\} = \{\dots, a - 2n, a - n, a, a + n, a + 2n, \dots\}$$

is the equivalence class of $a \in \mathbb{Z}$ for the equivalence relation defined on $\mathbb{Z}$ by

$$a \sim_{n\mathbb{Z}} a' \quad \Leftrightarrow \quad a \equiv a' \mod n \quad \Leftrightarrow \quad n \mid (a - a') \quad \Leftrightarrow \quad a - a' \in n\mathbb{Z} \quad \Leftrightarrow \quad a + n\mathbb{Z} = a' + n\mathbb{Z}.$$

We will essentially do the same definition in the case of vector spaces.

Definition 14.2. *Let V be a K-vector space and $W \subseteq V$ a vector subspace. The binary relation on V given by*

$$v_1 \sim_W v_2 \overset{\text{definition}}{\Longleftrightarrow} v_1 - v_2 \in W$$

for $v_1, v_2 \in V$ defines an equivalence relation.
The equivalence classes are the affine subspaces of the form

$$v + W = \{v + w \mid w \in W\}.$$

The set of these classes is denoted V/W and called the set of classes following W. *It is the set of all the affine subspace that are parallel to W.*

Let us also recall the 'modular' addition, that is the addition of $\mathbb{Z}/n\mathbb{Z}$. The sum of $a + n\mathbb{Z}$ and $b + n\mathbb{Z}$ is defined as

$$(a + n\mathbb{Z}) + (b + n\mathbb{Z}) := (a + b) + n\mathbb{Z}.$$

To see that this sum is well-defined, we make the **fundamental observation**: let $a, a', b, b' \in \mathbb{Z}$ such that

$$a \equiv a' \mod n \quad \text{and} \quad b \equiv b' \mod n,$$

i.e.,

$$a + n\mathbb{Z} = a' + n\mathbb{Z} \quad \text{and} \quad b + n\mathbb{Z} = b' + n\mathbb{Z}$$

then,

$$a + b \equiv a' + b' \mod n,$$

i.e.,

$$(a + b) + n\mathbb{Z} = (a' + b') + n\mathbb{Z}.$$

The proof is very easy: since $n \mid (a' - a)$ and $n \mid (b' - b)$, there exist $c, d \in \mathbb{Z}$ such that $a' = a + cn$ and $b' = b + dn$; thus

$$a' + b' = (a + cn) + (b + dn) = (a + b) + n(c + d)$$

so that, n divides $(a' + b') - (a + b)$, whence $(a' + b') + n\mathbb{Z} = (a + b) + n\mathbb{Z}$. A small example:

$$(3 \equiv 13 \mod 10 \quad \text{et} \quad 6 \equiv -24 \mod 10) \quad \Rightarrow \quad 9 \equiv -11 \mod 10.$$

Here comes the generalization to vector spaces. Note that it does not suffice to define an addition only, but one also needs to define a scalar multiplication.

Proposition 14.3. *Let K be a field, V a K-vector space, $W \le V$ a K-vector subspace and V/W the set of classes following W.*

(a) For all $v_1, v_2 \in V$ the class $(v_1 + v_2) + W$ only depends on the classes $v_1 + W$ and $v_2 + W$.

Thus, we can define the application, called addition,

$$+ : V/W \times V/W \to V/W, \quad (v_1 + W, v_2 + W) \mapsto (v_1 + W) + (v_2 + W) := (v_1 + v_2) + W.$$

(b) For all $a \in K$ and all $v \in V$, the class $a.v + W$ only depends on the class $v + W$. Thus, we can define the application, called scalar multiplication,

$$. : K \times V/W \to V/W, \quad (a, v + W) \mapsto a.(v + W) := a.v + W.$$

(c) $(V/W, +, ., 0 + W)$ is a K-vector space, called quotient of V by W.

(d) The application

$$\pi : V \to V/W, \quad v \mapsto v + W$$

is K-linear and surjective with kernel $\ker(\pi) = W$*; it is called* natural projection.

Proof. (a) Assume $v_1 + W = v_1' + W$ and $v_2 + W = v_2' + W$. Therefore there exist $w_1, w_2 \in W$ such that $v_1 = v_1' + w_1$ and $v_2 = v_2' + w_2$. Then $v_1 + v_2 = v_1' + v_2' + (w_1 + w_2)$ whence $(v_1 + v_2) - (v_1' - v_2') \in W$ and thus $(v_1 + v_2) + W = (v_1' + v_2') + W$.
(b) Assume $v + W = v' + W$. Therefore there exists $w \in W$ such that $v = v' + w$. Then $av = a(v' + w) = av' + aw$ whence $av - av' = aw \in W$ and thus $av + W = av' + W$.
(c) Standard verfication of the axioms defining a vector space (see Definition 1.1).
(d) Linearity: Let $v_1, v_2 \in V$ and $a \in K$, then $\pi(av_1 + v_2) = (av_1 + v_2) + W = a(v_1 + W) + (v_2 + W) = a\pi(v_1) + \pi(v_2)$.
Surjectivity: The class $v + W$ is the image of v under π.
Computation of the kernel: Let $v \in V$. Then $v \in \ker(\pi)$ if and only if $v + W = 0 + W = W$ and this is the case if and only if $v \in W$. □

Theorem 14.4 (1st isomorphism theorem/Homomorphiesatz). *Let K be a field and $\varphi : V \to Y$ a K-linear application. Let $W := \ker(\varphi)$ be its kernel.*

(a) For $v \in V$, the image $\varphi(v)$ only depends on the class $v + W$.

(b) Part (a) allows us to define $\overline{\varphi}(v + W) := \varphi(v)$ for $v \in V$. This defines an application

$$\overline{\varphi} : V/W \to Y, \quad v + W \mapsto \overline{\varphi}(v + W) := \varphi(v)$$

which is K-linear and injective. It gives rise to a K-linear isomorphism

$$\overline{\varphi} : V/W \to \operatorname{im}(\varphi).$$

Proof. (a) Let $v, v' \in V$ such that $v + W = v' + W$. Then there exists $w \in W$ such that $v = v' + w$. We have $\varphi(v) = \varphi(v' + w) = \varphi(v') + \varphi(w) = \varphi(v')$ because $\varphi(w) = 0$ as $w \in W = \ker(\varphi)$.
(b) Linearity: Let $v_1, v_2 \in V$ and $a \in K$. We have $\overline{\varphi}(a(v_1+W)+(v_2+W)) = \overline{\varphi}((av_1+v_2)+W) = \varphi(av_1 + v_2) = a\varphi(v_1) + \varphi(v_2) = a\overline{\varphi}(v_1) + \overline{\varphi}(v_2)$.
Injectivity: Let $v + W \in \ker(\overline{\varphi})$. Then $\overline{\varphi}(v + W) = \varphi(v) = 0$ whence $v \in \ker(\varphi) = W$, thus $v + W = 0 + W$. This shows $\ker(\overline{\varphi}) = \{0 + W\}$, so that $\overline{\varphi}$ is injective. □

The next proposition is important because it describes the vector subspaces of quotient vector spaces.

Proposition 14.5. *Let K be a field, V a K-vector space, $W \leq V$ a vector subspace, and $\pi : V \to V/W$ the natural projection.*

(a) The application

$$\Phi : \{\text{vector subspaces of } V/W\} \longrightarrow \{\text{vector subspaces of } V \text{ containing } W\},$$

given by $X \mapsto \pi^{-1}(X)$ is bijective. The inverse Ψ of Φ is $Y \mapsto \pi(Y)$.

(b) Let $X_1, X_2 \leq V/W$ be two vector subspaces. Then

$$X_1 \subseteq X_2 \quad \Leftrightarrow \quad \Phi(X_1) \subseteq \Phi(X_2).$$

Proof. (a)

- For a subspace $X \leq V/W$ the preimage $\Phi(X) = \pi^{-1}(X)$ is indeed a vector subspace: let $v_1, v_2 \in V$ such that $v_1 \in \pi^{-1}(X)$ and $v_2 \in \pi^{-1}(X)$, then $\pi(v_1) = v_1 + W \in X$ and $\pi(v_2) = v_2 + W \in X$. Then for $a \in K$, we have $a\pi(av_1 + v_2) = \pi(v_1) + \pi(v_2) \in X$, whence $av_1 + v_2 \in \pi^{-1}(X)$.

  Moreover, $\pi^{-1}(W) \supseteq \pi^{-1}(\{0\}) = \ker(\pi) = W$.

- We know by Proposition 1.36 that the images of the linear applications between vector spaces are vector subspaces, thus $\Psi(Y) = \pi(Y)$ is a vector subspace of V/W.

- Here is an auxiliary statement :

  Let $\pi : V \to V'$ be a K-linear homomorphism between vector spaces and $Y \leq V$ a vector subspace containing $\ker(\pi)$. Then $\pi^{-1}(\pi(Y)) = Y$.

  We verify this equality:
  "$\subseteq$": Let $x \in \pi^{-1}(\pi(Y))$, then $\pi(x) \in \pi(Y)$, i.e. $\pi(x) = \pi(y)$ for some $y \in Y$. Therefore $0 = \pi(x) - \pi(y) = \pi(x - y)$, thus $x - y \in \ker(\pi) \subseteq Y$, thus $x - y = y' \in Y$, thus $x = y + y' \in Y$.

  "$\supseteq$": Let $y \in Y$, then $\pi(y) \in \pi(Y)$, and therefore $y \in \pi^{-1}(\pi(Y))$.

- Let $Y \leq V$ be a vector subspace such that $W \subseteq Y$.

  By the auxiliary statement we have: $\Phi(\Psi(Y)) = \pi^{-1}(\pi(Y)) = Y$.

- Here is another auxiliary statement:

  Let $\pi : V \to V'$ be a surjective application (not necessarily between vector spaces) and $X \subseteq V'$ a vector subspace. Then $X = \pi(\pi^{-1}(X))$.

  We verify this equality.
  "$\subseteq$": Let $x \in X$. Since π is surjective, there exists $v \in V$ such that $\pi(v) = x$. Therefore $v \in \pi^{-1}(X)$ and $x = \pi(v) \in \pi(\pi^{-1}(X))$.

  "$\supseteq$": Let $v' \in \pi(\pi^{-1}(X))$. Then, there exists $v \in \pi^{-1}(X)$ such that $v' = \pi(v)$. But, $v' = \pi(v)$ belongs to X since $v \in \pi^{-1}(X)$.

- Let $X \leq V/W$ be a vector subspace.

  By the auxiliary statement we have: $\Psi(\Phi(X)) = \pi(\pi^{-1}(X)) = X$.

(b) is clear. □

Proposition 14.6 (Second isomorphism theorem)**.** *Let K be a field, V a K-vector space and $X, W \subseteq V$ vector subspaces. Then, the K-linear homomorphism*

$$\varphi : X \to (X + W)/W, \quad x \mapsto x + W,$$

"induces" (by the isomorphism theorem 14.4) the K-linear isomorphism

$$\overline{\varphi} : X/(X \cap W) \to (X + W)/W, \quad x + (X \cap W) \mapsto x + W.$$

Proof. The homomorphism φ is obviously surjective and its kernel consists of the elements $x \in X$ such that $x + W = W$, thus $x \in X \cap W$, showing $\ker(\varphi) = X \cap W$. The existence of $\overline{\varphi}$ hence follows from a direct application of the isomorphism theorem 14.4. □

Proposition 14.7 (Third isomorphism theorem)**.** *Let K be a field, V a K-vector space and $W_1 \subseteq W_2$ two vector subspaces of V. Then, the K-linear homomorphism*

$$\varphi : V/W_1 \to V/W_2, \quad v + W_1 \mapsto v + W_2$$

"induces" (by the isomorphism theorem 14.4) the K-linear isomorphism

$$\overline{\varphi} : (V/W_1)/(W_2/W_1) \to V/W_2, \quad v + W_1 + (W_2/W_1) \mapsto v + W_2.$$

Proof. The homomorphism φ is obviously surjective and its kernel consists of the elements $v + W_1 \in V/W_1$ such that $v + W_2 = W_2$ which is equivalent to $v + W_1 \in W_2/W_1$. Thus $\ker(\varphi) = W_2/W_1$. The existence of $\overline{\varphi}$ thus follows from a direct application of the isomorphism theorem 14.4. □