MATH 223 - Quadratic Forms and Geometry (UPMC 2008/09)

Jan Nekovář

0. Introduction

(0.0) What is this course about?

The first year course on Linear Algebra was about linear objects, such as vector spaces, linear maps and linear forms. Recall that, for example, $3x - 4y$ is a **linear form** on a two-dimensional vector space with coordinates x and y.

In the present course we shall study **quadratic forms** and related objects. For example, $2x^2 - 8xy + 9y^2$ is a quadratic form. A recurring theme will be **diagonalisation** of quadratic forms, such as the transformation

$$2x^2 - 8xy + 9y^2 = 2(x-2y)^2 + y^2 = 2x'^2 + y'^2, \qquad (x' = x - 2y,\ y' = y). \tag{0.0.0}$$

Warning: there are at least 3 different concepts of diagonalisation:

(1) Diagonalisaton of linear maps, recalled in §1.6 below.
(2) "Easy" diagonalisaton of quadratic forms, which includes the example (0.0.0) (see §3.3 below).
(3) "Difficult" diagonalisaton of quadratic forms (see §5.1 below).

(0.1) Where do we encounter quadratic forms in nature?

(0.1.0) Euclidean geometry: if $x \in \mathbf{R}^n$ is a vector with coordinates $x_1, \dots, x_n$, then its Euclidean length $\|x\|$ is given by the theorem of Pythagoras

$$\|x\|^2 = x_1^2 + \cdots + x_n^2 = (x \mid x)$$

(where $(x \mid y) = x_1y_1 + \cdots + x_ny_n$ denotes the standard Euclidean scalar product).

The equation $\|x\|^2 = 1$ defines the unit sphere in $\mathbf{R}^n$; for example, for $n = 2$, we obtain the unit circle $x_1^2 + x_2^2 = 1$ in $\mathbf{R}^2$.

One can consider similar equation for more general quadratic forms, such as

$$2x^2 - 8xy + 9y^2 = 1 \quad \text{(ellipse)}, \qquad 2x^2 - 8xy - 9y^2 = 1 \quad \text{(hyperbola)}.$$

In three dimensions, the equations

$$x_1^2 + x_2^2 - x_3^2 = 1, \qquad x_1^2 - x_2^2 - x_3^2 = 1$$

define a one-sheet and a two-sheet hyperboloid, respectively.

(0.1.1) Non-Euclidean (= pseudo-Euclidean) geometry: in theory of relativity, the usual space $\mathbf{R}^3$ is replaced by the Minkowski space ("space-time") $\mathbf{R}^{1,3}$. An element $x \in \mathbf{R}^{1,3}$ has coordinates x_0, x_1, x_2, x_3, where x_1, x_2, x_3 are the usual coordinates in $\mathbf{R}^3$ and $x_0 = ct$ (t being the time and c the speed of light). The pseudo-Euclidean length of x is defined by

$$\|x\|^2_{Min} = x_0^2 - x_1^2 - x_2^2 - x_3^2.$$

The equation

$$0 = \|x\|^2_{Min} = x_0^2 - x_1^2 - x_2^2 - x_3^2$$

defines the **light cone**, which is swept out by particles travelling at the speed of light.

1. Linear Algebra

In this chapter we recall useful background material from the Linear Algebra course.

There are two approaches to the subject:

Abstract linear algebra, in which one works with abstract vector spaces, vectors, linear maps, etc.

Matrix formulation of linear algebra, which is indispensable for calculations: after choosing bases (= systems of coordinates) of the vector spaces in question, one expresses all abstract objects in matrix terms (at least in the finite-dimensional case).

The dictionary between the two languages begins as follows:

Abstract object	Matrix object
vector space E	K^n
vector $x \in E$	column vector $\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$
linear map $\alpha : E \longrightarrow F$	matrix $A \in M_{p,n}(K)$

1.1 Generalities

(1.1.1) Fields of scalars. In the abstract theory, one works with vector spaces over a fixed **field of scalars** K. In practice, the most important cases are the following: $K = \mathbf{R}$ (the **real numbers**), $K = \mathbf{C}$ (the **complex numbers**) and $K = \mathbf{F}_q$ (the **finite field with** $q = p^r$ **elements**, where p is a prime number; for example, the elements of $\mathbf{F}_p = \mathbf{Z}/p\mathbf{Z}$ are the residue classes of integers modulo p).

(1.1.2) Vector spaces. Recall that elements of a K**-vector space** E (**"vectors"**) can be added together, and also multiplied by scalars. These operations

$$x, y \in E \mapsto x + y \in E, \qquad x \in E,\ \lambda \in K \mapsto \lambda x \in E$$

satisfy the **"usual rules"** (for all $x, y, z \in E$ and $\lambda, \mu \in K$):

$$\begin{gathered} x + y = y + x, \qquad x + (y + z) = (x + y) + z, \\ \lambda(\mu x) = (\lambda\mu)x, \qquad \lambda(x + y) = \lambda x + \lambda y, \qquad (\lambda + \mu)x = \lambda x + \mu x, \\ 1x = x, \qquad 0x = \vec{0}, \qquad x + \vec{0} = x. \end{gathered}$$

It is customary to denote the vector $(-1)x$ by $-x$, and the sum $x + (-y)$ by $x - y$.

Warning: one must distinguish between the **zero scalar** $0 \in K$ and the **zero vector** $\vec{0} \in E$, even though both of them are often denoted by the same symbol.

(1.1.3) Examples of vector spaces: (0) The zero vector space $0 = \{\vec{0}\}$ consisting only of the zero vector.

(1) The space of column vectors of dimension $m \geq 1$:

$$K^m = \left\{ \begin{pmatrix} a_1 \\ \vdots \\ a_m \end{pmatrix} \middle|\, a_i \in K \right\}$$

(2) The space of $m \times n$ matrices ($m =$ the number of rows, $n =$ the number of columns) with coefficients in K:

$$M_{m,n}(K) = \left\{ \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{m1} & \cdots & a_{mn} \end{pmatrix} \middle| \, a_{ij} \in K \right\}$$

The space of **square matrices** (for which $m = n$) is denoted by $M_n(K) = M_{n,n}(K)$.

(1.1.4) Vector subspaces. Let E be a K-vector space. A (K-)**vector subspace** of E is a non-empry subset $F \subset E$ satisfying

$$\begin{aligned} \forall x, y \in F \qquad & x + y \in F \\ \forall \lambda \in K \ \forall x \in F \qquad & \lambda x \in F \end{aligned}$$

(recall that the symbol "$\forall$" means **"for all"**). This implies that F is a K-vector space sharing the same zero vector $\vec{0}$ with E.

(1.1.5) Generating subsets of subspaces. Let S be a subset of a K-vector space E. There exists a **smallest vector subspace** of E containing S; it is called the **(vector) subspace generated by** S and is denoted by $\mathrm{vect}(S)$. The elements of $\mathrm{vect}(S)$ are the **linear combinations** of elements of S, i.e. **finite** sums of the form

$$\sum_{s \in S} \lambda_s \, s \qquad\qquad (\lambda_s \in K).$$

In particular, if the set $S = \{x_1, \ldots, x_n\}$ is finite, then

$$\mathrm{vect}(x_1, \ldots, x_n) = \{\lambda_1 x_1 + \cdots + \lambda_n x_n \mid \lambda_i \in K\}.$$

(1.1.6) Finite-dimensional vector spaces. A K-vector space E has **finite dimension** if there exists a finite set of vectors $S = \{x_1, \ldots, x_n\}$ generating E (i.e. such that $\mathrm{vect}(S) = E$). If this is the case, then the smallest number of elements of such a generating set is called **the dimension of** E (denoted by $\dim(E)$).

(1.1.7) Linear (in)dependence. We say that a finite collection of vectors $x_1, \ldots, x_n \in E$ in a K-vector space E is **linearly dependent** if there exists a linear relation

$$\lambda_1 x_1 + \cdots + \lambda_n x_n = \vec{0} \qquad\qquad (\lambda_i \in K)$$

which is non-trivial, i.e. in which at least one of the scalars $\lambda_i \neq 0$ is non-zero.

Otherwise, we say that the vectors $x_1, \ldots, x_n \in E$ are **linearly independent**.

(1.1.8) Bases (the finite-dimensional case). A finite (ordered) set of vectors $\mathcal{B} = \{e_1, \ldots, e_n\}$ in a K-vector space E is a **basis of** E if the vectors of $\mathcal{B}$ are **linearly independent** and if $\mathrm{vect}(\mathcal{B}) = E$ (i.e. if $\mathcal{B}$ **generates** E). In this case, each vector $x \in E$ can be written **uniquely** as

$$x = \lambda_1 e_1 + \cdots + \lambda_n e_n \qquad\qquad (\lambda_i \in K).$$

The scalars $\lambda_1, \ldots, \lambda_n$ are the **coordinates** of x in the basis $\mathcal{B}$.

A fundamental result states that every finite-dimensional vector space E admits a basis, and that the number of elements of each basis is the same, equal to $\dim(E)$.

Any **choice** of a basis $\mathcal{B}$ defines an **identification**

$$M_{\mathcal{B}} : E \xrightarrow{\sim} K^n \qquad\qquad (n = \dim(E)),$$

which depends on the chosen basis: one associates to a vector

$$x = \lambda_1 e_1 + \cdots + \lambda_n e_n \in E$$

the column vector

$$M_{\mathcal{B}}(x) = \begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_n \end{pmatrix} \in K^n$$

of its coordinates in $\mathcal{B}$. We say that the column vector $M_{\mathcal{B}}(x)$ **represents** x **in the basis** $\mathcal{B}$. More generally, one associates to each finite collection of vectors $x_1, \ldots, x_p \in E$ the matrix

$$M_{\mathcal{B}}(x_1, \ldots, x_p) = (M_{\mathcal{B}}(x_1) \mid \cdots \mid M_{\mathcal{B}}(x_p)) \in M_{n,p}(K)$$

whose columns represents the vectors $x_1, \ldots, x_p$ in the basis $\mathcal{B}$.

Examples: (1) The column vectors

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

form the **canonical basis** of K^n. In this case

$$\lambda_1 e_1 + \cdots + \lambda_n e_n = \begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_n \end{pmatrix}.$$

(2) The matrices $E(ij) \in M_{m,n}(K)$, where $i = 1, \ldots, m$, $j = 1, \ldots, n$ and

$$E(ij)_{ab} = \begin{cases} 1, & \text{if } a = i,\ b = j \\ 0, & \text{if not} \end{cases}$$

form a basis of $M_{m,n}(K)$. In this case

$$a_{11}E(11) + \cdots + a_{mn}E(mn) = \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{m1} & \cdots & a_{mn} \end{pmatrix}.$$

(3) The monomials $1, t, \ldots, t^d$ form a basis of the vector space

$$K[t]_{\deg \le d} = \{a_0 + a_1 t + \cdots + a_d t^d \mid a_i \in K\}$$

of polynomials of degree less than or equal to d.

(1.1.9) Infinite-dimensional case. One can define the concept of a basis (in the algebraic sense) even for vector spaces of infinite dimension. However, in the spaces one encounters in nature (such as the spaces of continuous or integrable functions $f : [a, b] \longrightarrow \mathbf{R}$ on a fixed interval $[a, b]$) it is often useful to consider suitable **infinite linear combinations** $\sum_{i=1}^{\infty} \lambda_i f_i$, provided they exist. This leads to various concepts of bases in the analytic sense, which are studied, for example, in Fourier analysis and its generalisations (such as wavelet theory).

1.2 Linear maps and their matrix representations

(1.2.1) Linear maps. A map $f : E \longrightarrow E'$ between two K-vector spaces is **linear** if it preserves the operations, i.e. if

$$\begin{aligned} \forall x, y \in E \qquad & f(x+y) = f(x) + f(y) \\ \forall \lambda \in K \ \forall x \in E \qquad & f(\lambda x) = \lambda\, f(x) \end{aligned}$$

(which implies that $f(\vec{0}) = \vec{0}$). **Notation:** the set of linear maps from E to E' will be denoted by $\mathscr{L}(E, E')$. It is again a K-vector space, with operations

$$(f+g)(x) = f(x) + g(x), \qquad (\lambda f)(x) = \lambda(f(x)) \qquad\qquad (f, g \in \mathscr{L}(E, E'),\ x \in E,\ \lambda \in K).$$

In sections 1.2.2-1.2.8 below we consider only vector spaces of finite dimension.

(1.2.2) Examples of linear maps: (0) The zero map $f = 0$ ($\forall x \in E \quad f(x) = \vec{0}$).
(1) The identity map $f = \mathrm{Id}_E$ in the case when $E = E'$ ($\forall x \in E \quad f(x) = x$).
(2) Suppose that $f : K^3 \longrightarrow K^2$ is a linear map satisfying

$$f(e_1) = f\left(\begin{pmatrix}1\\0\\0\end{pmatrix}\right) = \begin{pmatrix}2\\1\end{pmatrix}, \quad f(e_2) = f\left(\begin{pmatrix}0\\1\\0\end{pmatrix}\right) = \begin{pmatrix}-1\\4\end{pmatrix}, \quad f(e_3) = f\left(\begin{pmatrix}0\\0\\1\end{pmatrix}\right) = \begin{pmatrix}3\\5\end{pmatrix}.$$

Then

$$f\left(\begin{pmatrix}x\\y\\z\end{pmatrix}\right) = f\left(x\begin{pmatrix}1\\0\\0\end{pmatrix} + y\begin{pmatrix}0\\1\\0\end{pmatrix} + z\begin{pmatrix}0\\0\\1\end{pmatrix}\right) = x\, f\left(\begin{pmatrix}1\\0\\0\end{pmatrix}\right) + y\, f\left(\begin{pmatrix}0\\1\\0\end{pmatrix}\right) + z\, f\left(\begin{pmatrix}0\\0\\1\end{pmatrix}\right) =$$

$$= x\begin{pmatrix}2\\1\end{pmatrix} + y\begin{pmatrix}-1\\4\end{pmatrix} + z\begin{pmatrix}3\\5\end{pmatrix} = \begin{pmatrix}2x - y + 3z\\x + 4y + 5z\end{pmatrix} = \begin{pmatrix}2 & -1 & 3\\1 & 4 & 5\end{pmatrix}\begin{pmatrix}x\\y\\z\end{pmatrix}.$$

In other words, f is given by the left matrix multiplication by the matrix

$$\begin{pmatrix}2 & -1 & 3\\1 & 4 & 5\end{pmatrix} = (f(e_1) \mid f(e_2) \mid f(e_3)) \in M_{2,3}(K),$$

whose columns are equal to the values of f on the vectors e_1, e_2, e_3 of the canonical basis of K^3.
(3) In general, a linear map $f : E \longrightarrow E'$ is uniquely determined by its values on any basis $e_1, \ldots, e_n$ of E, as

$$f(\lambda_1 e_1 + \cdots + \lambda_n e_n) = \lambda_1\, f(e_1) + \cdots + \lambda_n\, f(e_n).$$

(1.2.3) Matrix multiplication. Recall that matrix multiplication

$$\begin{aligned} M_{m,n}(K) \times M_{n,p}(K) &\longrightarrow M_{m,p}(K) \\ A = (a_{ij}),\ B = (b_{kl}) &\ \mapsto\ AB = C = (c_{il}) \end{aligned}$$

is defined by the formula

$$c_{il} = \sum_{j=1}^{n} a_{ij}\, b_{jl} = \text{ the scalar product of the } i\text{−th row of } A \text{ with the } l\text{−th column of } B.$$

Warning: the product AB is defined if and only if the number of columns of A is equal to the number of rows of B.

Special case: If $p = 1$, then $M_{n,1} = K^n$ and $M_{m,1} = K^m$, hence the multiplication becomes

$$M_{m,n}(K) \times K^n \longrightarrow K^m, \qquad A, x \mapsto Ax. \tag{1.2.3.1}$$

Any matrix $A \in M_{m,n}(K)$ can be reconstructed from its products with the vectors of the canonical basis $e_1, \ldots, e_n$ of K^n (cf. 1.1.8), since

$$Ae_i = \begin{pmatrix} a_{1i} \\ \vdots \\ a_{ni} \end{pmatrix} = \text{ the } i\text{−th column of } A. \tag{1.2.3.2}$$

In other words, we have

$$A = (Ae_1 \mid \cdots \mid Ae_n). \tag{1.2.3.3}$$

(1.2.4) Matrices = linear maps. The example 1.2.2(2) is a special case of the general fact that

$$\mathscr{L}(K^n, K^m) = M_{m,n}(K) \tag{1.2.4.1}$$

(**warning:** note the reverse order of m and n).
Indeed, if $f : K^n \longrightarrow K^m$ is a linear map, then

$$f\left(\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}\right) = f(x_1 e_1 + \cdots + x_n e_n) = x_1\, f(e_1) + \cdots + x_n\, f(e_n) = (f(e_1) \mid \cdots \mid f(e_n)) \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix},$$

where

$$(f(e_1) \mid \cdots \mid f(e_n)) \in M_{m,n}(K) \tag{1.2.4.2}$$

denotes the matrix with columns $f(e_i) \in K^m$.
Conversely, left multiplication by a fixed matrix $A \in M_{m,n}(K)$ defines, by (1.2.3.1), a linear map

$$\begin{aligned} f : K^n &\longrightarrow K^m \\ X &\mapsto AX, \end{aligned} \tag{1.2.4.3}$$

which satisfies, by (1.2.3.3), the formula

$$A = (Ae_1 \mid \cdots \mid Ae_n) = (f(e_1) \mid \cdots \mid f(e_n)). \tag{1.2.4.4}$$

It will be convenient to denote this linear map simply as

$$K^n \xrightarrow{A} K^m. \tag{1.2.4.5}$$

(1.2.5) Matrix representation of linear maps. Let $f : E \longrightarrow E'$ be a linear map (between finite-dimensional vector spaces). Given respective bases $\mathcal{B} = \{e_1, \ldots, e_n\}$ and $\mathcal{B}' = \{e'_1, \ldots, e'_p\}$ of E and E' (where $n = \dim(E)$ and $p = \dim(E')$), the identifications

$$M_{\mathcal{B}} : E \xrightarrow{\sim} K^n, \qquad M_{\mathcal{B}'} : E' \xrightarrow{\sim} K^p$$

defined in 1.1.8 allow us to transport f to a linear map from K^n to K^p, which is necessarily given by a matrix $A \in M_{n,p}(K)$, as discussed in 1.2.4:

$$\begin{array}{cccc} M_{\mathcal{B}} : & E & \xrightarrow{\sim} & K^n \\ & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle A} \\ M_{\mathcal{B}'} : & E' & \xrightarrow{\sim} & K^p \end{array}$$

We say that the matrix

$$M_{\mathcal{B},\mathcal{B}'}(f) = A \in \mathscr{L}(K^n, K^p) = M_{n,p}(K)$$

represents f in the bases $\mathcal{B}$ and $\mathcal{B}'$.

Formulaire: (1) Denote by $X = M_{\mathcal{B}}(x) \in K^n$ and $Y = M_{\mathcal{B}'}(y) \in K^p$ the column vectors representing vectors $x \in E$ and $y \in E'$ in the bases $\mathcal{B}$ and $\mathcal{B}'$, respectively. Then we have

$$y = f(x) \iff Y = AX.$$

(2) In particular, if $x = e_i \in \mathcal{B}$ is an element of the basis $\mathcal{B}$ and $y = f(e_i)$, then

$$X = \begin{pmatrix} 0 \\ \vdots \\ 1 \\ \vdots \\ 0 \end{pmatrix} \qquad \text{(with 1 in the } i\text{−th row)}$$

is the eponymous element of the canonical basis of K^n, hence

$$Y = M_{\mathcal{B}'}(y) = M_{\mathcal{B}'}(f(e_i)) = Ae_i = \text{ the } i\text{−th column of } A,$$

by (1.2.3.2). Combined with (1.2.3.3), we obtain the formula

$$A = (Ae_1 \mid \cdots \mid Ae_n) = (M_{\mathcal{B}'}(f(e_1)), \ldots, M_{\mathcal{B}'}(f(e_n))) = M_{\mathcal{B}'}(f(\mathcal{B})).$$

In other words, the columns of A are the coordinates in the basis $\mathcal{B}'$ of the images under f of the vectors of the basis $\mathcal{B}$.

(3) If $E = E'$, $\mathcal{B} = \mathcal{B}'$ and $f = \mathrm{Id}_E$, then

$$A = I_n = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix} \in M_n(K)$$

is the identity matrix.

(1.2.6) Matrix multiplication = composition of linear maps. Let E, E', E'' be vector spaces of respective dimensions n, p, q. Given linear maps $f : E \longrightarrow E'$ and $g : E' \longrightarrow E''$, denote by $g \circ f : E \longrightarrow E''$ their composition

$$g \circ f : E \xrightarrow{f} E' \xrightarrow{g} E'' \qquad (g \circ f(x) = g(f(x)))$$

(the symbol $g \circ f$ reads "g **follows** f").

Given, in addition, respective bases $\mathcal{B}, \mathcal{B}', \mathcal{B}''$ of E, E', E'', we have identifications

$$M_{\mathcal{B}} : E \xrightarrow{\sim} K^n, \qquad M_{\mathcal{B}'} : E' \xrightarrow{\sim} K^p, \qquad M_{\mathcal{B}''} : E'' \xrightarrow{\sim} K^q,$$

which transform f and g into the multiplication maps

$$\begin{array}{ccc} K^n & \xrightarrow{A} & K^p \\ X & \mapsto & AX, \end{array} \qquad \begin{array}{ccc} K^p & \xrightarrow{B} & K^q \\ Y & \mapsto & BY, \end{array}$$

the composition of which is the multiplication map by BA:

$$\begin{array}{ccccc} K^n & \xrightarrow{A} & K^p & \xrightarrow{B} & K^q \\ X & \mapsto & AX & \mapsto & BAX \end{array}$$

In other words, the composition of the linear maps g and f corresponds to the matrix product

$$M_{q,p}(K) \times M_{p,n}(K) \longrightarrow M_{q,n}(K), \qquad B, A \mapsto BA.$$

In particular,

$$f \text{ is invertible} \iff A \text{ is invertible;}$$

if this is the case, then

$$g = f^{-1} \iff B = A^{-1}.$$

(1.2.7) Kernel, Image, Rank. Let $f : E \longrightarrow E'$ be a linear map. Its **kernel**

$$\mathrm{Ker}(f) = \{x \in E \mid f(x) = 0\} \subset E$$

is a vector subspace of E. Its **image**

$$\mathrm{Im}(f) = f(E) = \{f(x) \mid x \in E\} \subset E'$$

is a vector subspace of E'. The **rank** of f is defined as

$$\mathrm{rk}(f) = \dim(\mathrm{Im}(f)).$$

Example: for $f : K^2 \longrightarrow K^2$ given by the formula

$$f(\begin{pmatrix} x \\ y \end{pmatrix}) = f(xe_1 + ye_2) = \begin{pmatrix} x \\ 0 \end{pmatrix} = xe_1,$$

the kernel (resp., the image) of f is equal to the vertical (resp., to the horizontal) line $\mathrm{Ker}(f) = \mathrm{vect}(e_2)$ (resp., $\mathrm{Im}(f) = \mathrm{vect}(e_1)$); thus $\mathrm{rk}(f) = 1$.

The Rank formula: for each linear map $f : E \longrightarrow E'$,

$$\dim(E) = \dim(\mathrm{Ker}(f)) + \dim(\mathrm{Im}(f)) = \dim(\mathrm{Ker}(f)) + \mathrm{rk}(f). \qquad (1.2.7.1)$$

Matrix formulation: If $f : K^n \longrightarrow K^p$ is given by the matrix multiplication $f(X) = AX$ ($A \in M_{p,n}(K)$), then

$$\mathrm{Ker}(f) = \{X \in K^n \mid AX = 0\} \subset K^n$$

consists of the solutions of the homogeneous system of linear equations $AX = 0$. On the other hand

$$f(\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}) = f(x_1 e_1 + \cdots + x_n e_n) = x_1\, Ae_1 + \cdots + x_n\, Ae_n;$$

as Ae_i coincides with the i-th column of A, it follows that

$$\mathrm{Im}(f) = \{AX \mid X \in K^n\} = \mathrm{vect}(\text{the columns of } A) \subset K^p,$$

hence $\mathrm{rk}(f)$ is equal to the (column) rank of A, defined as

$$\mathrm{rk}(A) = \dim(\text{the vector space generated by the columns of } A)$$

(see 1.4 below for explicit methods of computing the rank of a matrix). The rank formula (1.2.7.1) then reads as follows.

The Rank formula for matrices: If $A \in M_{p,n}(K)$, then

$$n = \dim(\{X \in K^n \mid AX = 0\}) + \mathrm{rk}(A). \tag{1.2.7.2}$$

For example, if $A \in M_n(K)$ is a square matrix, then

$$\mathrm{rk}(A) = n \iff \text{the columns of } A \text{ form a basis of } K^n \iff \det(A) \neq 0, \tag{1.2.7.3}$$

which is a very useful criterion for **checking whether n vectors in K^n form a basis.**
In general, if $\mathcal{B}$ is a basis of a vector space E of dimension $\dim(E) = n$ and if $v_1, \ldots, v_k \in E$, then

$$\begin{aligned} v_1, \ldots, v_k \text{ are linearly independent in } E &\iff M_{\mathcal{B}}(v_1), \ldots, M_{\mathcal{B}}(v_k) \text{ are linearly independent in } K^n \\ &\iff \mathrm{rk}(M_{\mathcal{B}}(v_1, \ldots, v_k)) = k. \end{aligned} \tag{1.2.7.4}$$

In particular, if $k = n$, then

$$\begin{aligned} v_1, \ldots, v_n \text{ form a basis of } E &\iff M_{\mathcal{B}}(v_1), \ldots, M_{\mathcal{B}}(v_n) \text{ form a basis of } K^n \\ &\iff \mathrm{rk}(M_{\mathcal{B}}(v_1, \ldots, v_n)) = n \iff \det(M_{\mathcal{B}}(v_1, \ldots, v_n)) \neq 0. \end{aligned} \tag{1.2.7.5}$$

(1.2.8) Surjective, injective, bijective linear maps. A linear map $f : E \longrightarrow E'$ is called

(a) **surjective** if $f(E) = E'$;
(b) **injective** if $f(x) \neq f(y)$ whenever $x \neq y$ $(x, y \in E)$; this is equivalent (exercise!) to the condition $\mathrm{Ker}(f) = \{\vec{0}\} = 0$;
(c) **bijective** (or an **isomorphism**) if f is simultaneously surjective and injective; this is equivalent to the existence of the inverse map $g = f^{-1} : E' \longrightarrow E$ satisfying $g(f(x)) = x$ and $f(g(y)) = y$, for all $x \in E$ and $y \in E'$ (the map g is then automatically linear). In this case the spaces E and E' behave in the same way: for example, they have the same dimension, and f transforms a linearly independent set into a linearly independent set; thus $\dim(F) = \dim f(F)$ for any vector subspace $F \subset E$;
(d) **an endomorphism of** E if $E = E'$. In this case (more generally, in the case when $\dim(E) = \dim(E')$), the rank formula (1.2.7.1) implies that the above conditions (a) $\iff$ (b) $\iff$ (c) are equivalent.

Examples: (1) The map $M_{\mathcal{B}} : E \xrightarrow{\sim} K^n$ from 1.1.8 is an isomorphism.
(2) The map $M_{\mathcal{B},\mathcal{B}'} : \mathscr{L}(E, E') \longrightarrow \mathscr{L}(K^n, K^p) = M_{p,n}(K)$ from 1.2.5 is an isomorphism, hence

$$\dim(\mathscr{L}(E, E')) = \dim(M_{p,n}(K)) = np = \dim(E)\dim(E').$$

Matrix formulation: If $f : K^n \longrightarrow K^p$ is given by the matrix multiplication $f(X) = AX$ $(A \in M_{p,n}(K))$, then

f is surjective $\iff$ $\operatorname{rk}(A) = p$;
f is injective $\iff$ $X = 0 \in K^n$ is the unique solution of the homogeneous system $AX = 0$.
f is bijective $\iff$ $n = p = \operatorname{rk}(A)$ $\iff$ $n = p$ and $\det(A) \neq 0$ $\iff$ $n = p$ and A is invertible (see (1.2.7.2) and the remark (d)).

(1.2.9) An infinite-dimensional example. Let

$$E = \{(u_0, u_1, u_2, \ldots) \mid u_i \in \mathbf{R}\}$$

be the (real vector-)space of sequences of real numbers. The linear map

$$f : E \longrightarrow E, \qquad (u_0, u_1, u_2, \ldots) \mapsto (u_1, u_2, u_3, \ldots)$$

is surjective, but not injective. The linear map

$$g : E \longrightarrow E, \qquad (u_0, u_1, u_2, \ldots) \mapsto (0, u_1, u_2, \ldots)$$

is injective, but not surjective.

(1.2.10) Exercise. *Recall that the matrices* $E(11) = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$, $E(12) = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$, $E(21) = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$ *and* $E(22) = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$ *form a basis* $\mathcal{B}$ *of* $M_2(\mathbf{R})$*. Denote* $A = \begin{pmatrix} 1 & 2 \\ 3 & 5 \end{pmatrix}$ *and consider the map*

$$f : M_2(\mathbf{R}) \longrightarrow M_2(\mathbf{R}), \qquad M \mapsto AM.$$

(1) *Show that the map* f *is linear and determine its matrix in the basis* $\mathcal{B}$*.*
(2) *Show that* f *is invertible and compute its inverse.*

(1.2.11) Exercise. *Decide whether the elements of* S *are linearly independent and whether they form a basis of* E*:*

(1) $$S = \left\{ \begin{pmatrix} 1 \\ 0 \\ 2 \end{pmatrix}, \begin{pmatrix} -1 \\ 3 \\ 2 \end{pmatrix}, \begin{pmatrix} 3 \\ -3 \\ 2 \end{pmatrix} \right\}, \qquad E = \mathbf{R}^3$$

(2) $$S = \{t^3 - 2t^2 + t + 3,\ 2t^3 - 2t^2 + 5t,\ -t^3 + t^2 + 1\}, \qquad E = \mathbf{R}[t]_{\deg \le 3}$$

(3) $$S = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 0 & 3 \end{pmatrix}, \begin{pmatrix} -1 & 4 \\ -1 & 3 \end{pmatrix}, \begin{pmatrix} 4 & -5 \\ 3 & -2 \end{pmatrix} \right\}, \qquad E = M_2(\mathbf{R}).$$

[Hint: use (1.2.7.4-5) and 1.4 below.]

(1.2.12) Exercise. *Consider the derivative* $D : f \mapsto f'$ *as a map* $D : E \longrightarrow E$*, where* $E = \mathbf{R}[t]_{\deg \le 3}$ *is the space of real polynomials of degree less than or equal to* 3*.*
(1) *Show that* $D : E \longrightarrow E$ *is a linear map; determine its kernel and its image.*
(2) *Check the Rank formula (1.2.7.1) in this example.*
(3) *Determine the matrix* $M \in M_4(\mathbf{R})$ *of* D *in the basis* $\{1, t, t^2, t^3\}$ *of* E*.*
(4) *Determine the matrix of the map* $D^2 = D \circ D : f \mapsto f''$ *in the same basis.*
(5) *Without any calculation, determine* M^4*.*

1.3 Change of basis

All vector spaces in §1.3 are assumed to be finite-dimensional.

(1.3.1) Change of basis for vectors. Let E be a K-vector space of dimension $n = \dim(E)$. Given two bases $\mathcal{B}_1$ (= "old basis") and $\mathcal{B}_2$ (= "new basis") of E, the matrix

$$P = M_{\mathcal{B}_1}(\mathcal{B}_2) \in M_n(K)$$

(whose columns are the coordinates of the vectors of the new basis $\mathcal{B}_2$ in the old basis $\mathcal{B}_1$) is called **the matrix of change of basis from $\mathcal{B}_1$ to $\mathcal{B}_2$**. In the notation of 1.2.5, the diagram

$$\begin{array}{rccc} M_{\mathcal{B}_2}: & E & \xrightarrow{\sim} & K^n \\ & \Big\downarrow \mathrm{Id}_E & & \Big\downarrow P \\ M_{\mathcal{B}_1}: & E & \xrightarrow{\sim} & K^n \end{array} \tag{1.3.1.1}$$

shows that we have

$$P = M_{\mathcal{B}_2,\mathcal{B}_1}(\mathrm{Id}_E).$$

Interchanging the rôles of $\mathcal{B}_1$ and $\mathcal{B}_2$, it follows from 1.2.6 that P is invertible and $P^{-1} = M_{\mathcal{B}_1,\mathcal{B}_2}(\mathrm{Id}_E)$. Conversely, given $\mathcal{B}_1$, any invertible matrix $P \in M_n(K)$ is obtained in this way, for a unique basis $\mathcal{B}_2$.

Formulaire: (1) For $x \in E$, let $X_1 = M_{\mathcal{B}_1}(x) \in K^n$ and $X_2 = M_{\mathcal{B}_2}(x) \in K^n$ be the column vectors representing x in the bases $\mathcal{B}_1$ and $\mathcal{B}_2$, respectively. The diagram (1.3.1.1) implies that

$$X_1 = PX_2, \qquad X_2 = P^{-1}X_1. \tag{1.3.1.2}$$

(1.3.2) Examples: (1) If $E = K^n$ and $\mathcal{B}_1 = \{e_1, \ldots, e_n\}$ is the canonical basis of K^n, then the columns of P are just the elements of $\mathcal{B}_2$.
(2) For example, if $E = \mathbf{R}^2$ and

$$\mathcal{B}_1 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \qquad \mathcal{B}_2 = \begin{pmatrix} 3 \\ 2 \end{pmatrix}, \begin{pmatrix} 1 \\ 4 \end{pmatrix},$$

then

$$P = \begin{pmatrix} 3 & 1 \\ 2 & 4 \end{pmatrix}.$$

To check that $\mathcal{B}_2$ is indeed a basis of $\mathbf{R}^2$, it is enough to observe that the determinant

$$\begin{vmatrix} 3 & 1 \\ 2 & 4 \end{vmatrix} \neq 0$$

is non-zero (cf. (1.2.7.3)).
(3) Let $E = \mathbf{R}^2$ and

$$\mathcal{B}_1 = \begin{pmatrix} 2 \\ 3 \end{pmatrix}, \begin{pmatrix} 1 \\ 2 \end{pmatrix}, \qquad \mathcal{B}_2 = \begin{pmatrix} 2 \\ -1 \end{pmatrix}, \begin{pmatrix} 3 \\ 2 \end{pmatrix}.$$

As

$$\begin{vmatrix} 2 & 1 \\ 3 & 2 \end{vmatrix} \neq 0 \neq \begin{vmatrix} 2 & 3 \\ -1 & 2 \end{vmatrix},$$

both pairs of vectors $\mathcal{B}_1$ and $\mathcal{B}_2$ form a basis of $\mathbf{R}^2$. In order to compute the matrix $P = M_{\mathcal{B}_2,\mathcal{B}_1}(\mathrm{Id}_E)$, consider also the canonical basis $\mathcal{B} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix}$. According to (1), the matrix of change of basis P_1 (resp., P_2) from $\mathcal{B}$ to $\mathcal{B}_1$ (resp., to $\mathcal{B}_2$), is equal to

$$P_1 = \begin{pmatrix} 2 & 1 \\ 3 & 2 \end{pmatrix}, \qquad P_2 = \begin{pmatrix} 2 & 3 \\ -1 & 2 \end{pmatrix}.$$

Comparing the diagrams

$$\begin{array}{cccc} M_{\mathcal{B}_2}: & E & \xrightarrow{\sim} & \mathbf{R}^2 \\ & \Big\downarrow \mathrm{Id}_E & & \Big\downarrow P \\ M_{\mathcal{B}_1}: & E & \xrightarrow{\sim} & \mathbf{R}^2 \\ & \Big\downarrow \mathrm{Id}_E & & \Big\downarrow P_1 \\ M_{\mathcal{B}}: & E & \xrightarrow{\sim} & \mathbf{R}^2 \end{array} \qquad\qquad \begin{array}{cccc} M_{\mathcal{B}_2}: & E & \xrightarrow{\sim} & \mathbf{R}^2 \\ & \Big\downarrow \mathrm{Id}_E & & \Big\downarrow P_2 \\ M_{\mathcal{B}}: & E & \xrightarrow{\sim} & \mathbf{R}^2 \end{array}$$

(and applying 1.2.6), we see that

$$P_1 P = P_2,$$

hence

$$P = P_1^{-1} P_2 = \begin{pmatrix} 2 & 1 \\ 3 & 2 \end{pmatrix}^{-1} \begin{pmatrix} 2 & 3 \\ -1 & 2 \end{pmatrix} = \begin{pmatrix} 2 & -1 \\ -3 & 2 \end{pmatrix} \begin{pmatrix} 2 & 3 \\ -1 & 2 \end{pmatrix} = \begin{pmatrix} 5 & 4 \\ -8 & -5 \end{pmatrix}.$$

A quick check of the result:

$$5\begin{pmatrix} 2 \\ 3 \end{pmatrix} - 8\begin{pmatrix} 1 \\ 2 \end{pmatrix} = \begin{pmatrix} 2 \\ -1 \end{pmatrix}, \qquad 4\begin{pmatrix} 2 \\ 3 \end{pmatrix} - 5\begin{pmatrix} 1 \\ 2 \end{pmatrix} = \begin{pmatrix} 3 \\ 2 \end{pmatrix}.$$

Here is an alternative method for deducing the relation $P_1 P = P_2$: representing a vector $x \in \mathbf{R}^2$ in the respective bases $\mathcal{B}, \mathcal{B}_1, \mathcal{B}_2$, we obtain column vectors $X, X_1, X_2 \in \mathbf{R}^2$ satisfying

$$X = P_1 X_1, \qquad X = P_2 X_2, \qquad X_1 = P X_2,$$

by (1.3.1.2) (of course, $X = x$, since $\mathcal{B}$ is the canonical basis). Combining these relations, we obtain

$$P_1 P X_2 = P_1 X_1 = P_2 X_2 \implies P_1 P = P_2.$$

(1.3.3) Change of basis for linear maps. Let $f : E \longrightarrow E'$ be a linear map between vector spaces of dimensions $n = \dim(E)$ and $p = \dim(E')$. Assume that we are given two bases $\mathcal{B}_1, \mathcal{B}_2$ of E and two bases $\mathcal{B}'_1, \mathcal{B}'_2$ of E'. These data define the following matrices:

The matrix of change of basis $P = M_{\mathcal{B}_1}(\mathcal{B}_2) \in M_n(K)$ from $\mathcal{B}_1$ to $\mathcal{B}_2$.
The matrix of change of basis $P' = M_{\mathcal{B}'_1}(\mathcal{B}'_2) \in M_p(K)$ from $\mathcal{B}'_1$ to $\mathcal{B}'_2$.
The matrix $A_1 = M_{\mathcal{B}'_1}(f(\mathcal{B}_1)) \in M_{p,n}(K)$ representing f in the bases $\mathcal{B}_1$ and $\mathcal{B}'_1$.
The matrix $A_2 = M_{\mathcal{B}'_2}(f(\mathcal{B}_2)) \in M_{p,n}(K)$ representing f in the bases $\mathcal{B}_2$ and $\mathcal{B}'_2$.

Comparing the diagrams

$$\begin{array}{cccc} M_{\mathcal{B}_2}: & E & \xrightarrow{\sim} & K^n \\ & \Big\downarrow \mathrm{Id}_E & & \Big\downarrow P \\ M_{\mathcal{B}_1}: & E & \xrightarrow{\sim} & K^n \\ & \Big\downarrow f & & \Big\downarrow A_1 \\ M_{\mathcal{B}'_1}: & E' & \xrightarrow{\sim} & K^p \\ & \Big\uparrow \mathrm{Id}_{E'} & & \Big\uparrow P' \\ M_{\mathcal{B}'_2}: & E' & \xrightarrow{\sim} & K^p \end{array} \qquad\qquad \begin{array}{cccc} M_{\mathcal{B}_2}: & E & \xrightarrow{\sim} & K^n \\ & \Big\downarrow f & & \Big\downarrow A_2 \\ M_{\mathcal{B}'_2}: & E' & \xrightarrow{\sim} & K^p \end{array}$$

(and applying 1.2.6), we see that

$$A_2 = (P')^{-1} A_1 P. \tag{1.3.3.1}$$

Special case: if $E = E'$, $\mathcal{B}_1 = \mathcal{B}_1'$ and $\mathcal{B}_2 = \mathcal{B}_2'$, then $n = p$, $P' = P$, and $A_1, A_2 \in M_n(K)$, hence the formula (1.3.3.1) reads as follows:

$$A_2 = P^{-1} A_1 P. \tag{1.3.3.2}$$

(1.3.4) Exercise. *Consider the linear maps*

$$\begin{aligned} D : \mathbf{R}[t]_{\deg\le 3} &\longrightarrow \mathbf{R}[t]_{\deg\le 2}, \qquad f \mapsto f' \\ i : \mathbf{R}[t]_{\deg\le 2} &\longrightarrow \mathbf{R}[t]_{\deg\le 3}, \qquad f \mapsto \int_0^t f(u)\,du. \end{aligned}$$

Denote $\mathcal{B}_2 = \{1,\, 1-t,\, 1-2t+t^2\}$ *and* $\mathcal{B}_3 = \{1,\, 1-t,\, 1-2t+t^2,\, 1-3t+3t^2-t^3\}$.
(1) *Compute* $D \circ i$ *and* $i \circ D$.
(2) *Determine the kernel and the image of* D *(resp., of* i*).*
(3) *Check that* $\mathcal{B}_2$ *(resp.,* $\mathcal{B}_3$*) is a basis of* $\mathbf{R}[t]_{\deg\le 2}$ *(resp., of* $\mathbf{R}[t]_{\deg\le 3}$*) and determine the matrices of* D *and* i *with respect to these bases.*
(4) *Determine the matrices of change of basis between* $\mathcal{B}_2$ *and* $\mathcal{B}_2' = \{1, t, t^2\}$ *(resp., between* $\mathcal{B}_3$ *and* $\mathcal{B}_3' = \{1, t, t^2, t^3\}$*).*
(5) *Verify the formula (1.3.3.1) for the maps* D *and* i.

1.4 Computing the rank: Elementary operations

For a matrix $A \in M_{m,n}$, denote by $R_1, \ldots, R_m$ (resp., by $C_1, \ldots, C_n$) its rows (resp., its columns). We can perform with A the following operations.

(1.4.1) Elementary row operations:

- Interchange two rows: $R_i \longleftrightarrow R_j$.
- Replace R_i by $R_i + \lambda R_j$ ($\lambda \in K$).
- Multiply R_i by a non-zero scalar $\lambda \in K$, $\lambda \neq 0$.

(1.4.2) Elementary column operations:

- Interchange two columns: $C_i \longleftrightarrow C_j$.
- Replace C_i by $C_i + \lambda C_j$ ($\lambda \in K$).
- Multiply C_i by a non-zero scalar $\lambda \in K$, $\lambda \neq 0$.

(1.4.3) Basic facts: (0) Elementary operations are invertible; the inverse of an elementary row (resp., column) operation is an elementary row (resp., column) operation.
(1) Elementary operations preserve rank (see 1.4.6 below).
(2) Each matrix $A \in M_{m,n}$ can be transformed by a sequence of elementary operations to a matrix A' of the form

$$A' = \begin{pmatrix} d_1 & * & \cdots & * & * & \cdots & * \\ 0 & d_2 & \cdots & * & * & \cdots & * \\ \vdots & \vdots & \ddots & \vdots & * & \cdots & * \\ 0 & 0 & \cdots & d_r & * & \cdots & * \\ 0 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 & 0 & \cdots & 0 \end{pmatrix} \qquad (r \ge 0;\ d_1, \ldots, d_r \neq 0)$$

(with zeros below the main diagonal and below the r-row).
(3) In fact, an another sequence of elementary operations transforms A' into the matrix (written in block form)

$$A'' = \begin{pmatrix} I_r & 0 \\ 0 & 0 \end{pmatrix}$$

(4) Putting (1)–(3) together, we obtain

$$\mathrm{rk}(A) = \mathrm{rk}(A') = \mathrm{rk}(A'') = r.$$

(1.4.4) Example ($K = \mathbf{R}$): the calculation

$$A = \begin{pmatrix} 3 & 2 & -1 & 2 \\ 1 & -2 & 5 & 6 \\ 5 & 1 & 3 & 8 \end{pmatrix} \xrightarrow{[R_1 \longleftrightarrow R_2]} \begin{pmatrix} 1 & -2 & 5 & 6 \\ 3 & 2 & -1 & 2 \\ 5 & 1 & 3 & 8 \end{pmatrix} \xrightarrow{[R_2 := R_2 - 3R_1]} \begin{pmatrix} 1 & -2 & 5 & 6 \\ 0 & 8 & -16 & -16 \\ 5 & 1 & 3 & 8 \end{pmatrix} \xrightarrow{[R_2 := R_2/8]}$$

$$\xrightarrow{[R_2 := R_2/8]} \begin{pmatrix} 1 & -2 & 5 & 6 \\ 0 & 1 & -2 & -2 \\ 5 & 1 & 3 & 8 \end{pmatrix} \xrightarrow{[R_3 := R_3 - 5R_1]} \begin{pmatrix} 1 & -2 & 5 & 6 \\ 0 & 1 & -2 & -2 \\ 0 & 11 & -22 & -22 \end{pmatrix} \xrightarrow{[R_3 := R_3 - 11R_2]}$$

$$\xrightarrow{[R_3 := R_3 - 11R_2]} \begin{pmatrix} 1 & -2 & 5 & 6 \\ 0 & 1 & -2 & -2 \\ 0 & 0 & 0 & 0 \end{pmatrix} = A'$$

shows that $\mathrm{rk}(A) = \mathrm{rk}(A') = 2$. One can continue with column operations, obtaining

$$\begin{pmatrix} 1 & -2 & 5 & 6 \\ 0 & 1 & -2 & -2 \\ 0 & 0 & 0 & 0 \end{pmatrix} \xrightarrow{[C_2 := C_2 + 2C_1]} \begin{pmatrix} 1 & 0 & 5 & 6 \\ 0 & 1 & -2 & -2 \\ 0 & 0 & 0 & 0 \end{pmatrix} \xrightarrow{[C_3 := C_3 - 5C_1]} \begin{pmatrix} 1 & 0 & 0 & 6 \\ 0 & 1 & -2 & -2 \\ 0 & 0 & 0 & 0 \end{pmatrix} \xrightarrow{[C_4 := C_4 - 6C_1]}$$

$$\xrightarrow{[C_4 := C_4 - 6C_1]} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & -2 & -2 \\ 0 & 0 & 0 & 0 \end{pmatrix} \xrightarrow{[C_3 := C_3 + 2C_2]} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & -2 \\ 0 & 0 & 0 & 0 \end{pmatrix} \xrightarrow{[C_4 := C_4 + 2C_2]} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} = A''$$

(1.4.5) Matrix formulation. (1) Row operations (examples for matrices with 2 rows):

$$\begin{pmatrix} R_1 + 3R_2 \\ R_2 \end{pmatrix} = \begin{pmatrix} 1 & 3 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} R_1 \\ R_2 \end{pmatrix}, \qquad \begin{pmatrix} \lambda R_1 \\ R_2 \end{pmatrix} = \begin{pmatrix} \lambda & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} R_1 \\ R_2 \end{pmatrix}, \qquad \begin{pmatrix} R_2 \\ R_1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} R_1 \\ R_2 \end{pmatrix}.$$

(2) Column operations (example for matrices with 3 columns):

$$(C_1 \mid C_2 \mid C_3 + 2C_1) = (C_1 \mid C_2 \mid C_3) \begin{pmatrix} 1 & 0 & 2 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

$$(C_1 \mid \lambda C_2 \mid C_3) = (C_1 \mid C_2 \mid C_3) \begin{pmatrix} 1 & 0 & 0 \\ 0 & \lambda & 0 \\ 0 & 0 & 1 \end{pmatrix}, \qquad (C_2 \mid C_1 \mid C_3) = (C_1 \mid C_2 \mid C_3) \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

(3) The general case follows the same pattern. This means that any sequence of consecutive elementary operations transforms a matrix $A \in M_{m,n}(K)$ into a matrix of the form

$$gAh,$$

where $g \in M_m(K)$ (resp., $h \in M_n(K)$) is an invertible matrix representing a sequence of elementary row (resp., column) operations.

(1.4.6) Proposition. *Elementary operations preserve rank.*

Proof. We must show that, in the situation of 1.4.5(3), the two numbers

$$\begin{aligned}\mathrm{rk}(A) &= \dim(\mathrm{vect}(\text{the columns of } A))\\ \mathrm{rk}(gAh) &= \dim(\mathrm{vect}(\text{the columns of } gAh))\end{aligned}$$

are equal. The subspace (vect(the columns of A)) is unchanged by elementary column operations, hence $\mathrm{rk}(gAh) = \mathrm{rk}(gA)$. On the other hand, left multiplication by g defines a bijective linear map

$$g : \mathrm{vect}(\text{the columns of } A) \longrightarrow \mathrm{vect}(\text{the columns of } gA)$$

(its inverse being given by left multiplication by g^{-1}); thus the two spaces have the same dimension, which proves the desired equality $\mathrm{rk}(A) = \mathrm{rk}(gA)$.

(1.4.7) The transpose. (1) Recall that the **transpose** of a matrix $A \in M_{m,n}(K)$ is the matrix ${}^tA \in M_{n,m}(K)$ with entries

$$({}^tA)_{ij} = A_{ji}.$$

In other words, the rows of A coincide with the columns of ${}^tA$, and vice versa. For example,

$$A = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{pmatrix}, \qquad {}^tA = \begin{pmatrix} 1 & 4 \\ 2 & 5 \\ 3 & 6 \end{pmatrix}.$$

(2) **Warning:** taking the transpose reverses the order of a matrix product:

$${}^t(AB) = {}^tB\,{}^tA.$$

(3) A **square** matrix $A \in M_n(K)$ is **symmetric** (resp., **skew-symmetric**) if ${}^tA = A$ (resp., if ${}^tA = -A$).

(4) **Exercise:** determine the dimension of the subspace of symmetric (resp., skew-symmetric) matrices in $M_n(\mathbf{R})$.

(1.4.8) Proposition. *For each matrix $A \in M_{m,n}(K)$, we have $\mathrm{rk}(A) = \mathrm{rk}({}^tA)$. In other words, the vector spaces*

$$\begin{aligned}&\mathrm{vect}(\text{the columns of } A) \subset K^m\\ &\mathrm{vect}(\text{the columns of } {}^tA) = {}^t(\mathrm{vect}(\text{the rows of } A)) \subset K^n\end{aligned}$$

have the same dimension.

Proof. There exists a sequence of elementary operations which transforms A into

$$B = gAh = \begin{pmatrix} I_r & 0 \\ 0 & 0 \end{pmatrix} \in M_{m,n}(K).$$

Applying the transpose, we obtain a sequence of elementary operations transforming ${}^tA$ into

$$ {}^t B = {}^t h \, {}^t A \, {}^t g = \begin{pmatrix} I_r & 0 \\ 0 & 0 \end{pmatrix} \in M_{n,m}(K). $$

It is clear that $\mathrm{rk}(B) = \mathrm{rk}({}^tB) = r$. On the other hand, $\mathrm{rk}(A) = \mathrm{rk}(B)$ and $\mathrm{rk}({}^tA) = \mathrm{rk}({}^tB)$, by 1.4.6; thus $\mathrm{rk}(A) = r = \mathrm{rk}({}^tA)$.

(1.4.9) Computing the inverse matrix. If a square matrix $A \in M_n(K)$ has maximal rank $\mathrm{rk}(A) = n$, then it is not necessary tu use column operations; A can be transformed into the matrix $A'' = I_n$ by applying only elementary **row** operations. These operations can be expressed in matrix form as a left multiplication by a suitable (invertible) matrix $B \in M_n(K)$. The equality $BA = I_n$ implies that $B = A^{-1}$ in the inverse matrix of A, hence the same sequence of elementary row operations transforms the identity matrix I_n into $BI_n = B = A^{-1}$. This is best done in practice by putting A and I_n side by side and applying all row operations simultaneously to both matrices.

Example: Compute the inverse of the matrix

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

$$ \left(\begin{array}{ccc|ccc} 4 & 2 & 3 & 1 & 0 & 0 \\ 6 & 5 & 4 & 0 & 1 & 0 \\ 3 & 2 & 1 & 0 & 0 & 1 \end{array}\right) \xrightarrow{[R_1 := R_1 - R_3]} \left(\begin{array}{ccc|ccc} 1 & 0 & 2 & 1 & 0 & -1 \\ 6 & 5 & 4 & 0 & 1 & 0 \\ 3 & 2 & 1 & 0 & 0 & 1 \end{array}\right) \xrightarrow{[R_2 := R_2 - 2R_3]} \left(\begin{array}{ccc|ccc} 1 & 0 & 2 & 1 & 0 & -1 \\ 0 & 1 & 2 & 0 & 1 & -2 \\ 3 & 2 & 1 & 0 & 0 & 1 \end{array}\right) $$

$$ \xrightarrow{[R_3 := R_3 - 3R_1]} \left(\begin{array}{ccc|ccc} 1 & 0 & 2 & 1 & 0 & -1 \\ 0 & 1 & 2 & 0 & 1 & -2 \\ 0 & 2 & -5 & -3 & 0 & 4 \end{array}\right) \xrightarrow{[R_3 := R_3 - 2R_2]} \left(\begin{array}{ccc|ccc} 1 & 0 & 2 & 1 & 0 & -1 \\ 0 & 1 & 2 & 0 & 1 & -2 \\ 0 & 0 & -9 & -3 & -2 & 8 \end{array}\right) \xrightarrow{[R_3 := -R_3/9]} $$

$$ \xrightarrow{[R_3 := -R_3/9]} \left(\begin{array}{ccc|ccc} 1 & 0 & 2 & 1 & 0 & -1 \\ 0 & 1 & 2 & 0 & 1 & -2 \\ 0 & 0 & 1 & 1/3 & 2/9 & -8/9 \end{array}\right) \xrightarrow{[R_1 := R_1 - 2R_3]} \left(\begin{array}{ccc|ccc} 1 & 0 & 0 & 1/3 & -4/9 & 7/9 \\ 0 & 1 & 2 & 0 & 1 & -2 \\ 0 & 0 & 1 & 1/3 & 2/9 & -8/9 \end{array}\right) \xrightarrow{[R_2 := R_2 - 2R_3]} $$

$$ \xrightarrow{[R_2 := R_2 - 2R_3]} \left(\begin{array}{ccc|ccc} 1 & 0 & 0 & 1/3 & -4/9 & 7/9 \\ 0 & 1 & 0 & -2/3 & 5/9 & -2/9 \\ 0 & 0 & 1 & 1/3 & 2/9 & -8/9 \end{array}\right) $$

In other words,

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

In order to check the result, we compute

$$ \begin{pmatrix} 4 & 2 & 3 \\ 6 & 5 & 4 \\ 3 & 2 & 1 \end{pmatrix} \begin{pmatrix} 3 & -4 & 7 \\ -6 & 5 & -2 \\ 3 & 2 & -8 \end{pmatrix} = \begin{pmatrix} 9 & 0 & 0 \\ 0 & 9 & 0 \\ 0 & 0 & 9 \end{pmatrix} = 9I_3. $$

Warning: If the calculation breaks down, i.e. if one of the rows or columns of the left hand side matrix becomes zero, we conclude that $\mathrm{rk}(A) < n$, hence A is not invertible.

Small dimensions: For $n = 2$ one can write directly

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} = \frac{1}{ad-bc} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} \tag{1.4.9.1}$$

(provided $ad - bc \neq 0$, which ensures that the matrix is invertible).

(1.4.10) Exercise. *Using elementary operations on rows and/or columns, determine the ranks of the following matrices and, whenever possible, compute their inverse.*

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

(1.4.11) Exercise. *Determine the dimension of the space of solutions of the system of linear equations*

$$\begin{array}{ccccccccccc} x_1 & - & 2x_2 & + & 2x_3 & + & 3x_4 & + & x_5 & = & 0 \\ 2x_1 & - & 2x_2 & + & x_3 & + & 4x_4 & + & 3x_5 & = & 0 \\ x_1 & + & 2x_2 & - & 4x_3 & - & x_4 & + & 3x_5 & = & 0 \end{array}$$

(1.4.12) Exercise. *Show that there is a unique linear map $f : \mathbf{R}^3 \longrightarrow \mathbf{R}^2$ such that*

$$f\left(\begin{pmatrix} 0 \\ -1 \\ 1 \end{pmatrix}\right) = \begin{pmatrix} 1 \\ 1 \end{pmatrix}, \quad f\left(\begin{pmatrix} 1 \\ 2 \\ 0 \end{pmatrix}\right) = \begin{pmatrix} 3 \\ -1 \end{pmatrix}, \quad f\left(\begin{pmatrix} 1 \\ 3 \\ -2 \end{pmatrix}\right) = \begin{pmatrix} 0 \\ -3 \end{pmatrix};$$

determine its matrix $A \in M_{2,3}(\mathbf{R})$ in the canonical bases of $\mathbf{R}^3$ and $\mathbf{R}^2$ (i.e., $f(x) = Ax$ for all $x \in \mathbf{R}^3$).

1.5 Determinants

(1.5.1) Recall that the **determinant** of a **square matrix** $A \in M_n(K)$ is the scalar $\det(A) = |A| \in K$ defined recursively as follows:

(1) If $n = 1$, then $A = (a_{11})$ and $\det(A) = a_{11}$.
(2) If $n = 2$, then

$$\begin{vmatrix} a & b \\ c & d \end{vmatrix} = ad - bc.$$

(3) More generally, for $n \geq 2$, the determinant $\det(A)$ can be expanded with respect to each row (resp., each column). For example, expanding the following determinant with respect to the second row, we obtain

$$\begin{vmatrix} 1 & 4 & -2 \\ 7 & 3 & 5 \\ 1 & -3 & 2 \end{vmatrix} = -7 \begin{vmatrix} 4 & -2 \\ -3 & 2 \end{vmatrix} + 3 \begin{vmatrix} 1 & -2 \\ 1 & 2 \end{vmatrix} - 5 \begin{vmatrix} 1 & 4 \\ 1 & -3 \end{vmatrix} = -7 \cdot 2 + 3 \cdot 4 - 5(-7) = 33.$$

The general rule is the following: putting (for $1 \leq i, j \leq n$)

$$M_{ij} = (-1)^{i+j} \det(\text{the matrix obtained from } A \text{ by deleting the } i\text{−th row and the } j\text{−th column}),$$

then we have, for each $k = 1, \dots, n$,

$$\begin{aligned}\det(A) &= \sum_{j=1}^{n} a_{kj}\, M_{kj} \qquad \text{(expansion with respect to the } k\text{−th row)}\\ &= \sum_{i=1}^{n} a_{ik}\, M_{ik} \qquad \text{(expansion with respect to the } k\text{−th column)}\end{aligned}$$

(4) In particular, if

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

is an upper-triangular matrix ($\iff$ all elements below the main diagonal are zero), then the expansion with respect to the first column implies, recursively, that the determinant of A

$$\begin{vmatrix} a_{11} & * & \cdots & * \\ 0 & a_{22} & \cdots & * \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & a_{nn} \end{vmatrix} = a_{11} \begin{vmatrix} a_{22} & \cdots & * \\ \vdots & \ddots & \vdots \\ 0 & \cdots & a_{nn} \end{vmatrix} = \cdots = a_{11}a_{22}\cdots a_{nn}$$

is equal to the product of the elements of the main diagonal. The same result holds for lower-triangular matrices ($\iff$ all elements above the main diagonal are zero).

(1.5.2) Properties of determinants

(1) $\det({}^tA) = \det(A)$.
(2) $\det(AB) = \det(A)\det(B)$.
(3) The expansion rules from 1.5.1(3) can be reformulated in terms of the matrix $M = (M_{ij}) \in M_n(K)$ as follows:

$${}^tM\, A = \det(A) I_n.$$

In particular, if $\det(A) \neq 0$, then the matrix A is invertible and its inverse is equal to

$$A^{-1} = \frac{1}{\det(A)}\, {}^tM$$

(which generalises the formula (1.4.9.1)). However, this method of computing A^{-1} is not very useful in practice.
(4) A is invertible $\iff$ $\det(A) \neq 0$ (the implications "$\Longrightarrow$" and "$\Longleftarrow$" following respectively from (2) and (3)).

(1.5.3) Computing determinants using elementary operations

Elementary operations have the following effect on the determinant:

(1) Replacing R_i (resp., C_i) by $R_i + \lambda R_j$ (resp., by $C_i + \lambda C_j$) **does not change the determinant.**
(2) Replacing R_i (resp., C_i) by λR_i (resp., by λC_i) **multiplies the determinant by λ.**
(3) Interchanging two rows (resp., two columns) **multiplies the determinant by -1.**

Applying these rules, it is enough to transform A into a triangular matrix, for which the determinant is given by 1.5.1(4). For example, we compute

$$\begin{vmatrix} 1 & 4 & -2 \\ 7 & 3 & 5 \\ 1 & -3 & 2 \end{vmatrix} \xlongequal{[R_1:=R_1+R_3]} \begin{vmatrix} 2 & 1 & 0 \\ 7 & 3 & 5 \\ 1 & -3 & 2 \end{vmatrix} \xlongequal{[C_1:=C_1-2C_2]} \begin{vmatrix} 0 & 1 & 0 \\ 1 & 3 & 5 \\ 7 & -3 & 2 \end{vmatrix}.$$

Having reached this point, we can either expand the determinant with respect to the first row:

$$\begin{vmatrix} 0 & 1 & 0 \\ 1 & 3 & 5 \\ 7 & -3 & 2 \end{vmatrix} = -1 \begin{vmatrix} 1 & 5 \\ 7 & 2 \end{vmatrix} = -(1 \cdot 2 - 5 \cdot 7) = 33,$$

or apply additional elementary operations:

$$\begin{vmatrix} 0 & 1 & 0 \\ 1 & 3 & 5 \\ 7 & -3 & 2 \end{vmatrix} \xlongequal{[C_1 \longleftrightarrow C_2]} - \begin{vmatrix} 1 & 0 & 0 \\ 3 & 1 & 5 \\ -3 & 7 & 2 \end{vmatrix} \xlongequal{[C_3:=C_3-5C_2]} \begin{vmatrix} 1 & 0 & 0 \\ 3 & 1 & 0 \\ -3 & 7 & -33 \end{vmatrix} = 33.$$

(1.5.4) Exercise. *Compute the determinants of the matrices from 1.4.10.*

(1.5.5) Exercise. *What is the relation between* $\det(A)$ *and* $\det(\lambda A)$*, for* $A \in M_n(K)$ *and* $\lambda \in K$*?*

(1.5.6) Exercise. *Compute the determinants*

$$\begin{vmatrix} 1 & a \\ 1 & b \end{vmatrix}, \qquad \begin{vmatrix} 1 & a & a^2 \\ 1 & b & b^2 \\ 1 & c & c^2 \end{vmatrix}, \qquad \begin{vmatrix} 1 & a & a^2 & a^3 \\ 1 & b & b^2 & b^3 \\ 1 & c & c^2 & c^3 \\ 1 & d & d^2 & d^3 \end{vmatrix}.$$

Any comments?

(1.5.7) Exercise. *If* $A \in M_n(\mathbf{R})$ *satisfies* $A^2 = -I_n$*, show that* $n = 2m$ *is even.*

1.6 Eigenvectors, eigenvalues; diagonalisation of endomorphisms

(1.6.1) Definition. *Let* $f : E \longrightarrow E$ *be an endomorphism of a* K*-vector space* E*. An* **eigenvalue of** f *is a scalar* $\lambda \in K$ *for which there exists a non-zero vector* $x \in E$ *satisfying* $f(x) = \lambda x$ *(we say that* x *is an* **eigenvector of** f *with eigenvalue* λ*). If* $E = K^n$ *and* $f(x) = Ax$ *for* $A \in M_n(K)$*, we speak of eigenvalues and eigenvectors of the matrix* A*.*

(1.6.2) Examples: (1) For $f : K^2 \longrightarrow K^2$ given by the formula $f(X) = AX$, where

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

then

$$Ae_1 = \begin{pmatrix} 2 & 0 \\ 0 & 3 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 2 \\ 0 \end{pmatrix} = 2e_1, \qquad Ae_2 = \begin{pmatrix} 2 & 0 \\ 0 & 3 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 3 \end{pmatrix} = 3e_2;$$

Thus e_1 and e_2 are eigenvectors of f, with eigenvalues 2 and 3, respectively.
(2) More generally, if $E = K^n$ and $f(X) = AX$ with a diagonal matrix

$$A = \begin{pmatrix} d_1 & 0 & \cdots & 0 \\ 0 & d_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & d_n \end{pmatrix},$$

then all elements $e_1, \ldots, e_n$ of the canonical basis of K^n are eigenvectors of f, as $f(e_i) = Ae_i = d_i e_i$. In the special case when $d_1 = \cdots = d_n = d$ (i.e., when $A = dI_n$ is a multiple of the identity matrix, then $f(x) = dx$ for all $x \in K^n$, hence each non-zero vector is an eigenvector of f (with eigenvalue d).

(1.6.3) The condition $f(x) = \lambda x$ is equivalent to

$$0 = f(x) - \lambda x = (f - \lambda \operatorname{Id}_E)(x).$$

In other words,

$$\lambda \text{ is an eigenvalue of } f \iff \operatorname{Ker}(f - \lambda \operatorname{Id}_E) \neq 0.$$

If this is the case, then all eigenvectors with eigenvalue λ (together with the zero vector) form the subspace

$$\operatorname{Ker}(f - \lambda \operatorname{Id}_E) \subset E,$$

called the **eigenspace of f for eigenvalue λ**.

(1.6.4) Matrix formulation. Let $\mathcal{B} = \{e_1, \ldots, e_n\}$ ($n = \dim(E)$) be a basis of E and $A = M_{\mathcal{B},\mathcal{B}}(f) \in M_n(K)$ the matrix of f in the basis $\mathcal{B}$. Under the identification

$$\begin{aligned} M_{\mathcal{B}} : E &\xrightarrow{\sim} K^n \\ x &\mapsto X \end{aligned}$$

the map f becomes left multiplication by $A : X \mapsto AX$. This means that

$$\lambda \text{ is an eigenvalue of } f \iff \operatorname{Ker}(A - \lambda I_n) \neq 0 \iff P_A(\lambda) = 0,$$

where

$$P_A(t) = \det(t\, I_n - A)$$

is the **characteristic polynomial of** A. In other words, the eigenvalues of A (= of f) are precisely the roots of its characteristic polynomial. If we choose another basis, then the matrix A is replaced by $A' = P^{-1}AP$, for some invertible matrix $P \in M_n(K)$ (by (1.3.3.2)). Multiplicativity of determinants implies that

$$P_{A'}(t) = \det(t\, I_n - A') = \det(P^{-1}(t\, I_n - A)P) = \det(P)^{-1} \det(t\, I_n - A) \det(P) = \det(t\, I_n - A) = P_A(t),$$

hence the characteristic polynomial does not depend on the chosen basis; we can write $P_f(t)$ for $P_A(t)$.

(1.6.5) Examples: (1) $n = 2$: The characteristic polynomial of the matrix

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

is equal to

$$P_A(t) = \begin{vmatrix} t - a & -b \\ -c & t - d \end{vmatrix} = (t-a)(t-d) - (-b)(-c) = t^2 - (a+d)t + (ad - bc) = t^2 - \operatorname{Tr}(A)t + \det(A).$$

(2) In general,

$$P_A(t) = t^n - \mathrm{Tr}(A)t^{n-1} + \cdots + (-1)^n \det(A),$$

which implies that the eigenvalues $\lambda_1, \ldots, \lambda_n$ of A satisfy

$$\lambda_1 + \cdots + \lambda_n = \mathrm{Tr}(A), \qquad \lambda_1 \cdots \lambda_n = \det(A).$$

Recall that **the trace** of a square matrix $A \in M_n(K)$ is defined as the sum of all elements on the main diagonal: $\mathrm{Tr}(A) = A_{11} + A_{22} + \cdots + A_{nn}$.

(3) If A is a triangular matrix

$$A = \begin{pmatrix} A_{11} & A_{12} & \cdots & A_{1n} \\ 0 & A_{22} & \cdots & A_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & A_{nn} \end{pmatrix},$$

then

$$P_A(t) = (t - A_{11}) \cdots (t - A_{nn}),$$

hence the eigenvalues of A coincide with its diagonal elements $A_{11}, \ldots, A_{nn}$.

(1.6.6) Diagonalisable endomorphisms. As before, let $f : E \longrightarrow E$ be an endomorphism of a K-vector space E of dimension $\dim(E) = n$; choose a basis $\mathcal{B}$ of E and let $A \in M_n(K)$ be the (square) matrix representing f in this basis.

Definition. *We say that f (or A) is* **diagonalisable** *(over K) if there exists a basis $\mathcal{B}'$ of E in which the matrix A' of f is diagonal:*

$$A' = D = \begin{pmatrix} d_1 & 0 & \cdots & 0 \\ 0 & d_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & d_n. \end{pmatrix}$$

As $A' = P^{-1}AP$, where $P \in M_n(K)$ is the (invertible) matrix of change of basis from $\mathcal{B}$ to $\mathcal{B}'$, it follows that

$$A \text{ is diagonalisable over } K \iff \exists P \in M_n(K) \text{ invertible such that } P^{-1}AP = D \text{ is diagonal}$$

(the symbol "$\exists$" stands for **"there exists"**). Let us reformulate this condition in terms of the columns $v_1, \ldots, v_n$ of the matrix $P = (v_1 \mid \cdots \mid v_n)$. Firstly,

$$P \text{ is invertible} \iff \text{the vectors } v_1, \ldots, v_n \text{ are linearly independent.}$$

Secondly, the relation $P^{-1}AP = D$ is equivalent to $AP = PD$ (since P is invertible). As

$$AP = (Av_1 \mid \cdots \mid Av_n), \qquad PD = (d_1 v_1 \mid \cdots \mid d_n v_n),$$

it follows that

$$AP = PD \iff Av_1 = d_1 v_1, \ldots, Av_n = d_n v_n.$$

To sum up,

$$A \text{ is diagonalisable over } K \iff \exists n \text{ linearly independent eigenvectors } v_1, \ldots, v_n \in K^n \text{ of } A. \quad (1.6.6.1)$$

The matrix $P = (v_1 \mid \cdots \mid v_n) \in M_n(K)$ with columns $v_1, \ldots, v_n$ is then invertible and the matrix $P^{-1}AP$ is diagonal, with diagonal elements equal to the respective eigenvalues of $v_1, \ldots, v_n$ (in particular, all eigenvalues of A are contained in K).

It can happen that A is not diagonalisable over K, but becomes diagonalisable over a bigger field K'.

(1.6.7) Examples: (1) Consider the matrix

$$A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \in M_2(\mathbf{R}).$$

Its characteristic polynomial $P_A(t) = t^2 - \mathrm{Tr}(A)t + \det(A) = t^2 + 1 = (t-i)(t+i)$ has no real roots, hence A has no eigenvectors contained in $\mathbf{R}^2$. In particular, A **is not diagonalisable over R**. On the other hand, the complex eigenvectors

$$v_1 = \begin{pmatrix} 1 \\ -i \end{pmatrix} \in \mathrm{Ker}(A - iI), \qquad v_2 = \begin{pmatrix} 1 \\ i \end{pmatrix} \in \mathrm{Ker}(A + iI)$$

are linearly independent (as elements of the **C**-vector space $\mathbf{C}^2$), hence A **is diagonalisable over C:**

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

(2) The characteristic polynomial of the matrix

$$B = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \in M_2(K)$$

is equal to $P_B(t) = t^2$; thus $\lambda = 0$ is the only eigenvalue of B. The corresponding eigenspace $\mathrm{Ker}(B - \lambda I) = \mathrm{Ker}(B)$ is equal to the set of solutions of the linear equation

$$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix},$$

which consists of the multiples of the vector $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$. This means that two linearly independent eigenvectors of B do not exist, hence B **is not diagonalisable over** K (for any field K).

(3) More generally, if the characteristic polynomial of a matrix $A \in M_n(K)$ has only one root with multiplicity n, i.e. if $P_A(t) = (t - \lambda)^n$ $(\lambda \in K)$, then

$$A \text{ is diagonalisable over } K \iff A = \lambda\, I_n.$$

Indeed, if A is diagonalisable, then all diagonal elements of $P^{-1}AP$ are eigenvalues of A. As λ is the only eigenvalue of A, we must have $P^{-1}AP = \lambda\, I_n$, hence $A = P\lambda\, I_n P^{-1} = \lambda\, I_n$.

(1.6.8) General criteria of diagonalisability. Recall two general facts from the Linear Algebra course:

(a) Any set of eigenvectors of A corresponding to distinct eigenvalues is linearly independent.

(b) For each eigenvalue $\lambda \in K$ of A, the dimension of the eigenspace $\mathrm{Ker}(A - \lambda\, I_n)$ (the **geometric multiplicity of** λ) is at most equal to the multiplicity of λ as a root of $P_A(t)$ (the **algebraic multiplicity of** λ).

The fact (a) has as an immediate corollary the following

Criterion 1. *If $A \in M_n(K)$ has n distinct eigenvalues contained in K, then A is diagonalisable over K.*

If this criterion does not apply, namely in the case when the characteristic polynomial $P_A(t)$ has multiple roots, we must apply the following criterion (which is a consequence of (b)):

Criterion 2. *A matrix $A \in M_n(K)$ is diagonalisable over $K \iff$ all roots of P_A are contained in K, and the algebraic and geometric multiplicity of each root of P_A coincide.*

(1.6.9) Exercise. *Show that, if λ is an eigenvalue of A, then λ^7 is an eigenvalue of A^7.*

(1.6.10) Exercise. *Assume that $A \in M_n(\mathbf{R})$ satisfies $A^2 - 5A + 6I_n = 0$. What can we say about the eigenvalues of A?*

(1.6.11) Exercise. (1) *Which among the following matrices*

$$\begin{pmatrix} 2 & 2 \\ 2 & 2 \end{pmatrix}, \qquad \begin{pmatrix} 2 & -2 \\ 2 & 2 \end{pmatrix}, \qquad \begin{pmatrix} 2 & -2 \\ 2 & -2 \end{pmatrix}, \qquad \begin{pmatrix} 2 & -2 \\ -2 & 2 \end{pmatrix}$$

are diagonalisable over $\mathbf{R}$ (resp., over $\mathbf{C}$)?

(2) *For which $a \in \mathbf{R}$ is the matrix $\begin{pmatrix} -1 & a \\ 1 & 3 \end{pmatrix}$ diagonalisable over $\mathbf{R}$ (resp., over $\mathbf{C}$)?*

(3) *Which among the following matrices*

$$\begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix}, \qquad \begin{pmatrix} 0 & 1 & 0 \\ 1 & 1 & 1 \\ 0 & 1 & 0 \end{pmatrix}, \qquad \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$$

are diagonalisable over $\mathbf{R}$ (resp., over $\mathbf{C}$)?

(4) *Construct a complex matrix $A \in M_2(\mathbf{C})$ which is symmetric ($A = {}^tA$) and is not diagonalisable over $\mathbf{C}$.*

(1.6.12) Exercise. *Compute $P_A(A)$ in the following cases:*

(1) *$A \in M_2(K)$.*

(2) *$A \in M_n(K)$ is diagonal.*

(3) *$A \in M_n(K)$ is diagonalisable.*

Any comments?

1.7 The dual space*

(1.7.1) What is a row vector? Once we choose a basis of a finite-dimensional vector space E, then the elements of E are identified with **column vectors**. What do **row vectors** correspond to?

A row vector is an element of

$$M_{1,n}(K) = \mathscr{L}(K^n, K) = \{\text{linear maps } K^n \longrightarrow K\},$$

which motivates the following abstract definition.

(1.7.2) Definition. *The* **dual** *of a K-vector space E is the K-vector space*

$$E^* = \mathscr{L}(E, K) = \{\text{linear maps } E \longrightarrow K\};$$

an element of E^* is called a **linear form** *on E.*

(1.7.3) Examples: (1) If $E = K^n = M_{n,1}(K)$, then

$$E^* = (K^n)^* = \mathscr{L}(K^n, K) = M_{1,n}(K) = \{(a_1, \ldots, a_n) \mid a_i \in K\}$$

consists of row vectors. The linear form $f_a : K^n \longrightarrow K$ associated to a row vector $a = (a_1, \ldots, a_n)$ is given by the formula

*** This section is optional.**

$$f_a : x = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \mapsto (a_1, \ldots, a_n) \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = a_1 x_1 + \cdots + a_n x_n.$$

(2) For example, $(3, -2) \in (\mathbf{R}^2)^*$ is the linear form

$$f(x) = f(\begin{pmatrix} x_1 \\ x_2 \end{pmatrix}) = (3, -2) \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = 3x_1 - 2x_2.$$

(3) If $\dim(E) < \infty$, then the formula from 1.2.8(2) implies that $\dim(E^*) = \dim(E)\dim(K) = \dim(E)$.

(1.7.4) Dual basis. Assume that $n = \dim(E) < \infty$. Given a basis $\mathcal{B} = \{v_1, \ldots, v_n\}$ of E, each vector $x \in E$ can be written uniquely as

$$x = x_1 v_1 + \cdots + x_n v_n \qquad\qquad (x_i \in K).$$

For a fixed index $i = 1, \ldots, n$, associating to x its i-th coordinate in the basis $\mathcal{B}$ defines a linear map $E \longrightarrow K$, which will be denoted by

$$\begin{aligned} v_i^* : E &\longrightarrow K \\ x &\mapsto x_i. \end{aligned}$$

The **"coordinate functions"** $v_1^*, \ldots, v_n^* \in E^*$ are elements of the dual space, characterised by the property

$$v_i^*(v_j) = v_i(0 \cdot v_1 + \cdots + 1 \cdot v_j + \cdots + 0 \cdot v_n) = \delta_{ij} = \begin{cases} 1, & \text{if } i = j \\ 0, & \text{if } i \neq j, \end{cases} \tag{1.7.4.1}$$

which implies that $v_1^*, \ldots, v_n^*$ are linearly independent, hence form a basis $\mathcal{B}^*$ of E^* (since $\dim(E^*) = n$), called **the dual basis of $\mathcal{B}$**.

Example: If $E = K^n$ and if $\mathcal{B} = \{e_1, \ldots, e_n\}$ is the canonical basis of K^n, then

$$x = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = x_1 e_1 + \cdots + x_n e_n, \qquad x_i = (0, \ldots, 1, \ldots, 0) \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = e_i^*(x),$$

hence the dual basis $\mathcal{B}^*$ of $(K^n)^*$ consists of the row vectors

$$e_1^* = (1, 0, \ldots, 0), \qquad e_2^* = (0, 1, 0, \ldots, 0), \qquad \cdots \qquad e_n^* = (0, \ldots, 0, 1).$$

(1.7.5) Computing the dual basis. Given a basis $v_1, \ldots, v_n$ of K^n, how do we find the dual basis $v_1^*, \ldots, v_n^*$ of $(K^n)^*$?

The answer is simple: is is enough to consider the matrices

$$A = (v_1 \mid \cdots \mid v_n) \in M_n(K), \qquad B = \begin{pmatrix} v_1^* \\ \vdots \\ v_n^* \end{pmatrix} \in M_n(K).$$

The formula (1.7.4.1) implies that

$$BA = \begin{pmatrix} v_1^*(v_1) & \cdots & v_1^*(v_n) \\ \vdots & \ddots & \vdots \\ v_n^*(v_1) & \cdots & v_n^*(v_n) \end{pmatrix} = \begin{pmatrix} 1 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & 1 \end{pmatrix} = I_n,$$

hence $v_1^*, \dots, v_n^*$ are the rows of the matrix $B = A^{-1}$.

Example: Find the dual basis $v_1^*, v_2^* \in (\mathbf{R}^2)^*$ to the basis

$$v_1 = \begin{pmatrix} 3 \\ 2 \end{pmatrix}, \qquad v_2 = \begin{pmatrix} 8 \\ 5 \end{pmatrix}.$$

As

$$A = \begin{pmatrix} 3 & 8 \\ 2 & 5 \end{pmatrix}, \qquad A^{-1} = \frac{1}{3 \cdot 5 - 8 \cdot 2} \begin{pmatrix} 5 & -8 \\ -2 & 3 \end{pmatrix} = \begin{pmatrix} -5 & 8 \\ 2 & -3 \end{pmatrix},$$

we have $v_1^* = (-5, 8)$ and $v_2^* = (2, -3)$.

(1.7.6) What is the dual basis good for? It allows us to compute the coordinates of an arbitrary vector $x \in E$ in the basis $\mathcal{B} = \{v_1, \dots, v_n\}$:

$$x = v_1^*(x)\, v_1 + \cdots + v_n^*(x)\, v_n.$$

In the previous example, we have

$$x = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = (-5x_1 + 8x_2) \begin{pmatrix} 3 \\ 2 \end{pmatrix} + (2x_1 - 3x_2) \begin{pmatrix} 8 \\ 5 \end{pmatrix}.$$

(1.7.7) The dual map. Let $\alpha : E \longrightarrow F$ be a linear map between two K-vector spaces. Its **dual map** $\alpha^* : F^* \longrightarrow E^*$ is defined by the formula

$$\alpha^*(\lambda) = \lambda \circ \alpha : \, E \xrightarrow{\alpha} F \xrightarrow{\lambda} K.$$

Matrix formulation: assume that $n = \dim(E)$, $p = \dim(F)$. Given a basis $\mathcal{B} = \{e_1, \dots, e_n\}$ (resp., $\mathcal{C} = \{f_1, \dots, f_p\}$) of E (resp., of F), let $\mathcal{B}^* = \{e_1^*, \dots, e_n^*\}$ (resp., $\mathcal{C}^* = \{f_1^*, \dots, f_p^*\}$) be the dual basis of E^* (resp., of F^*). Let

$$\begin{aligned} A &= M_{\mathcal{B},\mathcal{C}}(\alpha) = M_{\mathcal{C}}(\alpha(\mathcal{B})) \in M_{p,n}(K) \\ M &= M_{\mathcal{C}^*,\mathcal{B}^*}(\alpha^*) = M_{\mathcal{B}^*}(\alpha^*(\mathcal{C}^*)) \in M_{n,p}(K) \end{aligned}$$

be the matrices representing α and α^*, respectively. By definition, we have

$$\begin{aligned} A_{ij} &= (\text{the } i\text{-th coordinate of } \alpha(e_j) \text{ in the basis } \mathcal{C}) = f_i^*(\alpha(e_j)) = (f_i^* \circ \alpha)(e_j) \qquad (1.7.7.1) \\ M_{ji} &= (\text{the } j\text{-th coordinate of } \alpha^*(f_i^*) \text{ in the basis } \mathcal{B}^*) = (\alpha^*(f_i^*))(e_j). \end{aligned}$$

However,

$$\alpha^*(f_i^*) = f_i^* \circ \alpha,$$

which means that $A_{ij} = M_{ji}$ (for all pairs of indices i, j), hence **the dual map is represented (in the dual bases) by the transpose matrix:**

$$M = {}^t\!A.$$

(1.7.8) Summary: The dictionary from the beginning of this chapter can be extended as follows:

Abstract object	Matrix object
vector space E	K^n
vector $x \in E$	column vector $\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$
linear map $\alpha : E \longrightarrow F$	matrix $A \in M_{p,n}(K)$
$\mathscr{L}(E, F)$	$M_{p,n}(K)$
linear form $f \in E^*$	row vector $(a_1, \ldots, a_n)$
dual map $\alpha^* : F^* \longrightarrow E^*$	transpose matrix ${}^tA \in M_{n,p}(K)$

(1.7.9) Double dual: evaluation at any vector $x \in E$ defines a linear form on E^*, hence an element ev_x of E^{**}:

$$\begin{aligned} \mathrm{ev}_x : E^* &\longrightarrow K \\ \lambda &\mapsto \lambda(x). \end{aligned}$$

Moreover, the map

$$\begin{aligned} \mathrm{ev} : E &\longrightarrow E^{**} \\ x &\mapsto \mathrm{ev}_x \end{aligned}$$

is linear and injective. If $n = \dim(E) < \infty$, then ev is an isomorphism, since $\dim(E^{**}) = \dim(E^*) = \dim(E)$. Moreover, if $\mathcal{B} = \{e_1, \ldots, e_n\}$ is a basis of E and $\mathcal{B}^* = \{e_1^*, \ldots, e_n^*\}$ the dual basis of E^*, then the dual basis $\mathcal{B}^{**}$ to $\mathcal{B}^*$ coincides with $\mathrm{ev}(\mathcal{B}) = \{\mathrm{ev}(e_1), \ldots, \mathrm{ev}(e_n)\}$. In this case one usually identifies E with its double dual E^{**} via ev, hence also $\mathcal{B}^{**}$ with $\mathcal{B}$.

2. Multilinear maps

2.1 Examples

(2.1.1) Euclidean scalar product. The standard Euclidean scalar product

$$(x \mid y) = x_1 y_1 + \cdots + x_n y_n \qquad\qquad (x, y \in \mathbf{R}^n)$$

is a **bilinear** function of the vectors x and y. This means that

- **for fixed x, it is linear in y:**

$$\begin{aligned} (x \mid y + y') &= (x \mid y) + (x \mid y') \\ (x \mid \lambda y) &= \lambda\,(x \mid y) \end{aligned} \qquad\qquad (x, y, y' \in \mathbf{R}^n,\ \lambda \in \mathbf{R})$$

- **for fixed y, it is linear in x:**

$$\begin{aligned} (x + x' \mid y) &= (x \mid y) + (x' \mid y) \\ (\lambda x \mid y) &= \lambda\,(x \mid y) \end{aligned} \qquad\qquad (x, x', y \in \mathbf{R}^n,\ \lambda \in \mathbf{R}).$$

(2.1.2) Definition. *Let E, F be K-vector spaces. A map $f : \underbrace{E \times \cdots \times E}_{p-\text{times}} \longrightarrow F$ (in other words, a function $f(x_1, \ldots, x_p)$ in p variables $x_i \in E$ with values in F) is called* **p-linear** *if, whenever we fix all but one variable, we obtain a linear map $E \longrightarrow F$ in the remaining variable. If $p = 2$, we say that f* **bilinear**. *In the special case when $F = K$ (i.e., when f is scalar-valued), we say that f is a* **p-linear form** *(a* **bilinear form** *if $p = 2$).*

(2.1.3) Examples: (1) **Euclidean scalar product** is a bilinear form

$$f : \mathbf{R}^n \times \mathbf{R}^n \longrightarrow \mathbf{R}, \qquad f(x, y) = (x \mid y) = x_1 y_1 + \cdots + x_n y_n.$$

(2) **Vector product** is a bilinear map

$$f : \mathbf{R}^3 \times \mathbf{R}^3 \longrightarrow \mathbf{R}^3, \quad f(x, y) = x \times y = z, \quad z_1 = \begin{vmatrix} x_2 & y_2 \\ x_3 & y_3 \end{vmatrix}, \quad z_2 = -\begin{vmatrix} x_1 & y_1 \\ x_3 & y_3 \end{vmatrix}, \quad z_3 = \begin{vmatrix} x_1 & y_1 \\ x_2 & y_2 \end{vmatrix}.$$

(3) **Determinant** of an $n \times n$ matrix can be viewed as an n-linear form on the columns of the matrix:

$$f : \underbrace{K^n \times \cdots \times K^n}_{n-\text{times}} \longrightarrow K, \qquad f(v_1, \ldots, v_n) = \det(v_1 \mid \cdots \mid v_n).$$

If $K = \mathbf{R}$, then $f(v_1, \ldots, v_n)$ is equal to the algebraic volume of the parallelopiped generated by the vectors $v_1, \ldots, v_n$. For example, if $n = 2$, then

$$f(x, y) = \begin{vmatrix} x_1 & y_1 \\ x_2 & y_2 \end{vmatrix}$$

is equal, up to a sign, to the area of the parallelogram generated by $x, y \in \mathbf{R}^2$.

2.2 Bilinear forms

(2.2.1) In particular, a **bilinear form on a K-vector space** E is a map $f : E \times E \longrightarrow K$ (i.e., a scalar-valued function in two variables $x, y \in E$) satisfying

$$f(x+x',y) = f(x,y) + f(x',y) \qquad f(x,y+y') = f(x,y) + f(x,y') \qquad (x,x',y,y' \in E,\ \lambda \in K).$$
$$f(\lambda x,y) = \lambda\, f(x,y) \qquad f(x,\lambda y) = \lambda\, f(x,y)$$

(2.2.2) Definition. *A bilinear form $f : E \times E \longrightarrow K$ is*

$$\begin{array}{rcll} \textbf{symmetric} & \Longleftrightarrow & \forall x,y \in E & f(y,x) = f(x,y) \\ \textbf{skew}-\textbf{symmetric} & \Longleftrightarrow & \forall x,y \in E & f(y,x) = -f(x,y). \end{array}$$

(2.2.3) Examples: (1) The Euclidean scalar product is symmetric, since $(y \mid x) = (x \mid y)$ for all $x,y \in \mathbf{R}^n$.
(2) The algebraic area $f : \mathbf{R}^2 \times \mathbf{R}^2 \longrightarrow \mathbf{R}$ (defined in 2.1.3(3) with $n=2$) is skew-symmetric, as

$$f(y,x) = \begin{vmatrix} y_1 & x_1 \\ y_2 & x_2 \end{vmatrix} = -\begin{vmatrix} x_1 & y_1 \\ x_2 & y_2 \end{vmatrix} = -f(x,y).$$

2.3 Matrix representation of bilinear forms

(2.3.1) Assume that $n = \dim(E) < \infty$. Given a basis $\mathcal{B} = \{e_1,\ldots,e_n\}$ of E, we identify E with K^n as in 1.1.8. In particular, if $x = x_1e_1 + \cdots + x_ne_n$, $y = y_1e_1 + \cdots + y_ne_n \in E$ are two vectors in E, denote by

$$X = M_{\mathcal{B}}(x) = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}, \quad Y = M_{\mathcal{B}}(y) = \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} \in K^n$$

the column vectors representing x and y in the basis $\mathcal{B}$.
If $f : E \times E \longrightarrow K$ is a bilinear form, then

$$f(x,y) = f(\sum_{i=1}^n x_ie_i, \sum_{j=1}^n y_je_j) = \sum_{i=1}^n x_i\, f(e_i, \sum_{j=1}^n y_je_j) = \sum_{i=1}^n x_i \sum_{j=1}^n y_j\, f(e_i,e_j) = \sum_{i,j=1}^n f(e_i,e_j)\, x_iy_j. \quad (2.3.1.1)$$

(2.3.2) Definition. *In the situation of 2.3.1, the square matrix $A = (A_{ij}) \in M_n(K)$, where $A_{ij} = f(e_i,e_j)$, is called* **the matrix of f in the basis $\mathcal{B}$**.

(2.3.3) Matrix formulas. Using this notation, the formula (2.3.1.1) can be written as a matrix product

$$f(x,y) = \sum_{i,j=1}^n A_{ij}\, x_iy_j = (x_1 \cdots x_n) \begin{pmatrix} A_{11} & \cdots & A_{1n} \\ \vdots & \ddots & \vdots \\ A_{n1} & \cdots & A_{nn} \end{pmatrix} \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} = {}^tXAY. \quad (2.3.3.1)$$

Conversely, for each matrix $A \in M_n(K)$, the formula (2.3.3.1) (where $X = M_{\mathcal{B}}(x)$ and $Y = M_{\mathcal{B}}(y)$) defines a bilinear form $f : E \times E \longrightarrow K$, for which $f(e_i,e_j) = A_{ij}$.

Summary: The matrix $A = (f(e_i,e_j))$ is uniquely determined by the bilinear form f, and vice versa: f is expressed in terms of A as in (2.3.3.1). In abstract terms, associating to f the matrix $A = (f(e_i,e_j))$ defines a bijection (in fact, an isomorphism of K-vector spaces)

$$\{\text{bilinear forms } f : E \times E \longrightarrow K\} \xrightarrow{\sim} M_n(K).$$

This correspondence depends on the chosen basis $\{e_1,\ldots,e_n\}$.

(2.3.4) Examples: (1) For $n = 2$, $E = \mathbf{R}^2$ and $\mathcal{B} = \{e_1, e_2\}$ (the canonical basis), the matrix $\begin{pmatrix} 3 & 2 \\ 4 & 5 \end{pmatrix}$ corresponds to the bilinear form

$$f(x,y) = f\left(\begin{pmatrix} x_1 \\ x_2 \end{pmatrix}, \begin{pmatrix} y_1 \\ y_2 \end{pmatrix}\right) = (x_1\ x_2) \begin{pmatrix} 3 & 2 \\ 4 & 5 \end{pmatrix} \begin{pmatrix} y_1 \\ y_2 \end{pmatrix} = (x_1\ x_2) \begin{pmatrix} 3y_1 + 2y_2 \\ 4y_1 + 5y_2 \end{pmatrix} =$$
$$= 3x_1y_1 + 2x_1y_2 + 4x_2y_1 + 5x_2y_2.$$

(2) In the canonical basis of $\mathbf{R}^n$, the standard Euclidean scalar product corresponds to the matrix $A = ((e_i \mid e_j)) = I_n$. Equivalently, we can write

$$(x \mid y) = x_1y_1 + \cdots + x_ny_n = (x_1 \cdots x_n) \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} = (x_1 \cdots x_n) \begin{pmatrix} 1 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & 1 \end{pmatrix} \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}.$$

(3) The algebraic area $f : \mathbf{R}^2 \times \mathbf{R}^2 \longrightarrow \mathbf{R}$ (see 2.2.3(2)) can be written in the matrix form as

$$f(x,y) = \begin{vmatrix} x_1 & y_1 \\ x_2 & y_2 \end{vmatrix} = x_1y_2 - x_2y_1 = (x_1\ x_2) \begin{pmatrix} y_2 \\ -y_1 \end{pmatrix} = (x_1\ x_2) \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} y_1 \\ y_2 \end{pmatrix},$$

hence it is represented in the canonical basis of $\mathbf{R}^2$ by the matrix $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$.

(2.3.5) (Skew-)symmetric bilinear forms and (skew-)symmetric matrices.
Let

$$f(x,y) = {}^tXAY \qquad\qquad (x, y \in E) \tag{2.3.5.1}$$

be a bilinear form written in a matrix form (in a fixed basis $\mathcal{B}$ of E). Any scalar $\lambda \in K$ can be considered as a 1×1 matrix $\lambda \in M_1(K)$; in this case it is equal to its own transpose $\lambda = {}^t\lambda$. Applying this elementary observation to $\lambda = f(y,x)$, we obtain

$$f(y,x) = {}^tf(y,x) = {}^t({}^tYAX) = {}^tX\,{}^tAY \tag{2.3.5.2}$$

As f is uniquely determined by A and vice versa, a comparison of (2.3.5.1) with (2.3.5.2) shows that

$$f \text{ is symmetric} \iff {}^tA = A$$
$$f \text{ is skew} - \text{symmetric} \iff {}^tA = -A.$$

As the basis $\mathcal{B}$ was arbitrary and the (skew-)symmetry of f does not depend on the choice of a basis, we deduce that

$$f \text{ is symmetric} \iff {}^tA = A \text{ for one choice of a basis} \iff {}^tA = A \text{ for every choice of a basis}$$
$$f \text{ is skew} - \text{symmetric} \iff {}^tA = -A \text{ for one choice of a basis} \iff {}^tA = -A \text{ for every choice of a basis.} \tag{2.3.5.3}$$

(2.3.6) Change of basis. Let $f : E \times E \longrightarrow K$ be a bilinear form; let $\mathcal{B} = \{e_1, \ldots, e_n\}$ and $\mathcal{B}' = \{e'_1, \ldots, e'_n\}$ be two bases of E. Let

$$A = (A_{ij}) = (f(e_i, e_j)) = (\text{the matrix of } f \text{ in the basis } \mathcal{B}) \in M_n(K)$$
$$A' = (A'_{ij}) = (f(e'_i, e'_j)) = (\text{the matrix of } f \text{ in the basis } \mathcal{B}') \in M_n(K).$$

Denote by $P \in M_n(K)$ the matrix of change of basis from $\mathcal{B}$ to $\mathcal{B}'$. If $x, y \in E$ are two vectors in E and $X = M_{\mathcal{B}}(x), Y = M_{\mathcal{B}}(y) \in K^n$ (resp., $X' = M_{\mathcal{B}'}(x), Y' = M_{\mathcal{B}'}(y) \in K^n$) the column vectors representing x and y in the basis $\mathcal{B}$ (resp., in the basis $\mathcal{B}'$), then we have

$$X = PX', \qquad Y = PY'$$

(see (1.3.1.2)). Comparing the matrix formulas

$$\begin{aligned} &f(x,y) = {}^tX'A'Y' \\ &f(x,y) = {}^tXAY = {}^t(PX')A(PY') = {}^tX'\,{}^tPAP\,Y', \end{aligned}$$

we deduce that

$$A' = {}^tPAP. \tag{2.3.6.1}$$

Note that

$${}^tA' = {}^t({}^tPAP) = {}^tP\,{}^tAP,$$

which means that

$$A' \text{ is (skew}-\text{)symmetric} \iff A \text{ is (skew}-\text{)symmetric},$$

in line with (2.3.5.3).

Example: If $E = \mathbf{R}^2$, $\mathcal{B} =$ the canonical basis, $\mathcal{B}' = \begin{pmatrix} 3 \\ -2 \end{pmatrix}, \begin{pmatrix} 2 \\ -1 \end{pmatrix}$, $A = \begin{pmatrix} 2 & 1 \\ 4 & 3 \end{pmatrix}$, then we have

$$x = x_1 \begin{pmatrix} 1 \\ 0 \end{pmatrix} + x_2 \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = X = x_1' \begin{pmatrix} 3 \\ -2 \end{pmatrix} + x_2' \begin{pmatrix} 2 \\ -1 \end{pmatrix} = \begin{pmatrix} 3 & 2 \\ -2 & -1 \end{pmatrix} \begin{pmatrix} x_1' \\ x_2' \end{pmatrix} = PX',$$

hence $x_1 = 3x_1' + 2x_2'$, $x_2 = -2x_1' - x_2'$ (and similarly for y). It follows that

$$A' = {}^tPAP = \begin{pmatrix} 3 & -2 \\ 2 & -1 \end{pmatrix} \begin{pmatrix} 2 & 1 \\ 4 & 3 \end{pmatrix} \begin{pmatrix} 3 & 2 \\ -2 & -1 \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ 2 & 1 \end{pmatrix},$$

hence

$$f(x,y) = -x_1'y_2' + 2x_2'y_1' + x_2'y_2'.$$

To check the calculation, we can also compute directly

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

(2.3.7) Rank. The **rank** of a bilinear form $f : E \times E \longrightarrow K$ is defined to be the rank of the matrix $A = (f(e_i, e_j)) \in M_n(K)$ representing f in a basis $\mathcal{B} = \{e_i\}$ of E:

$$\mathrm{rk}(f) = \mathrm{rk}(A).$$

The rank is **well-defined:** if we replace $\mathcal{B}$ by another basis $\mathcal{B}'$, then the matrix A is replaced by $A' = {}^tPAP$, where $P \in M_n(K)$ is an **invertible** matrix. However, we know (cf. the proof of 1.4.6) that left (resp., right) multiplication by invertible matrices preserves rank, hence $\mathrm{rk}(A) = \mathrm{rk}(A')$.

(2.3.8) Bilinear forms and the dual space*

Let $f : E \times E \longrightarrow K$ be a bilinear form. By definition, for fixed $x \in E$, the map

$$\begin{aligned} f(x,\cdot) : E &\longrightarrow K \\ y &\mapsto f(x,y) \end{aligned}$$

is linear, i.e. $f(x,\cdot) \in E^*$. Moreover,

$$f(x+x',\cdot) = f(x,\cdot) + f(x',\cdot), \qquad f(\lambda x,\cdot) = \lambda f(x,\cdot),$$

which means that the map

$$\begin{aligned} f_1 : E &\longrightarrow E^* \\ x &\mapsto f(x,\cdot) \end{aligned}$$

is linear. Let $\mathcal{B} = \{e_1, \ldots, e_n\}$ be a basis of E; denote by $\mathcal{B}^* = \{e_1^*, \ldots, e_n^*\}$ the corresponding dual basis of E^*. We are going to relate the matrix $A_1 \in M_n(K)$ of f_1 in the bases $\mathcal{B}, \mathcal{B}^*$ to the matrix $A = (f(e_i, e_j)) \in M_n(K)$. Applying the formula (1.7.7.1) to the map f_1 (and identifying E^{**} with E as in 1.7.9), we obtain

$$(A_1)_{ij} = e_i^{**}(f_1(e_j)) = (f_1(e_j))(e_i) = f(e_j, e_i) = A_{ji}, \qquad A_1 = {}^tA.$$

Similarly, if we fix $y \in E$, then the map

$$\begin{aligned} f(\cdot,y) : E &\longrightarrow K \\ x &\mapsto f(x,y) \end{aligned}$$

is linear (i.e. $f(\cdot,y) \in E^*$) and depends linearly on y in the sense that the map

$$\begin{aligned} f_2 : E &\longrightarrow E^* \\ y &\mapsto f(\cdot,y) \end{aligned}$$

is linear, too. If $A_2 \in M_n(K)$ denotes the matrix of f_2 in the bases $\mathcal{B}, \mathcal{B}^*$, then we have

$$(A_2)_{ij} = e_i^{**}(f_2(e_j)) = (f_2(e_j))(e_i) = f(e_i, e_j) = A_{ij}, \qquad A_2 = A.$$

In particular, one can define the rank of f in an abstract way as

$$\mathrm{rk}(f) := \mathrm{rk}(f_1) \ (= \mathrm{rk}(f_2)).$$

(2.3.9) Exercise. *A* **scalar product** *on an* $\mathbf{R}$*-vector space* E *is a bilinear symmetric form* $f : E \times E \longrightarrow \mathbf{R}$ *satisfying* $f(x,x) > 0$ *for all non-zero vectors* $x \in E$.
Which among the following maps $f : E \times E \longrightarrow \mathbf{R}$ *are bilinear? symmetric? define a scalar product?*
(1) $E = \mathbf{R}^n$, $f(x,y) = \sum_{j=1}^n j x_j y_j$.
(2) $E = M_n(\mathbf{R})$, $f(A,B) = \mathrm{Tr}(AB)$.
(3) $E = M_n(\mathbf{R})$, $f(A,B) = \mathrm{Tr}({}^tAB)$.
(4) $E = M_n(\mathbf{R})$, $f(A,B) = \mathrm{Tr}(A)\mathrm{Tr}(B)$.
(5) $E = \mathbf{R}[t]_{\deg \leq n}$, $f(P,Q) = \int_0^1 tP(t)Q(t)\,dt$.

* **This section is optional.**

3. Quadratic forms

Important assumption: From now on, **until the end of the course**, we assume that the characteristic of the field K is not equal to 2, i.e. that $2 \neq 0$ in K ($\iff$ 2 is invertible in K).
This assumption **is** satisfied by $K = \mathbf{R}, \mathbf{C}$ or $\mathbf{F}_{p^n}$ for primes $p \neq 2$, but **is not** satisfied by $K = \mathbf{F}_{2^n}$.

3.1 Basic concepts

(3.1.1) Example: The standard Euclidean scalar product

$$(x \mid y) = x_1 y_1 + \cdots + x_n y_n$$

is a symmetric bilinear form $\mathbf{R}^n \times \mathbf{R}^n \longrightarrow \mathbf{R}$. The square of the length

$$\|x\|^2 = (x \mid x) = x_1^2 + \cdots + x_n^2$$

is a **quadratic form** on $\mathbf{R}^n$. This example motivates the following general definition.

(3.1.2) Definition. *Let $f : E \times E \longrightarrow K$ be a* **symmetric** *bilinear form on a K-vector space E. The* **quadratic form associated to** *f is the function $q : E \longrightarrow K$ defined by the formula $q(x) = f(x,x)$. [Note that this implies that $\forall \lambda \in K\ \forall x \in E \quad q(\lambda x) = \lambda^2 q(x)$.]*

(3.1.3) Matrix formulas. In the situation of 3.1.2, let $\mathcal{B} = \{e_1, \ldots, e_n\}$ be a basis of E. The matrix $A = (A_{ij}) \in M_n(K)$ of f in the basis $\mathcal{B}$ is symmetric, as $A_{ji} = f(e_j, e_i) = f(e_i, e_j) = A_{ij}$. Associating to a vector $x = \sum_{i=1}^n x_i e_i \in E$ the column vector $X = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \in K^n$ of its coordinates in $\mathcal{B}$, we have

$$q(x) = f(x,x) = {}^tXAX = \sum_{i,j=1}^n A_{ij}\, x_i x_j = \sum_{i=1}^n A_{ii}\, x_i^2 + 2 \sum_{i<j} A_{ij}\, x_i x_j. \tag{3.1.3.1}$$

As in 2.3.6, a change of basis given by the formula $X = PX'$ (where P is the matrix of the change of basis from $\mathcal{B}$ to a new basis $\mathcal{B}'$) replaces A by the matrix $A' = {}^tPAP$ (which is again symmetric).
Conversely, any symmetric matrix $A = {}^tA \in M_n(K)$ defines a quadratic form on E, as in the formula (3.1.3.1).

Example: If $K = \mathbf{R}$, $E = \mathbf{R}^2$, $\mathcal{B}$ = the canonical basis and $A = \begin{pmatrix} 3 & -1 \\ -1 & 5 \end{pmatrix}$, then

$$q(x) = q\left(\begin{pmatrix} x_1 \\ x_2 \end{pmatrix}\right) = (x_1\ x_2) \begin{pmatrix} 3 & -1 \\ -1 & 5 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = (x_1\ x_2) \begin{pmatrix} 3x_1 - x_2 \\ -x_1 + 5x_2 \end{pmatrix} = 3x_1^2 - 2x_1x_2 + 5x_2^2.$$

(3.1.4) Proposition ("f is determined by q"). *Any quadratic form $q : E \longrightarrow K$ is associated to a* **unique** *symmetric bilinear form $f : E \times E \longrightarrow K$ (we say that f is the* **polar form of** *q). [This statement uses the assumption that $2 \neq 0$.]*

Proof. We use, essentially, the formula $(a+b)^2 - a^2 - b^2 = 2ab$. More precisely, the fact that f is symmetric implies that we have, for all $x, y \in E$,

$$q(x+y) = f(x+y, x+y) = f(x,x) + f(x,y) + f(y,x) + f(y,y) = q(x) + 2f(x,y) + q(y),$$

hence

$$f(x,y) = \frac{1}{2}\left(q(x+y) - q(x) - q(y)\right).$$

(3.1.5) Finding the polar form (example): If $q : \mathbf{R}^2 \longrightarrow \mathbf{R}$ is given by $q(x) = x_1^2 - 4x_1x_2 + 7x_2^2$, then we rewrite q as

$$q(x) = x_1^2 - 4x_1x_2 + 7x_2^2 = x_1^2 - 2x_1x_2 - 2x_2x_1 + 7x_2^2 = (x_1\ x_2)\begin{pmatrix} 1 & -2 \\ -2 & 7 \end{pmatrix}\begin{pmatrix} x_1 \\ x_2 \end{pmatrix},$$

which implies that

$$f(x,y) = (x_1\ x_2)\begin{pmatrix} 1 & -2 \\ -2 & 7 \end{pmatrix}\begin{pmatrix} y_1 \\ y_2 \end{pmatrix} = x_1y_1 - 2x_1y_2 - 2x_2y_1 + 7x_2y_2.$$

3.2 Rank, kernel (= radical) of a quadratic form

(3.2.1) Definition. *Let $q : E \longrightarrow K$ be a quadratic form and $f : E \times E \longrightarrow K$ its polar form. Let $x, y \in E$ be two vectors. We say that x* **is orthogonal to** *y* **(with respect to** *f***)** *if $f(x,y) = 0$ (***notation:** *$x \perp y$; if we wish to stress the dependence on f, we write $x \perp_f y$ or $x \perp_q y$). [As f is symmetric, we have $x \perp y \iff y \perp x$.]*
The **rank of** *q is defined as $\mathrm{rk}(q) = \mathrm{rk}(f)$; the* **kernel** *(= the* **radical***) of q is the vector subspace of E*

$$N(q) = \mathrm{rad}(q) = \{x \in E \mid \forall y \in E \quad x \perp y\} = \{x \in E \mid \forall y \in E \quad y \perp x\}.$$

Warning: in general,

$$N(q) \neq \{x \in E \mid q(x) = 0\}$$

(the right hand side need not be a subspace of E; see 3.2.3(3) and 3.6.7-8 below).

(3.2.2) Matrix formulas

(3.2.2.1) Choosing a basis $\mathcal{B}$ of E (assuming that $n = \dim(E) < \infty$), we write, using the notation of 2.3.1 and 3.1.3, $f(x,y) = {}^tXAY$ and $q(x) = {}^tXAX$ (where $A = {}^tA \in M_n(K)$ is a symmetric matrix). By definition, we have

$$\mathrm{rk}(q) = \mathrm{rk}(f) = \mathrm{rk}(A).$$

(3.2.2.2) Proposition. *Under the identification $M_{\mathcal{B}} : E \xrightarrow{\sim} K^n$, the subspace $N(q) \subset E$ corresponds to the subspace $\{X \in K^n \mid AX = 0\} \subset K^n$. In particular,*

$$\dim N(q) = \dim\{X \in K^n \mid AX = 0\} = n - \mathrm{rk}(A) = n - \mathrm{rk}(q).$$

Proof. By definition, $N(q)$ corresponds to the following subspace of K^n:

$$F = \{X \in K^n \mid \forall Y \in K^n \quad {}^tYAX = 0\} = \{X \in K^n \mid \forall i = 1, \ldots, n \quad {}^te_iAX = 0\},$$

where $e_1, \ldots, e_n$ is the canonical basis of K^n. Denoting the column vector $AX \in K^n$ by b and observing that ${}^te_ib$ coincides with the i-th coordinate of b, we deduce that F consists precisely of those vectors X for which $b(= AX) = 0$. The dimension of this space is given by the Rank formula (1.2.7.2).

(3.2.2.3) Definition. *The quadratic form q is* **non-degenerate** *if $N(q) = 0$.*

(3.2.2.4) It follows from 3.2.2.2 that the following conditions are equivalent:

$$q \text{ is non} - \text{degenerate} \iff N(q) = 0 \iff \mathrm{rk}(q) = \dim(E) \iff A \text{ is invertible} \iff \det(A) \neq 0.$$

(3.2.3) Examples: (0) $q = 0$: in this case $f = 0$, $A = 0$, $N(q) = E$, $\mathrm{rk}(q) = 0$.
(1) $E = K^n$, $q(x) = x_1^2 + \cdots + x_n^2$: in this case $f(x, y) = x_1y_1 + \cdots + x_ny_n$, $A = I_n$, $N(q) = 0$, $\mathrm{rk}(q) = n$.
(2) $E = K^n$, $q(x) = x_1^2 + \cdots + x_r^2$ $(0 \leq r \leq n)$: in this case $f(x, y) = x_1y_1 + \cdots + x_ry_r$,

$$A = \begin{pmatrix} I_r & 0 \\ 0 & 0 \end{pmatrix} \in M_n(K), \qquad N(q) = \{x \in K^n \mid Ax = 0\} = \{{}^t(0, \ldots, 0, x_{r+1}, \ldots, x_n) \mid x_i \in K\},$$

$\mathrm{rk}(q) = \mathrm{rk}(A) = r$, $\dim(N(q)) = n - r$.
(3) $E = \mathbf{R}^2$, $q(x) = x_1^2 - 4x_1x_2 - 5x_2^2$: in this case

$$A = \begin{pmatrix} 1 & -2 \\ -2 & -5 \end{pmatrix}.$$

As $\det(A) = -9 \neq 0$, we have $\mathrm{rk}(q) = \mathrm{rk}(A) = 2$ and $N(q) = 0$. Note that

$$q(x) = x_1^2 - 4x_1x_2 - 5x_2^2 = (x_1 - 2x_2)^2 - (3x_2)^2 = (x_1 - 5x_2)(x_1 + x_2),$$

hence

$$\{x \in E \mid q(x) = 0\} = \{x \in \mathbf{R}^2 \mid x_1 - 5x_2 = 0\} \cup \{x \in \mathbf{R}^2 \mid x_1 + x_2 = 0\} \neq N(q)$$

is a union of two lines passing through the origin.
(4) $E = \mathbf{R}^2$, $q(x) = x_1^2 - 4x_1x_2 + 4x_2^2$: in this case

$$A = \begin{pmatrix} 1 & -2 \\ -2 & 4 \end{pmatrix}.$$

As $\det(A) = 0$, we have $\mathrm{rk}(q) = \mathrm{rk}(A) < 2$. On the other hand, $A \neq 0$, hence $\mathrm{rk}(A) > 0$, which implies that $\mathrm{rk}(A) = 1$ and $\dim(N(q)) = 2 - 1 = 1$. More precisely,

$$N(q) = \{\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \Bigm| \begin{pmatrix} 1 & -2 \\ -2 & 4 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = 0\} = \mathrm{vect}(\begin{pmatrix} 2 \\ 1 \end{pmatrix}).$$

This also follows from the formula $q(x) = (x_1 - 2x_2)^2$, which implies that $f(x, y) = (x_1 - 2x_2)(y_1 - 2y_2)$.

(3.2.4) Exercise. *For each of the following quadratic forms on $\mathbf{R}^4$, determine the rank, the kernel and the polar form.*

$$q_1(x) = x_1x_2 + x_4^2, \qquad q_2(x) = x_1x_2 + x_3x_4 + x_4^2, \qquad q_3(x) = x_1^2 - x_2^2 + x_3^2 - x_4^2.$$

3.3 "Easy" diagonalisation of a quadratic form (by "completing the square")

The basic result of the theory of quadratic forms is the following theorem (which uses the assumption that $2 \neq 0$ in K).

(3.3.1) Theorem. *For each quadratic form $q : E \longrightarrow K$ (where $n = \dim(E) < \infty$) there exists a basis $\mathcal{B}' = \{e'_1, \ldots, e'_n\}$ of E in which the matrix of q is diagonal, i.e.*

$$q(x) = d_1 x_1'^2 + \cdots + d_n x_n'^2 \qquad\qquad (x = \sum_{i=1}^{n} x'_i e'_i)$$

(**terminology:** *we say that $\mathcal{B}'$ is an* **orthogonal basis** *of E (with respect to q)).*
Matrix formulation: *For each* **symmetric** *matrix $A = {}^tA \in M_n(K)$ there exists an invertible matrix $P \in M_n(K)$ such that*

$${}^tPAP = \begin{pmatrix} d_1 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & d_n \end{pmatrix}.$$

(3.3.2) Examples: In the following examples, $K = \mathbf{R}$, $E = \mathbf{R}^n$ and $x_1, \ldots, x_n$ are the coordinates on $\mathbf{R}^n$ with respect to the canonical basis. The new coordinates $x'_1, \ldots, x'_n$ are obtained by successive elimination of the terms containing the variables $x_1, \ldots, x_n$ (not necessarily in this order) from $q(x)$.
(1) $E = \mathbf{R}^2$, $q(x) = x_1^2 - 4x_1x_2 + 7x_2^2$; then

$$q(x) = x_1^2 - 4x_1x_2 + 7x_2^2 = (x_1 - 2x_2)^2 + 3x_2^2 = x_1'^2 + 3x_2'^2,$$

where

$$X' = \begin{pmatrix} x'_1 \\ x'_2 \end{pmatrix} = \begin{pmatrix} x_1 - 2x_2 \\ x_2 \end{pmatrix} = \begin{pmatrix} 1 & -2 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = P'X.$$

We can rewrite this change of variables as in (1.3.1.2), namely

$$X = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} 1 & -2 \\ 0 & 1 \end{pmatrix}^{-1} \begin{pmatrix} x'_1 \\ x'_2 \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} x'_1 \\ x'_2 \end{pmatrix} = PX',$$

which implies that x'_1 and x'_2 are the coordinates of x in the basis $\mathcal{B}'$ consisting of the columns of P:

$$\mathcal{B}' = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 2 \\ 1 \end{pmatrix}, \qquad\qquad x = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = x'_1 \begin{pmatrix} 1 \\ 0 \end{pmatrix} + x'_2 \begin{pmatrix} 2 \\ 1 \end{pmatrix}.$$

The matrices A and A' of q in the respective bases $\mathcal{B}$ and $\mathcal{B}'$ are equal to

$$A = \begin{pmatrix} 1 & -2 \\ -2 & 7 \end{pmatrix}, \qquad A' = \begin{pmatrix} 1 & 0 \\ 0 & 3 \end{pmatrix};$$

thus $\mathrm{rk}(q) = \mathrm{rk}(A') = 2$.
(2) $E = \mathbf{R}^2$, $q(x) = x_1^2 - 6x_1x_2 + 9x_2^2$; then

$$q(x) = x_1^2 - 6x_1x_2 + 9x_2^2 = (x_1 - 3x_2)^2 = x_1'^2 = x_1'^2 + 0 \cdot x_2'^2,$$

where $x'_1 = x_1 - 3x_2$. However, we still have to choose x'_2 (a linear form in x_1 and x_2) in such a way that x'_1 and x'_2 are the coordinates on $\mathbf{R}^2$ in a suitable basis $\mathcal{B}'$. In concrete terms, this means that

$$x'_2 = cx_1 + dx_2, \qquad X' = \begin{pmatrix} x'_1 \\ x'_2 \end{pmatrix} = \begin{pmatrix} 1 & -3 \\ c & d \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = P'X$$

(for some $c, d \in \mathbf{R}$), and we must make sure that the matrix P' is **invertible** (as it will be equal to the matrix of change of basis from $\mathcal{B}'$ to the canonical basis $\mathcal{B}$. Once this is done, we compute $P = (P')^{-1}$ (= the matrix of change of basis from $\mathcal{B}$ to $\mathcal{B}'$), whose columns will be the elements of $\mathcal{B}'$. It is a good idea to make the matrix P' as simple as possible, for example, by taking

$$x_2' = x_2, \qquad \begin{pmatrix} x_1' \\ x_2' \end{pmatrix} = \begin{pmatrix} 1 & -3 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}, \qquad P' = \begin{pmatrix} 1 & -3 \\ 0 & 1 \end{pmatrix}.$$

In this case we see immediately that $\det(P') = 1 \cdot 1 = 1 \neq 0$, hence P' is invertible. Computing as in (1), we obtain

$$X = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} 1 & -3 \\ 0 & 1 \end{pmatrix}^{-1} \begin{pmatrix} x_1' \\ x_2' \end{pmatrix} = \begin{pmatrix} 1 & 3 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} x_1' \\ x_2' \end{pmatrix} = PX',$$

hence $q(x) = x_1'^2$ in the basis

$$\mathcal{B}' = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 3 \\ 1 \end{pmatrix}, \qquad x = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = x_1' \begin{pmatrix} 1 \\ 0 \end{pmatrix} + x_2' \begin{pmatrix} 3 \\ 1 \end{pmatrix}.$$

The matrices A and A' of q in the respective bases $\mathcal{B}$ and $\mathcal{B}'$ are equal to

$$A = \begin{pmatrix} 1 & -3 \\ -3 & 9 \end{pmatrix}, \qquad A' = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix};$$

thus $\mathrm{rk}(q) = \mathrm{rk}(A') = 1$.

(3) $E = \mathbf{R}^3$, $q(x) = x_1^2 + 4x_1x_2 - 6x_1x_3 + 3x_2^2 + 2x_2x_3 - 40x_3^2$:

$$\begin{aligned} q(x) = & \underbrace{x_1^2 + 4x_1x_2 - 6x_1x_3}_{\text{part of } (x_1+2x_2-3x_3)^2 = x_1^2+4x_1x_2-6x_1x_3+4x_2^2-12x_2x_3+9x_3^2} + 3x_2^2 + 2x_2x_3 - 40x_3^2 = \\ &= (x_1 + 2x_2 - 3x_3)^2 - x_2^2 + 14x_2x_3 - 49x_3^2 = (x_1 + 2x_2 - 3x_3)^2 - (x_2 - 7x_3)^2 = \\ &= x_1'^2 - x_2'^2 + 0 \cdot x_3'^2, \end{aligned}$$

where

$$X' = \begin{pmatrix} x_1' \\ x_2' \\ x_3' \end{pmatrix} = \begin{pmatrix} x_1 + 2x_2 - 3x_3 \\ x_2 - 7x_3 \\ x_3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & -3 \\ 0 & 1 & -7 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = P'X.$$

As $\det(P') = 1 \cdot 1 \cdot 1 = 1 \neq 1$, the matrix P' is invertible. We can compute its inverse $P = (P')^{-1}$ either by the method explained in 1.4.9, or by computing directly

$$x_3 = x_3', \qquad x_2 = x_2' + 7x_3', \qquad x_1 = x_1' - 2(x_2' + 7x_3') + 3x_3' = x_1' - 2x_2' - 11x_3'$$

$$\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} 1 & -2 & -11 \\ 0 & 1 & 7 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} x_1' \\ x_2' \\ x_3' \end{pmatrix} = x_1' \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} + x_2' \begin{pmatrix} -2 \\ 1 \\ 0 \end{pmatrix} + x_3' \begin{pmatrix} -11 \\ 7 \\ 1 \end{pmatrix},$$

hence $q(x) = x_1'^2 - x_2'^2 + 0 \cdot x_3'^2$ in the coordinates x_1', x_2', x_3' with respect to the basis

$$\mathcal{B}' = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} -2 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} -11 \\ 7 \\ 1 \end{pmatrix}.$$

The matrices A and A' of q in the respective bases $\mathcal{B}$ and $\mathcal{B}'$ are equal to

$$A = \begin{pmatrix} 1 & 2 & -3 \\ 2 & 3 & 1 \\ -3 & 1 & -40 \end{pmatrix}, \qquad A' = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 0 \end{pmatrix};$$

thus $\mathrm{rk}(q) = \mathrm{rk}(A') = 2$ (in practice, it is useful to compute $\mathrm{rk}(A)$ by the method from 1.4, in order to **check the result**).

(4) $E = \mathbf{R}^3$, $q(x) = x_1x_2 + x_1x_3 + x_2x_3$. In this case there are no diagonal elements x_j^2, so we use the following trick:

$$x_1x_2 = \frac{(x_1+x_2)^2 - (x_1-x_2)^2}{4} = \left(\frac{x_1+x_2}{2}\right)^2 - \left(\frac{x_1-x_2}{2}\right)^2.$$

Introducing the new coordinates

$$\begin{pmatrix} x_1' \\ x_2' \end{pmatrix} = \begin{pmatrix} (x_1+x_2)/2 \\ (x_1-x_2)/2 \end{pmatrix}, \qquad \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} x_1'+x_2' \\ x_1'-x_2' \end{pmatrix}$$

(and keeping x_3), we obtain

$$\begin{aligned} q(x) &= (x_1'+x_2')(x_1'-x_2') + (x_1'+x_2')x_3 + (x_1'-x_2')x_3 = \\ &= x_1'^2 + 2x_1'x_3 - x_2'^2 = (x_1'+x_3)^2 - x_2'^2 - x_3^2 = \\ &= y_1^2 - y_2^2 - y_3^2, \end{aligned}$$

where

$$Y = \begin{pmatrix} y_1 \\ y_2 \\ y_3 \end{pmatrix} = \begin{pmatrix} x_1'+x_3 \\ x_2' \\ x_3 \end{pmatrix} = \begin{pmatrix} (x_1+x_2)/2+x_3 \\ (x_1-x_2)/2 \\ x_3 \end{pmatrix} = \begin{pmatrix} 1/2 & 1/2 & 1 \\ 1/2 & -1/2 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = P'X.$$

As we have

$$\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} y_1+y_2-y_3 \\ y_1-y_2-y_3 \\ y_3 \end{pmatrix} = \begin{pmatrix} 1 & 1 & -1 \\ 1 & -1 & -1 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} y_1 \\ y_2 \\ y_3 \end{pmatrix} = y_1 \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix} + y_2 \begin{pmatrix} 1 \\ -1 \\ 0 \end{pmatrix} + y_3 \begin{pmatrix} -1 \\ -1 \\ 1 \end{pmatrix}$$

(either by computing $(P')^{-1}$, or by a direct calculation), it follows that $q(x) = y_1^2 - y_2^2 - y_3^2$ in the coordinates with respect to the basis

$$\begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ -1 \\ 0 \end{pmatrix}, \begin{pmatrix} -1 \\ -1 \\ 1 \end{pmatrix}.$$

(3.3.3) Proof of Theorem 3.3.1: The method used in the previous examples works in general. Fix a basis $\mathcal{B} = \{e_1, \ldots, e_n\}$ of E; let $A = {}^tA \in M_n(K)$ be the matrix of q in $\mathcal{B}$. If $A = 0$, then we can take $\mathcal{B}' = \mathcal{B}$. Assume that $A \neq 0$. As in (3.1.3.1), we have

$$q(x) = \sum_{i,j=1}^n A_{ij}\, x_i x_j = \sum_{i=1}^n A_{ii}\, x_i^2 + 2\sum_{i<j} A_{ij}\, x_i x_j \qquad \left(x = \sum_{i=1}^n x_i e_i\right).$$

(a) There exists a non-zero diagonal term $A_{ii} \neq 0$: Exchanging the coordinates x_1 and x_i, we can assume that $A_{11} \neq 0$. As

$$q(x) = A_{11}x_1^2 + 2A_{12}\,x_1x_2 + \cdots + 2A_{1n}\,x_1x_n + q_1(x)$$

(where $q_1(x)$ does not contain the variable x_1), we write

$$q(x) = A_{11}\left(x_1 + \frac{A_{12}}{A_{11}}x_2 + \cdots + \frac{A_{1n}}{A_{11}}x_n\right)^2 + q_2(x) = A_{11}\,x_1'^2 + q_2(x),$$

where

$$x_1' = x_1 + \frac{A_{12}}{A_{11}}x_2 + \cdots + \frac{A_{1n}}{A_{11}}x_n$$

and q_2 does not contain the variable x_1, i.e. q_2 is a quadratic form on the subspace $E' = \mathrm{vect}(e_2, \ldots, e_n) \subset E$ of dimension $n-1$.

(b) All diagonal terms vanish $A_{11} = \cdots = A_{nn} = 0$: There exists a non-zero off-diagonal term $A_{ij} \neq 0$, $i < j$. After exchanging the coordinates $x_1 \longleftrightarrow x_i$ and $x_2 \longleftrightarrow x_j$, we can assume that $A_{12} \neq 0$ (but all diagonal terms vanish). This implies that $q(x)$ is of the form

$$q(x) = 0 \cdot x_1^2 + 2A_{12}\,x_1x_2 + 0 \cdot x_2^2 + \cdots.$$

Applying the change of coordinates used in 3.3.2(4)

$$\begin{pmatrix} x_1' \\ x_2' \end{pmatrix} = \begin{pmatrix} (x_1+x_2)/2 \\ (x_1-x_2)/2 \end{pmatrix}, \qquad \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} x_1'+x_2' \\ x_1'-x_2' \end{pmatrix}$$

(and keeping the coordinates $x_3, \ldots, x_n$), we obtain

$$q(x) = 2A_{12}\,x_1'^2 + \cdots,$$

which means that we are back in the case (a) if we use the coordinates $x_1', x_2', x_3, \ldots, x_n$. Applying (a), we get

$$q(x) = 2A_{12}\,(x_1'')^2 + q_2(x),$$

with q_2 containing only the variables $x_2', x_3, \ldots, x_n$.

Afterwards we apply the same argument to q_2, etc. After at most n steps, we obtain a diagonal quadratic form.

(3.3.4) Rank, kernel and diagonalisation: In the situation of Theorem 3.3.1, we can reorder the vectors of the basis $\mathcal{B}'$ in such a way that

$$d_1, \ldots, d_r \neq 0, \qquad d_{r+1} = \cdots = d_n = 0, \qquad q(x) = d_1x_1'^2 + \cdots + d_rx_r'^2.$$

This means that the matrix A' of q in the basis $\mathcal{B}'$ is equal to

$$A' = \begin{pmatrix} d_1 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ 0 & d_2 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & d_r & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 & 0 & \cdots & 0 \end{pmatrix} \qquad (d_1, \ldots, d_r \neq 0),$$

hence

$$\mathrm{rk}(q) = r. \tag{3.3.4.1}$$

The system of equations

$$A' \begin{pmatrix} x'_1 \\ \vdots \\ x'_n \end{pmatrix} = 0$$

is equivalent to

$$x'_1 = \cdots = x'_r = 0, \tag{3.3.4.2}$$

which implies (by 3.2.2.2) that the kernel of q is given, **in the coordinates with respect to $\mathcal{B}'$**, by the equations (3.3.4.2). In other words,

$$N(q) = \{\sum_{i=1}^{n} x'_i e'_i \mid x'_1 = \cdots = x'_r = 0\} = \mathrm{vect}(e'_{r+1}, \ldots, e'_n\}. \tag{3.3.4.3}$$

Examples: (1) In Example 3.3.2(1), $r = 2 = \dim(E)$, hence $N(q) = 0$.
(2) In Example 3.3.2(2), $r = 1$ and

$$N(q) = \{ \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \mid x_1 - 3x_2 = 0\} = \mathrm{vect}(\begin{pmatrix} 3 \\ 1 \end{pmatrix}).$$

(3) In Example 3.3.2(3), $r = 2$ and

$$N(q) = \left\{ \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} \middle| x_1 + 2x_2 - 3x_3 = x_2 - 7x_3 = 0 \right\} = \mathrm{vect}\left(\begin{pmatrix} -11 \\ 7 \\ 1 \end{pmatrix} \right).$$

(4) In Example 3.3.2(4), $r = 3 = \dim(E)$, hence $N(q) = 0$.

(3.3.5) If the number of non-zero terms $r = \mathrm{rk}(q)$ in

$$q(x) = d_1 x'^2_1 + \cdots + d_r x'^2_r$$

is less than n, how do we choose the remaining new coordinates $x'_{r+1}, \ldots, x'_n$ in order to make sure that the linear forms $x'_1, \ldots, x'_n$ are linearly independent (i.e., that the matrix P' in the formula $X' = P'X$ is **invertible**)? For example, if the terms $x'_1, \ldots, x'_r$ were obtained by successive elimination of the old variables $x_{i_1}, \ldots, x_{i_r}$, then we can take $x'_{r+1}, \ldots, x'_n$ to be the remaining $n - r$ old variables $x_{j_1}, \ldots, x_{j_{n-r}}$ (where $\{i_1, \ldots, i_r, j_1, \ldots, j_{n-r}\} = \{1, \ldots, n\}$).

(3.3.6) Example: We are going to find a chage of coordinates which diagonalises the quadratic form $q : \mathbf{R}^4 \longrightarrow \mathbf{R}$, where

$$q(\begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix}) = x_1^2 - 2x_1x_2 + 4x_1x_3 + 2x_1x_4 + x_2^2 - 4x_2x_3 + 6x_2x_4 + 4x_3^2 - 4x_3x_4 + 5x_4^2.$$

We eliminate first x_1:

$$q(x) = (x_1 - x_2 + 2x_3 + x_4)^2 + 8x_2x_4 - 8x_3x_4 + 4x_4^2,$$

then x_4:

$$8x_2x_4 - 8x_3x_4 + 4x_4^2 = 4(x_4 + x_2 - x_3)^2 - 4x_2^2 + 8x_2x_3 - 4x_3^2,$$

and finally x_2:

$$-4x_2^2 + 8x_2x_3 - 4x_3^2 = -4(x_2 - x_3)^2.$$

Putting

$$x_1' = x_1 - x_2 + 2x_3 + x_4, \qquad x_2' = x_4 + x_2 - x_3, \qquad x_3' = x_2 - x_3$$

and $x_4' = x_3$ (the last remaining old variable that has not been eliminated), we obtain

$$q(x) = x_1'^2 + 4x_2'^2 - 4x_3'^2$$

and

$$X' = \begin{pmatrix} x_1' \\ x_2' \\ x_3' \\ x_4' \end{pmatrix} = \begin{pmatrix} x_1 - x_2 + 2x_3 + x_4 \\ x_4 + x_2 - x_3 \\ x_2 - x_3 \\ x_3 \end{pmatrix} = \begin{pmatrix} 1 & -1 & 2 & 1 \\ 0 & 1 & -1 & 1 \\ 0 & 1 & -1 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} = P'X,$$

$$X = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} = \begin{pmatrix} x_1' - x_2' + 2x_3' - x_4' \\ x_3' + x_4' \\ x_4' \\ x_2' - x_3' \end{pmatrix} = \begin{pmatrix} 1 & -1 & 2 & -1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & -1 & 0 \end{pmatrix} \begin{pmatrix} x_1' \\ x_2' \\ x_3' \\ x_4' \end{pmatrix} = PX'.$$

WARNING: We **cannot** take $x_4' = x_4$, as the linear forms x_1', x_2', x_3' and x_4 are **linearly dependent:**

$$x_2' - x_3' - x_4 = 0.$$

In other words, the formulas

$$\begin{pmatrix} x_1' \\ x_2' \\ x_3' \\ x_4' \end{pmatrix} = \begin{pmatrix} x_1 - x_2 + 2x_3 + x_4 \\ x_4 + x_2 - x_3 \\ x_2 - x_3 \\ x_4 \end{pmatrix} = \begin{pmatrix} 1 & -1 & 2 & 1 \\ 0 & 1 & -1 & 1 \\ 0 & 1 & -1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix}$$

do not define a change of coordinates of $\mathbf{R}^4$, as the matrix

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

is not invertible (its rank is equal to 3).

(3.3.7) Exercise. *For each of the following quadratic forms $q : \mathbf{R}^3 \longrightarrow \mathbf{R}$, determine the rank, the kernel and find a chage of coordinates which diagonalises q.*

$$q_1(x) = x_1^2 - x_2^2 + 2x_1x_3, \qquad q_2(x) = x_1x_2 - 2x_1x_3 + 3x_2x_3, \qquad q_3(x) = x_1x_2 - 2x_1x_3.$$

3.4 Quadratic forms over C and R

(3.4.1) Proposition. *For each quadratic form $q : E \longrightarrow \mathbf{C}$ on a $\mathbf{C}$-vector space E of dimension $n < \infty$ there exists a basis $e_1, \ldots, e_n$ of E such that*

$$q(x) = x_1^2 + \cdots + x_r^2 \qquad\qquad (x = \sum_{j=1}^{n} x_j e_j).$$

The integer r $(0 \leq r \leq n)$ is determined by q; in fact, $r = \mathrm{rk}(q)$.
Matrix formulation: *For each symmetric complex matrix $A = {}^tA \in M_n(\mathbf{C})$ there exists an invertible matrix $P \in M_n(\mathbf{C})$ such that ${}^tPAP = \begin{pmatrix} I_r & 0 \\ 0 & 0 \end{pmatrix}$.*

Proof. Let $r = \mathrm{rk}(q)$. According to Theorem 3.3.1, there exist a basis $e'_1, \ldots, e'_n$ of E and non-zero scalars $d_1, \ldots, d_r \in \mathbf{C}$ such that

$$q(x) = d_1 x_1'^2 + \cdots + d_r x_r'^2 \qquad\qquad (x = \sum_{j=1}^{n} x'_j e'_j).$$

For each $j = 1, \ldots, r$, choose $\alpha_j \in \mathbf{C}$ such that $\alpha_j^2 = d_j$. As $d_j x_j'^2 = (\alpha_j x'_j)^2$, the change of coordinates

$$x_j = \begin{cases} \alpha_j x'_j, & j = 1, \ldots, r \\ x'_j, & j = r+1, \ldots, n, \end{cases} \qquad\qquad e_j = \begin{cases} \frac{1}{\alpha_j} e'_j, & j = 1, \ldots, r \\ e'_j, & j = r+1, \ldots, n \end{cases}$$

transforms q into the desired form.

(3.4.2) Theorem (Sylvester). *For each quadratic form $q : E \longrightarrow \mathbf{R}$ on a $\mathbf{R}$-vector space E of dimension $n < \infty$ there exists a basis $e_1, \ldots, e_n$ of E such that*

$$q(x) = x_1^2 + \cdots + x_s^2 - x_{s+1}^2 - \cdots - x_{s+t}^2 \qquad\qquad (x = \sum_{j=1}^{n} x_j e_j).$$

The pair (s, t) is determined by q; it is called **the signature of** *q. The rank of q is equal to $\mathrm{rk}(q) = s + t$.*
Matrix formulation: *For each symmetric real matrix $A = {}^tA \in M_n(\mathbf{R})$ there exists an invertible matrix $P \in M_n(\mathbf{R})$ such that ${}^tPAP = \begin{pmatrix} I_s & 0 & 0 \\ 0 & -I_t & 0 \\ 0 & 0 & 0 \end{pmatrix}$.*

Proof. Let $r = \mathrm{rk}(q)$. According to Theorem 3.3.1, there exist a basis $e'_1, \ldots, e'_n$ of E and non-zero scalars $d_1, \ldots, d_r \in \mathbf{R}$ such that

$$q(x) = d_1 x_1'^2 + \cdots + d_r x_r'^2 \qquad\qquad (x = \sum_{j=1}^{n} x'_j e'_j).$$

After reordering the variables, we can assume that

$$d_1, \dots, d_s > 0 > d_{s+1}, \dots, d_r;$$

set $t = r - s$. The change of coordinates

$$x_j = \begin{cases} \sqrt{d_j}\, x'_j, & j = 1, \dots, s \\ \sqrt{-d_j}\, x'_j, & j = s+1, \dots, s+t = r \\ x'_j, & j = r+1, \dots, n \end{cases}$$

transforms q into the desired form

$$q(x) = x_1^2 + \cdots + x_s^2 - x_{s+1}^2 - \cdots - x_{s+t}^2.$$

It remains to show that s (and hence also $t = \mathrm{rk}(q) - s$) is determined by q. Assume that $f_1, \dots, f_n$ is a basis of E such that

$$q(x) = y_1^2 + \cdots + y_{s'}^2 - y_{s'+1}^2 - \cdots - y_r^2 \qquad\qquad (x = \sum_{j=1}^{n} y_j f_j).$$

The vector subspaces

$$F_1 = \mathrm{vect}(e_{s+1}, \dots, e_n), \qquad F_2 = \mathrm{vect}(f_1, \dots, f_{s'})$$

of E satisfy

$$\left.\begin{array}{rl} \forall x \in F_1 & q(x) \leq 0 \\ (\forall x \in F_2,\, x \neq \vec{0}) & q(x) > 0 \end{array}\right\} \implies F_1 \cap F_2 = \{\vec{0}\}.$$

In particular,

$$s' = \dim(F_2) \leq \dim(E) - \dim(F_1) = s.$$

Exchanging the rôles of the two bases, we obtain, by the same argument, that $s \leq s'$; thus $s = s'$.

(3.4.3) Examples (computing the signature): As in the proof of Sylvester's, theorem, the integer s (resp., t) is equal to the number of positive (resp., negative) diagonal terms in an arbitrary diagonalisation of the quadratic form q.

(1) The quadratic form

$$q(x) = x_1^2 + 4x_1x_2 - 6x_1x_3 + 3x_2^2 + 2x_2x_3 - 40x_3^2$$

from 3.3.2(3) can be diagonalised as

$$q(x) = (x_1 + 2x_2 - 3x_3)^2 - (x_2 - 7x_3)^2 = x_1'^2 - x_2'^2 + 0 \cdot x_3'^2,$$

hence

$$\mathrm{rk}(q) = 2, \qquad \mathrm{sign}(q) = (1, 1).$$

(2) For

$$E = \{\text{real symmetric matrices } X = {}^tX = \begin{pmatrix} x_1 & x_2 \\ x_2 & x_3 \end{pmatrix} \in M_2(\mathbf{R})\}, \qquad q(X) = \det(X) = x_1x_3 - x_2^2,$$

we write

$$\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} x_1' + x_3' \\ x_2' \\ x_1' - x_3' \end{pmatrix}, \qquad q(X) = x_1x_3 - x_2^2 = x_1'^2 - x_2'^2 - x_3'^2,$$

hence

$$\mathrm{rk}(q) = 3, \qquad \mathrm{sign}(q) = (1, 2).$$

(3.4.4) Exercise. *Determine the polar form, the rank, the kernel and the signature of the following quadratic forms on* $\mathbf{R}^4$.

$$\begin{aligned} q_1(x) &= x_1^2 + 2x_1x_2 - 4x_1x_4 + 3x_2^2 + 8x_2x_3 + 6x_3^2 - 2x_4^2 \\ q_2(x) &= 4x_1x_2 + 4x_2x_3 - 2x_3x_4 \\ q_3(x) &= x_1x_2 + x_1x_3 + x_2x_4 + x_3x_4. \end{aligned}$$

[Compute the rank and the kernel by two independent methods, in order to check the result.]

(3.4.5) Exercise. *Let* $E = M_n(\mathbf{R})$, $q(X) = \mathrm{Tr}(X^2)$ $(X \in E)$.
(1) *Determine the polar form* $f : E \times E \longrightarrow \mathbf{R}$ *of* q.
(2) *Show that* $E = E_- \perp E_+$, *where*

$$E_\pm = \{X \in M_n(\mathbf{R}) \mid {}^tX = \pm X\}.$$

(3) *Show that, for each non-zero element* $X \in E_\pm$, *we have* $\pm q(X) > 0$.
(4) *Determine the rank and the signature of* q.
[Hint: $\mathrm{Tr}(XY) = \mathrm{Tr}(YX)$.*]*

3.5 Sum, direct sum

(3.5.1) Definition (sum of subspaces). *Let* $F_1, \ldots, F_n$ *be vector subspaces of a* K*-vector space* E. *Their* **sum** *is the vector subspace* $F \subset E$ *generated by the union* $F_1 \cup \cdots \cup F_n$; *it is denoted by* $F_1 + \cdots + F_n = \sum_{i=1}^n F_i$. *In concrete terms,*

$$F_1 + \cdots + F_n = \mathrm{vect}(F_1 \cup \cdots \cup F_n) = \{x_1 + \cdots + x_n \mid x_i \in F_i\}.$$

(3.5.2) Example: If $F_1, F_2 \subset \mathbf{R}^3$ are distinct planes in $\mathbf{R}^3$ (containing the origin), then $F_1 + F_2 = \mathbf{R}^3$ and $F_1 \cap F_2$ is a line.
In general, if $F_1, F_2 \subset E$ are vector subspaces of an arbitrary K-vector space, then

$$\dim(F_1 \cap F_2) + \dim(F_1 + F_2) = \dim(F_1) + \dim(F_2)$$

(in the above example, $1 + 3 = 2 + 2$).

(3.5.3) Definition (direct sum of subspaces). *In the situation of 3.5.1, we say that the sum* $F_1 + \cdots + F_n$ *is* **direct** *(notation:* $F_1 \oplus \cdots \oplus F_n = \bigoplus_{i=1}^n F_i$*) if each element* $x \in F_1 + \cdots + F_n$ *admits a* **unique** *decomposition* $x = x_1 + \cdots + x_n$ $(x_i \in F_i)$. *If this is the case, let* $\mathcal{B}_i$ *be a basis of* F_i $(i = 1, \ldots, n)$; *then* $\mathcal{B}_1 \cup \cdots \cup \mathcal{B}_n$ *is a basis of* $F_1 \oplus \cdots \oplus F_n$, *hence*

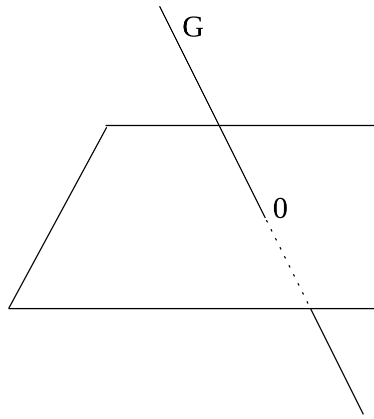
$$\dim(F_1 \oplus \cdots \oplus F_n) = \dim(F_1) + \cdots + \dim(F_n).$$

(3.5.4) Examples: (1) $K^n = F_1 \oplus + \cdots \oplus F_n$, where the subspaces $F_i = \mathrm{vect}(e_i) = Ke_i$ are the lines generated by the vectors of the canonical basis of K^n.
(2) If $n = 2$, then: the sum $F_1 + F_2$ is direct $\iff$ $F_1 \cap F_2 = 0$.

(3.5.5) Exercise. *Find an example of vector subspaces $F_1, F_2, F_3 \subset E$ satisfying $F_1 \cap F_2 = F_1 \cap F_3 = F_2 \cap F_3 = 0$, for which the sum $F_1 + F_2 + F_3$ is not direct.*

(3.5.6) Definition (complementary subspace). *Let $F, G \subset E$ be vector subspaces of E. We say that G is a* **complementary subspace of** *F if $F \oplus G = E$ ($\iff$ $F \cap G = 0$ and $F + G = E \iff F \cap G = 0$ and $\dim(E) = \dim(F) + \dim(G)$).*

(3.5.7) Example:



3.6 Orthogonal sum

Throughout this section, $f : E \times E \longrightarrow K$ is a symmetic bilinear form on a K-vector space E and $q : E \longrightarrow K$ is the associated quadratic form: $q(x) = f(x, x)$.

Recall from 3.2.1 that two vectors $x, y \in E$ are **orthogonal** to each other with respect to f (notation: $x \perp y$, or $x \perp_f y$, or $x \perp_q y$) if $f(x, y) = 0$ ($\iff$ $y \perp x$).

(3.6.1) Definition. *Let $S \subset E$ be a non-empty subset. Its* **orthogonal** *is defined as*

$$S^\perp = \{x \in E \mid \forall y \in S \quad x \perp y\} \subset E.$$

(3.6.2) Remarks: (1) $S^\perp$ always contains the radical (= the kernel) of q: $S^\perp \supset N(q)$.
(2) $\{\vec{0}\}^\perp = E$.
(3) $E^\perp = N(q)$.
(4) Bilinearity of f implies that

$$\begin{aligned} x \perp y, \quad x' \perp y \quad &\Longrightarrow \quad (x + x') \perp y \\ x \perp y, \quad \lambda \in K \quad &\Longrightarrow \quad (\lambda x) \perp y. \end{aligned}$$

(5) It follows from the property (4) that, for each non-empty subset $S \subset E$, the orthogonal $S^\perp$ is a **vector subspace** of E and $S^\perp = (\mathrm{vect}(S))^\perp$. In other words, it is enough to study the orthogonals of vector subspaces of E.

(3.6.3) Definition (Orthogonal sum). *Let $F_1, F_2 \subset E$ be vector subspaces of E. We say that F_1* **is orthogonal to** *F_2 (with respect to f) if*

$$\forall x \in F_1 \, \forall y \in F_2 \quad x \perp y$$

*(***notation:** *$F_1 \perp F_2$, or $F_1 \perp_f F_2$, or $F_1 \perp_q F_2$).*
We say that E is equal to the **orthogonal sum** *of F_1 and F_2 (***notation:** *$E = F_1 \perp F_2$) if $E = F_1 \oplus F_2$ and $F_1 \perp F_2$.*

(3.6.4) Example (Euclidean plane): Assume that $E = \mathbf{R}^2$ ($K = \mathbf{R}$) and f = the standard Euclidean scalar product (hence $q(x) = x_1^2 + x_2^2$). If $F_1, F_2 \subset E$ are distinct lines passing through the origin, then $E = F_1 \oplus F_2$. Moreover, $E = F_1 \perp F_2 \iff F_1$ is orthogonal to F_2 in the usual sense.

(3.6.5) Example (hyperbolic plane): Assume that $E = K^2$ and $q(x) = x_1^2 - x_2^2$ (hence $f(x, y) = x_1 y_1 - x_2 y_2$). For each $a \in K$, let $L_a = \mathrm{vect}\{\begin{pmatrix} 1 \\ a \end{pmatrix}\}$ be the line of slope a passing through the origin. We also denote by $L_\infty = \mathrm{vect}\{\begin{pmatrix} 0 \\ 1 \end{pmatrix}\}$ the vertical line passing through the origin.

If $a \neq 0$, then we have

$$\begin{pmatrix} y_1 \\ y_2 \end{pmatrix} \in L_a^\perp \iff \begin{pmatrix} 1 \\ a \end{pmatrix} \perp \begin{pmatrix} y_1 \\ y_2 \end{pmatrix} \iff y_1 - a y_2 = 0 \iff \begin{pmatrix} y_1 \\ y_2 \end{pmatrix} = y_1 \begin{pmatrix} 1 \\ 1/a \end{pmatrix} \iff \begin{pmatrix} y_1 \\ y_2 \end{pmatrix} \in L_{1/a}.$$

Similarly,

$$\begin{pmatrix} y_1 \\ y_2 \end{pmatrix} \in L_0^\perp \iff y_1 = 0 \iff \begin{pmatrix} y_1 \\ y_2 \end{pmatrix} \in L_\infty, \qquad \begin{pmatrix} y_1 \\ y_2 \end{pmatrix} \in L_\infty^\perp \iff y_2 = 0 \iff \begin{pmatrix} y_1 \\ y_2 \end{pmatrix} \in L_0.$$

To sum up, we have (with the convention that $1/0 = \infty$ and $1/\infty = 0$)

$$\forall a \in K \cup \{\infty\} \qquad L_a^\perp = L_{1/a}. \tag{3.6.5.1}$$

This implies that the two lines

$$L_1^\perp = L_1, \qquad L_{-1}^\perp = L_{-1} \tag{3.6.5.2}$$

are self-orthogonal (in particular, $x \perp x$ for each $x \in L_1$ or $x \in L_{-1}$)! On the other hand, if $a \neq \pm 1$, then $L_a \cap L_{1/a} = 0$, hence $E = L_a \oplus L_{1/a}$; thus

$$\forall a \neq \pm 1 \qquad E = L_a \perp L_{1/a} = L_a \perp L_a^\perp.$$

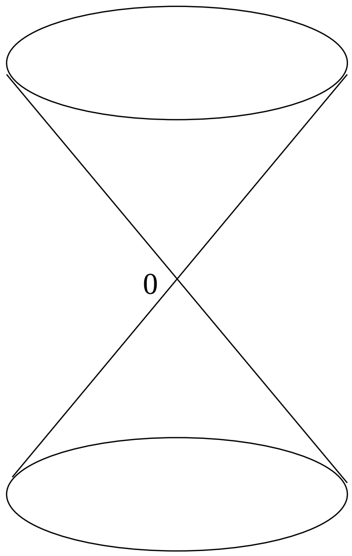
(3.6.6) Definition. *Let $q : E \longrightarrow K$ be a quadratic form. A vector $x \in E$ is called* **isotropic** *(for q) if $x \neq \vec{0}$ and $x \perp x$ ($\iff q(x) = 0$). The vector subspace* $\mathrm{vect}(x)$ *generated by an isotropic vector x is called an* **isotropic line**. *The subset of E*

$$C(q) := \{x \in E \mid q(x) = 0\} = \{\vec{0}\} \cup \{\text{isotropic vectors of } q\}$$

is called the **isotropic cone of** *q (if $x \in C(q)$ and $\lambda \in K$, then $\lambda x \in C(q)$, since $q(\lambda x) = \lambda^2 q(x)$; thus $C(q)$ is the union of isotropic lines).*

(3.6.7) Example (hyperbolic plane): If $(E, q) = (K^2, x_1^2 - x_2^2)$ is the hyperbolic plane, then $C(q) = L_1 \cup L_{-1}$ is the union of the two isotropic lines from (3.6.5.2).

(3.6.8) Example: If $E = K^3$ and $q(x) = x_1^2 - x_2^2 - x_3^2$, then $C(q)$ is the "usual" cone (where x_1 is the vertical coordinate):



C(q)

If $L \subset E$ is any line passing through the origin, then there are two possibilities (exercise !):

If $L \not\subset C(q)$ (i.e., if L is not isotropic), then $L^\perp$ is a plane not containing L and $E = L \perp L^\perp$.

If $L \subset C(q)$ (i.e., if L is isotropic), then $L^\perp$ is a plane containing L (thus $L + L^\perp = L^\perp \neq E$). More precisely, $L^\perp$ is the plane tangent to $C(q)$ along the line L.

(3.6.9) Orthogonal sum (matrix formulation): Assume that $E = F_1 \oplus F_2$ (and that $n_i = \dim(F_i) < \infty$). Fix a basis $\mathcal{B}_i$ of F_i; then $\mathcal{B} = \mathcal{B}_1 \cup \mathcal{B}_2$ is a basis of E. The matrix of f in the basis $\mathcal{B}$ decomposes naturally into blocks

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

where each block $B_{ij} \in M_{n_i,n_j}(K)$ represents the restriction $f_{ij} : F_i \times F_j \longrightarrow K$ of f to $F_i \times F_j$ (i.e., the function $f(x,y)$ for $x \in F_i$ and $y \in F_j$) in the bases $\mathcal{B}_i$ and $\mathcal{B}_j$ $(i,j = 1,2)$. As the matrix $A = {}^tA$ is symmetric, we have

$$B_{ii} = {}^tB_{ii}, \qquad B_{12} = {}^tB_{21}.$$

By definition, we have

$$E = F_1 \perp F_2 \iff f_{12} = 0,\ f_{21} = 0 \iff B_{12} = 0,\ B_{21} = 0 \iff A = \begin{pmatrix} A_1 & 0 \\ 0 & A_2 \end{pmatrix}, \qquad (3.6.9.1)$$

where $A_i = B_{ii} \in M_{n_i}(K)$ is the matrix of the restriction of f to $F_i \times F_i$ in the basis $\mathcal{B}_i$.

(3.6.10) Definition (Orthogonal sum − general case). *Let $F_1, \dots, F_k \subset E$ be vector subspaces of E such that $E = F_1 \oplus \cdots \oplus F_k$. We say that E is equal to the* **orthogonal sum** *of $F_1, \dots, F_k$ if $F_i \perp F_j$ for all $i \neq j$ (***notation:** *$E = F_1 \perp \cdots \perp F_k$).*

(3.6.11) Matrix formulation: If $E = F_1 \oplus \cdots \oplus F_k$, let $\mathcal{B}_i$ be a basis of F_i $(i = 1, \dots, k)$; let $A \in M_n(K)$ be the matrix of f in the basis $\mathcal{B} = \mathcal{B}_1 \cup \cdots \cup \mathcal{B}_k$ of E. As in (3.6.9.1), we have

$$E = F_1 \perp \cdots \perp F_k \iff A = \begin{pmatrix} A_1 & 0 & \cdots & 0 \\ 0 & A_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & A_k \end{pmatrix}, \qquad (3.6.11.1)$$

where $A_i \in M_{n_i}(K)$ ($n_i = \dim(F_i)$) is the matrix of the restriction of f to $F_i \times F_i$ in the basis $\mathcal{B}_i$ ($i = 1, \ldots, k$).
Example: Let $\mathcal{B} = \{e_1, \ldots, e_n\}$ be a basis of E; then $E = F_1 \oplus \cdots \oplus F_n$, where $F_i = \mathrm{vect}(e_i)$ is the line generated by e_i. In this case

$$E = F_1 \perp \cdots \perp F_n \iff \forall i \neq j \quad e_i \perp e_j \iff A \text{ is a diagonal matrix} \iff \mathcal{B} \text{ is an orthogonal basis.}$$

3.7 Orthogonality in the non-degenerate case

We continue to use the notation from §3.6.
(3.7.1) Example (reduction to the non-degenerate case): Let $E = K^n$, $f(x,y) = x_1y_1 + \cdots + x_ry_r$ ($0 \leq r \leq n$). The matrix $A \in M_n(K)$ of f in the canonical basis $\mathcal{B} = \{e_1, \ldots, e_n\}$ of K^n can be written in the block form

$$A = \begin{pmatrix} I_r & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} A_1 & 0 \\ 0 & A_2 \end{pmatrix}.$$

As in 3.6.9, this means that the decomposition $E = F_1 \oplus F_2$, where $F_1 = \mathrm{vect}(e_1, \ldots, e_r)$ and $F_2 = \mathrm{vect}(e_{r+1}, \ldots, e_n)$, is **orthogonal:** $E = F_1 \perp F_2$. More precisely, $F_2 = N(q)$ is equal to the radical (= the kernel) of q. As the matrix $A_1 = I_r \in M_r(K)$ is invertible, we have a decomposition

$$E = F_1 \perp N(q), \qquad \text{the restriction of } q \text{ to } F_1 \text{ is non} - \text{degenerate.}$$

The general case is similar:

(3.7.2) Proposition. *Let $q : E \longrightarrow K$ be a quadratic form, $n = \dim(E) < \infty$. If $F \subset E$ is any complementary subspace of $N(q)$, then $E = F \perp N(q)$ and the restriction q_F of q to F ($q_F : F \longrightarrow K$, $q_F(x) = q(x)$) is* **non-degenerate**.

Proof. Let $\mathcal{B}_1$ (resp., $\mathcal{B}_2$) be a basis of F (resp., of $N(q)$). As the restrictions of f (= the polar form of q) to $E \times N(q)$ and to $N(q) \times E$ are equal to zero (by definition of $N(q)$), it follows that the matrix $A \in M_n(K)$ of f in the basis $\mathcal{B}_1 \cup \mathcal{B}_2$ of E is equal to

$$A = \begin{pmatrix} A_1 & 0 \\ 0 & 0 \end{pmatrix},$$

where $A_1 \in M_r(K)$ ($r = \dim(F)$) is the matrix of q_F in the basis $\mathcal{B}_1$. As

$$r = \dim(F) = n - \dim(N(q)) \overset{(3.2.2.2)}{=\!=} \mathrm{rk}(q) = \mathrm{rk}(A) = \mathrm{rk}(A_1),$$

the matrix A_1 is invertible, hence q_F is non-degenerate.

(3.7.3) Proposition. *Let $q : E \longrightarrow K$ be a* **non-degenerate** *quadratic form on a vector space of dimension $n = \dim(E) < \infty$. If $F \subset E$ is a vector subspace, then*

$$\dim(F^\perp) = n - \dim(F), \qquad (F^\perp)^\perp = F.$$

Proof. It is enough to prove the equality $\dim(F^{\perp}) = n - \dim(F)$ for all subspaces of E (if we apply it to F and $F^{\perp}$, we obtain $\dim(F^{\perp})^{\perp} = n - \dim(F^{\perp}) = n - (n - \dim(F)) = \dim(F)$; as $F \subset (F^{\perp})^{\perp}$ by definition, we must have $F = (F^{\perp})^{\perp}$).

Fixing a basis of E, we identify E with K^n and the polar form f of q with the function $f(x,y) = {}^t x A y$ ($x, y \in K^n$). As q is non-degenerate by assumption, the matrix $A \in M_n(K)$ is **invertible**. Let $v_1, \dots, v_r$ ($r = \dim(F)$) be a basis of $F \subset K^n$; denote by

$$C = (v_1 \mid \cdots \mid v_r) \in M_{n,r}(K)$$

the matrix with columns $v_1, \dots, v_r$. As the rows of the transpose matrix ${}^tC \in M_{r,n}(K)$ are equal to ${}^tv_1, \dots, {}^tv_r$, we have

$$F^{\perp} = \{y \in K^n \mid v_1 \perp y, \dots, v_r \perp y\} = \{y \in K^n \mid {}^tv_1 A y = \cdots = {}^tv_r A y = 0\} = \{y \in K^n \mid {}^tC A y = 0\}.$$

We have

$$\begin{aligned} \dim(F^{\perp}) &= n - \mathrm{rk}({}^tCA) && \text{by the rank formula (1.2.7.2)} \\ \mathrm{rk}({}^tCA) = \mathrm{rk}({}^t({}^tCA)) &= \mathrm{rk}({}^tAC) = \mathrm{rk}(C) && \text{as } {}^tA \text{ is invertible} \\ \mathrm{rk}(C) = \dim \mathrm{vect}(v_1, \dots, v_r) &= \dim(F) && \text{by definition,} \end{aligned}$$

hence $\dim(F^{\perp}) = n - \dim(F)$, as claimed.

(3.7.4) Corollary. *Under the assumptions of 3.7.3, if $F \cap F^{\perp} = \{\vec{0}\}$, then $E = F \perp F^{\perp}$ is the orthogonal sum of F and $F^{\perp}$.*

Proof. It follows from $F \cap F^{\perp} = \{\vec{0}\}$ and $\dim(F) + \dim(F^{\perp}) = \dim(E)$ that $E = F \oplus F^{\perp}$. As $F \perp F^{\perp}$ by definition, we have $E = F \perp F^{\perp}$.

(3.7.5) Examples: Assume that $\dim(F) = 1$, i.e. $F = \mathrm{vect}(x)$ ($x \in E$, $x \neq \vec{0}$).
(1) If x **is isotropic**, then $x \perp x$, hence $F \subset F^{\perp}$ and $F + F^{\perp} = F^{\perp}$ is a hyperplane in E (a vector subspace of dimension equal to $\dim(E) - 1$).
(2) If x **is not isotropic**, then $f(x, \lambda x) = \lambda f(x,x) = \lambda q(x) \neq 0$ for any non-zero $\lambda \in K$, hence $F \cap F^{\perp} = \{\vec{0}\}$; thus $E = F \perp F^{\perp}$.

(3.7.6) Exercise (the degenerate case). *Let $q : E \longrightarrow K$ be a quadratic form on a finite-dimensional vector space. For each vector subspace $F \subset E$, we have $(F^{\perp})^{\perp} = F + N(q)$.*

(3.7.7) We can now give an abstract proof of the diagonalisation result 3.3.1.

(3.7.8) = (3.3.1) Theorem. *For each quadratic form $q : E \longrightarrow K$ ($n = \dim(E) < \infty$) there exists a basis $\mathcal{B} = \{e_1, \dots, e_n\}$ of E for which $E = Ke_1 \perp \cdots \perp Ke_n$ ($\Longleftrightarrow$ $\mathcal{B}$ is an orthogonal basis of E, by 3.6.11).*

Proof. Thanks to Proposition 3.7.2, we can assume that $E = F$, hence q is non-degenerate. If $n = 1$, we take e_1 to be an arbitrary non-zero vector of E. If $n > 1$, then $q \neq 0$, hence there exists $e_1 \in E$ such that $q(e_1) \neq 0$. Applying 3.7.5(2), we obtain $E = Ke_1 \perp E_1$, where $E_1 = (Ke_1)^{\perp}$ is a vector subspace of E of dimension $n - 1$. As the restriction of q to E_1 is non-degenerate (exercise: why?), there exists $e_2 \in E_1$ such that $q(e_2) \neq 0$, hence $E_1 = Ke_2 \perp (Ke_2)^{\perp}$. Continuing this process, we obtain $E = Ke_1 \perp \cdots \perp Ke_n$.

(3.7.9) Exercise. *Let $q : E \longrightarrow K$ be a quadratic form, and $F, G \subset E$ vector subspaces; then $(F + G)^{\perp} = F^{\perp} \cap G^{\perp}$. If, in addition, $\dim(E) < \infty$ and q is non-degenerate, then $(F \cap G)^{\perp} = F^{\perp} + G^{\perp}$.*

4. Euclidean spaces

A **Euclidean space** is an abstract version of the real vector space $\mathbf{R}^n$ equipped with the standard Euclidean scalar product $(x \mid y) = x_1y_1 + \cdots + x_ny_n$. An important difference between the two is the following: $\mathbf{R}^n$ has a **canonical orthonormal basis**, namely the canonical basis, whereas a general Euclidean space has lots of orthonormal bases, but none of them is distinguished (example: any vector subspace of $\mathbf{R}^n$ is a Euclidean space). Throughout Chapter 4, $K = \mathbf{R}$.

4.1 Basic concepts

(4.1.1) Definition. *Let $q : E \longrightarrow \mathbf{R}$ be a quadratic form on a real vector space E. We say that q is* **positive definite** *(resp.,* **negative definite***) if $(\forall x \in E,\ x \neq \vec{0})\ \ q(x) > 0$ (resp., $q(x) < 0$). We say that q is* **positive semi-definite** *(resp.,* **negative semi-definite***) if $(\forall x \in E)\ \ q(x) \geq 0$ (resp., $q(x) \leq 0$). Finally, q is* **indefinite** *if there exist $x, y \in E$ such that $q(x) > 0 > q(y)$.*

(4.1.2) Example: If $\dim(E) = n < \infty$, then it follows from Sylvester's Theorem 3.4.2 that there exists a basis of E in which

$$q(x) = x_1^2 + \cdots x_s^2 - x_{s+1}^2 - \cdots - x_{s+t}^2\ (+0 \cdot x_{s+t+1}^2 + \cdots + 0 \cdot x_n^2),$$

where $s, t \geq 0$, $\mathrm{rk}(q) = s + t \leq n$, $\mathrm{sign}(q) = (s, t)$. This implies that

$$\begin{aligned}
q \text{ is positive semi-definite} &\iff t = 0\\
q \text{ is negative semi-definite} &\iff s = 0\\
q \text{ is indefinite} &\iff s, t > 0\\
q \text{ is positive definite} &\iff s = n \iff t = 0,\ \mathrm{rk}(q) = n\\
q \text{ is negative definite} &\iff t = n \iff s = 0,\ \mathrm{rk}(q) = n
\end{aligned}$$

In particular, a **positive definite** (resp., a **negative definite**) quadratic form is always **non-degenerate** (this also follows directly from the definitions – exercise!).

(4.1.3) Definition. *A (real)* **pre-Hilbert space** *is a real vector space E equipped with a symmetric bilinear form $f : E \times E \longrightarrow \mathbf{R}$ (the* **scalar product***) whose associated quadratic form is* **positive definite***. We denote $(x \mid y) = f(x, y)$. A* **Euclidean space** *is a (real) pre-Hilbert space of finite dimension.*

(4.1.4) Examples of pre-Hilbert spaces: (1) $E = \mathbf{R}^n$ with the standard Euclidean scalar product

$$(x \mid y) = x_1y_1 + \cdots + x_ny_n.$$

(2) $E = \{f : [a, b] \longrightarrow \mathbf{R} \mid f \text{ continuous}\} = C([a, b]; \mathbf{R})$,

$$(f \mid g) = \int_a^b f(t)g(t)\,dt.$$

(3) Each vector subspace of a pre-Hilbert (resp., Euclidean) space is a pre-Hilbert (resp., Euclidean) space.

(4.1.5) Orthonormal bases. As remarked in 4.1.2, Sylvester's theorem implies that every Euclidean space E (of dimension $n = \dim(E)$) admits a basis $e_1, \ldots, e_n$ such that

$$(x \mid x) = x_1^2 + \cdots + x_n^2 \qquad\qquad (x = \sum_{i=1}^{n} x_ie_i);$$

such a basis is called an **orthonormal basis** of E. Note that the following properties are equivalent:

$$\{e_i\} \text{ is an orthonormal basis} \iff f(x,y) = (x \mid y) = x_1y_1 + \cdots + x_ny_n \qquad (y = \sum_{i=1}^{n} y_ie_i) \iff$$

$$\iff \text{the matrix of the scalar product in the basis } \{e_i\} \text{ is equal to } I_n \iff$$

$$\iff (e_i \mid e_j) = \delta_{ij} = \begin{cases} 1, & i = j \\ 0, & i \neq j \end{cases}$$

(4.1.6) Notation: From now on, until the end of Chapter 4, E will be a (real) pre-Hilbert space and $(x \mid y)$ the scalar product on E ($x, y \in E$). Using the notation of 3.2.1, we have: $x \perp y \iff (x \mid y) = 0$.

(4.1.7) Definition. *An* **orthonormal system** *in E is a non-empty subset $\{e_i\}$ of E such that*

$$(e_i \mid e_j) = \begin{cases} 1, & i = j \\ 0, & i \neq j. \end{cases}$$

(4.1.8) Proposition. *If $\{e_i\}$ is an orthonormal system in E and if $x = \sum_i \lambda_i e_i$ ($\lambda_i \in \mathbf{R}$ and the sum is finite), then*

$$\lambda_j = (x \mid e_j).$$

In particular, the vectors $\{e_i\}$ are **linearly independent** *(take $x = \vec{0}$).*

Proof. We have

$$(x \mid e_j) = (\sum_i \lambda_i e_i \mid e_j) = \sum_i \lambda_i \, (e_i \mid e_j) = \lambda_j.$$

(4.1.9) More generally, an **orthogonal system** in E is any non-empty subset $\{f_i\}$ of E such that $f_i \neq \vec{0}$ and $(f_i \mid f_j) = 0$ ($\iff f_i \perp f_j$) if $i \neq j$. In this case $(f_i \mid f_i) > 0$ and the vectors

$$e_i = \frac{f_i}{\sqrt{(f_i \mid f_i)}}$$

form an orthonormal system. The statement of 4.1.8 is replaced by

$$x = \sum_i \lambda_i f_i \implies \lambda_j = \frac{(x \mid f_j)}{(f_j \mid f_j)},$$

since

$$(x \mid f_j) = (\sum_i \lambda_i f_i \mid f_j) = \sum_i \lambda_i \, (f_i \mid f_j) = \lambda_j \, (f_j \mid f_j).$$

As in 4.1.8, this shows that the vectors $\{f_i\}$ are linearly independent.

(4.1.10) In particular, if $\dim(E) = n < \infty$ and $u_1, \ldots, u_n \in E$, then

$$u_1, \ldots, u_n \text{ is an orthogonal system in } E \iff u_1, \ldots, u_n \text{ is an orthogonal basis of } E$$
$$u_1, \ldots, u_n \text{ is an orthonormal system in } E \iff u_1, \ldots, u_n \text{ is an orthonormal basis of } E.$$

4.2 The norm (= the length)

(4.2.1) Definition. *The* **norm** *of a vector* $x \in E$ *is the real number* $\|x\| := \sqrt{(x \mid x)} \geq 0$. *In particular, if* $\dim(E) = n < \infty$ *and if we write* $x = \sum_{i=1}^{n} x_i e_i$ *in an* **orthonormal** *basis* $\{e_i\}$, *then* $\|x\| = \sqrt{x_1^2 + \cdots + x_n^2}$.

(4.2.2) Basis properties of the norm: (1) $\|x\| \geq 0$, and $\|x\| = 0 \iff x = \vec{0}$.
(2) For each $\lambda \in \mathbf{R}$, $\|\lambda x\| = |\lambda| \, \|x\|$.
(3) As in 3.1.4, we have, for all $x, y \in E$,

$$\|x+y\|^2 = (x+y \mid x+y) = (x \mid x) + (y \mid y) + (x \mid y) + (y \mid x) = \|x\|^2 + \|y\|^2 + 2(x \mid y),$$

hence

$$(x \mid y) = \frac{1}{2}(\|x+y\|^2 - \|x\|^2 - \|y\|^2).$$

(4.2.3) The Cauchy-Schwarz Inequality. *For all* $x, y \in E$, $\quad |(x \mid y)| \leq \|x\| \|y\|$.

Proof. If $x = \vec{0}$, then the statement says that $0 \leq 0$. Assume that $x \neq \vec{0}$; then $(x \mid x) = \|x\|^2 > 0$. For each $t \in \mathbf{R}$, the expression

$$\|tx+y\|^2 = (tx+y \mid tx+y) = t^2\,(x \mid x) + 2t\,(x \mid y) + (y \mid y) \geq 0$$

is non-negative. As

$$t^2\,(x \mid x) + 2t\,(x \mid y) + (y \mid y) = (x \mid x)\left(t + \frac{(x \mid y)}{(x \mid x)}\right)^2 + \frac{(x \mid x)(y \mid y) - (x \mid y)^2}{(x \mid x)},$$

taking

$$t = -\frac{(x \mid y)}{(x \mid x)},$$

we obtain

$$\frac{(x \mid x)(y \mid y) - (x \mid y)^2}{(x \mid x)} \geq 0,$$

hence (using the fact that $(x \mid x) > 0$)

$$(x \mid x)(y \mid y) \geq (x \mid y)^2 \implies \sqrt{(x \mid x)}\sqrt{(y \mid y)} \geq \sqrt{(x \mid y)^2} = |(x \mid y)|.$$

(4.2.4) Exercise. *The above argument shows that*

$$|(x \mid y)| = \|x\| \cdot \|y\| \iff x, y \text{ are linearly dependent.}$$

(4.2.5) Corollary ("triangle inequality"). *For all* $x, y \in E$, $\quad \|x \pm y\| \leq \|x\| + \|y\|$.

Proof. We have

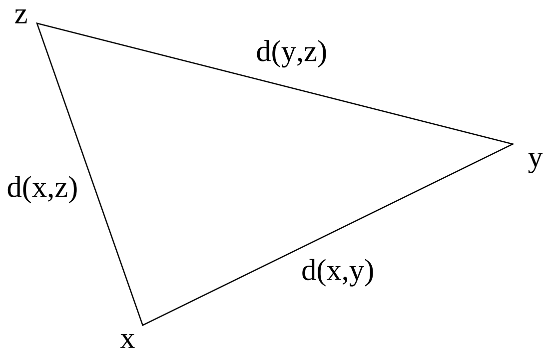
$$(\|x\| + \|y\|)^2 - (\|x \pm y\|)^2 = \|x\|^2 + 2\|x\|\|y\| + \|y\|^2 - (\|x\|^2 \pm 2\,(x \mid y) + \|y\|^2) = 2(\|x\|\|y\| \mp (x \mid y)) \geq 0.$$

(4.2.6) Distance. If we define the **distance** of (the endpoints of) two vectors $x, y \in E$ as

$$d(x,y) := \|x - y\|, \tag{4.2.6.1}$$

then the triangle inequality can be rewritten in the more familiar form (for $x, y, z \in E$)

$$d(x,z) = \|x-z\| = \|(x-y)+(y-z)\| \le \|x-y\| + \|y-z\| = d(x,y) + d(y,z). \tag{4.2.6.2}$$



(4.2.7) In particular, for the space $E = C([a,b],\mathbf{R})$ from Example 4.1.4(2), the distance of two continuous functions $f,g : [a,b] \longrightarrow \mathbf{R}$ becomes

$$d(f,g) = \sqrt{\int_a^b (f(t)-g(t))^2\,dt}. \tag{4.2.7.1}$$

This means that $d(f,g)$ is small if $f(t)$ and $g(t)$ are close "on average". There are other useful ways of measuring closeness in $C([a,b],\mathbf{R})$, for example by using the distances

$$d_\infty(f,g) = \sup_{t\in[a,b]} |f(t)-g(t)|$$
$$d_p(f,g) = \left(\int_a^b |f(t)-g(t)|^p\,dt\right)^{1/p} \qquad (p \ge 1).$$

It turns out that there is a close link ("duality") between the distances d_p and d_q whenever

$$\frac{1}{p} + \frac{1}{q} = 1,$$

which explains a special rôle played by the "self-dual" distance $d(f,g) = d_2(f,g)$.

(4.2.8) Angle. The **angle** of two non-zero vectors $x, y \in E$ is the unique element $\beta \in [0,\pi]$ such that

$$\cos(\beta) = \frac{(x \mid y)}{\|x\|\|y\|}. \tag{4.2.8.1}$$

This definition makes sense, as the expression on the right hand side of (4.2.8.1) is contained in $[-1,1]$, thanks to the Cauchy-Schwarz inequality. Moreover,

$$\beta = \frac{\pi}{2} \iff \cos(\beta) = 0 \iff (x \mid y) = 0 \iff x \perp y.$$

4.3 Orthogonality, orthogonalisation

(4.3.1) The orthogonalisation process of Gram-Schmidt

Let $u_1, \ldots, u_m \in E$ $(m \ge 1)$ be **linearly independent** vectors. We are going to construct an **orthogonal system** $f_1, \ldots, f_m \in E$ satisfying

$$\mathrm{vect}(u_1) = \mathrm{vect}(f_1), \qquad \mathrm{vect}(u_1,u_2) = \mathrm{vect}(f_1,f_2), \qquad \mathrm{vect}(u_1,u_2,\ldots,u_m) = \mathrm{vect}(f_1,f_2,\ldots,f_m).$$

Putting $e_i = f_i/\|f_i\|$, we obtain an **orthonormal system** $e_1, \ldots, e_m \in E$ satisfying

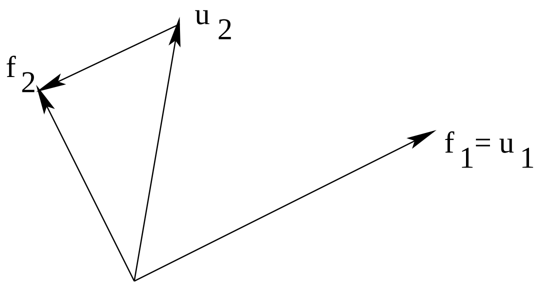
$$\mathrm{vect}(u_1) = \mathrm{vect}(e_1), \qquad \mathrm{vect}(u_1, u_2) = \mathrm{vect}(e_1, e_2), \qquad \mathrm{vect}(u_1, u_2, \ldots, u_m) = \mathrm{vect}(e_1, e_2, \ldots, e_m).$$

Step 1. We let $f_1 = u_1$; linear independence of $u_1, \ldots, u_m$ implies that $f_1 \neq 0$, hence $(f_1 \mid f_1) > 0$.
Step 2. We are looking for a vector of the form

$$f_2 = u_2 + \lambda f_1 \qquad\qquad (\lambda \in \mathbf{R})$$

satisfying

$$f_1 \perp f_2.$$



As

$$f_1 \perp f_2 \iff 0 = (f_1 \mid u_2 + \lambda f_1) = (f_1 \mid u_2) + \lambda (f_1 \mid f_1) \iff \lambda = -\frac{(f_1 \mid u_2)}{(f_1 \mid f_1)},$$

we define

$$f_2 = u_2 - \frac{(f_1 \mid u_2)}{(f_1 \mid f_1)} f_1.$$

As $u_2 = f_2 - \lambda f_1$, we have

$$\mathrm{vect}(u_1, u_2) = \mathrm{vect}(f_1, u_2) = \mathrm{vect}(f_1, f_2).$$

Step 3. We are looking for a vector of the form

$$f_3 = u_3 + \lambda_1 f_1 + \lambda_2 f_2 \qquad\qquad (\lambda_i \in \mathbf{R})$$

satisfying

$$\mathrm{vect}(f_1, f_2) \perp f_3.$$

As before, we have (using the fact that $f_1 \perp f_2$)

$$f_1 \perp f_3 \iff 0 = (f_1 \mid u_3 + \lambda_1 f_1 + \lambda_2 f_2) = (f_1 \mid u_3) + \lambda_1 (f_1 \mid f_1) \iff \lambda_1 = -\frac{(f_1 \mid u_3)}{(f_1 \mid f_1)}$$
$$f_2 \perp f_3 \iff 0 = (f_2 \mid u_3 + \lambda_1 f_1 + \lambda_2 f_2) = (f_2 \mid u_3) + \lambda_2 (f_2 \mid f_2) \iff \lambda_2 = -\frac{(f_2 \mid u_3)}{(f_2 \mid f_2)},$$

hence we define

$$f_3 = u_3 - \frac{(f_1 \mid u_3)}{(f_1 \mid f_1)} f_1 - \frac{(f_2 \mid u_3)}{(f_2 \mid f_2)} f_2.$$

As $u_3 = f_3 - \lambda_1 f_1 - \lambda_2 f_2$, we have

$$\mathrm{vect}(u_1, u_2, u_3) = \mathrm{vect}(f_1, f_2, u_3) = \mathrm{vect}(f_1, f_2, f_3).$$

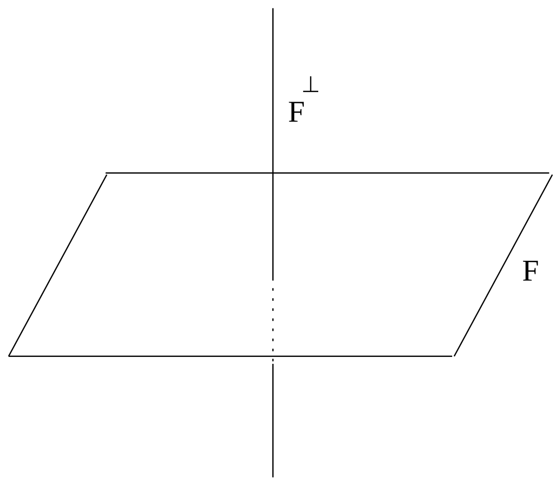
Continuing this procedure, we obtain, after m steps, the required orthogonal system $f_1, \ldots, f_m$; putting $e_i = f_i/\|f_i\|$, we obtain the corresponding orthonormal system $e_1, \ldots, e_m$.

(4.3.2) Exercise. *Apply the Gram-Schmidt process to the elements*

(1) $u_1 = \begin{pmatrix} 1 \\ 2 \\ -2 \end{pmatrix}$, $u_2 = \begin{pmatrix} 0 \\ -1 \\ 2 \end{pmatrix}$, $u_3 = \begin{pmatrix} -1 \\ 3 \\ 1 \end{pmatrix}$ *of* $E = \mathbf{R}^3$ *(equipped with the standard Euclidean scalar product);*
(2) $u_1 = 1$, $u_2 = t$, $u_3 = t^2$, $u_4 = t^3$ *of* $E = C([-1, 1], \mathbf{R})$ *(one obtains the first four* **Legendre polynomials***).*
(3) of the canonical basis of the space $\mathbf{R}^3$*, equipped with the scalar product*

$$f(x, y) = (x_1 - 2x_2)(y_1 - 2y_2) + x_2 y_2 + (x_2 + x_3)(y_2 + y_3).$$

(4.3.3) Proposition-Definition("Orthogonal complement"). *Let* $F \subset E$ *be a vector subspace. Then* $F \cap F^{\perp} = \{\vec{0}\}$ *(in the notation of §3.6). If* $\dim(F) < \infty$*, then* $E = F \oplus F^{\perp} = F \perp F^{\perp}$ *(***terminology:** $F^{\perp}$ *is* **the orthogonal complement of** F*).*



Proof. If $x \in F \cap F^{\perp}$, then $x \perp x$, hence $\|x\|^2 = (x \mid x) = 0$, which implies that $x = \vec{0}$. If $\dim(E) < \infty$, then the decomposition $E = F \oplus F^{\perp}$ follows from Corollary 3.7.4. In general (assuming $m = \dim(F) < \infty$), then we must show that $E \stackrel{?}{=} F + F^{\perp}$ (see 3.5.4(2)), i.e. that each vector $x \in E$ admits a decomposition

$$x \stackrel{?}{=} y + z, \qquad y \in F, \qquad z \in F^{\perp} \quad (\Longrightarrow y \perp z).$$

Assuming that such a decomposition exists and choosing an orthonormal basis $e_1, \ldots, e_m$ of F (which exists, by 4.1.5), then

$$y = \sum_{i=1}^{m} y_i e_i, \qquad z = x - y = x - \sum_{i=1}^{m} y_i e_i \qquad (y_i \in \mathbf{R}),$$

hence

$$z \in F^{\perp} \iff (\forall i = 1, \ldots, m) \quad e_i \perp z \iff (\forall i = 1, \ldots, m) \quad 0 = (e_i \mid z) = (e_i \mid x) - y_i.$$

Conversely, if we put

$$y := \sum_{i=1}^{m} (e_i \mid x) e_i \in F, \qquad z = x - y, \tag{4.3.3.1}$$

then

$$x = y + z, \qquad y \in F, \qquad z \in F^{\perp}. \tag{4.3.3.2}$$

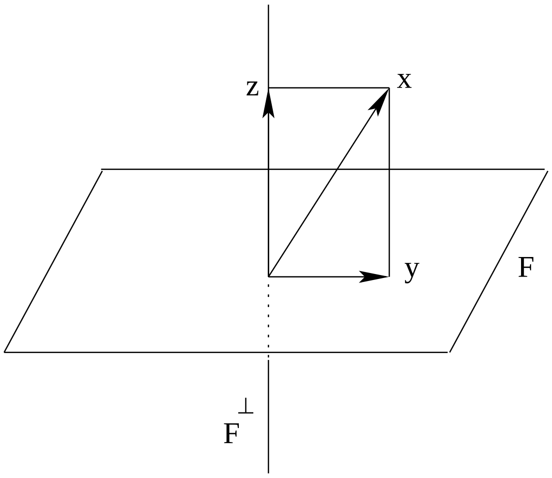
(4.3.4) Example: If $a \in \mathbf{R}^n$ is a non-zero vector, then the orthogonal complement of the line $\mathrm{vect}(a)$ generated by a (with respect to the standard Euclidean scalar product on $\mathbf{R}^n$) is the hyperplane

$$H_a : a_1 x_1 + \cdots + a_n x_n = 0.$$

Conversely, $H_a^{\perp} = \mathrm{vect}(a)$.

(4.3.5) Orthogonal projection. If $F \subset E$ is a vector subspace of finite dimension $m = \dim(F) < \infty$, then the proof of 4.3.3 shows that each vector $x \in E$ admits a unique decomposition (4.3.3.2). The map

$$\begin{aligned} p_F : E &\longrightarrow F \\ x &\mapsto y, \end{aligned}$$



which associates to x its "F-component" y is linear; it is called **the orthogonal projection of** E **on** F. If $e_1, \ldots, e_m$ is any orthonormal basis of F, then we have

$$y = p_F(x) = \sum_{i=1}^{m} (e_i \mid x) e_i, \tag{4.3.5.1}$$

by (4.3.3.1). Furthermore, the orthogonality $y \perp z$ implies that

$$\|x\|^2 = \|y\|^2 + \|z\|^2 + 2(y \mid z) = \|y\|^2 + \|z\|^2 = \sum_{i=1}^{m} (e_i \mid x)^2 + \|z\|^2 \geq \sum_{i=1}^{m} (e_i \mid x)^2,$$

with equality $\iff$ $z = 0$ $\iff$ $x = y \in F$, which proves the following

(4.3.6) Proposition("Bessel's Inequality"). *For each $x \in E$ and each orthonormal system $e_1, \ldots, e_m$ in E,*

$$\sum_{i=1}^{m} (e_i \mid x)^2 \leq \|x\|^2,$$

with equality $\iff$ $x \in \mathrm{vect}(e_1, \ldots, e_m)$.

(4.3.7) An infinite-dimensional example*

Let E be the space $E = C([-1,1], \mathbf{R})$ with the scalar product

$$(f \mid g) = \int_{-1}^{1} f(t)g(t)\, dt.$$

The functions

$$e_0 = \frac{1}{\sqrt{2}}, \qquad e_n = \cos(\pi n t), \qquad f_n = \sin(\pi n t) \qquad\qquad (n \geq 1)$$

form an orthonormal system in E (exercise !). Fix a function $g \in E$ and put

$$a_0 = (g \mid 1), \qquad a_n = (g \mid \cos(\pi n t)), \qquad b_n = (g \mid \sin(\pi n t)) \qquad\qquad (n \geq 1).$$

Applying 4.3.6 to the orthonormal system $e_0, e_1, \ldots, e_m, f_1, \ldots, f_m$ (for fixed $m \geq 1$), we obtain

$$\frac{a_0^2}{2} + \sum_{n=1}^{m} (a_n^2 + b_n^2) \leq \|g\|^2.$$

As m is arbitrary (and the terms $a_n^2 + b_n^2$ are non-negative), it follows that

$$\frac{a_0^2}{2} + \sum_{n=1}^{\infty} (a_n^2 + b_n^2) \leq \|g\|^2 = \int_{-1}^{1} g(t)^2\, dt. \tag{4.3.7.1}$$

For example, for $g(t) = t$,

$$a_i = 0, \qquad b_n = \int_{-1}^{1} t \sin(\pi n t)\, dt = (-1)^{n-1} \frac{2}{\pi n}, \qquad \|t\|^2 = \frac{2}{3}, \tag{4.3.7.2}$$

hence (4.3.7.1) becomes

$$\sum_{n=1}^{\infty} \frac{1}{n^2} \leq \frac{\pi^2}{6}. \tag{4.3.7.3}$$

Exercise. *Let* $F = \mathrm{vect}(f_1, f_2, \ldots)$. *Show that* $g(t) = t$ *cannot be written as a sum*

$$g = y + z, \qquad y \in F, \qquad z \in F^{\perp};$$

in particular, $F + F^{\perp} \neq E$.

What is going on? One should consider suitable **infinite linear combinations**. In fact,

$$\text{“}t = \sum_{n=1}^{\infty} b_n f_n\text{”}$$

(with b_n as in (4.3.7.2)) in the sense of **convergence with respect to the norm** $\| \cdot \|$**:**

$$\lim_{m \longrightarrow \infty} \|t - \sum_{n=1}^{m} b_n f_n\| = 0,$$

which implies that (4.3.7.3) is, in fact, an equality:

$$\sum_{n=1}^{\infty} \frac{1}{n^2} = \frac{\pi^2}{6}.$$

* **This section is optional.**

For a general function $g \in C([-1,1], \mathbf{R})$,

$$\lim_{m \longrightarrow \infty} \|g - \frac{a_0}{2} - \sum_{n=1}^{m} (a_n\, e_n + b_n\, f_n)\| = 0,$$

which implies that (4.3.7.1) also becomes an equality (**Parseval's equality**):

$$\frac{a_0^2}{2} + \sum_{n=1}^{\infty} (a_n^2 + b_n^2) = \|g\|^2.$$

4.4 Isometries, orthogonal matrices

In this section, E is a Euclidean space of dimension $n \geq 1$. We are going to give an algebraic description of isometries of E (= distance preserving linear maps $E \longrightarrow E$).

(4.4.1) Change of orthonormal bases. Recall from 4.1.5 that a basis $\mathcal{B} = e_1, \ldots, e_n$ of E is **orthonormal** $\iff$ the matrix A of the scalar product in the basis $\mathcal{B}$ is equal to the identity matrix I_n. If this is the case, and if $\mathcal{B}' = e'_1, \ldots, e'_n$ is another basis of E, then the matrix A' of the scalar product in the basis $\mathcal{B}'$ is equal to

$$A' = {}^tPAP = {}^tPI_nP = {}^tPP,$$

where $P \in M_n(\mathbf{R})$ is the (invertible) matrix of change of basis from $\mathcal{B}$ to $\mathcal{B}'$ (by (2.3.6.1)). In particular,

$$\mathcal{B}' \text{ is also orthonormal} \quad \iff \quad {}^tPP = I_n. \tag{4.4.1.1}$$

(4.4.2) Definition. *A matrix $P \in M_n(\mathbf{R})$ is* **orthogonal** *if ${}^tPP = I_n$ (which implies that $\det(P)^2 = 1$, hence $\det(P) = \pm 1$).*

(4.4.3) Reformulation: (1) If $v_1, \ldots, v_n \in \mathbf{R}^n$ are the columns of a matrix $P \in M_n(\mathbf{R})$, then ${}^tv_1, \ldots, {}^tv_n$ are the rows of ${}^tP$, and the entries of the matrix $Q = {}^tPP$ are equal to the scalar products

$$Q_{ij} = (v_i \mid v_j).$$

In particular,

P is **orthogonal** $\iff$ $Q = I_n$ $\iff$ the columns $v_1, \ldots, v_n$ form an **orthonormal system** in $\mathbf{R}^n$
$\iff$ the columns $v_1, \ldots, v_n$ form an **orthonormal basis** of $\mathbf{R}^n$.

(2) According to (4.4.1.1), the matrix of change of basis between two orthonormal bases is always orthogonal.

(4.4.4) Proposition-Definition. *A linear map $u : E \longrightarrow E$ satisfying the following equivalent conditions is called* **an isometry of** *E:*
(1) $\forall x, y \in E \qquad (u(x) \mid u(y)) = (x \mid y)$.
(2) $\forall x \in E \qquad \|u(x)\| = \|x\|$.
(3) $\forall$ *orthonormal basis $e_1, \ldots, e_n$ of E, $u(e_1), \ldots, u(e_n)$ is also an orthonormal basis of E.*
(3') $\exists$ *orthonormal basis $e_1, \ldots, e_n$ of E such that $u(e_1), \ldots, u(e_n)$ is also an orthonormal basis of E.*
(4) $\forall$ *orthonormal basis $e_1, \ldots, e_n$ of E, the matrix U of u in the basis $\{e_i\}$ is orthogonal: ${}^tUU = I_n$.*
(4') $\exists$ *orthonormal basis $e_1, \ldots, e_n$ of E such that the matrix U of u in the basis $\{e_i\}$ is orthogonal: ${}^tUU = I_n$.*
[In particular, isometries of $\mathbf{R}^n$ (equipped with the standard Euclidean scalar product) are the linear maps $X \mapsto UX$, where $U \in M_n(\mathbf{R})$ is an orthogonal matrix.]

Proof. We must show that the conditions are equivalent. The implications (3) $\Longrightarrow$ (3') and (4) $\Longrightarrow$ (4') are automatic.
(1) $\Longrightarrow$ (2): If (1) holds, then $\|u(x)\|^2 = (u(x) \mid u(x)) \overset{(1)}{=} (x \mid x) = \|x\|^2$.

(2) $\Longrightarrow$ (1): If (2) holds, then

$$2(u(x) \mid u(y)) = \|u(x)+u(y)\|^2 - \|u(x)\|^2 - \|u(y)\|^2 = \|u(x+y)\|^2 - \|u(x)\|^2 - \|u(y)\|^2 \overset{(2)}{=} \\ = \|x+y\|^2 - \|x\|^2 - \|y\|^2 = 2(x \mid y).$$

(1) $\Longrightarrow$ (3): If (1) holds, then the condition $(e_i \mid e_j) = \delta_{ij}$ implies that $(u(e_i) \mid u(e_j)) = (e_i \mid e_j) = \delta_{ij}$.
(3') $\Longrightarrow$ (1): If (3') holds, then $(e_i \mid e_j) = (u(e_i) \mid u(e_j)) = \delta_{ij}$ for all $i, j = 1, \ldots, n$. If $x = \sum_{i=1}^n x_i e_i$, $y = \sum_{j=1}^n y_j e_j$ are arbitrary vectors in E, then

$$(u(x) \mid u(y)) = \left(\sum_{i=1}^n x_i u(e_i) \,\middle|\, \sum_{j=1}^n y_j u(e_j) \right) = \sum_{i,j=1}^n x_i y_j \, (u(e_i) \mid u(e_j)) = \sum_{i=1}^n x_i y_i = (x \mid y).$$

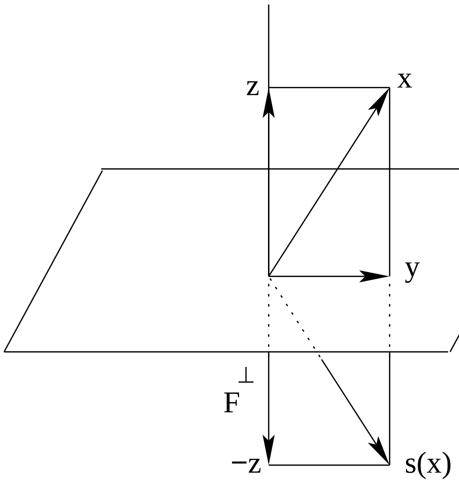
(4') $\Longrightarrow$ (1) $\Longrightarrow$ (4): Let $\mathcal{B} = e_1, \ldots, e_n$ be an orthonormal basis of E. Associating to $x = \sum_{i=1}^n x_i e_i \in E$ the column vector $X = {}^t(x_1, \ldots, x_n) \in \mathbf{R}^n$ (and similarly for y), the map u (resp., the scalar product) is written in the matrix form $X \mapsto UX$ (resp., $(x \mid y) = {}^tXY$), where $U \in M_n(\mathbf{R})$ is the matrix of u in the basis $\mathcal{B}$. The desired implications (4') $\Longrightarrow$ (1) $\Longrightarrow$ (4) then follow from the formula

$$(u(x) \mid u(y)) = {}^t(UX)\, UY = {}^tX\, {}^tUUY.$$

(4.4.5) Example (orthogonal symmetries): (1) For each vector subspace $F \subset E$, the orthogonal decomposition $E = F \perp F^\perp$ from 4.3.3 defines a linear map

$$\begin{aligned} s = s_F : E &\longrightarrow E \\ y + z &\mapsto y - z \end{aligned} \qquad\qquad (y \in F,\ z \in F^\perp),$$

called **the orthogonal symmetry with respect to** F.



This map is an isometry, since

$$(x \mid x') = (y + z \mid y' + z') = (y \mid y') + (z \mid z') + (y \mid z') + (z \mid y') = (y \mid y') + (z \mid z')$$
$$(s(x) \mid s(x')) = (y - z \mid y' - z') = (y \mid y') + (z \mid z') - (y \mid z') - (z \mid y') = (y \mid y') + (z \mid z')$$

for all $y, y' \in F$, $z, z' \in F^\perp$ and $x = y + z$, $x' = y' + z'$.
(2) The subspaces $F, F^\perp \subset E$ are equal to

$$F = \{x \in E \mid s(x) = x\} = \mathrm{Ker}(s - \mathrm{Id}), \qquad F^\perp = \{x \in E \mid s(x) = -x\} = \mathrm{Ker}(s + \mathrm{Id}).$$

(3) Relation to orthogonal projections: using the notation from 4.3.5, we have

$$s_F(x) = y - z = 2y - (y+z) = 2p_F(x) - x = (y+z) - 2z = x - 2p_{F^\perp}(x).$$

(4) Matrix representation: let $e_1, \ldots, e_m$ (resp., $e_{m+1}, \ldots, e_n$) be any orthonormal basis of F (resp., of $F^\perp$); then $\mathcal{B} = e_1, \ldots, e_n$ is an orthonormal basis of E. As

$$s(e_i) = \begin{cases} e_i, & i \le m \\ -e_i, & i > m, \end{cases}$$

the matrix of s in the basis $\mathcal{B}$ is equal to

$$\begin{pmatrix} I_m & 0 \\ 0 & -I_{n-m} \end{pmatrix}.$$

(5) **Reflections:** if $\dim(F^\perp) = 1$ ($\iff \dim(F) = n-1$), then we say that s_F is a **reflection** with respect to the hyperplane F. If $u \in F^\perp$, $u \ne \vec{0}$, then $e_n := u/\|u\|$ is an orthonormal basis of the line $F^\perp$. The formula (4.3.5.1) (for $F^\perp$ instead of F) reads as follows:

$$p_{F^\perp}(x) = (x \mid e_n)e_n = \frac{(x \mid u)u}{(u \mid u)},$$

hence

$$s_F(x) = x - 2p_{F^\perp}(x) = x - \frac{2(x \mid u)u}{(u \mid u)}.$$

If $e_1, \ldots, e_{n-1}$ is any orthonormal basis of F, then the matrix of s in the (orthonormal) basis $e_1, \ldots, e_n$ of E is equal to

$$\begin{pmatrix} I_{n-1} & 0 \\ 0 & -1 \end{pmatrix};$$

in particular, $\det(s_F) = -1$.

(4.4.6) Exercise. *Describe geometrically orthogonal symmetries in* $\mathbf{R}^3$ *(for all possible dimensions* $\dim(F) = 0, 1, 2, 3$ *of* $F \subset \mathbf{R}^3$*).*

(4.4.7) Example. Let $\mathbf{R}^3$ be equipped with the standard Euclidean scalar product. Let $F \subset \mathbf{R}^3$ be the plane

$$F : x_1 + 2x_2 - 3x_3 = 0.$$

We are going to compute $p_F(x)$ and $s_F(x)$ (for a general vector $x \in \mathbf{R}^3$) and determine the matrix P (resp., S) of $p_F : \mathbf{R}^3 \longrightarrow F \subset \mathbf{R}^3$ (resp., of $s_F : \mathbf{R}^3 \longrightarrow \mathbf{R}^3$) in the canonical basis of $\mathbf{R}^3$.

The main idea is to compute first $p_{F^\perp}(x)$. The line $F^\perp$ is generated by the vector

$$u = \begin{pmatrix} 1 \\ 2 \\ -3 \end{pmatrix}.$$

It follows from 4.4.5(3),(5) that

$$p_F(x) = x - p_{F^\perp}(x), \qquad s_F(x) = x - 2p_{F^\perp}(x)$$

and

$$p_{F^\perp}(x) = \frac{(x \mid u)u}{(u \mid u)} = \frac{x_1 + 2x_2 - 3x_3}{14} \begin{pmatrix} 1 \\ 2 \\ -3 \end{pmatrix},$$

which implies that

$$p_F(x) = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} - \frac{x_1 + 2x_2 - 3x_3}{14} \begin{pmatrix} 1 \\ 2 \\ -3 \end{pmatrix} = \frac{1}{14} \begin{pmatrix} 13x_1 - 2x_2 + 3x_3 \\ -2x_1 + 10x_2 + 6x_3 \\ 3x_1 + 6x_2 + 5x_3 \end{pmatrix} = \frac{1}{14} \begin{pmatrix} 13 & -2 & 3 \\ -2 & 10 & 6 \\ 3 & 6 & 5 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix}$$

$$s_F(x) = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} - \frac{x_1 + 2x_2 - 3x_3}{7} \begin{pmatrix} 1 \\ 2 \\ -3 \end{pmatrix} = \frac{1}{7} \begin{pmatrix} 6x_1 - 2x_2 + 3x_3 \\ -2x_1 + 3x_2 + 6x_3 \\ 3x_1 + 6x_2 - 2x_3 \end{pmatrix} = \frac{1}{7} \begin{pmatrix} 6 & -2 & 3 \\ -2 & 3 & 6 \\ 3 & 6 & -2 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix},$$

hence

$$P = \frac{1}{14} \begin{pmatrix} 13 & -2 & 3 \\ -2 & 10 & 6 \\ 3 & 6 & 5 \end{pmatrix}, \qquad S = \frac{1}{7} \begin{pmatrix} 6 & -2 & 3 \\ -2 & 3 & 6 \\ 3 & 6 & -2 \end{pmatrix}.$$

(4.4.8) Isometries - matrix formulation. If we fix an arbitrary orthonormal basis $e_1, \ldots, e_n$ of E, then E is identified with $\mathbf{R}^n$ and the scalar product with the standard Euclidean scalar product. Moreover, the isometries of E are then identified with isometries of $\mathbf{R}^n$, i.e. with maps $X \mapsto UX$, where $U \in M_n(\mathbf{R})$ is an orthogonal matrix (by 4.4.4).

Notation: For each $n \geq 1$, denote

$$\begin{aligned} O(n) &= \{U \in M_n(\mathbf{R}) \mid {}^tUU = I_n\} = \{\text{isometries of } \mathbf{R}^n\} = O^+(n) \cup O^-(n) \\ SO(n) = O^+(n) &= \{U \in O(n) \mid \det(U) = +1\} \\ O^-(n) &= \{U \in O(n) \mid \det(U) = -1\} \end{aligned}$$

(terminology: $O(n)$ (resp., $SO(n) = O^+(n)$) is the **orthogonal group** (resp., the **special orthogonal group**) of $\mathbf{R}^n$).

(4.4.9) Examples: (1) $O(1) = \{\pm 1\}$, $\quad SO(1) = \{1\}$.

(2) We shall see in 4.5.5-6 below that

$$\begin{aligned} SO(2) = O^+(2) &= \{\text{rotations in } \mathbf{R}^2 \text{ with centre at the origin}\} \\ O^-(2) &= \{\text{reflections in } \mathbf{R}^2\}. \end{aligned}$$

(3) We shall see in 4.6.5 below that

$$SO(3) = O^+(3) = \{\text{rotations in } \mathbf{R}^3 \text{ fixing the origin}\}.$$

(4.4.10) Exercise. *Let $F \subset E$ be a vector subspace of a Euclidean space E. Show that the matrix of $s_F : E \longrightarrow E$ (resp., of $p_F : E \longrightarrow F \subset E$) in any orthonormal basis of E is symmetric.*

(4.4.11) Exercise. *Let E be an $\mathbf{R}$-vector space and $u : E \longrightarrow E$ a linear map such that $u^2 = \mathrm{Id}$.*

(1) *Show that $E = E_+ \oplus E_-$, where $E_\pm = \{x \in E \mid u(x) = \pm x\}$.*

(2) *If E is a Euclidean space, show that*

$$E_+ \perp E_- \iff u \text{ is an isometry.}$$

If this is the case, show that $u = s_{E_+}$. Deduce that an isometry $f : E \longrightarrow E$ is an orthogonal symmetry $\iff$ $f^2 = \mathrm{Id}$.

(4.4.12) Exercise. *In this exercise, $\mathbf{R}^n$ is equipped with the standard Euclidean scalar product.*
(1) *Show that a matrix $S \in M_n(\mathbf{R})$ represents an orthogonal symmetry of $\mathbf{R}^n$ $\iff$ ${}^tS = S$ and $S^2 = I$.*
(2) *Show that a matrix $P \in M_n(\mathbf{R})$ represents an orthogonal projection on a subspace of $\mathbf{R}^n$ $\iff$ ${}^tP = P$ and $P^2 = P$.*

4.5 Isometries of $\mathbf{R}^2$

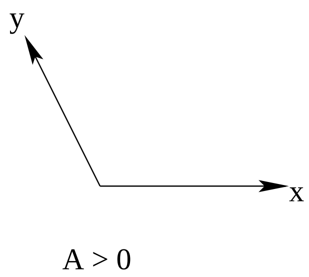
In this section, $E = \mathbf{R}^2$ is equipped with the standard Euclidean scalar product $(x \mid y) = x_1y_1 + x_2y_2$.

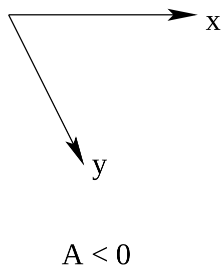
(4.5.1) Oriented angles in $\mathbf{R}^2$. Let $x = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$ and $y = \begin{pmatrix} y_1 \\ y_2 \end{pmatrix}$ be non-zero vectors in $\mathbf{R}^2$. The general definition (see (4.2.8.1)) of the (non-oriented) angle $\beta \in [0, \pi]$ of x and y (which does not depend on the order of x and y) can be refined as follows. We set

$$A = \begin{vmatrix} x_1 & y_1 \\ x_2 & y_2 \end{vmatrix}$$

and define **the oriented angle between x and y** (in this order) as

$$\widehat{xy} = \gamma = \begin{cases} \beta, & \text{if } A \geq 0 \quad (\gamma \in [0, \pi]) \\ -\beta, & \text{if } A < 0 \quad (\gamma \in (-\pi, 0)) \end{cases}$$





From an abstract point of view, it is more convenient to consider (the size of) an oriented angle not as a number contained in the interval $(-\pi, \pi]$, but a "residue class of real numbers modulo 2π". This means that oriented angles are represented by arbitrary real numbers, with two real numbers determining the same oriented angle $\iff$ their difference is an integral multiple of 2π (for example, -5π and π represent the same oriented angle). Each oriented angle has a unique representative contained in the interval $(-\pi, \pi]$.

(4.5.2) Geometric description of isometries of $\mathbf{R}^2$

Rotations (with centre at the origin):

For each oriented angle α, the (anti-clockwise) rotation with centre at the origin and angle α is the (unique) isometry $r : \mathbf{R}^2 \longrightarrow \mathbf{R}^2$ such that

$$(\forall x \in \mathbf{R}^2,\ x \neq \vec{0}) \qquad \text{the oriented angle between } x \text{ and } r(x) \text{ is equal to } \alpha.$$

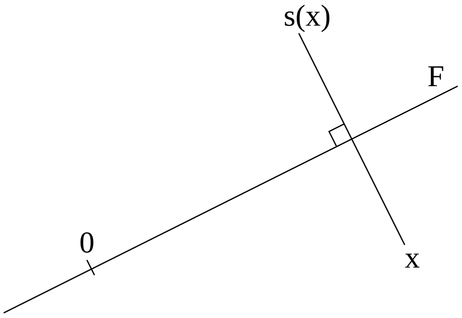
Reflections:

For each line F passing through the origin, the reflection with respect to F (see 4.4.5(5)) is an isometry $s = s_F : \mathbf{R}^2 \longrightarrow \mathbf{R}^2$ satisfying

$$\forall x \in \mathbf{R}^2 \quad s(s(x)) = x, \qquad s \circ s = \mathrm{Id}.$$

The line F (= **the axis of** s") is equal to

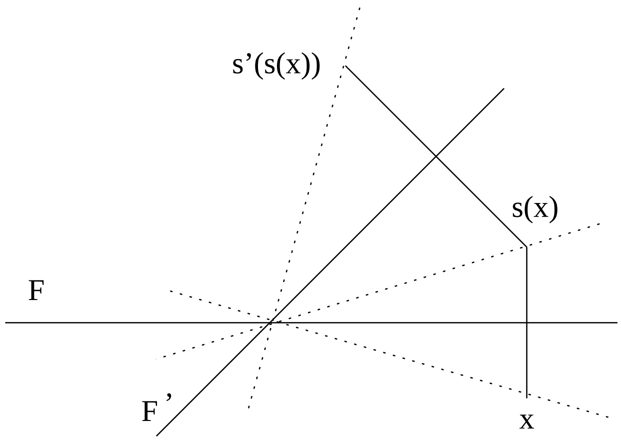
$$F = \{x \in \mathbf{R}^2 \mid s(x) = x\} = \mathrm{Ker}(s - \mathrm{Id}).$$



(4.5.3) Composition of two reflections = rotation
Let $F, F' \subset \mathbf{R}^2$ be lines passing through the origin; denote by $s = s_F$, $s' = s_{F'}$ the corresponding reflections. Fix non-zero vectors $u \in F$ and $u' \in F'$. If α is the oriented angle between u and u', then

$$s' \circ s = r$$

is the rotation around the origin with (oriented) angle 2α.



Similarly,

$$s \circ s' = s^{-1} \circ (s')^{-1} = (s' \circ s)^{-1} = r^{-1}$$

is the rotation around the origin with (oriented) angle -2α.

(4.5.4) Proposition. *We have*

$$O(2) = \left\{ \begin{pmatrix} a & -\lambda c \\ c & \lambda a \end{pmatrix} \,\middle|\, \lambda = \pm 1,\, a, c \in \mathbf{R},\, a^2 + c^2 = 1 \right\}, \qquad \det \begin{pmatrix} a & -\lambda c \\ c & \lambda a \end{pmatrix} = \lambda.$$

Proof. Let $a, b, c, d \in \mathbf{R}$. We have

$$\begin{aligned} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in O(2) &\iff \begin{pmatrix} a \\ c \end{pmatrix}, \begin{pmatrix} b \\ d \end{pmatrix} \text{ is an orthonormal basis of } \mathbf{R}^2 \\ &\iff a^2 + c^2 = b^2 + d^2 = 1,\ \begin{pmatrix} b \\ d \end{pmatrix} \in \left(\mathrm{vect}\left(\begin{pmatrix} a \\ c \end{pmatrix}\right)\right)^{\perp} = \mathrm{vect}\left(\begin{pmatrix} -c \\ a \end{pmatrix}\right) \\ &\iff a^2 + c^2 = 1,\ \begin{pmatrix} b \\ d \end{pmatrix} = \lambda \begin{pmatrix} -c \\ a \end{pmatrix},\ \lambda^2 = 1. \end{aligned}$$

(4.5.5) Proposition. (1) *We have*

$$SO(2) = O^+(2) = \left\{ \begin{pmatrix} a & -c \\ c & a \end{pmatrix} \,\middle|\, a, c \in \mathbf{R},\ a^2 + c^2 = 1 \right\} = \left\{ R(\alpha) = \begin{pmatrix} \cos(\alpha) & -\sin(\alpha) \\ \sin(\alpha) & \cos(\alpha) \end{pmatrix} \,\middle|\, \alpha \in \mathbf{R} \right\}.$$

(2) *The isometry corresponding to $R(\alpha)$ is the rotation with centre at the origin and (oriented) angle α.*

Proof. (1) The first equality follows from 4.5.4; the second from the fact that the points of the circle defined by the equation $a^2 + c^2 = 1$ are parametrised by $a = \cos(\alpha)$, $c = \sin(\alpha)$ ($\alpha \in \mathbf{R}$).
(2) As $\sin(\alpha + 2\pi) = \sin(\alpha)$ (and similarly for cos), the matrix $R(\alpha)$ depends only on the "residue class of α modulo 2π" in the sense of 4.5.1, hence we can assume that $\alpha \in (-\pi, \pi]$.
For each vector $x = \begin{pmatrix} u \\ v \end{pmatrix} \in \mathbf{R}^2$, we have $\|R(\alpha)x\| = \|x\| = \sqrt{u^2 + v^2}$ (since the multiplication by $R(\alpha)$ is an isometry). Let $\beta \in [0, \pi]$ be the (non-oriented) angle between x and $R(\alpha)x$ (in the sense of 4.2.8); as

$$(x \mid R(\alpha)x) = \left(\begin{pmatrix} u \\ v \end{pmatrix} \,\middle|\, \begin{pmatrix} au - cv \\ cu + av \end{pmatrix} \right) = u(au - cv) + v(cu + av) = a(u^2 + v^2),$$

we have

$$\cos(\beta) = \frac{(x \mid R(\alpha))}{\|x\| \|R(\alpha)x\|} = a = \cos(\alpha),$$

hence $\alpha = \pm\beta$. On the other hand, the oriented angle between x and $R(\alpha)x$ is equal to

$$\gamma = \begin{cases} \beta, & \text{if } A \geq 0 \\ -\beta, & \text{if } A < 0, \end{cases}$$

where

$$A = \begin{vmatrix} u & au - cv \\ v & cu + av \end{vmatrix} = c(u^2 + v^2) = (u^2 + v^2)\sin(\alpha);$$

thus

$$\begin{aligned} A \geq 0 \iff \sin(\alpha) \geq 0 \iff \alpha \in [0, \pi] \iff \alpha = \beta \\ A < 0 \iff \sin(\alpha) < 0 \iff \alpha \in (-\pi, 0) \iff \alpha = -\beta, \end{aligned}$$

hence $\gamma = \alpha$, as claimed.

(4.5.6) Proposition. *We have*

$$O^-(2) = \left\{ \begin{pmatrix} a & c \\ c & -a \end{pmatrix} \,\middle|\, a, c \in \mathbf{R},\ a^2 + c^2 = 1 \right\} = \left\{ g \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \,\middle|\, g \in O^+(2) \right\} = \{\text{reflections in } \mathbf{R}^2\}.$$

Proof. The first two equalities follow from 4.5.4-5. We know that $\{\text{reflections in } \mathbf{R}^2\} \subset O^-(2)$, by 4.4.5(5). Conversely, the linear map

$$s : \mathbf{R}^2 \longrightarrow \mathbf{R}^2, \qquad s : \begin{pmatrix} u \\ v \end{pmatrix} \mapsto \begin{pmatrix} u \\ -v \end{pmatrix},$$

represented by the matrix

$$S = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \in O^-(2),$$

is a reflection with respect to the horizontal axis $F = \mathrm{vect}(u)$, $u = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$. Given a matrix

$$g = \begin{pmatrix} a & c \\ c & -a \end{pmatrix} \in O^-(2) \qquad\qquad (a^2 + c^2 = 1),$$

we have

$$g = \begin{pmatrix} a & -c \\ c & a \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = R(\alpha)S.$$

Let $u' \in \mathbf{R}^2$ be any non-zero vector such that the oriented angle between u and u' is equal to $\alpha/2$. If we denote by $S' \in O^-(2)$ the matrix representing the reflection with respect to $F' = \mathrm{vect}(u')$, then $S'S = R(\alpha)$, by 4.5.3; thus

$$g = R(\alpha)S = S'SS = S'$$

represents a reflection, hence $\{\text{reflections in } \mathbf{R}^2\} = O^-(2)$.

(4.5.7) Formulaire. For simplicity, we do not distinguish between a matrix $g \in O(2)$ and the isometry of $\mathbf{R}^2$ represented by g.

(1) $R(\alpha)R(\beta) = R(\alpha+\beta) = R(\beta)R(\alpha)$, $R(\alpha)^{-1} = R(-\alpha)$.

(2) For each reflection $s \in O^-(2)$ and each rotation $r = R(\alpha) \in O^+(2)$, we have $s^2 = I$ ($\iff s^{-1} = s$) and

$$srs^{-1} = sR(\alpha)s = R(-\alpha) = R(\alpha)^{-1} = r^{-1}.$$

This can be seen directly by drawing a picture (exercise !), or by writing

$$s = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} R(\beta), \qquad sR(\alpha)s^{-1} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} R(\beta)R(\alpha)R(-\beta) \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} =$$
$$= \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} R(\alpha) \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = R(-\alpha) = R(\alpha)^{-1}.$$

(3) The eigenvalues of the rotation matrix $R(\alpha)$ are equal to $\cos(\alpha) \pm i\sin(\alpha) = e^{\pm i\alpha}$ (see 4.5.9(5) below for a more general statement).

(4) The eigenvalues of any reflection $s \in O^-(2)$ are equal to ± 1; the axis of s is equal to $\mathrm{Ker}(s - I)$ (by 4.4.5(5) and 4.4.5(2)).

(4.5.8) Complex formulas. There is a natural ($\mathbf{R}$-linear) identification of vectors in $\mathbf{R}^2$ with complex numbers, given by the formula

$$\mathbf{R}^2 \longrightarrow \mathbf{C}, \qquad \begin{pmatrix} x \\ y \end{pmatrix} \mapsto x + iy. \tag{4.5.8.1}$$

For each complex number $w = u + iv$, the multiplication by w

$$z = x + iy \mapsto wz = (u+iv)(x+iy) = (ux - vy) + i(vx + uy)$$

defines, via the identification (4.5.8.1), an $\mathbf{R}$-linear map $\mathbf{R}^2 \longrightarrow \mathbf{R}^2$

$$\begin{pmatrix} x \\ y \end{pmatrix} \mapsto \begin{pmatrix} ux - vy \\ vx + uy \end{pmatrix} = \begin{pmatrix} u & -v \\ v & u \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix};$$

let

$$M(w) = M(u+iv) = \begin{pmatrix} u & -v \\ v & u \end{pmatrix} \in M_2(\mathbf{R}) \tag{4.5.8.2}$$

be the matrix representing this multiplication.

(4.5.9) Properties of the matrices $M(w)$

(1) $M(w+w') = M(w) + M(w')$ (as $(w+w')z = wz + w'z$);
(2) $M(ww') = M(w)M(w')$ (as $(ww')z = w(w'z)$);
(3) $\forall w \in \mathbf{R} \quad M(w) = \begin{pmatrix} w & 0 \\ 0 & w \end{pmatrix}$;
(4) If $\alpha \in \mathbf{R}$ and $w = e^{i\alpha} = \cos(\alpha) + i\sin(\alpha)$, then $M(e^{i\alpha}) = \begin{pmatrix} \cos(\alpha) & -\sin(\alpha) \\ \sin(\alpha) & \cos(\alpha) \end{pmatrix} = R(\alpha)$;
(5) The eigenvalues of $M(u+iv)$ are the roots of the polynomial $\lambda^2 - 2u\lambda + (u^2+v^2) = 0$, namely $\lambda_{1,2} = u \pm iv$ (in particular, the eigenvalues of $R(\alpha)$ are $\cos(\alpha) \pm i\sin(\alpha) = e^{\pm i\alpha}$).

(4.5.10) Complex numbers and isometries of $\mathbf{R}^2$. The discussion in 4.5.8-9, combined with 4.5.5-6, implies that the isometries of $\mathbf{R}^2$ can be written in the following complex form (using the identification (4.5.8.1)):

$$\text{rotations}: \quad z \mapsto e^{i\alpha}z; \qquad \text{reflections}: \quad z \mapsto e^{i\alpha}\overline{z}. \tag{4.5.10.1}$$

The second formula follows from the fact that the action of the complex conjugation $z = x+iy \mapsto \overline{z} = x - iy$ corresponds to the action of the matrix $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$.

(4.5.11) Exercise. (1) *Which among the following matrices*

$$\frac{1}{2}\begin{pmatrix} \sqrt{3} & 1 \\ 1 & -\sqrt{3} \end{pmatrix}, \qquad \frac{1}{2}\begin{pmatrix} \sqrt{3} & -1 \\ 1 & -\sqrt{3} \end{pmatrix}, \qquad \frac{1}{2}\begin{pmatrix} \sqrt{3} & -1 \\ -1 & -\sqrt{3} \end{pmatrix}, \qquad \frac{1}{2}\begin{pmatrix} \sqrt{3} & -1 \\ -1 & \sqrt{3} \end{pmatrix}$$

are orthogonal?
(2) *For each orthogonal matrix from (1), describe geometrically the corresponding isometry of* $\mathbf{R}^2$.
(3) *Write each isometry from (2) in the complex form (4.5.10.1).*

(4.5.12) Exercise. *Determine the eigenvectors of the matrix* $M(u+iv)$. *Is this matrix diagonalisable?*

4.6 Isometries of $\mathbf{R}^n$

(4.6.1) Proposition. *Every eigenvalue* $\lambda \in \mathbf{C}$ *of an orthogonal matrix* $U \in O(n)$ *satisfies* $|\lambda| = 1$.

Proof. See 6.5.6 below.

(4.6.2) Theorem. *For every isometry* $u : E \longrightarrow E$ *of a Euclidean space* E *of dimension* $\dim(E) = n$ *there exists an* **orthonormal** *basis in which the matrix of* u *is equal to*

$$\begin{pmatrix} I_a & 0 & 0 & \cdots & 0 \\ 0 & -I_b & 0 & \cdots & 0 \\ 0 & 0 & R(\alpha_1) & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & R(\alpha_m) \end{pmatrix}$$

where $a+b+2m=n$ and α_j is not an integral multiple of π. In particular, $\det(u)=(-1)^b$.
Matrix formulation: *For every* **orthogonal** *matrix $U \in O(n)$ there exists an* **orthogonal** *matrix $P \in O(n)$ such that $P^{-1}UP$ is of the above form.*

(4.6.3) Theorem. *Every* **orthogonal** *matrix $U \in O(n)$ can be written as a product $U = s_1 \cdots s_r$ of $r \le n$ reflections s_j.*

(4.6.4) Example ($n=2$): If $U \in O^-(2)$, then $U = s_1$ is a reflection. If $U \in O^+(2)$, then U is a rotation, hence a product of two reflections $U = s_1 s_2$.
(4.6.5) Example ($n=3$): If $U \in O(3)$, then there exists a change of orthonormal basis (given by a matrix $P \in O(3)$) such that $P^{-1}UP$ belongs to precisely one of the following four types of matrices:

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \qquad \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix}, \qquad \begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos(\beta) & -\sin(\beta) \\ 0 & \sin(\beta) & \cos(\beta) \end{pmatrix}, \qquad \begin{pmatrix} -1 & 0 & 0 \\ 0 & \cos(\beta) & -\sin(\beta) \\ 0 & \sin(\beta) & \cos(\beta) \end{pmatrix}$$

(with β not being an integral multiple of 2π). Geometrically, the four types can be described as follows:

(0) The identity map.
(1) A reflection with respect to the plane $\mathrm{Ker}(U - I_3)$.
(2) A rotation with axis $\mathrm{Ker}(U - I_3)$ and angle $\beta \neq 0$ such that $\mathrm{Tr}(U) = 1 + 2\cos(\beta)$.
(3) A product of three reflections (which itself is not a reflection).

Moreover, U belongs to the type $n = 0,1,2,3 \iff \mathrm{rk}(U - I_3) = n \iff U$ is a product of n, but not fewer, reflections.

(4.6.6) Exercise. (1) *Verify that the following matrices are orthogonal:*

$$\frac{1}{3}\begin{pmatrix} 1 & -2 & -2 \\ -2 & 1 & -2 \\ -2 & -2 & 1 \end{pmatrix}, \qquad \frac{1}{3}\begin{pmatrix} 1 & -2 & 2 \\ -2 & 1 & 2 \\ -2 & -2 & -1 \end{pmatrix}, \qquad \frac{1}{3}\begin{pmatrix} 1 & 2 & 2 \\ -2 & -1 & 2 \\ -2 & 2 & -1 \end{pmatrix}, \qquad \frac{1}{3}\begin{pmatrix} -1 & 2 & 2 \\ 2 & -1 & 2 \\ 2 & 2 & -1 \end{pmatrix}.$$

(2) *For each matrix from (1), describe geometrically the corresponding isometry of $\mathbf{R}^3$ (according to the discussion in 4.6.5).*

(4.6.7) Exercise. *Let $U \in O(3)$.* (1) *Show that $\lambda = \det(U)$ is an eigenvalue of U.*
(2) *Let $x \in \mathbf{R}^3$ be an eigenvector of U corresponding to the eigenvalue λ. Show that the plane $x^\perp$ satisfies $U(x^\perp) = x^\perp$.*
(3) *Deduce from (2) the statement of 4.6.5.*

5. “Difficult” diagonalisation of real quadratic forms

5.1 The main result

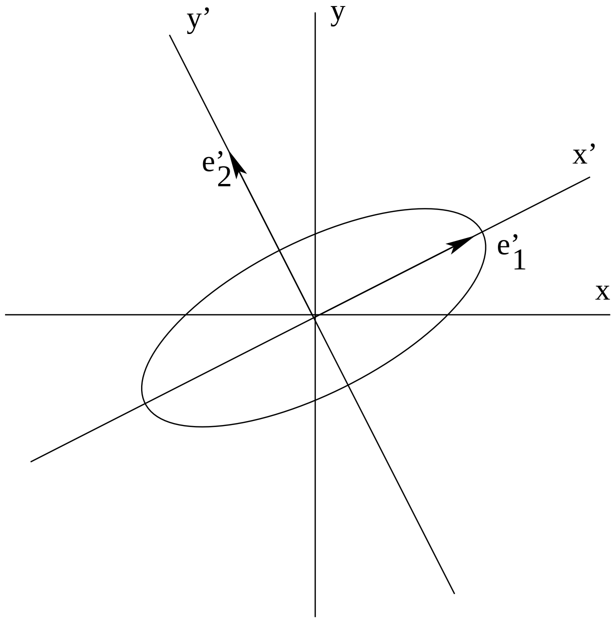
(5.1.1) Example: The quadratic form

$$q : \mathbf{R}^2 \longrightarrow \mathbf{R}, \qquad q\left(\begin{pmatrix} x \\ y \end{pmatrix}\right) = 2x^2 - 4xy + 5y^2$$

is positive definite; the equation

$$q = 2x^2 - 4xy + 5y^2 = 1 \tag{5.1.1.1}$$

defines an **ellipse:**



We would like to find a **rotation** $P \in O^+(2)$ diagonalising the quadratic form q, i.e. transforming the equation (5.1.1.1) into a diagonal form

$$d_1 x'^2 + d_2 y'^2 = 1, \qquad \begin{pmatrix} x \\ y \end{pmatrix} = P \begin{pmatrix} x' \\ y' \end{pmatrix}.$$

The matrix of q in the canonical basis $e_1 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$, $e_2 = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$ is equal to $A = \begin{pmatrix} 2 & -2 \\ -2 & 5 \end{pmatrix}$. We are looking for a matrix $P \in M_2(\mathbf{R})$ such that

$$^tPP = I_2, \qquad \det(P) = 1 \tag{5.1.1.2}$$

$$^tPAP = \begin{pmatrix} d_1 & 0 \\ 0 & d_2 \end{pmatrix} = D. \tag{5.1.1.3}$$

As $^tP = P^{-1}$, the condition (5.1.1.3) is equivalent to

$$P^{-1}AP = D \iff (Ae'_1 \mid Ae'_2) = AP = PD = (d_1e'_1 \mid d_2e'_2), \tag{5.1.1.4}$$

where we have denoted by e'_1, e'_2 the columns of the matrix $P = (e'_1 \mid e'_2)$. In other words, (5.1.1.4) says that e'_1, e'_2 are **eigenvectors** of A, and d_1, d_2 are the corresponding **eigenvalues** (see 1.6.6). The first of the conditions (5.1.1.2) states that the vectors e'_1, e'_2 form an **orthonormal basis** of $\mathbf{R}^2$.

Let us compute the eigenvalues and eigenvectors of A. The characteristic polynomial

$$P_A(t) = t^2 - \mathrm{Tr}(A)t + \det(A) = t^2 - 7t + 6 = (t-1)(t-6)$$

has roots $\lambda_1 = 1$ and $\lambda_2 = 6$. Solving the equations

$$(A - I)e'_1 = 0, \qquad \|e'_1\| = 1, \qquad (A - 6I)e'_2 = 0, \qquad \|e'_2\| = 1,$$

we obtain

$$e'_1 = \pm\frac{1}{\sqrt{5}}\begin{pmatrix} 2 \\ 1 \end{pmatrix}, \qquad e'_2 = \pm\frac{1}{\sqrt{5}}\begin{pmatrix} -1 \\ 2 \end{pmatrix}.$$

These vectors satisfy $e'_1 \perp e'_2$ (see 6.5.6(2) below), hence all possible choices of signs give rise to an **orthogonal** matrix $P \in O(2)$. If we choose the signs so that $\det(P) = 1$, for example, by putting

$$P = (e'_1 \mid e'_2) = \frac{1}{\sqrt{5}}\begin{pmatrix} 2 & -1 \\ 1 & 2 \end{pmatrix},$$

then $P \in O^+(2)$ will define a **rotation** satisfying

$${}^tPAP = P^{-1}AP = \begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 6 \end{pmatrix}.$$

We can verify this by brute force, writing

$$\begin{pmatrix} x \\ y \end{pmatrix} = P\begin{pmatrix} x' \\ y' \end{pmatrix} = x'e'_1 + y'e'_2, \qquad x = \frac{2x' - y'}{\sqrt{5}}, \qquad y = \frac{x' + 2y'}{\sqrt{5}}$$

$$2x^2 - 4xy + 5y^2 = \frac{2(4x'^2 - 4x'y' + y'^2) - 4(2x' - y')(x' + 2y') + 5(x'^2 + 4x'y' + 4y'^2)}{5} = x'^2 + 6y'^2$$

The general statement is the following.

(5.1.2) Theorem. *For every* **symmetric real** *matrix $A = {}^tA \in M_n(\mathbf{R})$ there exist n eigenvectors $e'_1, \ldots, e'_n \in \mathbf{R}^n$ of A forming an* **orthonormal basis** *of $\mathbf{R}^n$ (with respect to the standard Euclidean scalar product). The matrix $P = (e'_1 \mid \cdots \mid e'_n) \in M_n(\mathbf{R})$ is orthogonal (${}^tPP = I_n$) and satisfies*

$${}^tPAP = P^{-1}AP = \begin{pmatrix} \lambda_1 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & \lambda_n \end{pmatrix} \qquad (Ae'_j = \lambda_j e'_j,\ \lambda_j \in \mathbf{R}).$$

The isometry $X = PX'$ transforms the quadratic form $q(x) = {}^tXAX$ into a diagonal quadratic form

$${}^t(PX')A(PX') = {}^tX'\,{}^tPAPX' = \lambda_1 x_1'^2 + \cdots + \lambda_n x_n'^2.$$

(5.1.3) Remarks. Let $A = {}^tA \in M_n(\mathbf{R})$ be a symmetric real matrix.

(1) We can always ensure that P in Theorem 5.1.2 satisfies $\det(P) = 1$ ($\iff P \in O^+(n)$), by replacing one of the eigenvectors e'_j by $-e'_j$, if necessary.
(2) All eigenvalues of A are real (proof: 6.5.6 below).
(3) Eigenvectors of A corresponding to distinct eigenvalues are orthogonal with respect to the standard Euclidean scalar product (proof: 6.5.6 below).
(4) If the eigenvalues of A are distinct, then Theorem 5.1.2 follows from the remarks (2) and (3).
(5) In the presence of multiple eigenvalues, the remarks (2) and (3) imply that Theorem 5.1.2 is equivalent to the diagonalisability of A (in that case one must fix an orthogonal basis of each eigenspace $\mathrm{Ker}(A - \lambda_i I)$, and then take their union).
(6) In order to prove Theorem 5.1.2, we reformulate it in an abstract language (see 5.2.4 below).

(5.1.4) Central quadrics. In the situation of 5.1.2, the equation

$$Q : q(x) = {}^tXAX = 1$$

defines a **central quadric** $Q \subset \mathbf{R}^n$ with centre at the origin. We say that Q is **non-degenerate** if q is ($\iff \det(A) \neq 0$).

In the coordinate system $x'_1, \ldots, x'_n$ associated to the orthonormal basis $e'_1, \ldots, e'_n$ consisting of eigenvectors of A, the equation of Q simplifies to

$$Q : \lambda_1 x'^2_1 + \cdots + \lambda_n x'^2_n = 1,$$

where $\lambda_1, \ldots, \lambda_n$ are the corresponding (real) eigenvalues of A. After renumbering, we can assume that

$$\lambda_1, \ldots, \lambda_s > 0, \qquad \lambda_{s+1}, \ldots, \lambda_r < 0, \qquad \lambda_{r+1}, \ldots, \lambda_n = 0,$$

where (s, t) is the signature of the quadratic form q and $r = s + t = \mathrm{rk}(q)$. This implies that Q is obtained by translating the non-degenerate quadric

$$Q' : \lambda_1 x'^2_1 + \cdots + \lambda_r x'^2_r = 1$$

in the r-dimensional Euclidean space $F = \mathrm{vect}(e'_1, \ldots, e'_r)$ (equipped with the coordinates $x'_1, \ldots, x'_r$) in the directions of the $(n-r)$-dimensional space $F^\perp = \mathrm{vect}(e'_{r+1}, \ldots, e'_n)$.

Examples of non-degenerate central quadrics: (1) If $n = 2$, then Q is an ellipse (resp., a hyperbola) with axes $\mathrm{vect}(e'_1), \mathrm{vect}(e'_2)$, if $\lambda_1, \lambda_2 > 0$ (resp., if $\lambda_1\lambda_2 < 0$).
(2) If $n = 3$, then Q is a

$$\begin{aligned} \text{ellipsoid} \quad &\iff \quad \lambda_1, \lambda_2, \lambda_3 > 0 \\ \text{one}-\text{sheeted hyperboloid} \quad &\iff \quad \lambda_1, \lambda_2 > 0 > \lambda_3 \\ \text{two}-\text{sheeted hyperboloid} \quad &\iff \quad \lambda_1 > 0 > \lambda_2, \lambda_3 \end{aligned}$$

with axes $\mathrm{vect}(e'_1), \mathrm{vect}(e'_2), \mathrm{vect}(e'_3)$.

(5.1.5) Exercise. (1) *Find a rotation $P \in O^+(3)$ diagonalising the quadratic form $x^2 - 16xy + 8xz + y^2 + 8yz + 7z^2$ (where x, y, z are the coordinates with respect to the canonical basis of $\mathbf{R}^3$). Describe geometrically the subset of $\mathbf{R}^3$ defined by the equation*

$$x^2 - 16xy + 8xz + y^2 + 8yz + 7z^2 = 1.$$

(2) *The same for the quadratic form $4x^2 - 8xy - 2xz + 4yz$.*

5.2 Adjoint

First we need an abstract reformulation of the symmetry condition $A = {}^tA$.

(5.2.1) Example: The standard Euclidean scalar product $(x \mid y) = x_1y_1 + \cdots + x_ny_n$ on $\mathbf{R}^n$ has the following property:

$$\forall M \in M_n(\mathbf{R}) \quad \forall x, y \in \mathbf{R}^n \qquad (Mx \mid y) = {}^t(Mx)y = {}^tx\,{}^tMy = (x \mid {}^tMy).$$

The passage to the transpose matrix has the following abstract counterpart.

(5.2.2) Proposition-Definition. *Let E be a Euclidean space. For each linear map $f : E \longrightarrow E$ there exists a unique linear map ${}^tf : E \longrightarrow E$ (called* **the adjoint of** *f) satisfying*

$$\forall x, y \in E \qquad (f(x) \mid y) = (x \mid {}^tf(y)).$$

For each **orthonormal** *basis $\mathcal{B}$ of E,*

$$\text{(the matrix of } {}^tf \text{ in the basis } \mathcal{B}) = {}^t\text{(the matrix of } f \text{ in the basis } \mathcal{B}).$$

Proof. Fix an arbitrary orthonormal basis $\mathcal{B}$ of E; let $M \in M_n(\mathbf{R})$ be the matrix of f in $\mathcal{B}$. Associating to each $x \in E$ the column vector $X \in \mathbf{R}^n$ of its coordinates in $\mathcal{B}$, we have $(x \mid y) = {}^tXY$. Assume that ${}^tf$ exists; let $N \in M_n(\mathbf{R})$ be its matrix in the basis $\mathcal{B}$. Repeating the calculation from 5.2.1, we obtain

$$\forall x, y \in E \quad {}^tX\,{}^tMY = {}^t(MX)Y = (f(x) \mid y) = (x \mid {}^tf(y)) = {}^tX(NY) = {}^tXNY,$$

hence

$$\forall X, Y \in \mathbf{R}^n \qquad {}^tX\,{}^tMY = {}^tXNY \iff N = {}^tM.$$

In particular, the matrix N is determined by M, so if ${}^tf$ exists, it is unique. Conversely, if we **define** ${}^tf : E \longrightarrow E$ to be the linear map whose matrix in $\mathcal{B}$ is equal to ${}^tM$, the previous calculation shows that

$$\forall x, y \in E \quad (f(x) \mid y) = (x \mid {}^tf(y)).$$

(5.2.3) Definition. *Let E be a Euclidean space. A linear map $f : E \longrightarrow E$ is called* **symmetric** *if ${}^tf = f$. Equivalent conditions: $\forall x, y \in E \qquad (f(x) \mid y) = (x \mid f(y)) \iff$ the matrix of f in one ($\iff$ in every) orthonormal basis of E is symmetric.*

(5.2.4) Theorem (abstract version of 5.2.1). *Let E be a Euclidean space. For each* **symmetric** *linear map $f = {}^tf : E \longrightarrow E$ there exists an* **orthonormal** *basis $e'_1, \ldots, e'_n$ of E consisting of eigenvectors of f: $f(e'_j) = \lambda_j e'_j \ \ (\lambda_j \in \mathbf{R})$.*

Proof. We admit a weak form of Remark 5.1.3(2), namely the existence of at least one real eigenvalue $\lambda \in \mathbf{R}$ of f; let $x \in E$, $x \neq \vec{0}$, $f(x) = \lambda x$. The vector subspace $\mathbf{R}x = \mathrm{vect}(x) \subset E$ is a line; its orthogonal complement $E_1 = (\mathbf{R}x)^\perp \subset E$ is a Euclidean space of dimension $n - 1$. We claim that $f(E_1) \subseteq E_1$: indeed, if $y \in E_1$, then $(x \mid y) = 0$, hence

$$(x \mid f(y)) = (f(x) \mid y) = (\lambda x \mid y) = \lambda(x \mid y) = 0,$$

which implies that $f(y) \in E_1$. Thus the restriction of f to E_1 defines a linear map

$$f_1 : E_1 \longrightarrow E_1, \qquad y \mapsto f(y).$$

As f is symmetric, so is f_1. Putting $e'_1 = x/\|x\|$ and applying the same argument to f_1, we obtain, recursively, the required orthonormal basis of E.

6. Hermitian forms, unitary spaces

Unitary spaces are complex analogues of Euclidean spaces. Their infinite-dimensional generalisations (complex Hilbert spaces) appear as fundamental objects in quantum theory.

6.1 Basic concepts

(6.1.1) The positivity of the standard Euclidean scalar product relies on the fact that

$$\forall x \in \mathbf{R} \qquad x^2 \geq 0.$$

This property admits a complex analogue

$$\forall z \in \mathbf{C} \qquad z\overline{z} \geq 0,$$

which motivates the following basic example:

(6.1.2) Example: the **standard hermitian scalar product** on $\mathbf{C}^n$, which is defined as

$$(x \mid y) = {}^t x\, \overline{y} = x_1\overline{y}_1 + \cdots + x_n\overline{y}_n \qquad\qquad (x, y \in \mathbf{C}^n),$$

satisfies the positivity property

$$(\forall x \in \mathbf{C}^n, x \neq \vec{0}) \qquad (x \mid x) = x_1\overline{x}_1 + \cdots + x_n\overline{x}_n > 0,$$

but **is not bilinear**; it is linear in the variable x

$$(x + x' \mid y) = (x \mid y) + (x' \mid y), \qquad (\lambda x \mid y) = \lambda\,(x \mid y) \qquad\qquad (x, x', y \in \mathbf{C}^n;\ \lambda \in \mathbf{C})$$

and **anti-linear** in the variable y:

$$(x \mid y + y') = (x \mid y) + (x \mid y'), \qquad (x \mid \lambda y) = \overline{\lambda}\,(x \mid y) \qquad\qquad (x, y, y' \in \mathbf{C}^n;\ \lambda \in \mathbf{C}).$$

This is a special case of the following abstract concept.

(6.1.3) Definition. *Let E be a $\mathbf{C}$-vector space. A* **hermitian form on** *E is a map $f : E \times E \longrightarrow \mathbf{C}$ (in other words, a complex-valued function $f(x, y)$ in two variables $x, y \in E$) such that*
(1) *For fixed $y \in E$, the function $f(x, y)$ is linear in x:*

$$f(x + x', y) = f(x, y) + f(x', y), \qquad f(\lambda x, y) = \lambda\, f(x, y) \qquad\qquad (x, x', y \in E;\ \lambda \in \mathbf{C}).$$

(2) *For fixed $x \in E$, the function $f(x, y)$ is anti-linear in y:*

$$f(x, y + y') = f(x, y) + f(x, y'), \qquad f(x, \lambda y) = \overline{\lambda}\, f(x, y) \qquad\qquad (x, y, y' \in E;\ \lambda \in \mathbf{C}).$$

(3) $\forall x, y \in E \qquad f(y, x) = \overline{f(x, y)}$.
[In fact, (1) and (3) imply (2).]

6.2 Matrix representation of hermitian forms

(6.2.1) Assume that $n = \dim(E) < \infty$. Given a basis $\mathcal{B} = \{e_1, \ldots, e_n\}$ of E, we identify E with $\mathbf{C}^n$ as in 1.1.8. In particular, if $x = x_1e_1 + \cdots + x_ne_n$, $y = y_1e_1 + \cdots + y_ne_n \in E$ are two vectors in E, denote by

$$X = M_{\mathcal{B}}(x) = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}, \quad Y = M_{\mathcal{B}}(y) = \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} \in \mathbf{C}^n$$

the column vectors representing x and y in the basis $\mathcal{B}$.
If $f : E \times E \longrightarrow \mathbf{C}$ is a hermitian form, then

$$f(x,y) = f(\sum_{j=1}^{n} x_j e_j, \sum_{k=1}^{n} y_k e_k) = \sum_{j=1}^{n} x_j\, f(e_j, \sum_{k=1}^{n} y_k e_k) = \sum_{j=1}^{n} x_j \sum_{k=1}^{n} \overline{y}_k\, f(e_j, e_k) = \sum_{j,k=1}^{n} f(e_j, e_k)\, x_j \overline{y}_k. \tag{6.2.1.1}$$

(6.2.2) Definition. *In the situation of 6.2.1, the square matrix $A = (A_{jk}) \in M_n(\mathbf{C})$, where $A_{jk} = f(e_j, e_k)$, is called* **the matrix of f in the basis $\mathcal{B}$**. *This matrix satisfies*

$$A_{kj} = f(e_k, e_j) = \overline{f(e_j, e_k)} = \overline{A_{jk}}, \qquad {}^t\!A = \overline{A}.$$

(6.2.3) Matrix formulas. Using this notation, the formula (6.2.1.1) can be written as a matrix product

$$f(x,y) = \sum_{j,k=1}^{n} A_{jk}\, x_j \overline{y}_k = (x_1 \cdots x_n) \begin{pmatrix} A_{11} & \cdots & A_{1n} \\ \vdots & \ddots & \vdots \\ A_{n1} & \cdots & A_{nn} \end{pmatrix} \begin{pmatrix} \overline{y}_1 \\ \vdots \\ \overline{y}_n \end{pmatrix} = {}^t\!XA\overline{Y}. \tag{6.2.3.1}$$

(6.2.4) Definition. *A complex square matrix $B = (B_{jk}) \in M_n(\mathbf{C})$ is called* **hermitian** *if ${}^tB = \overline{B}$ ($\Longleftrightarrow$ $B_{kj} = \overline{B}_{jk}$ for all $j, k \implies$ all diagonal terms $B_{jj} \in \mathbf{R}$ are real). In particular, a real square matrix is hermitian $\Longleftrightarrow$ it is symmetric.*

(6.2.5) By 6.2.2, the matrix of a hermitian form in any basis $\mathcal{B}$ of E is hermitian. Conversely, for each hermitian matrix $A \in M_n(\mathbf{C})$, the formula (6.2.3.1)

$$f(x,y) = {}^t\!XA\overline{Y}$$

defines a hermitian form on E: the properties 6.1.3(1)-(2) are clear, and the property 6.1.3(3) follows from the same calculation as in 2.3.5: as $f(y,x) \in \mathbf{C} = M_1(\mathbf{C})$ is equal to its own transpose, we have, for all $x, y \in E$,

$$f(y,x) = {}^t YA\overline{X} = {}^t({}^tYA\overline{X}) = {}^t\overline{X}\,{}^tAY = {}^t\overline{X}\,\overline{A}\,Y = \overline{{}^tXA\overline{Y}} = \overline{f(x,y)}.$$

(6.2.6) Change of basis. If $\mathcal{B}' = e'_1, \ldots, e'_n$ is an other basis of E, let $P \in M_n(\mathbf{C})$ be the (invertible) matrix of change of basis from $\mathcal{B}$ to $\mathcal{B}'$. The usual formulas

$$x = \sum_{j=1}^{n} x_j e_j = \sum_{j=1}^{n} x'_j e'_j, \qquad X = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}, \qquad X' = \begin{pmatrix} x'_1 \\ \vdots \\ x'_n \end{pmatrix}, \qquad X = PX'$$

relating the column vectors of coordinates of any $x \in E$ in the respective beses $\mathcal{B}, \mathcal{B}'$ allow us to compute the (hermitian) matrix $A' \in M_n(\mathbf{C})$ representing f in the basis $\mathcal{B}'$:

$$\left.\begin{aligned} f(x,y) &= {}^t\!XA\overline{Y} = {}^t(PX')A\overline{(PY')} = {}^tX'({}^tPA\overline{P})\overline{Y'} \\ f(x,y) &= {}^tX'A'\overline{Y'} \end{aligned}\right\} \implies A' = {}^tPA\overline{P}.$$

6.3 Parallels with the theory of quadratic forms

(6.3.1) The hermitian quadratic form associated to a hermitian form $f : E \times E \longrightarrow \mathbf{C}$ is defined to be the function

$$q : E \longrightarrow \mathbf{C}, \qquad q(x) = f(x,x) = {}^tXA\overline{X}.$$

For example, if $E = \mathbf{C}^2$ and the matrix of f in the canonical basis is equal to

$$A = \begin{pmatrix} 1 & 1+2i \\ 1-2i & 3 \end{pmatrix},$$

then

$$\begin{aligned} f(x,y) &= x_1\overline{y}_1 + (1+2i)x_1\overline{y}_2 + (1-2i)x_2\overline{y}_1 + 3x_2\overline{y}_2 \\ q(x) &= x_1\overline{x}_1 + (1+2i)x_1\overline{x}_2 + (1-2i)x_2\overline{x}_1 + 3x_2\overline{x}_2 \end{aligned} \qquad (6.3.1.1)$$

As in the case of quadratic forms, f is determined by q; this is clear from the matrix representation (as in the example (6.3.1.1)), but it can also be deduced from the following abstract formulas:

$$\begin{aligned} q(x \pm y) &= f(x \pm y, x \pm y) = f(x,x) + f(y,y) \pm (f(x,y) + f(y,x)) = q(x) + q(y) \pm (f(x,y) + f(y,x)) \\ q(x \pm iy) &= f(x \pm iy, x \pm iy) = f(x,x) + f(y,y) \pm i(-f(x,y) + f(y,x)) = q(x) + q(y) \pm i(-f(x,y) + f(y,x)) \\ 4f(x,y) &= q(x+y) - q(x-y) + iq(x+iy) - iq(x-iy). \end{aligned}$$

(6.3.2) All definitions and results from chapter 3 have obvious hermitian analogues: in the situation of 6.2.1, we define

$$\begin{gathered} \mathrm{rk}(f) := \mathrm{rk}(A) \\ f \text{ is non-degenerate} \iff \mathrm{rk}(f) = n \iff \det(A) \neq 0 \\ x \perp y \iff f(x,y) = 0 \ (\iff y \perp x) \qquad\qquad (x, y \in E) \\ \forall S \subset E \ (S \text{ non-empty}) \qquad S^\perp := \{y \in E \mid \forall x \in S \quad x \perp y\} = (\mathrm{vect}(S))^\perp \text{ is a vector subspace of } E \\ N(f) := E^\perp \end{gathered}$$

The results of §3.7 hold: If f is non-degenerate and $F \subset E$ is a vector subspace, then $\dim(F^\perp) = \dim(E) - \dim(F)$. Moreover, if $F \cap F^\perp = \{\overrightarrow{0}\}$, then $E = F \oplus F^\perp = F \perp F^\perp$. Similarly, Theorem 3.3.1 ("easy diagonalisation of quadratic forms") and Theorem 3.4.2 ("Sylvester's theorem") have the following hermitian analogues, which are proved by a straightforward modification of the proofs from chapter 3.

(6.3.3) Theorem (Easy diagonalisation of hermitian forms). *For each hermitian form $f : E \times E \longrightarrow \mathbf{C}$ on a finite-dimensional complex vector space E there exists a basis $\mathcal{B}' = \{e'_1, \ldots, e'_n\}$ of E in which the matrix of f is diagonal, i.e.*

$$f(x,y) = d_1 x'_1\overline{y'_1} + \cdots + d_n x'_n\overline{y'_n} \qquad\qquad (x = \sum_{j=1}^n x'_j e'_j,\ y = \sum_{j=1}^n y'_j e'_j)$$

(with $d_1, \ldots, d_n \in \mathbf{R}$).

(6.3.4) Examples: (1) For the hermitian form (6.3.1.1),

$$\begin{aligned} q(x) &= x_1\overline{x}_1 + (1+2i)x_1\overline{x}_2 + (1-2i)x_2\overline{x}_1 + 3x_2\overline{x}_2 = (x_1 + (1-2i)x_2)(\overline{x}_1 + (1+2i)\overline{x}_2) - 2x_2\overline{x}_2 = \\ &= x'_1\overline{x'_1} - 2x'_2\overline{x'_2}, \qquad\qquad x'_1 = x_1 + (1-2i)x_2, \qquad x'_2 = x_2. \end{aligned}$$

(2) For the hermitian form f represented in the canonical basis of $\mathbf{C}^2$ by the hermitian matrix

$$A = \begin{pmatrix} 0 & a \\ \overline{a} & 0 \end{pmatrix} \qquad\qquad (a \in \mathbf{C},\ a \neq 0),$$

we have

$$q(x) = a x_1 \overline{x}_2 + \overline{a} x_2 \overline{x}_1.$$

The change of coordinates

$$\begin{pmatrix} x_1' \\ x_2' \end{pmatrix} = \begin{pmatrix} (ax_1 + x_2)/2 \\ (ax_1 - x_2)/2 \end{pmatrix}, \qquad \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} (x_1' + x_2')/a \\ x_1' - x_2' \end{pmatrix}$$

transforms q into

$$q(x) = 2(x_1'\overline{x_1'} - x_2'\overline{x_2'}).$$

(6.3.5) Theorem (hermitian version of Sylvester's theorem). *For each hermitian form $f : E \times E \longrightarrow \mathbf{C}$ on a finite-dimensional complex vector space E there exists a basis $\mathcal{B} = \{e_1, \ldots, e_n\}$ of E in which*

$$f(x,y) = x_1\overline{y_1} + \cdots + x_s\overline{y_s} - x_{s+1}\overline{y_{s+1}} - \cdots - x_{s+t}\overline{y_{s+t}}.$$

The integers $s, t \geq 0$ depend only on f (and satisfy $s + t = \mathrm{rk}(f)$).

(6.3.6) Exercise. *Decide whether the following maps $f : E \times E \longrightarrow \mathbf{C}$ are hermitian forms. If it is the case, determine the corresponding hermitian quadratic form.*
(1) $E = M_n(\mathbf{C})$, $f(A,B) = \mathrm{Tr}(A\overline{B})$.
(2) $E = \mathbf{C}^n$, $f(X,Y) = {}^tX\overline{Y}$.
(3) $E = \mathbf{C}^2$, $f(x,y) = 2x_1\overline{y_1} + ix_1\overline{y_2} - ix_2\overline{y_1} + 5x_2\overline{y_2}$.
(4) $E = \mathbf{C}^2$, $f(x,y) = (1+i)x_1\overline{y_1} + 2x_1\overline{y_2} + 2x_2\overline{y_1} + 5ix_2\overline{y_2}$.
(5) $E = \mathbf{C}^2$, $f(x,y) = x_1\overline{y_2} + y_2\overline{x_1}$.
(6) $E = \mathbf{C}^2$, $f(x,y) = x_1\overline{y_2} + x_2\overline{y_1}$.

(6.3.7) Exercise. *Show that all diagonal terms of an hermitian matrix are real.*

6.4 Unitary spaces

(6.4.1) Definition. *A hermitian form $f : E \times E \longrightarrow \mathbf{C}$ is called* **positive definite** *if $(\forall x \in E,\ x \neq \vec{0})$ $f(x,x) > 0$. If this is the case, then we say that E, equipped with the hermitian scalar product $(x \mid y) = f(x,y)$, is a* **complex pre-Hilbert space** *(resp., a* **unitary space** *if $\dim(E) < \infty$). A hermitian matrix $A \in M_n(\mathbf{C})$ is* **positive definite** *if the associated hermitian form $f(x,y) = {}^tXA\overline{Y}$ is: $(\forall X \in \mathbf{C}^n,\ X \neq \vec{0})$ ${}^tXA\overline{X} > 0$.*

(6.4.2) Examples: (1) $E = \mathbf{C}^n$ with the standard hermitian scalar product $(x \mid y) = x_1\overline{y}_1 + \cdots + x_n\overline{y}_n$ is a unitary space.
(2) The space of complex-valued continuous functions

$$E = \{f : [a,b] \longrightarrow \mathbf{C} \mid f \text{ continuous}\} = C([a,b];\mathbf{C}), \qquad (f \mid g) = \int_a^b f(t)\,\overline{g(t)}\,dt$$

is a complex pre-Hilbert space.

(6.4.3) (1) It follows from Theorem 6.3.5 that each unitary space E admits a basis $\mathcal{B} = e_1, \ldots, e_n$ in which

$$(x \mid y) = x_1\overline{y}_1 + \cdots + x_n\overline{y}_n \qquad\qquad (x = \sum_{j=1}^n x_j e_j,\ y = \sum_{j=1}^n y_j e_j)$$

is as in 6.4.2(1); we say that $\mathcal{B}$ is an **orthonormal basis** of E.

(2) One defines the concept of an **orthonormal system** in E as in 4.1.7. For example, the functions

$$f_m(t) = e^{2\pi imt} = \cos(2\pi mt) + i\ \sin(2\pi mt) \qquad\qquad (m = 0, \pm 1, \pm 2, \ldots)$$

form an orthonormal system in the space $C([0,1]; \mathbf{C})$ from 6.4.2(2).

(6.4.4) Norm. The norm of a vector x of a complex pre-Hilbert space E is defined as

$$\|x\| := \sqrt{(x \mid x)} \geq 0.$$

The **Cauchy-Schwarz inequality** states that

$$\forall x, y \in E \qquad |(x \mid y)| \leq \|x\|\|y\|. \tag{6.4.4.1}$$

The proof of (6.4.4.1) proceeds as in 4.2.3: assuming that $x \neq \vec{0}$, we have, for each $t \in \mathbf{R}$,

$$\begin{aligned} 0 \leq \|tx + y\|^2 &= t^2(x \mid x) + t\left((x \mid y) + \overline{(x \mid y)}\right) + (y \mid y) = \\ &= (x \mid x)\left|t + \frac{(x \mid y)}{(x \mid x)}\right|^2 + \frac{(x \mid x)(y \mid y) - |(x \mid y)|^2}{(x \mid x)}; \end{aligned}$$

taking $t = -(x \mid y)/(x \mid x)$ (and using $(x \mid x) > 0$), we obtain (6.4.4.1).

6.5 Isometries, unitary matrices

Let E be a unitary space of dimension $n \geq 1$. The discussion from 4.4 carries over with only minor modifications.

(6.5.1) Fix an orthonormal basis $\mathcal{B}$ of E; let $\mathcal{B}'$ be an arbitrary basis of E and $P \in M_n(\mathbf{C})$ the (invertible) matrix of the change of basis from $\mathcal{B}$ to $\mathcal{B}'$. The matrices A, A' of the hermitian scalar product in the respective bases $\mathcal{B}, \mathcal{B}'$ are equal to

$$A = I_n, \qquad A' = {}^tPA\overline{P} = {}^tP\overline{P};$$

thus

$$\mathcal{B}' \text{ is an orthonormal basis} \iff A' = I_n \iff {}^tP\overline{P} = I_n.$$

(6.5.2) Definition. *A matrix $P \in M_n(\mathbf{C})$ is* **unitary** *if ${}^tP\overline{P} = I_n$ (which implies that $\det(P)$ is a complex number of absolute value $|\det(P)| = 1$). Note that, if P is unitary, so is $\overline{P}$.*

(6.5.3) Isometries. An **isometry of** E is a linear map $u : E \longrightarrow E$ satisfying the equivalent properties

$$\forall x \in E \qquad \|u(x)\| = \|x\| \iff \forall x, y \in E \qquad (u(x) \mid u(y)) = (x \mid y).$$

Writing $u(x) = UX$ and $(x \mid y) = {}^tX\overline{Y}$ in an orthonormal basis of E, the same calculation as in 4.4.4

$$(u(x) \mid u(y)) = {}^t(UX)\overline{UY} = {}^tX({}^tU\overline{U})\overline{Y}$$

implies that

$$\begin{aligned} u \text{ is an isometry} &\iff \text{the matrix } U \text{ of } u \text{ in one orthonormal basis of } E \text{ is unitary} \\ &\iff \text{the matrix of } u \text{ in each orthonormal basis of } E \text{ is unitary.} \end{aligned}$$

In particular, isometries of $\mathbf{C}^n$ (equipped with the standard hermitian scalar product) are the linear maps

$$u : \mathbf{C}^n \longrightarrow \mathbf{C}^n, \qquad X \mapsto UX, \qquad U \in M_n(\mathbf{C}) \textbf{ unitary}.$$

If we use the notation

$$U(n) = \{\text{unitary matrices } U \in M_n(\mathbf{C})\} = \{\text{isometries of } \mathbf{C}^n\}$$
$$SU(n) = \{U \in U(n) \mid \det(U) = 1\},$$

then

$$U(n) \cap M_n(\mathbf{R}) = O(n),$$

and

$$U(1) = \{\lambda \in \mathbf{C} \mid \ |\lambda| = 1\}$$

can be identified with $SO(2)$, thanks to (4.5.10.1).

(6.5.4) Exercise. *Show that*

$$SU(2) = \Big\{ \begin{pmatrix} a & -\overline{c} \\ c & \overline{a} \end{pmatrix} \Big| \, a, c \in \mathbf{C},\, |a|^2 + |c|^2 = 1 \Big\}.$$

(6.5.5) Proposition (eigenvalues of unitary and hermitian matrices). *Let $A \in M_n(\mathbf{C})$ be a complex matrix, let $x, y \in \mathbf{C}^n$ be eigenvectors of A: $x, y \neq \vec{0}$, $Ax = \lambda x$, $Ay = \mu y$ ($\lambda, \mu \in \mathbf{C}$). Denote by $(x \mid y) = {}^t x\, \overline{y}$ the standard hermitian scalar product on $\mathbf{C}^n$.*
(1) If A is unitary, then $|\lambda| = |\mu| = 1$. If $\lambda \neq \mu$, then $(x \mid y) = 0$.
(2) If A is hermitian, then $\lambda, \mu \in \mathbf{R}$. If $\lambda \neq \mu$, then $(x \mid y) = 0$.

Proof. (1) As A is unitary, we have

$$\forall u, v \in \mathbf{C}^n \qquad (Au \mid Av) = {}^t(Au)\overline{Av} = {}^t u\, {}^t A\, \overline{A}\, \overline{v} = {}^t u\, \overline{v} = (u \mid v).$$

Taking $u = v = x$, we obtain

$$0 \neq (x \mid x) = (Ax \mid Ax) = (\lambda x \mid \lambda x) = \lambda\overline{\lambda}\,(x \mid x) = |\lambda|^2\,(x \mid x),$$

hence $|\lambda| = 1$ (similarly, $|\mu| = 1$). Taking $u = x$ and $v = y$ yields

$$(x \mid y) = (Ax \mid Ay) = (\lambda x \mid \mu y) = \lambda\overline{\mu}\,(x \mid y) = \lambda\mu^{-1}\,(x \mid y);$$

if $\lambda \neq \mu$, it follows that $(x \mid y) = 0$.
(2) As ${}^t A = \overline{A}$, we have

$$\forall u, v \in \mathbf{C}^n \qquad (Au \mid v) = {}^t(Au)\overline{v} = {}^t u\, {}^t A\, \overline{v} = {}^t u\, \overline{Av} = (u \mid Av).$$

Taking $u = v = x$, we obtain

$$\lambda\,(x \mid x) = (\lambda x \mid x) = (Ax \mid x) = (x \mid Ax) = (x \mid \lambda x) = \overline{\lambda}\,(x \mid x);$$

as $(x \mid x) \neq 0$, it follows that $\lambda = \overline{\lambda}$ is real (similarly, μ is real). Taking $u = x$ and $v = y$ yields

$$\lambda\,(x \mid y) = (\lambda x \mid y) = (Ax \mid y) = (x \mid Ay) = (x \mid \mu y) = \overline{\mu}\,(x \mid y) = \mu\,(x \mid y);$$

if $\lambda \neq \mu$, it follows that $(x \mid y) = 0$.

(6.5.6) Corollary (eigenvalues of orthogonal and symmetric real matrices). *Let $A \in M_n(\mathbf{R})$ be a real matrix, let $x, y \in \mathbf{C}^n$ be complex eigenvectors of A: $x, y \neq \vec{0}$, $Ax = \lambda x$, $Ay = \mu y$ ($\lambda, \mu \in \mathbf{C}$). Denote by $(x \mid y) = {}^t x\,\overline{y}$ the standard hermitian scalar product on $\mathbf{C}^n$.*
(1) *If A is orthogonal, then $|\lambda| = |\mu| = 1$. If $\lambda \neq \mu$, then $(x \mid y) = 0$.*
(2) *If A is symmetric, then $\lambda, \mu \in \mathbf{R}$. If $\lambda \neq \mu$, then $(x \mid y) = 0$.*

(6.5.7) Theorem ("difficult diagonalisation of hermitian forms"). *For each hermitian form f on a unitary space E there exists an* **orthonormal** *basis of E in which the matrix of f is diagonal (with real diagonal elements).*
Matrix formulation: *For each* **hermitian** *matrix $A \in M_n(\mathbf{C})$ there exists a* **unitary** *matrix $P \in U(n)$ such that the matrix ${}^t\overline{P}AP = P^{-1}AP$ is diagonal (with real diagonal elements). More precisely, the columns of P form an orthonormal basis of $\mathbf{C}^n$ (with respect to the standard hermitian scalar product) consisting of eigenvectors of A.*

Proof. This is proved in an analogous way as Theorem 5.2.4. All one needs to do is to define the hermitian adjoint ${}^h f$ of f satisfying the relation $(f(x) \mid y) = (x \mid {}^h f(y))$, and note that, in any orthonormal basis of E, the respective matrices M, N of $f, {}^h f$ satisfy $N = {}^t\overline{M}$. The argument can be easily adapted to give a proof of the following result.

(6.5.8) Theorem (hermitian version of Theorem 4.6.2). *For each isometry $u : E \longrightarrow E$ of a unitary space E there exists an* **orthonormal** *basis of E in which the matrix of u is diagonal (with diagonal elements $\lambda_1, \ldots, \lambda_n \in \mathbf{C}$ satisfying $|\lambda_1| = \cdots = |\lambda_n| = 1$).*
Matrix formulation: *For each* **unitary** *matrix $U \in U(n)$ there exists a* **unitary** *matrix $P \in U(n)$ such that the matrix ${}^t\overline{P}UP = P^{-1}UP \in U(n)$ is diagonal (with diagonal elements of modulus 1).*

(6.5.9) It is useful to keep in mind the following dictionary between matrices and complex numbers:

Numbers	Matrices
$z \in \mathbf{C}$	$A \in M_n(\mathbf{C})$
$\overline{z} \in \mathbf{C}$	${}^t\overline{A}$
$\overline{z} = z \in \mathbf{R}$	${}^t\overline{A} = A$ is hermitian
$\overline{u}u = 1 \iff \|u\| = 1$	${}^t\overline{U}U = I \iff U \in U(n)$
$\|u\| = 1 \iff u = e^{it},\ t \in \mathbf{R}$	$U \in U(n) \iff U = e^{iA},\ A = {}^t\overline{A}$
$z \in \mathbf{C}$, $z \neq 0$ $\iff z = ru,\ r \in \mathbf{R}_{>0},\ \|u\| = 1$	$M \in M_n(\mathbf{C})$, $\det(M) \neq 0$ $\iff M = PU,\ P = {}^t\overline{P} >> 0,\ U \in U(n)$

(6.5.10) Exercise. *Diagonalise, in the sense of 6.5.7, the following hermitian matrices.*

$$\begin{pmatrix} 4 & i & i \\ -i & 4 & 1 \\ -i & 1 & 4 \end{pmatrix}, \qquad \begin{pmatrix} 1 & 0 & i \\ 0 & 1 & -1 \\ -i & -1 & 1 \end{pmatrix}.$$

(6.5.11) Exercise. *Show that the following matrix is unitary. Diagonalise it in the sense of 6.5.8.*

$$\frac{1}{3}\begin{pmatrix} 1+2i & 1+i & 1+i \\ -1-i & 1+2i & 1-i \\ -1-i & 1-i & 1+2i \end{pmatrix}.$$

7. Examples of finite groups arising from geometry*

In this chapter we shall investigate, for certain geometric objects $C \subset \mathbf{R}^n$ (for example, for the cube and the tetrahedron in $\mathbf{R}^3$) their "isometry groups"

$$G(C) = \{g \in O(n) \mid g(C) = C\}$$
$$G^+(C) = \{g \in O^+(n) \mid g(C) = C\}.$$

7.1 Groups

(7.1.1) Most groups appear naturally as **transformation groups:** each element of a group G is a transformation of a given object X; this transformation is required to be **invertible**, and its inverse should be an element of G. Finally, the composition of two transformations of X belonging to G should lie in G.

One can forget the object X and consider the group G as an abstract group in the following sense.

(7.1.2) Definition. *A* **group** *is a set G equipped with a* **binary operation** $*$ *(in other words, for each pair of elements $g, h \in G$ there is defined their "product" $g * h \in G$) satisfying the following properties:*
(1) (Associativity) $\forall g, h, k \in G \qquad g * (h * k) = (g * h) * k.$
(2) (Neutral element) *There exists an element $e = e_G \in G$ such that $\forall g \in G \quad g * e = e * g = g$. This element is unique; we say that e is the* **neutral element** *(or the* **identity***) of G.*
(3) (Inverse) *For each $g \in G$ there exists an element $h \in G$ such that $g * h = h * g = e$. The element h is unique; it is called the* **inverse of** g *and is denoted by $h = g^{-1}$.*
Notation: *we sometimes write $(G, *)$ to make the operation on G explicit.*
We say that the group G is **commutative** *(or abelian) if $\forall g, h \in G \quad g * h = h * g$.*

(7.1.3) Examples: (1) $G = \mathbf{R}^n$, $* =$ sum ($e = \vec{0}$); this group if commutative.
(2) $G = \mathbf{R}^* = \{r \in \mathbf{R} \mid r \neq 0\}$, $* =$ product ($e = 1$); this group if commutative.
(3) $G = GL_n(\mathbf{R}) = \{A \in M_n(\mathbf{R}) \mid \det(A) \neq 0\}$, $* =$ matrix product ($e = I_n$); if $n > 1$, then this group is not commutative.
(4) For any set X, the **permutations of** X

$$G = S_X = \{f : X \longrightarrow X \mid f \text{ bijective } (= \text{ invertible) map}\}$$

form a group with respect to the composition $* = \circ$:

$$\begin{tikzcd} X \arrow[r, "f"] \arrow[dr, "g\circ f"'] & X \arrow[d, "g"] \\ & X \end{tikzcd} \qquad\qquad (g \circ f)(x) = g(f(x)).$$

The neutral element is the identity map

$$\mathrm{Id} = \mathrm{Id}_X : X \longrightarrow X, \qquad \forall x \in X \quad \mathrm{Id}(x) = x.$$

If X has at least 3 elements, then S_X is not commutative.

7.2 The symmetric and alternating groups

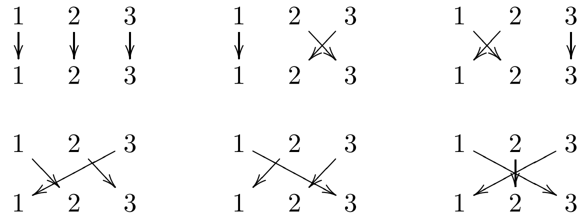
(7.2.1) Definition. *Fix an integer $n \geq 1$. The permutations of the set $X = \{1, 2, \ldots, n\}$ (i.e., the bijective maps $\sigma : X \longrightarrow X$) form the* **symmetric group on** n **letters** $S_n = S_{\{1,2,\ldots,n\}}$ *(with respect to the composition).*

(7.2.2) Examples: (1) S_1 consists only of the identity map

*** This chapter is optional.**

(2) S_2 contains two elements

(3) S_3 contains six elements



(4) **Notation:** for any permutation $\sigma : \{1, \ldots, n\} \longrightarrow \{1, \ldots, n\}$, one writes

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}.$$

For example, the above elements of S_3 can be written as

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \qquad \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \qquad \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \qquad \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \qquad \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

(5) **Composition of permutations:** by definition, $\sigma\tau = \sigma \circ \tau$, hence $(\sigma\tau)(i) = \sigma(\tau(i))$. For example, for

$$\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \qquad \tau = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix},$$

we compute

$$\begin{aligned} (\sigma\tau)(1) &= \sigma(\tau(1)) = \sigma(3) = 3 \\ (\sigma\tau)(2) &= \sigma(\tau(2)) = \sigma(1) = 2 \\ (\sigma\tau)(3) &= \sigma(\tau(3)) = \sigma(2) = 1, \end{aligned} \qquad \sigma\tau = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}.$$

Equivalently, we can draw the following diagram, using the notation from (3):

(6) **Order of S_n:** the number of elements of S_n is equal to

$$|S_n| = n \cdot (n-1) \cdot \dots \cdot 2 \cdot 1 = n!$$

(for $\sigma \in S_n$, there are n possibilities for the value of $\sigma(1)$; fixing $\sigma(1)$, there are $n-1$ possibilities for the value of $\sigma(2)$, etc.).

(7) **Cyclic notation:** each permutation $\sigma \in S_n$ can be written (uniquely) as a product of **disjoint cycles**. For example,

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 5 & 3 & 6 & 2 & 1 \end{pmatrix} \in S_6 \qquad\qquad 1 \longrightarrow 4 \longrightarrow 6, \qquad 2 \longrightarrow 5, \qquad 3$$

is a product of three cycles, of lengths $3, 2, 1$, respectively. One writes

$$\sigma = (146)(25)(3).$$

(7.2.3) Definition. *A* **transposition** *is a permutation $\sigma \in S_n$ ($n \geq 2$) which interchanges two elements of $\{1, \dots, n\}$ and fixes the remaining ones. For example,*

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 5 & 3 & 4 & 2 & 6 \end{pmatrix} = (25)(1)(3)(4)(6) \in S_6$$

is a transposition.

(7.2.4) Theorem. *Fix $n \geq 2$.* (1) *Each permutation $\sigma \in S_n$ can be writen (not uniquely) as a product of transpositions $\sigma = s_1 \cdots s_r$.*
(2) *The parity of r depends only on σ; one defines the* **sign of** *σ as $\mathrm{sgn}(\sigma) = (-1)^r$.*
(3) $\forall \sigma, \tau \in S_n \qquad \mathrm{sgn}(\sigma\tau) = \mathrm{sgn}(\sigma)\,\mathrm{sgn}(\tau)$.
Terminology: *if $\mathrm{sgn}(\sigma) = +1$ (resp., $\mathrm{sgn}(\sigma) = -1$), we say that σ is an* **even** *(resp., an* **odd***) permutation.*

(7.2.5) Example: The group S_3 contains three transpositions (for which $\mathrm{sgn} = -1$)

$$s_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \qquad s_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \qquad s_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = s_1 s_2 s_1 = s_2 s_1 s_2.$$

The remaining three elements (for which $\mathrm{sgn} = +1$) can be written, for example, as

$$e = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = s_1^2 = s_1 s_1, \qquad \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = s_1 s_2 = s_2 s_1 s_2 s_1, \qquad \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = s_2 s_1 = s_1 s_2 s_1 s_2.$$

(7.2.6) Definition. *Let $(G, *)$ be a group. A* **subgroup of** *G is a subset $H \subset G$ such that*
(1) *$e \in H$;*
(2) *$\forall h_1, h_2 \in H \qquad h_1 * h_2 \in H$;*
(3) *$\forall h \in H \qquad h^{-1} \in H$.*
If this is the case, then $(H, *)$ is also a group.

(7.2.7) Examples: (1) For each $n \geq 2$, the set of all even permutations is a subgroup of S_n

$$A_n = \{\sigma \in S_n \mid \mathrm{sgn}(\sigma) = +1\},$$

called the **alternating group on n letters**; its order is equal to $|A_n| = |S_n|/2 = n!/2$. For example,

$$A_3 = \{(1)(2)(3),\ (123),\ (132)\},$$
$$A_4 = \{(1)(2)(3)(4),\ (123)(4),\ (132)(4), \dots, (1)(234),\ (1)(243),\ (12)(34),\ (13)(24),\ (14)(23)\}.$$

(2) If $G = (S_X, \circ)$ is the group of all permutations of a set X and $Y \subset X$ is a subset of X, then

$$H = \{g \in G \mid g(Y) = Y\}$$

is a subgroup of G. For example, taking $X = \{1, \ldots, n\}$ and $Y = \{n\}$, then $G = S_n$ and $H = S_{n-1}$. More generally, if $Y = \{k+1, \ldots, n\}$ with $1 \leq k \leq n-1$, then H has every right to be called $S_k \times S_{n-k}$ (can you guess why?).

(3) Let K be a field, V a K-vector space and

$$\begin{aligned} G &= (S_V, \circ) = \{f : V \longrightarrow V \mid f \text{ bijective } (= \text{invertible})\} \\ H &= GL(V) = \{f : V \longrightarrow V \mid f \text{ bijective and linear}\}; \end{aligned}$$

then $GL(V)$ is a subgroup of S_V.

If $V = K^n$ $(n \geq 1)$, then we identify linear maps $K^n \longrightarrow K^n$ with matrices in $M_n(K)$ in the usual way (1.2.4.3), which leads to an identification of $GL(K^n)$ with

$$GL_n(K) = \{A \in M_n(K) \mid A \text{ is invertible}\} = \{A \in M_n(K) \mid \det(A) \neq 0\}.$$

(4) If $K = \mathbf{R}$, then we obtain a chain of subgroups of $S_{\mathbf{R}^n}$

$$SO(n) = O^+(n) \subset O(n) \subset GL_n(\mathbf{R}) \subset S_{\mathbf{R}^n}.$$

7.3 Examples of finite subroups of $O(n)$

We return to the original question, namely to the investigation of the subgroups of $O(n)$

$$\begin{aligned} G(Y) &= \{g \in O(n) \mid g(Y) = Y\} \\ G^+(Y) &= \{g \in O^+(n) \mid g(Y) = Y\} \end{aligned}$$

(for a given subset $Y \subset \mathbf{R}^n$).

(7.3.1) Exercise. *If the set*

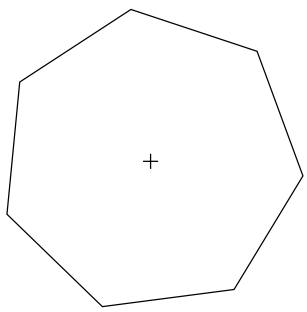
$$G^-(Y) = \{g \in O^-(n) \mid g(Y) = Y\}$$

is not empty, show that

$$G^-(Y) = \{sh \mid h \in G^+(Y)\},$$

for any $s \in G^-(Y)$.

(7.3.2) Cyclic and dihedral groups. Let $Y \subset \mathbf{R}^2$ be a regular polygon with $n \geq 3$ sides and the centre at the origin.



n=7

(7.3.2.1) In this case

$$G^+(Y) = \{\text{rotations around the origin with angles } 2\pi k/n \mid k = 0, \ldots, n-1\} =$$
$$= \{r, r^2, \ldots, r^{n-1}, r^n = e\} = C_n$$

is the **cyclic group of order** n, generated by the rotation r (around the origin) with angle $2\pi/n$.

(7.3.2.2) Let $s \in O^-(2)$ be the reflection with respect to the line passing through the origin and any fixed vertex of Y; then

$$G^-(Y) := \{g \in O^-(2) \mid g(Y) = Y\} = \{s, sr, \ldots, sr^{n-1}\}$$

and

$$G(Y) = \{r, r^2, \ldots, r^{n-1}, r^n = e, s, sr, \ldots, sr^{n-1}\} = D_n$$

(sometimes denoted by D_{2n} instead of D_n) is the **dihedral group of order** $2n$, generated by two elements r, s satisfying the relations

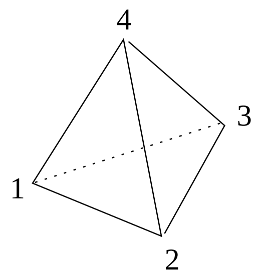
$$r^n = e = s^2, \qquad srs^{-1} = r^{-1}$$

(see 4.5.7(2)). Each element of $G(Y)$ defines a permutation of the vertices of Y; after labeling the vertices $1, \ldots, n$, we realize D_n as a subgroup of S_n $(n \geq 3)$. For example, for $n = 3$, we obtain

$$C_3 = A_3, \qquad D_3 = S_3.$$

(7.3.2.3) Exercise. *Give a geometric description of all elements of $G^-(Y)$.*
[Distinguish two cases, according to the parity of n.]

(7.3.3) The tetrahedron group. Let $T \subset \mathbf{R}^3$ be a regular tetrahedron with centre at the origin; label its vertices $1, \ldots, 4$.



We claim that

$$G(T) = S_4, \qquad G^+(T) = A_4;$$

in particular, $|G(T)| = 24$, $|G^+(T)| = 12$.

(7.3.3.1) More precisely, each element $g \in G(T)$ defines a permutation $\sigma(g) \in S_4$ of the vertices of the tetrahedron, and this correspondence is compatible with group operations:

$$\forall g_1, g_2 \in G(T) \qquad \sigma(g_1 \circ g_2) = \sigma(g_1) \circ \sigma(g_2);$$

in other words, the map

$$\sigma : G(T) \longrightarrow S_4, \qquad g \mapsto \sigma(g)$$

is a **group homomorphism:**

(7.3.3.2) Definition. *Let $(G, *)$ and $(H, \#)$ be groups. A map $f : G \longrightarrow H$ is a* **group homomorphism** *if it satisfies $\forall g_1, g_2 \in G \quad f(g_1 * g_2) = f(g_1) \# f(g_2)$. In this case $f(e_G) = e_H$ and $f(g^{-1}) = f(g)^{-1}$ (for all $g \in G$).*

(7.3.3.3) We want to show that the map σ not only preserves operations, but is bijective, i.e. each permutation $\tau \in S_4$ is of the form $\tau = \sigma(g)$, for **unique** $g \in G(T)$. Once we show that, we can identify $G(T) = (G(T), \circ)$ with $S_4 = (S_4, \circ)$, using the map σ.

The existence of g follows from the fact that each $\tau = s_1 \cdots s_r \in S_4$ is a product of transpositions, and each transposition

$$s_t = (ij)(k)(l) \in S_4$$

is equal to $s_t = \sigma(g_t)$, where $g_t \in G(T)$ is the reflection with respect to the plane passing through k, l and the midpoint of ij; then $\tau = \sigma(g_1) \cdots \sigma(g_r) = \sigma(g)$ for $g = g_1 \cdots g_r$. Why is g unique? If $\tau = \sigma(g) = \sigma(h)$ $(g, h \in G(T))$, then $\sigma(gh^{-1}) = \sigma(g)\sigma(h)^{-1} = \tau\tau^{-1} = e = (1)(2)(3)(4)$ fixes all vertices of T, hence $gh^{-1} \in G(T)$ fixes vectors $\vec{12}, \vec{13}, \vec{14}$; as these vectors form a basis of $\mathbf{R}^3$, gh^{-1} fixes all vectors of $\mathbf{R}^3$, hence $gh^{-1} = I_3$, $g = h$. This proves that σ is, indeed, a bijective group homomorphism (= a **group isomorphism**).

(7.3.3.4) Using the notation of 7.3.3.3, we have

$$\mathrm{sgn}(s_t) = -1 = \det(g_t)$$

for all $t = 1, \ldots, r$, hence

$$\mathrm{sgn}(\sigma(g)) = \mathrm{sgn}(\sigma(g_1) \cdots \sigma(g_r)) = \mathrm{sgn}(s_1 \cdots s_r) = (-1)^r = \det(g_1 \cdots g_r) = \det(g).$$

It follows that, for $g \in G(T)$,

$$g \in G^+(T) \iff \det(g) = +1 \iff \mathrm{sgn}(\sigma(g)) = +1 \iff \sigma(g) \in A_4;$$

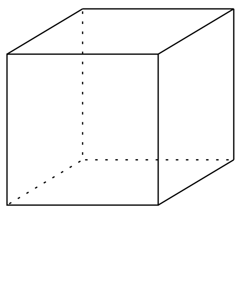
thus σ identifies $G^+(T)$ with A_4.

(7.3.3.5) Exercise. *Give a geometric description of all elements of $G^+(T)$.*

(7.3.4) The group of the cube. Let $C \subset \mathbf{R}^3$ be the cube with vertices

$$\begin{pmatrix} \pm 1 \\ \pm 1 \\ \pm 1 \end{pmatrix}$$

(for all possible combinations of signs).



We claim that

$$G^+(C) = S_4, \qquad G(C) = S_4 \times \{\pm 1\}$$

(7.3.4.1) The cube has 4 diagonals, which join vertices P and $-P$; label the diagonals $1, \ldots, 4$. As in 7.3.3, each isometry $g \in G(C)$ induces a permutation $\tau(g) \in S_4$ of the diagonals, and the map

$$\tau : G(C) \longrightarrow S_4$$

is a group homomorphism. An easy geometric argument shows that, for $g \in G(C)$,

$$\tau(g) = e = (1)(2)(3)(4) \iff g = \pm I_3;$$

thus we have, for $g_1, g_2 \in G(C)$,

$$\tau(g_1) = \tau(g_2) \iff \tau(g_1 g_2^{-1}) = \tau(g_1)\tau(g_2)^{-1} = e \iff g_1 g_2^{-1} = \pm I_3 \iff g_1 = \pm g_2.$$

In particular, $g_1 \in G^+(C)$ is uniquely determined by $\tau(g_1)$, hence

$$|G^+(C)| \leq |S_4| = 24, \qquad |G(C)| \leq 2 \cdot |S_4| = 48.$$

(7.3.4.2) On the other hand, one can write down explicitly 48 elements of $G(C)$, namely the following matrices:

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

(7.3.4.3) Putting together 7.3.4.1-2, we obtain that

$$|G(C)| = 48, \qquad |G^+(C)| = 24,$$

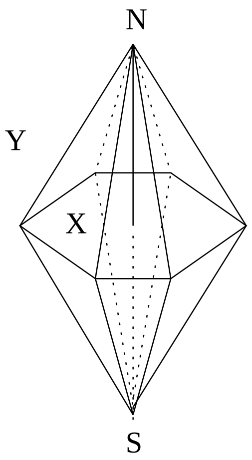
hence τ induces a group isomorphism between $G^+(C)$ and S_4. Finally, as $-I_3 \in G^-(C)$ commutes with every element of $G^+(C)$, we have $G(C) = G^+(C) \times \{\pm I_3\}$.

(7.3.4.4) Exercise. *Generalize 7.3.4.2 to the case of an n-dimensional cube in $\mathbf{R}^n$.*

(7.3.4.5) Exercise. *Relate 7.3.4.4 for $n = 2$ to 7.3.2.2.*

(7.3.5) The icosahedron group. If $Y \subset \mathbf{R}^3$ is a regular icosahedron (or a dodecahedron) with centre at the origin, then $G^+(Y) = A_5$.

(7.3.6) Dihedral groups revisited. Let $X \subset \mathbf{R}^2 \subset \mathbf{R}^3$ be a regular polygon with $n \geq 3$ sides and with centre at the origin. On the line perpendicular to $\mathbf{R}^2$ passing through the origin, fix two points N, S with the same distance from the origin ("the north pole and the south pole"); let $Y \subset \mathbf{R}^3$ be the set obtained by joining N and S with all points of X:



In this case one can realize the dihedral group

$$G(X) = D_n \subset O(2)$$

also as

$$G^+(Y) = G(X) = D_n \subset O^+(3).$$

Indeed, each element of $C_n = G^+(X) = D_n \cap O^+(2)$ extends to a rotation in $\mathbf{R}^3$ around the axis NS (and angle $2\pi k/n$ for some k), while each reflection $s_H \in G^-(X)$ (where $H \subset \mathbf{R}^2$ is a line passing through the origin and a vertex or the midpoint of one of the sides of X) extends to a rotation in $O^+(3)$ around the axis H with angle π.

(7.3.7) Here is a complete description of all finite subgroups $G \subset O^+(3)$, due to Felix Klein:

(1) $G = C_n$ or $G = D_n$ as in 7.3.6 (degenerate values $n = 1, 2$ are also allowed).
(2) $G = A_4$; in this case there exists a regular tetrahedron T such that $G = G^+(T)$.
(3) $G = S_4$; in this case there exists a cube C and a regular octahedron O such that $G = G^+(C) = G^+(O)$.
(4) $G = A_5$; in this case there exists a regular dodecahedron D and a regular icosahedron I such that $G = G^+(D) = G^+(I)$.

Note that this description includes a classification of regular polyhedra in $\mathbf{R}^3$.

7.4 Orbits and stabilizers

(7.4.1) It is sometimes possible to determine the order of the group $G(Y)$ (or $G^+(Y)$) directly, using the formula 7.4.3 below.

(7.4.2) Definition. *Let X be a set, G a group and $\sigma : G \longrightarrow S_X$ a group homomorphism (for example, G can be a subgroup of S_X). In this case we say that G* **acts on** *X. For an element $x \in X$, we define* **the orbit of** *x*

$$O(x) = \{\sigma(g)(x) \mid g \in G\}$$

to be the set of elements of X to which x can be transformed by the action of G; we define the **stabilizer of** *x*

$$G_x = \{g \in G \mid \sigma(g)(x) = x\}$$

to be the subgroup of G consisting of all elements that fix x.

(7.4.3) Proposition (orbit-stabilizer formula). *Let G be a finite group acting on a set X. Then, for each $x \in X$, we have*

$$|G| = |O(x)| \cdot |G_x|.$$

(7.4.4) Examples: (1) For $G = S_n$ $(n \geq 2)$, $X = \{1, \ldots, n\}$ and $x = n$, we have

$$O(x) = \{1, \dots, n\}, \qquad G_x = S_{n-1},$$

thus

$$|S_n| = n \cdot |S_{n-1}|,$$

which implies, by induction,

$$|S_n| = n \cdot (n-1) \cdots 2 \cdot 1 = n!$$

(2) For a cube $C \subset \mathbf{R}^3$ with centre at the origin, the group $G = G(C)$ acts on the set X of all faces of C. Each of the six faces $x \in X$ is a square; we have

$$O(x) = X, \qquad G_x = D_4,$$

thus $\quad |G(C)| = 6 \cdot 8 = 48.$

(3) For an n-dimensional cube $C(n) \subset \mathbf{R}^n$ with centre at the origin, the group $G(n) = G(C(n))$ acts on the set X of $(n-1)$-dimensional faces of $C(n)$. Each $x \in X$ is an $(n-1)$-dimensional cube,

$$O(x) = X, \qquad G_x = C(n-1);$$

thus

$$|C(n)| = 2n \cdot |C(n-1)|,$$

which implies, by induction,

$$|C(n)| = 2n \cdot (2n-2) \cdots 4 \cdot 2 = 2^n \cdot n!$$

(7.4.5) Exercise. *Relate 7.4.4(3) to 7.3.4.4.*