Linear algebra II

Universität Wuppertal, WS 2017

Jürgen Müller

Contents

0 Reminder: Determinants

(0.1) Signs. For $n \in \mathbb{N}_0$ let $\mathcal{S}_n$ be the symmetric group on the set $\{1, \ldots, n\}$, and the **sign** map $\operatorname{sgn}\colon \mathcal{S}_n \to \{\pm 1\}\colon \pi \mapsto \prod_{1 \leq i < j \leq n} \frac{\pi(j)-\pi(i)}{j-i} = (-1)^{l(\pi)}$, where $l(\pi) := |\{\{i,j\}; i < j, \pi(i) > \pi(j)\}| \in \mathbb{N}_0$ is its **inversion number**. If $\rho \in \mathcal{S}_n$ is a k**-cycle**, for some $k \in \mathbb{N}$, then we have $\operatorname{sgn}(\pi) = (-1)^{k-1}$; in particular $\operatorname{sgn}(\mathrm{id}) = 1$, and for a **transposition** $\sigma \in \mathcal{S}_n$ we have $\operatorname{sgn}(\sigma) = -1$.

For $\pi, \rho \in \mathcal{S}_n$ we have **multiplicativity** $\operatorname{sgn}(\pi\rho) = \operatorname{sgn}(\pi) \cdot \operatorname{sgn}(\rho)$, and we have $\operatorname{sgn}(\pi^{-1}) = \operatorname{sgn}(\pi)$. The elements of $\mathcal{A}_n := \{\pi \in \mathcal{S}_n; \operatorname{sgn}(\pi) = 1\}$ and $\mathcal{S}_n \setminus \mathcal{A}_n = \{\pi \in \mathcal{S}_n; \operatorname{sgn}(\pi) = -1\}$ are called **even** and **odd** permutations, respectively; then $\mathcal{A}_n \leq \mathcal{S}_n$ is a subgroup, being called the associated **alternating group**.

(0.2) Determinants. a) Let K be a field. Then the **determinant** of a square matrix $A := [a_{ij}]_{ij} \in K^{n \times n}$, where $n \in \mathbb{N}_0$, is defined as $\det(A) := \sum_{\pi \in \mathcal{S}_n} \operatorname{sgn}(\pi) \cdot \prod_{j=1}^{n} a_{\pi(j),j} \in K$.

For example, for an **upper triangular** matrix $A \in K^{n \times n}$, that is $a_{ij} = 0$ for all $i > j \in \{1, \ldots, n\}$, we get $\det(A) = \prod_{j=1}^{n} a_{jj} \in K$; in particular, for the **identity matrix** $E_n \in K^{n \times n}$ we get $\det(E_n) = 1$.

For $n = 0$ we have $\det([]) = 1$; for $n = 1$ we have $\det([a]) = a$; for $n = 2$ we have $\det \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} = a_{11}a_{22} - a_{12}a_{21}$; for $n = 3$ we have $\det \begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{bmatrix} = (a_{11}a_{22}a_{33} + a_{12}a_{23}a_{31} + a_{13}a_{21}a_{32}) - (a_{13}a_{22}a_{31} + a_{12}a_{21}a_{33} + a_{11}a_{23}a_{32})$, called the **Sarrus rule**.

b) The map $\det\colon (K^{n \times 1})^n \to K\colon [v_1, \ldots, v_n] \mapsto \det([v_1, \ldots, v_n])$, where by $[v_1, \ldots, v_n] \in K^{n \times n}$ we denote the matrix having columns $v_1, \ldots, v_n$, has the following properties: It is K**-multilinear**, that is K**-linear** in each argument, and it is **alternating**, that is $\det(\ldots, v, \ldots, v, \ldots) = 0$ for all $v \in K^{n \times 1}$.

Hence we have $\det(\ldots, v, \ldots, w, \ldots) = -\det(\ldots, w, \ldots, v \ldots)$ for all $v, w \in K^{n \times 1}$, and $\det(\ldots, v, \ldots, w, \ldots) = \det(\ldots, v + aw, \ldots, w \ldots)$ for all $a \in K$.

Moreover, we have $\det(A^{\mathrm{tr}}) = \det(A)$. Hence det is row multilinear and row alternating as well, and the above properties also hold row-wise. Hence this allows to compute the determinant of A by applying the Gauß algorithm, keeping track of the row operations made, and to read off the determinant of its Gaussian normal form which is an upper triangular matrix.

(0.3) Theorem: Multiplicativity. a) For $A, B \in K^{n \times n}$ we have $\det(AB) = \det(A) \cdot \det(B)$. Hence if $A \in \mathrm{GL}_n(K)$ then we have $\det(A^{-1}) = \det(A)^{-1} \neq 0$.

Hence $\mathrm{SL}_n(K) := \{A \in \mathrm{GL}_n(K); \det(A) = 1\} \leq \mathrm{GL}_n(K)$ is a subgroup, being called the **special linear group** of degree n over K.

b) If V is a finitely generated K-vector space, and $B \subseteq V$ a K-basis, then the **determinant** of $\varphi \in \mathrm{End}_K(V)$ is defined as $\det(\varphi) := \det(M_B^B(\varphi))$, which by

base change indeed is independent of the K-basis chosen.

(0.4) Theorem: Laplace expansion. Let $A = [a_{ij}]_{ij} \in K^{n\times n}$ where $n \in \mathbb{N}$, and for $i, j \in \{1, \ldots, n\}$ let

$$A_{ij} := \begin{bmatrix} a_{11} & \ldots & a_{1,j-1} & a_{1,j+1} & \ldots & a_{1n} \\ \vdots & & \vdots & \vdots & & \vdots \\ a_{i-1,1} & \ldots & a_{i-1,j-1} & a_{i-1,j+1} & \ldots & a_{i-1,n} \\ a_{i+1,1} & \ldots & a_{i+1,j-1} & a_{i+1,j+1} & \ldots & a_{i+1,n} \\ \vdots & & \vdots & \vdots & & \vdots \\ a_{n1} & \ldots & a_{n,j-1} & a_{n,j+1} & \ldots & a_{nn} \end{bmatrix} \in K^{(n-1)\times(n-1)}$$

be the matrix obtained from A by deleting row i and column j, where $\det(A_{ij}) \in K$ is called the (i,j)-th $(n-1)$**-minor** of A.

a) Then we have **column expansion** $\det(A) = \sum_{i=1}^{n} (-1)^{i+j} \cdot a_{ij} \cdot \det(A_{ij})$, for all $j \in \{1, \ldots, n\}$, as well as **row expansion** $\det(A) = \sum_{j=1}^{n} (-1)^{i+j} \cdot a_{ij} \cdot \det(A_{ij})$, for all $i \in \{1, \ldots, n\}$.

b) Let $\operatorname{adj}(A) := [(-1)^{i+j} \cdot \det(A_{ji})]_{ij} \in K^{n\times n}$ be the **adjoint matrix** of A. Then we have $A \cdot \operatorname{adj}(A) = \operatorname{adj}(A) \cdot A = \det(A) \cdot E_n \in K^{n\times n}$.

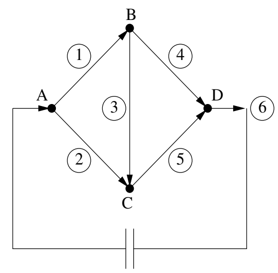
Hence we have $A \in \mathrm{GL}_n(K)$ if and only if $\det(A) \neq 0$, and in this case we have $A^{-1} = \det(A)^{-1} \cdot \operatorname{adj}(A) \in \mathrm{GL}_n(K)$;

c) For $A \in \mathrm{GL}_n(K)$ and $w \in K^{n\times 1}$, the unique solution $v = [x_1, \ldots, x_n]^{\mathrm{tr}} \in K^{n\times 1}$ of the system of linear equations $Av = w$ is by **Cramer's rule** given as $x_i := \det(A)^{-1} \cdot \det(A_i(w)) \in K$, for all $i \in \{1, \ldots, n\}$, where $A_i(w) \in K^{n\times n}$ is the matrix obtained from A by replacing column i by w.

(0.5) Example: Direct current networks. We consider the **Wheatstone bridge** as depicted in Table 1: We have electrical connections between the vertices (A, B), (A, C), (B, C), (B, D), (C, D), and (D, A), whose internal resistances are given as $r := [r_1, \ldots, r_6] \in \mathbb{R}^6$, respectively, where $r_j > 0$. Voltage $v \in \mathbb{R}$ is fed into (D, A), and the task is to determine the currents $c := [c_1, \ldots, c_6]^{\mathrm{tr}} \in \mathbb{R}^{6\times 1}$ in the connections. In particular, we wonder whether it is possible to adjust the internal resistances such that the current c_3 through the bridge (B, C) vanishes.

By **Kirchhoff's laws**, incoming and outgoing currents cancel out at each of the vertices A, B, C, D, leading to the first four of the following equations. Moreover the voltage between two vertices is given as the product of the internal resistance and the current, and the voltages cancel out along all closed circuits in the network without source or sink; using the circuits (A, B, C) and (B, C, D) this leads to the next two of the following equations, while using the circuit (A, B, D) the last one is due to the voltage v fed into the network. Hence we

Table 1: The Wheatstone bridge.



---

have the 'overdetermined' system $A'X^{\mathrm{tr}} = w'$, where

$$[A'|w'] := \left[\begin{array}{cccccc|c} -1 & -1 & . & . & . & 1 & . \\ 1 & . & -1 & -1 & . & . & . \\ . & 1 & 1 & . & -1 & . & . \\ . & . & . & 1 & 1 & -1 & . \\ \hline r_1 & -r_2 & r_3 & . & . & . & . \\ . & . & r_3 & -r_4 & r_5 & . & . \\ r_1 & . & . & r_4 & . & r_6 & v \end{array}\right] \in \mathbb{R}^{7\times(6+1)}.$$

Since the currents are accounted for with opposite signs at their respective end vertices, the column sums of the equations coming from the balance of currents all vanish. Thus summing up the first four rows of A' yields a zero row, and we may leave out row 4 and look at the system $AX^{\mathrm{tr}} = w$, where

$$[A|w] := \left[\begin{array}{cccccc|c} -1 & -1 & . & . & . & 1 & . \\ 1 & . & -1 & -1 & . & . & . \\ . & 1 & 1 & . & -1 & . & . \\ r_1 & -r_2 & r_3 & . & . & . & . \\ . & . & r_3 & -r_4 & r_5 & . & . \\ r_1 & . & . & r_4 & . & r_6 & v \end{array}\right] \in \mathbb{R}^{6\times(6+1)}.$$

If Kirchhoff's laws describe direct current networks completely, the above system should have a unique solution. Thus we check that $A \in \mathbb{R}^{6\times 6}$ is invertible:

Adding column 6 to columns 1 and 2, and using row expansion with respect to row 1 we get

$$\det(A) = -\det \begin{bmatrix} 1 & . & -1 & -1 & . \\ . & 1 & 1 & . & -1 \\ r_1 & -r_2 & r_3 & . & . \\ . & . & r_3 & -r_4 & r_5 \\ r_1 + r_6 & r_6 & . & r_4 & . \end{bmatrix}.$$

Adding the r_5-fold of row 2 to row 4, and using column expansion with respect to column 5; and adding column 1 to columns 3 and 4, and using row expansion with respect to row 1, the right hand side equals

$$-\det\begin{bmatrix} 1 & . & -1 & -1 \\ r_1 & -r_2 & r_3 & . \\ . & r_5 & r_3+r_5 & -r_4 \\ r_1+r_6 & r_6 & . & r_4 \end{bmatrix} = -\det\begin{bmatrix} -r_2 & r_1+r_3 & r_1 \\ r_5 & r_3+r_5 & -r_4 \\ r_6 & r_1+r_6 & r_1+r_4+r_6 \end{bmatrix}.$$

The Sarrus rule implies $\det(A) = r_2(r_3+r_5)(r_1+r_4+r_6) + (r_1+r_3)r_4r_6 - r_1r_5(r_1+r_6) + r_1(r_3+r_5)r_6 + (r_1+r_3)r_5(r_1+r_4+r_6) + r_2r_4(r_1+r_6) = r_1r_2r_3 + r_1r_2r_4 + r_1r_2r_5 + r_1r_3r_5 + r_1r_3r_6 + r_1r_4r_5 + r_1r_4r_6 + r_1r_5r_6 + r_2r_3r_4 + r_2r_3r_6 + r_2r_4r_5 + r_2r_4r_6 + r_2r_5r_6 + r_3r_4r_5 + r_3r_4r_6 + r_3r_5r_6 > 0$, where the only summand with negative sign cancels out.

Hence we have $A \in \mathrm{GL}_6(\mathbb{R})$, and the system $AX^{\mathrm{tr}} = w$ has a unique solution $c = [c_1, \ldots, c_6]^{\mathrm{tr}} \in \mathbb{R}^{6\times 1}$. By Cramer's rule we have

$$c_3 \cdot \det(A) = \det\begin{bmatrix} -1 & -1 & . & . & . & 1 \\ 1 & . & . & -1 & . & . \\ . & 1 & . & . & -1 & . \\ r_1 & -r_2 & . & . & . & . \\ . & . & . & -r_4 & r_5 & . \\ r_1 & . & v & r_4 & . & r_6 \end{bmatrix}.$$

Using column expansion with respect to column 3, and column expansion with respect to column 5, the right hand side equals

$$-v\cdot\det\begin{bmatrix} -1 & -1 & . & . & 1 \\ 1 & . & -1 & . & . \\ . & 1 & . & -1 & . \\ r_1 & -r_2 & . & . & . \\ . & . & -r_4 & r_5 & . \end{bmatrix} = -v\cdot\det\begin{bmatrix} 1 & . & -1 & . \\ . & 1 & . & -1 \\ r_1 & -r_2 & . & . \\ . & . & -r_4 & r_5 \end{bmatrix}.$$

Adding column 1 to column 3, adding column 2 to column 4, and using row expansion with respect to rows 1 and 2, this in turn equals

$$-v\cdot\det\begin{bmatrix} 1 & . & . & . \\ . & 1 & . & . \\ r_1 & -r_2 & r_1 & -r_2 \\ . & . & -r_4 & r_5 \end{bmatrix} = -v\cdot\det\begin{bmatrix} r_1 & -r_2 \\ -r_4 & r_5 \end{bmatrix}.$$

Hence we have $c_3 \cdot \det(A) = v \cdot (r_2r_4 - r_1r_5)$. Thus for $v \neq 0$ the current c_3 vanishes if and only if the internal resistances fufill $r_2r_4 = r_1r_5$, in other words if and only if we have $\frac{r_1}{r_2} = \frac{r_4}{r_5}$. $\sharp$

The physical interpretation is as follows: The voltage v applied to vertex A is distributed to vertices B and C according to the quotient $\frac{r_1}{r_2}$, similarly the voltage $-v$ applied to vertex D is distributed to vertices B and C according to the quotient $\frac{r_4}{r_5}$. There is no current through through the bridge (B, C) if and only if B and C are on the same potential, thus if and only if $\frac{r_1}{r_2} = \frac{r_4}{r_5}$.

(0.6) Motivating example. We conclude with a motivating example, indicating the aim of the considerations to come next:

We consider $V := \mathbb{R}^{2\times 1}$ with standard $\mathbb{R}$-basis B, and $\mathbb{R}$-basis C given by $M_B^C(\mathrm{id}) = \begin{bmatrix} 1 & -1 \\ 1 & 1 \end{bmatrix} \in \mathrm{GL}_2(\mathbb{R})$; hence $M_C^B(\mathrm{id}) = (M_B^C(\mathrm{id}))^{-1} = \frac{1}{2} \cdot \begin{bmatrix} 1 & 1 \\ -1 & 1 \end{bmatrix}$.

i) For the **reflection** $\sigma \in \mathrm{End}_{\mathbb{R}}(V)$ at the hyperplane perpendicular to $[-1,1]^{\mathrm{tr}}$ we get $M_B^B(\sigma) = \begin{bmatrix} . & 1 \\ 1 & . \end{bmatrix} \in \mathbb{R}^{2\times 2}$, and $M_C^C(\sigma) = M_C^B(\mathrm{id}) \cdot M_B^B(\sigma) \cdot M_B^C(\mathrm{id}) = \begin{bmatrix} 1 & . \\ . & -1 \end{bmatrix} \in \mathbb{R}^{2\times 2}$. The $\mathbb{R}$-basis C seems to be better adjusted to σ, inasmuch $M_C^C(\sigma)$ is a diagonal matrix, in other words any vector in C is mapped by σ to a multiple of itself.

ii) To the contrary, for the **rotation** $\rho \in \mathrm{End}_{\mathbb{R}}(V)$ with respect to the angle $\omega \in \mathbb{R}$ we get $M_B^B(\rho) = \begin{bmatrix} \cos(\omega) & -\sin(\omega) \\ \sin(\omega) & \cos(\omega) \end{bmatrix} \in \mathbb{R}^{2\times 2}$. For $\omega \notin \pi\mathbb{Z}$ it is geometrically clear that there is no non-zero vector being mapped by ρ to a multiple of itself.

Hence the question arises, under which circumstances such nicely adjusted bases exist, and if so how to find them.

1 Rings and polynomials

(1.1) Monoids. A set M together with a **multiplication** $\cdot\colon M \times M \to M$ fulfilling the following conditions is called a **monoid**: There is a **neutral element** $1 \in M$ such that $1 \cdot a = a = a \cdot 1$ for all $a \in M$, and we have **associativity** $(ab)c = a(bc)$ for all $a, b, c \in M$. If additionally $ab = ba$ holds for all $a, b \in M$, then M is called **commutative** or **abelian**.

An element $a \in M$ is called **invertible** or a **unit**, if there is an **inverse** $a^{-1} \in M$ such that $aa^{-1} = 1 = a^{-1}a$. In this case, if $a' \in M$ also is an inverse, we have $a' = 1 \cdot a' = a^{-1}aa' = a^{-1} \cdot 1 = a^{-1}$, hence the inverse is uniquely determined.

Let $M^* \subseteq M$ be the set of units. Then we have $1 \in M^*$, where $1^{-1} = 1$; for all $a, b \in M^*$ we from $ab(b^{-1}a^{-1}) = 1 = (b^{-1}a^{-1})ab$ conclude $ab \in M^*$, where $(ab)^{-1} = b^{-1}a^{-1}$; and we have $(a^{-1})^{-1} = a$, thus $a^{-1} \in M^*$.

A monoid M such that $M^* = M$ is called a **group**. In particular, for any monoid M the subset M^* is a group, called the **group of units** of M.

For example, $\mathbb{N}_0$ is a commutative additive monoid with neutral element 0, and $\mathbb{N}$ is a commutative multiplicative monoid with neutral element 1, while $\mathbb{Z}$ is a commutative additive group with neutral element 0, and a commutative multiplicative monoid with neutral element 1.

(1.2) Rings. a) A set R together with an addition $+\colon R \times R \to R$ and a multiplication $\cdot\colon R \times R \to R$ fulfilling the following conditions is called a **ring**: The set R is a commutative additive group with neutral element 0, and a multiplicative monoid with neutral element 1, such that **distributivity** $a(b+c) = ab+ac$ and $(b+c)a = ba+ca$ holds, for all $a, b, c \in R$. If additionally $ab = ba$ holds, for all $a, b \in R$, then R is called **commutative**.

Here are few immediate consequences: We have $0 \cdot a = 0 = a \cdot 0$, and $(-1) \cdot a = -a = a \cdot (-1)$, and $(-a)b = -(ab) = a(-b)$, for all $a, b \in R$:

From $0+0 = 0$ we get $0 \cdot a = (0+0) \cdot a = 0 \cdot a + 0 \cdot a$ and hence $0 = 0 \cdot a - (0 \cdot a) = (0 \cdot a + 0 \cdot a) - (0 \cdot a) = 0 \cdot a$; for $a \cdot 0 = 0$ we argue similarly. We have $(-1) \cdot a + a = (-1) \cdot a + 1 \cdot a = (-1+1) \cdot a = 0 \cdot a = 0$, hence $(-1) \cdot a = -a$; for $a \cdot (-1) = -a$ we argue similarly. Finally, we have $-(ab) = (-1) \cdot ab = (-a)b$ and $-(ab) = ab \cdot (-1) = a(-b)$. $\sharp$

For example, $\mathbb{Z}$ is a commutative ring, but $\mathbb{N}_0$ is not a ring. $K^{n \times n}$ is a ring, for any field K and $n \in \mathbb{N}$, which is commutative if and only if $n = 1$. Moreover, letting $R := \{0\}$ with addition $0+0 = 0$ and multiplication $0 \cdot 0 = 0$ and $1 := 0$, then R is a commutative ring, being called the **zero ring**; conversely, if a ring R fulfills $1 = 0$, then we have $a = a \cdot 1 = a \cdot 0 = 0$, for all $a \in R$, hence $R = \{0\}$.

b) The subset $R^* \subseteq R$ is again called its **group of units**. If $R \neq \{0\}$ then we have $0 \notin R^*$: Assume to the contrary that $0 \in R^*$, then there is $0^{-1} \in R$ such that $1 = 0 \cdot 0^{-1} = 0$, a contradiction.

A commutative ring $R \neq \{0\}$ such that $R^* = R \setminus \{0\}$ is called a **field**. For example, we have $\mathbb{Z}^* = \{\pm 1\}$, and $\mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$ are fields.

Let $R \neq \{0\}$ be commutative. An element $0 \neq a \in R$ such that $ab = 0$ for some $0 \neq b \in R$ is called a **zero-divisor**. If there are no zero-divisors, that is for all $0 \neq a, b \in R$ we have $ab \neq 0$, then R is called an **integral domain**.

Any $a \in R^*$ is not a zero-divisor: For $b \in R$ such that $ab = 0$ we have $b = 1 \cdot b = a^{-1}ab = a^{-1} \cdot 0 = 0$. In particular, any field is an integral domain; but $\mathbb{Z}$ is an integral domain but not a field.

c) Let R and S be rings. A map $\varphi \colon R \to S$ is called a **ring homomorphism**, if $\varphi(1_R) = 1_S$ and $\varphi(a+b) = \varphi(a)+\varphi(b)$ and $\varphi(ab) = \varphi(a)\varphi(b)$, for all $a, b \in R$.

In particular, φ is a homomorphism between the additive groups of R and S, and hence $\varphi(0_R) = 0_S$ and $\varphi(-a) = -\varphi(a)$, for all $a \in R$.

(1.3) Factorial domains. a) Let R be an integral domain. Then $a \in R$ is called a **divisor** of $b \in R$, and b is called a **multiple** of a, if there is $c \in R$ such that $ac = b$; we write $a \mid b$. Elements $a, b \in R$ are called **associate** if $a \mid b$ and $b \mid a$; we write $a \sim b$, where in particular $\sim$ is an equivalence relation on R.

We have $a \sim b$ if and only if there is $u \in R^*$ such that $b = au \in R$:

If $b = au$ then we also have $a = bu^{-1}$, thus $a \mid b$ and $b \mid a$. Conversely, if $a \mid b$ and $b \mid a$, then there are $u, v \in R$ such that $b = au$ and $a = bv$, thus $a = auv$, implying $a(1-uv) = 0$, hence $a = 0$ or $uv = 1$, where in the first case $a = b = 0$, and in the second case $u, v \in R^*$. $\sharp$

b) Let $\emptyset \neq M \subseteq R$ be a subset. Then $d \in R$ such that $d \mid a$ for all $a \in M$ is called a **common divisor** of M; any $u \in R^*$ is a common divisor of M. If for all common divisors $c \in R$ of M we have $c \mid d$, then $d \in R$ is called a **greatest common divisor** of M. Let $\gcd(M) \subseteq R$ be the set of all greatest common divisors of M. Elements $a, b \in R$ such that $\gcd(a, b) = R^*$ are called **coprime**.

In general greatest common divisors do not exist; but if $\gcd(M) \neq \emptyset$ then, since for $d, d' \in \gcd(M)$ we have $d \mid d'$ and $d' \mid d$, it consists of a single associate class. For $a \in R$ we have $a \in \gcd(a) = \gcd(0, a)$.

Similarly, we get the notion of **least common multiples** $\mathrm{lcm}(M) \subseteq R$; again, if $\mathrm{lcm}(M) \neq \emptyset$ then it consists of a single associate class.

c) Let $0 \neq c \in R \setminus R^*$. Then c is called **irreducible** or **indecomposable**, if $c = ab$ implies $a \in R^*$ or $b \in R^*$ for all $a, b \in R$; otherwise c is called **reducible** or **decomposable**; hence if c is irreducible then all its associates also are. Let $\mathcal{P} \subseteq R$ be a set of representatives of the associate classes of irreducible elements of R; these exist by the Axiom of Choice.

R is called **factorial** or a **Gaussian domain**, if any element $0 \neq a \in R$ can be written uniquely, up to reordering and taking associates, in the form $a = u \cdot \prod_{i=1}^{n} p_i \in R$, where the $p_i \in R$ are irreducible, $n \in \mathbb{N}_0$ and $u \in R^*$.

In this case any $0 \neq a \in R$ has a unique **factorisation** $a = u_a \cdot \prod_{p \in \mathcal{P}} p^{\nu_p(a)}$, where $u_a \in R^*$ and $\nu_p(a) \in \mathbb{N}_0$ is called the associated **multiplicity**; we have $\nu_p(a) = 0$ for almost all $p \in \mathcal{P}$, and $\sum_{p \in \mathcal{P}} \nu_p(a) \in \mathbb{N}_0$ is called the **length** of the factorisation, and a is called **squarefree** if $\nu_p(a) \leq 1$ for all $p \in \mathcal{P}$.

For any subset $\emptyset \neq M \subseteq R \setminus \{0\}$ we have $\prod_{p \in \mathcal{P}} p^{\min\{\nu_p(a); a \in M\}} \in \gcd(M)$, and similarly $\prod_{p \in \mathcal{P}} p^{\max\{\nu_p(a); a \in M\}} \in \mathrm{lcm}(M)$; but note that in order to use this in practice, the relevant elements of R have to be factorized completely first.

By the **Fundamental Theorem of Arithmetic** the integers $\mathbb{Z}$ are a factorial domain: Any $0 \neq z \in \mathbb{Z}$ can be written uniquely as $z = \mathrm{sgn}(z) \cdot \prod_{p \in \mathcal{P}} p^{\nu_p(z)}$, where the **sign** $\mathrm{sgn}(z) \in \{\pm 1\} = \mathbb{Z}^*$ is defined by $z \cdot \mathrm{sgn}(z) > 0$, and $\nu_p(z) \in \mathbb{N}_0$, and $\mathcal{P} \subseteq \mathbb{N}$ is the set of positive 'primes', being a set of representatives of the associate classes of irreducible elements. Actually, this is a consequence of the following much stronger property of $\mathbb{Z}$:

(1.4) Euclidean domains. a) An integral domain R is called **Euclidean**, if R has a **degree map** $\delta\colon R \setminus \{0\} \to \mathbb{N}_0$ having the following property: For all $a, b \in R$ such that $b \neq 0$ there are $q, r \in R$, called **quotient** and **remainder**, respectively, such that $a = qb + r$ where $r = 0$ or $\delta(r) < \delta(b)$; and whenever $a \mid b$ we have **monotonicity** $\delta(a) \leq \delta(b)$.

In particular, have $\delta(a) = \delta(b)$ whenever $a \sim b \neq 0$. Kind of conversely, if $a \mid b \neq 0$ such that $\delta(a) = \delta(b)$, then we have $a \sim b$: There are $q, r \in R$ such that $a = qb + r$, where $r = 0$ or $\delta(r) < \delta(b)$; but assuming $r \neq 0$ from $a \mid a - qb = r$ we get $\delta(a) \leq \delta(r) < \delta(b)$, a contradiction; hence we infer $r = 0$, that is $b \mid a$ as well.

Table 2: Extended Euclidean algorithm in $\mathbb{Z}$.

i	q_i	r_i	s_i	t_i
0		126	1	0
1	3	35	0	1
2	1	21	1	-3
3	1	14	-1	4
4	2	7	2	-7
5		0	-5	18

For example, any field K is Euclidean with respect to $\delta\colon K^* \to \mathbb{N}_0\colon x \mapsto 0$, and $\mathbb{Z}$ is Euclidean with respect to $\delta\colon \mathbb{Z} \setminus \{0\} \to \mathbb{N}_0\colon z \mapsto |z|$.

b) The major feature of Euclidean domains is that greatest common divisors always exist, and that they can be computed without factorizing:

Given $a, b \in R$, a greatest common divisor $r \in R$ and Bézout coefficients $s, t \in R$ such that $r = sa + tb \in R$ can be computed by the **extended Euclidean algorithm**; leaving out the steps indicated by $\circ$, needed to compute the $s_i, t_i \in R$, just yields a greatest common divisor:

- $\bullet$ $r_0 \leftarrow a$, $r_1 \leftarrow b$, $i \leftarrow 1$
- $\circ$ $s_0 \leftarrow 1$, $t_0 \leftarrow 0$, $s_1 \leftarrow 0$, $t_1 \leftarrow 1$
- $\bullet$ while $r_i \neq 0$ do
  - $\bullet$ $[q_i, r_{i+1}] \leftarrow \mathsf{QuotRem}(r_{i-1}, r_i)$ # quotient and remainder
  - $\circ$ $s_{i+1} \leftarrow s_{i-1} - q_i s_i$, $t_{i+1} \leftarrow t_{i-1} - q_i t_i$
  - $\bullet$ $i \leftarrow i + 1$
- $\bullet$ return $[r; s, t] \leftarrow [r_{i-1}; s_{i-1}, t_{i-1}]$

Since $\delta(r_i) > \delta(r_{i+1}) \geq 0$ for $i \in \mathbb{N}$, there is $l \in \mathbb{N}_0$ such that $r_l \neq 0$ and $r_{l+1} = 0$, hence the algorithm terminates. We have $r_i = s_i a + t_i b$ for all $i \in \{0, \ldots, l+1\}$, hence $r = r_l = sa + tb$. From $r_{i+1} = r_{i-1} - q_i r_i$, for all $i \in \{1, \ldots, l\}$, we get $r = r_l \in \gcd(r_l, 0) = \gcd(r_l, r_{l+1}) = \gcd(r_i, r_{i+1}) = \gcd(r_0, r_1) = \gcd(a, b)$. $\sharp$

Example. For $R := \mathbb{Z}$ let $a := 2 \cdot 3^2 \cdot 7 = 126$ and $b := 5 \cdot 7 = 35$, then Table 2 shows that $d := 7 = 2a - 7b \in \gcd(a, b)$. $\sharp$

(1.5) Theorem: Euclid implies Gauß. Any Euclidean domain is factorial.

Proof. Let R be an Euclidean domain with (monotonous) degree map δ. We first show that any $0 \neq a \in R \backslash R^*$ is a product of irreducible elements: Assuming the contrary, let a be chosen of minimal degree not having this property. Then a is reducible, hence there are $b, c \in R \setminus R^*$ such that $a = bc$. Thus we have $\delta(b) < \delta(a)$ and $\delta(c) < \delta(a)$, implying that both b and c are irreducible, hence a is a product of irreducible elements, a contradiction.

In order to show uniqueness of factorizations, we next show that any irreducible element $0 \neq a \in R \setminus R^*$ has the following property: Given $b, c \in R$ such that $a \nmid b$ and $a \mid bc$, then we have $1 \in \gcd(a,b)$, hence there are Bézout coefficients $s, t \in R$ such that $1 = sa + tb$, implying that $a \mid sac + tbc = c$.

Now let $a = u \cdot \prod_{i=1}^{n} p_i \in R$, where the p_i are irreducible, $n \in \mathbb{N}_0$ and $u \in R^*$. We proceed by induction on $n \in \mathbb{N}_0$, where we have $n = 0$ if and only if $a \in R^*$. Hence let $n \geq 1$, and let $a = \prod_{j=1}^{m} q_j \in R$, where the q_j are irreducible and $m \in \mathbb{N}$. Since p_n is irreducible, by the property proven above, we may assume that $p_n \mid q_m$, hence since q_m is irreducible, too, we infer $p_n \sim q_m$. Thus we have $u' \cdot \prod_{i=1}^{n-1} p_i = \prod_{j=1}^{m-1} q_j \in R$, for some $u' \in R^*$, and we are done by induction. $\sharp$

(1.6) Polynomial rings. a) Let X be a **symbol** or **indeterminate**. Then the set $X^* := \{X^i; i \in \mathbb{N}_0\}$ of **words** in X becomes a commutative monoid with respect to **concatenation** given by $X^i \cdot X^j := X^{i+j}$, for all $i, j \in \mathbb{N}_0$, having neutral element $1 := X^0$. Thus we may identify the additive monoid $\mathbb{N}_0$ with X^* via $\mathbb{N}_0 \to X^* \colon i \mapsto X^i$.

Let $K[X] := \{[a_0, a_1, \ldots] \in \mathrm{Maps}(X^*, K); a_i = 0 \text{ for almost all } i \in \mathbb{N}_0\}$, where K is a field. The map $f \colon X^* \to K \colon X^i \mapsto a_i$ is (essentially uniquely) written as a **formal sum** $f = \sum_{i \geq 0} a_i X^i$, and is called a **polynomial** in X, where $a_i \in K$ is called its i-th **coefficient**.

If $f \neq 0$ then $\deg(f) := \max\{i \in \mathbb{N}_0; a_i \neq 0\} \in \mathbb{N}_0$ is called its **degree**, where polynomials of degree $0, \ldots, 3$ are called **constant**, **linear**, **quadratic**, and **cubic**, respectively, and $\mathrm{lc}(f) := a_{\deg(f)} \in K$ is called its **leading coefficient**; if $\mathrm{lc}(f) = 1$ then f is called **monic**.

b) We define addition on $K[X]$ **componentwise** by letting $(\sum_{i \geq 0} a_i X^i) + (\sum_{j \geq 0} b_j X^j) := \sum_{k \geq 0} (a_k + b_k) X^k$. Similarly, we define scalar multiplication $K \times K[X] \to K[X]$ componentwise by letting $a \cdot (\sum_{i \geq 0} a_i X^i) := \sum_{i \geq 0} a a_i X^i$.

Thus $K[X]$ becomes a K-vector space, having K-basis $\{1 \cdot X^i; i \in \mathbb{N}_0\}$, which we may identify with X^*. Hence the formal sum notation just expresses elements of $K[X]$ as K-linear combinations of the K-basis X^*.

We define **convolutional** multiplication on $K[X]$ by letting $(1 \cdot X^i) \cdot (1 \cdot X^j) := (1 \cdot X^{i+j})$, and extending K-linearly in both arguments. In other words, we have $(\sum_{i \geq 0} a_i X^i) \cdot (\sum_{j \geq 0} b_j X^j) = \sum_{i,j \geq 0} a_i b_j X^{i+j} = \sum_{k \geq 0} (\sum_{l=0}^{k} a_l b_{k-l}) X^k$.

Since X^* is a commutative monoid, and multiplication on K fulfills associativity and commutativity, $K[X]$ becomes a commutative multiplicative monoid with neutral element $1 := 1 \cdot X^0$. Since arithmetic in K fulfills distributivity, this also holds for $K[X]$. Thus $K[X]$ is a commutative ring, being called the **(univariate) polynomial ring** in X over K.

$K[X]$ is an integral domain, such that $f \mid g$ implies $\deg(f) \leq \deg(g)$: For $0 \neq f, g \in K[X]$ we have $\mathrm{lc}(f) \neq 0 \neq \mathrm{lc}(g)$, hence from K being an integral domain we infer that $fg \neq 0$, where $\deg(fg) = \deg(f) + \deg(g)$ and $\mathrm{lc}(fg) = \mathrm{lc}(f)\mathrm{lc}(g)$.

Table 3: Extended Euclidean algorithm in $\mathbb{Q}[X]$.

i	q_i	r_i	s_i	t_i
0		$X^5 - X^3 + 2X^2 - 2$	1	0
1	$X^2 - 2X + 1$	$X^3 + 2X^2 + 2X + 1$	0	1
2	$\frac{1}{3}(X+2)$	$3X^2 - 3$	1	$-X^2 + 2X - 1$
3	$X - 1$	$3X + 3$	$\frac{-1}{3}(X+2)$	$\frac{1}{3}(X^3 - 3X + 5)$
4		0	$\frac{1}{3}(X^2 + X + 1)$	$\frac{-1}{3}(X^4 - X^3 + 2X - 2)$

We may consider K as a subset of $K[X]$ via $K \to K[X]\colon a \mapsto a \cdot 1$. Then we have $K[X]^* = K^*$; in particular $K[X]$ is not a field: We have $K^* = K \setminus \{0\} = \{a \cdot X^0; 0 \neq a \in K\} \subseteq K[X]^*$, and the additivity of degrees implies that for any $0 \neq f \in K[X]$ such that $\deg(f) \geq 1$ we have $f \notin K[X]^*$.

(1.7) Theorem: Polynomial division. Let $f, g \in K[X]$ such that $g \neq 0$. Then there are (uniquely determined) $q, r \in K[X]$, called **quotient** and **remainder**, respectively, such that $f = qg + r$ where $r = 0$ or $\deg(r) < \deg(g)$.

Proof. Let $qg + r = f = q'g + r'$ where $q, q', r, r' \in R[X]$ such that $r = 0$ or $\deg(r) < \deg(g)$, and $r' = 0$ or $\deg(r') < \deg(g)$. Then we have $(q - q')g = r' - r$, where $r' - r = 0$ or $\deg(r' - r) < \deg(g)$, and where $(q - q')g = 0$ or $\deg((q - q')g) = \deg(g) + \deg(q - q') \geq \deg(g)$. Hence we have $r' = r$ and $(q - q')g = 0$, implying $q = q'$, showing uniqueness.

To show existence, we may assume that $f \neq 0$ and $m := \deg(f) \geq \deg(g) := n$. We proceed by induction on $m \in \mathbb{N}_0$: Letting $f' := f - \mathrm{lc}(f)\mathrm{lc}(g)^{-1}gX^{m-n} \in K[X]$, the m-th coefficient of f' shows that $f' = 0$ or $\deg(f') < m$. By induction there are $q', r' \in K[X]$ such that $f' = q'g + r'$, where $r' = 0$ or $\deg(r') < \deg(g)$, hence $f = (q'g + r') + \mathrm{lc}(f)\mathrm{lc}(g)^{-1}gX^{m-n} = (q' + \mathrm{lc}(f)\mathrm{lc}(g)^{-1}X^{m-n})g + r'$. $\sharp$

(1.8) Corollary: Polynomial implies Euclid. $K[X]$ is an Euclidean domain with respect to the degree map deg.

Thus any $0 \neq f \in K[X]$ can be written uniquely as $f = \mathrm{lc}(f) \cdot \prod_{p \in \mathcal{P}} p^{\nu_p(f)}$, where $\nu_p(f) \in \mathbb{N}_0$ and $\mathcal{P} \subseteq K[X]$ is the set of monic irreducible polynomials, being a set of representatives of the associate classes of irreducible polynomials; we have $\deg(f) = \sum_{p \in \mathcal{P}} \nu_p(f) \deg(p) \in \mathbb{N}_0$.

Example. For $f := (X^3 + 2)(X + 1)(X - 1) = X^5 - X^3 + 2X^2 - 2 \in \mathbb{Q}[X]$ and $g := (X^2 + X + 1)(X + 1) = X^3 + 2X^2 + 2X + 1 \in \mathbb{Q}[X]$ we get $f = qg + r$, where $q := X^2 - 2X + 1 \in \mathbb{Q}[X]$ and $r := 3X^2 - 3 \in \mathbb{Q}[X]$. Table 3 shows that $d := X + 1 \in \gcd(f, g)$, where $d = \frac{-1}{9}(X + 2) \cdot f + \frac{-1}{9}(X^4 - X^3 + 2X - 2) \cdot g$. $\sharp$

(1.9) Evaluation. a) Let $\varphi\colon K \to S$ be a ring homomorphism into a ring S, such that $\varphi(a)z = z\varphi(a)$, for all $a \in K$ and $z \in S$. Then for $z \in S$ we have the associated **evaluation map** $\varphi_z\colon K[X] \to S\colon f = \sum_{i\geq 0} a_i X^i \mapsto \sum_{i\geq 0} \varphi(a_i)z^i =: f_\varphi(z)$; in particular, for $\varphi = \mathrm{id}_K$ we just write $f(z) = \sum_{i\geq 0} a_i z^i$.

Then φ_z is a ring homomorphism: We have $\varphi_z(1) = \varphi(1) = 1$, additivity $\varphi_z(f+g) = \varphi_z(\sum_{i\geq 0}(a_i+b_i)X^i) = \sum_{i\geq 0} \varphi(a_i+b_i)z^i = \sum_{i\geq 0} \varphi(a_i)z^i + \sum_{i\geq 0} \varphi(b_i)z^i = \varphi_z(f) + \varphi_z(g)$, and multiplicativity $\varphi_z(fg) = \varphi_z(\sum_{i\geq 0}(\sum_{j=0}^i a_j b_{i-j})X^i) = \sum_{i\geq 0}(\sum_{j=0}^i \varphi(a_j)\varphi(b_{i-j}))z^i = (\sum_{i\geq 0} \varphi(a_i)z^i) \cdot (\sum_{i\geq 0} \varphi(b_i)z^i) = \varphi_z(f)\varphi_z(g)$.

b) For $f \in K[X]$ we get the associated **polynomial map** $\widehat{f}_\varphi\colon S \to S\colon z \mapsto f_\varphi(z)$; in particular, for $\varphi = \mathrm{id}_K$ we just write $\widehat{f}\colon K \to K\colon z \mapsto f(z)$.

Since S is a ring, the set $\mathrm{Maps}(S, S)$ also becomes a ring with **pointwise** addition $F + G\colon S \to S\colon z \mapsto F(z) + G(z)$ and multiplication $F \cdot G\colon S \to S\colon z \mapsto F(z)G(z)$, neutral elements being the constant maps $S \to S\colon z \mapsto 0$ and $S \to S\colon z \mapsto 1$, respectively.

Hence, since the evaluation map $\varphi_z\colon K[X] \to S$ is a ring homomorphism for all $z \in S$, we infer that $\widehat{\varphi}\colon K[X] \to \mathrm{Maps}(S, S)\colon f \mapsto \widehat{f}_\varphi$ is a ring homomorphism.

c) If $f_\varphi(z) = 0$ then $z \in S$ is called a **root** or **zero** of f in S.

For $\varphi = \mathrm{id}_K$, an element $a \in K$ is a root of $f \in K[X]$, if and only if $(X - a) \mid f$: Writing $f = q \cdot (X - a) + r$, where $r = 0$ or $\deg(r) < \deg(X - a) = 1$, that is $r \in K$, we get $r = f(a) - q(a) \cdot (a - a) = f(a)$.

Then $a \in K$ is called a root of $f \neq 0$ of **multiplicity** $\nu_a(f) := \nu_{X-a}(f) \in \mathbb{N}_0$; note that $(X - a) \in \mathcal{P}$. From $\sum_{a\in K} \nu_a(f) \leq \deg(f)$ we conclude that $f \neq 0$ has at most $\deg(f) \in \mathbb{N}_0$ roots in K, counted with multiplicity.

The field K is called **algebraically closed** if any polynomial in $K[X] \setminus K$ has a root in K, or equivalently if $\mathcal{P} = \{X - a \in K[X]; a \in K\}$. By the **Fundamental Theorem of Algebra [Gauß, 1801]** the field of complex numbers $\mathbb{C}$ is algebraically closed.

The map $\widehat{\varphi}\colon K[X] \to \mathrm{Maps}(K, K)$ is injective if and only if K is infinite; in this case we may identify polynomials and polynomial maps:

If K is finite, then for $f := \prod_{a\in K}(X - a) \in K[X]$ we get $f(z) = 0 \in K$ for all $z \in K$, thus $\widehat{f} = \widehat{0} \in \mathrm{Maps}(K, K)$. If K is infinite, then for $f, g \in K[X]$ such that $\widehat{f} = \widehat{g} \in \mathrm{Maps}(K, K)$ we conclude that $f - g$ has all infinitely many elements of K as roots, implying that $f - g = 0 \in K[X]$. $\sharp$

2 Eigenvalues

(2.1) Similarity. a) Let K be a field. Matrices $A, D \in K^{n\times n}$, where $n \in \mathbb{N}_0$, are called **similar**, if there is $P \in \mathrm{GL}_n(K)$ such that $D = P^{-1}AP$. Similarity is an equivalence relation, the equivalence classes are called **similarity classes**.

The matrix A is called **diagonalisable**, if it is similar to a diagonal matrix. The matrix A is called **triangularisable**, if it is similar to a **(lower) triangular matrix**, that is a matrix $M := [b_{ij}]_{ij} \in K^{n \times n}$ such that $b_{ij} = 0$ for all $j > i \in \{1, \ldots, n\}$; in particular a diagonalisable matrix is triangularisable.

Triangularisability is equivalent to requiring that A is similar to an **upper triangular matrix**, that is a matrix $N := [c_{ij}]_{ij} \in K^{n \times n}$ such that $c_{ij} = 0$ for all $i > j \in \{1, \ldots, n\}$: Letting $P := [a_{ij}]_{ij} \in K^{n \times n}$, where $a_{ij} := 1$ if and only if $i + j = n + 1$, and $a_{ij} := 0$ elsewise, for any lower triangular matrix $M \in K^{n \times n}$ the matrix $P^{-1}NP \in K^{n \times n}$ is an upper triangular.

b) Let V be a K-vector space such that $\dim_K(V) = n$. Then $\varphi, \psi \in \mathrm{End}_K(V)$ are called **similar**, if there are K-bases B and C of V such that $M_B^B(\varphi) = M_C^C(\psi) \in K^{n \times n}$. Since $P := M_B^C(\mathrm{id}) \in \mathrm{GL}_n(K)$ and $M_C^C(\psi) = P^{-1} \cdot M_B^B(\psi) \cdot P$ this is equivalent to saying that $M_B^B(\varphi)$ and $M_B^B(\psi)$ are similar.

Moreover, φ is called **diagonalisable** or **triangularisable**, if $M_B^B(\varphi)$ is diagonalisable or triangularisable, respectively, for some, hence any K-basis $B \subseteq V$.

(2.2) Eigenvalues. a) Let K be a field, let V be a K-vector space, and let $\varphi \in \mathrm{End}_K(V)$. Then $a \in K$ is called an **eigenvalue** of φ, if there is an **eigenvector** $0 \neq v \in V$ such that $\varphi(v) = av$.

Given $a \in K$, we have $\varphi - a \cdot \mathrm{id} \in \mathrm{End}_K(V)$ as well, hence we have $T_a(\varphi) := \ker(\varphi - a \cdot \mathrm{id}) = \{v \in V; \varphi(v) = av\} \leq V$, being called the associated **eigenspace** of φ. Hence $T_a(\varphi) \setminus \{0\}$ is the associated set of eigenvectors of φ.

Letting $\gamma_a(\varphi) := \dim_K(T_a(\varphi)) \in \mathbb{N}_0 \,\dot\cup\, \{\infty\}$ be the associated **geometric multiplicity**, a is an eigenvalue of φ if and only if $\gamma_a(\varphi) \geq 1$. In particular, from $\ker(\varphi) = T_0(\varphi)$ we infer that φ is injective if and only if 0 is not an eigenvalue.

b) Let $\mathcal{I}$ be a set, and let $[a_i \in K; i \in \mathcal{I}]$ be pairwise different eigenvalues of φ. Then any sequence $[v_i \in T_{a_i}(\varphi) \setminus \{0\}; i \in \mathcal{I}]$ is K-linearly independent:

Let $\mathcal{J} \subseteq \mathcal{I}$ be finite, where we may assume that $\mathcal{J} = \{1, \ldots, n\}$ for some $n \in \mathbb{N}_0$. We proceed by induction, the case $n = 0$ being trivial: Let $b_1, \ldots, b_n \in K$ such that $\sum_{i=1}^n b_i v_i = 0$. Hence we have $0 = \varphi(\sum_{i=1}^n b_i v_i) = \sum_{i=1}^n a_i b_i v_i$, and thus $0 = a_n \cdot \sum_{i=1}^n b_i v_i - \sum_{i=1}^n a_i b_i v_i = \sum_{i=1}^{n-1} (a_n - a_i) b_i v_i$. By induction we get $(a_n - a_i) b_i = 0$, and $a_n - a_i \neq 0$ implies $b_i = 0$, for all $i \in \{1, \ldots, n-1\}$. Thus finally $v_n \neq 0$ implies $b_n = 0$. ♯

Example. Let $C^\infty(\mathbb{R}) := \{f \colon \mathbb{R} \to \mathbb{R}; f \text{ smooth}\} \leq \mathrm{Maps}(\mathbb{R}, \mathbb{R})$, and let $\frac{\partial}{\partial x} \in \mathrm{End}_{\mathbb{R}}(C^\infty(\mathbb{R}))$, a **differential operator**. Then for $\epsilon_a \colon \mathbb{R} \to \mathbb{R} \colon x \mapsto \exp(ax)$, where $a \in \mathbb{R}$, we have $\frac{\partial}{\partial x}(\epsilon_a) = a\epsilon_a$. Hence a is an eigenvalue of $\frac{\partial}{\partial x}$, having $\epsilon_a \in C^\infty(\mathbb{R})$ as an eigenvector, and $[\epsilon_a \in C^\infty(\mathbb{R}); a \in \mathbb{R}]$ is $\mathbb{R}$-linearly independent. But note that, since all non-trivial (finite) $\mathbb{R}$-linear combinations of $[\epsilon_a \in C^\infty(\mathbb{R}); a \in \mathbb{R}]$ are unbounded maps, this is not an $\mathbb{R}$-basis of $C^\infty(\mathbb{R})$. ♯

c) The above behaviour of eigenvectors can be rephrased in terms of the following general notion: Let $\mathcal{I}$ be a set, and let $U_i \leq V$ for all $i \in \mathcal{I}$. Then the sum

$U := \sum_{i\in\mathcal{I}} U_i \leq V$ is called **direct**, if any sequence $[v_i \in U_i \setminus \{0\}; i \in \mathcal{I}, U_i \neq \{0\}]$ is K-linearly independent; we write $U = \bigoplus_{i\in\mathcal{I}} U_i$.

Thus we have $U = \bigoplus_{i\in\mathcal{I}} U_i$ if and only if any $v \in U$ can be written essentially uniquely as a K-linear combination $v = \sum_{j\in\mathcal{J}} a_j v_j$, where $\mathcal{J} \subseteq \mathcal{I}$ is finite, and $v_j \in U_j$ for all $j \in \mathcal{J}$. In other words, we have $U = \bigoplus_{i\in\mathcal{I}} U_i$ if and only if $U_i \cap (\sum_{j\neq i} U_j) = \{0\}$, for all $i \in \mathcal{I}$.

Moreover, if $\mathcal{I}$ is finite and the U_i are finitely generated K-vector spaces, then iterating the dimension formula for subspaces, saying that $\dim_K(U_i) + \dim_K(U_j) = \dim_K(U_i + U_j) + \dim_K(U_i \cap U_j)$ for all $i, j \in \mathcal{I}$, implies that $U = \bigoplus_{i\in\mathcal{I}} U_i$ if and only if $\dim_K(U) = \sum_{i\in\mathcal{I}} \dim_K(U_i)$.

For example, if $[v_i \in V; i \in \mathcal{I}]$ is a K-basis of V, then we have $V = \bigoplus_{i\in\mathcal{I}} \langle v_i \rangle_K$. And coming back to eigenspaces, letting $U := \sum_{a\in K} T_a(\varphi) \leq V$, we have $U = \bigoplus_{a\in K} T_a(\varphi) = \bigoplus_{a\in K, \gamma_a(\varphi)\geq 1} T_a(\varphi)$.

(2.3) Eigenvalues of matrices. If $\dim_K(V) = n \in \mathbb{N}_0$, then choosing a K-basis $B \subseteq V$ and identifying $V \to K^{n\times 1}\colon v \mapsto M_B(v)$ translates notions for $\varphi \in \mathrm{End}_K(V)$ into those of $M_B^B(\varphi) \in K^{n\times n}$:

The eigenvalues and eigenvectors of a matrix $A \in K^{n\times n}$ are defined to be those of $\varphi_A\colon K^{n\times 1} \to K^{n\times 1}\colon v \mapsto Av$. Hence $a \in K$ is an eigenvalue of A if and only if $T_a(A) := \ker(A - aE_n) \neq \{0\}$. For the associated geometric multiplicity we have $\gamma_a(A) := \dim_K(T_a(A)) = \dim_K(\ker(A-aE_n)) = n-\mathrm{rk}(A-aE_n)$. Since for $P \in \mathrm{GL}_n(K)$ we have $\mathrm{rk}(P^{-1}AP-aE_n) = \mathrm{rk}(P^{-1}(A-aE_n)P) = \mathrm{rk}(A-aE_n)$, we conclude that geometric multiplicities only depend on similarity classes.

The matrix A is diagonalisable if and only if there is a K-basis $\{v_1, \ldots, v_n\} \subseteq K^{n\times 1}$ consisting of eigenvectors of A. In this case, for $P := [v_1, \ldots, v_n] \in \mathrm{GL}_n(K)$ we have $P^{-1}AP = D := \mathrm{diag}[a_1, \ldots, a_n] \in K^{n\times n}$. Since $\gamma_a(A) = \dim_K(T_a(D)) = |\{i \in \{1, \ldots, n\}; a_i = a\}|$, for all $a \in K$, we conclude that the (not necessarily pairwise different) diagonal entries $\{a_1, \ldots, a_n\}$ are precisely the eigenvalues of A, each occurring with multiplicity $\gamma_a(A)$. The eigenvalues together with their geometric multiplicities are called the **spectrum** of A.

Since the various eigenspaces of A form a direct sum, we conclude that A has at most n pairwise different eigenvalues. In this case, picking associated eigenvectors, we infer that $K^{n\times 1}$ has a K-basis consisting of eigenvectors of A, that is A is diagonalisable, and we have $\gamma_a(A) \leq 1$ for all $a \in K$.

Example. We reconsider the reflection given in (0.6): In terms of matrices, let $A := \begin{bmatrix} . & 1 \\ 1 & . \end{bmatrix} \in \mathbb{R}^{2\times 2}$. Then for the vectors $v_1 := [1, 1]^{\mathrm{tr}} \in \mathbb{R}^{2\times 1}$ and $v_2 := [-1, 1]^{\mathrm{tr}} \in \mathbb{R}^{2\times 1}$ we have $A \cdot v_1 = v_1$ and $A \cdot v_2 = -v_2$, that is they are are eigenvectors of A with respect to the eigenvalues 1 and -1, respectively. Letting $P := \begin{bmatrix} 1 & -1 \\ 1 & 1 \end{bmatrix} \in \mathrm{GL}_2(\mathbb{R})$ we have $P^{-1} := \frac{1}{2} \cdot \begin{bmatrix} 1 & 1 \\ -1 & 1 \end{bmatrix}$, and indeed $P^{-1}AP =$

$\frac{1}{2} \cdot \begin{bmatrix} 1 & 1 \\ -1 & 1 \end{bmatrix} \cdot \begin{bmatrix} . & 1 \\ 1 & . \end{bmatrix} \cdot \begin{bmatrix} 1 & -1 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} 1 & . \\ . & -1 \end{bmatrix} =: D$. Thus A is diagonalisable, where $\{\pm 1\}$ are the eigenvalues of A, both occurring with geometric multiplicity 1. $\sharp$

(2.4) Characteristic polynomials. Let K be a field and let $A \in K^{n \times n} \subseteq K[X]^{n \times n}$, where $n \in \mathbb{N}_0$. Then $XE_n - A \in K[X]^{n \times n}$ is called the **characteristic matrix** associated with A, and $\chi_A := \det(XE_n - A) \in K[X]$ is called the **characteristic polynomial** of A.

Note that we have defined determinants only for matrices over fields. But the definition given in (0.2) makes perfect sense in the more general setting of matrices over a commutative ring. Moreover, it can be checked that the basic properties, such as the arithmetical rules given in (0.2), multiplicativity in Theorem (0.3), and Laplace expansion in Theorem (0.4) continue to hold.

Then $\chi_A \neq 0$ is monic of degree $\deg(\chi_A) = n$, and we have $\chi_A(0) = \det(-A) = (-1)^n \cdot \det(A) \in K$. For example, for $D := \operatorname{diag}[a_1, \ldots, a_n] \in K^{n \times n}$ we have $\chi_D = \det(XE_n - D) = \prod_{i=1}^n (X - a_i) \in K[X]$.

Moreover, since for $P \in \mathrm{GL}_n(K)$ we have $\chi_{P^{-1}AP} = \det(XE_n - P^{-1}AP) = \det(P^{-1}(XE_n - A)P) = \det(XE_n - A) = \chi_A \in K[X]$, we conclude that $\chi_A \in K[X]$ only depends on the similarity class of A.

If V is a finitely generated K-vector space and $\varphi \in \operatorname{End}_K(V)$, choosing a K-basis $B \subseteq V$ yields the **characteristic polynomial** $\chi_\varphi := \chi_{M_B^B(\varphi)} \in K[X]$.

b) Given $a \in K$, the multiplicity $\nu_a(A) := \nu_a(\chi_A) = \nu_{X-a}(\chi_A) \in \mathbb{N}_0$ is called the associated **algebraic multiplicity**. Hence we have $\sum_{a \in K} \nu_a(A) \leq n$, and algebraic multiplicities only depend on the similarity class of A.

Hence a is an eigenvalue of A, that is $T_a(A) = \ker(A - aE_n) \neq \{0\}$, in other words $\gamma_a(A) \geq 1$, if and only if $\det(aE_n - A) = (-1)^n \cdot \det(A - aE_n) = 0$, or equivalently $\chi_A(a) = 0$, that is a is a root of χ_A, in other words $\nu_a(A) \geq 1$.

In particular, this again shows that A has at most n pairwise different eigenvalues, in which case we have $\nu_a(A) \leq 1$ for all $a \in K$. Moreover, if K is algebraically closed and $n \geq 1$ then A has an eigenvalue.

c) For any $a \in K$ we have $\nu_a(A) \geq \gamma_a(A)$:

Let $P := [v_1, \ldots, v_n] \in \mathrm{GL}_n(K)$ be a K-basis of $K^{n \times 1}$ such that $[v_1, \ldots, v_m]$ is a K-basis of $T_a(A) \leq K^{n \times 1}$, where $m := \gamma_a(A) \in \{0, \ldots, n\}$. Then $P^{-1}AP = \left[\begin{array}{c|c} D & * \\ \hline 0 & A' \end{array}\right]$, where $D = \operatorname{diag}[a, \ldots, a] \in K^{m \times m}$ and $A' \in K^{(n-m) \times (n-m)}$, yields $\chi_A = \det \left[\begin{array}{c|c} XE_m - D & * \\ \hline 0 & XE_{n-m} - A' \end{array}\right] = \det(XE_m - D) \cdot \det(XE_{n-m} - A') = \chi_D \cdot \chi_{A'} = (X-a)^m \cdot \chi_{A'} \in K[X]$, hence we infer $\nu_a(A) \geq m$. $\sharp$

In particular, since $\gamma_a(A) = 0$ if and only if $\nu_a(A) = 0$, we infer that $\nu_a(A) = 1$ entails $\gamma_a(A) = 1$.

(2.5) Diagonalisability. Let K be a field and let $A \in K^{n\times n}$, where $n \in \mathbb{N}_0$. Then A is diagonalisable if and only if $\chi_A \in K[X]$ splits into linear factors and for all $a \in K$ we have $\nu_a(A) = \gamma_a(A)$:

If $A = \mathrm{diag}[a_1, \ldots, a_n] \in K^{n\times n}$, then we have $\chi_A = \prod_{i=1}^n (X - a_i) \in K[X]$, where $\nu_a(A) = |\{i \in \{1, \ldots, n\}; a_i = a\}| = \gamma_a(A)$, for all $a \in K$.

Conversely, if $\chi_A = \prod_{i=1}^s (X - a_i)^{\nu_{a_i}(A)} \in K[X]$, where $\{a_1, \ldots, a_s\} \subseteq K$ are the eigenvalues of A with multipliticities $\nu_{a_i}(A) = \gamma_{a_i}(A) \in \mathbb{N}$, for some $s \in \mathbb{N}_0$, then $\sum_{i=1}^s \dim_K(T_{a_i}(A)) = \sum_{i=1}^s \gamma_{a_i}(A) = \sum_{i=1}^s \nu_{a_i}(A) = \deg(\chi_A) = n$, hence $\bigoplus_{i=1}^s T_{a_i}(A)$ being a direct sum, we infer $\bigoplus_{i=1}^s T_{a_i}(A) = K^{n\times 1}$, implying that there is a K-basis consisting of eigenvectors of A, that is A is diagonalisable. $\sharp$

Note that the condition on the equality of algebraic and geometric multiplicities is non-trivial only for the eigenvalues of A. Moreover, if A has n pairwise different eigenvalues, then χ_A splits into linear factors, and we have $\nu_a(A) = \gamma_a(A) = 1$ for all eigenvalues a of A, hence we recover the fact that A is diagonalisable.

Example. i) Let $A := \begin{bmatrix} . & 1 \\ 1 & . \end{bmatrix} \in \mathbb{R}^{2\times 2}$, that is we reconsider the reflection given in (0.6). Then we have $XE_n - A = \begin{bmatrix} X & -1 \\ -1 & X \end{bmatrix} \in \mathbb{R}[X]^{2\times 2}$, thus $\chi_A = X^2 - 1 = (X-1)(X+1) \in \mathbb{R}[X]$. Hence A has the eigenvalues $\{\pm 1\} \subseteq \mathbb{R}$, where $\nu_{\pm 1}(A) = \gamma_{\pm 1}(A) = 1$. We have $\ker(A - E_2) = \langle [1, 1]^{\mathrm{tr}} \rangle_{\mathbb{R}}$ and $\ker(A + E_2) = \langle [-1, 1]^{\mathrm{tr}} \rangle_{\mathbb{R}}$. Hence picking the vectors indicated we indeed recover the $\mathbb{C}$-basis consisting of eigenvectors chosen above.

ii) Let $A := \begin{bmatrix} \cos(\omega) & -\sin(\omega) \\ \sin(\omega) & \cos(\omega) \end{bmatrix} \in \mathbb{R}^{2\times 2}$, that is we reconsider the rotation with respect to the angle $\omega \in \mathbb{R}$ given in (0.6); in particular, the rotation with respect to the angle $\frac{\pi}{2}$ is given by $\begin{bmatrix} . & -1 \\ 1 & . \end{bmatrix}$. Then we have $XE_n - A = \begin{bmatrix} X - \cos(\omega) & \sin(\omega) \\ -\sin(\omega) & X - \cos(\omega) \end{bmatrix} \in \mathbb{R}[X]^{2\times 2} \subseteq \mathbb{C}[X]^{2\times 2}$, from which we get $\chi_A = X^2 - 2\cos(\omega)X + 1 \in \mathbb{R}[X] \subseteq \mathbb{C}[X]$, having roots $a_\pm := \cos(\omega) \pm i \cdot \sin(\omega) = \exp(\pm i\omega) \in \mathbb{C}$. Hence we have $a_\pm \in \mathbb{R}$ if and only if $\omega = k\pi$, where $k \in \mathbb{Z}$; in this case we have $A = (-1)^k \cdot E_2$, which already is a diagonal matrix, and $\chi_A = (X - (-1)^k)^2$, thus $\nu_{(-1)^k}(A) = \gamma_{(-1)^k}(A) = 2$.

If $\omega \notin \pi\mathbb{Z}$ then $a_\pm \in \mathbb{C} \setminus \mathbb{R}$. Thus $\chi_A \in \mathbb{R}[X]$ is irreducible, and A does not have any eigenvalues in $\mathbb{R}$, in particular A is not diagonalisable. Note that this is the algebraic counterpart of the geometric observation that for these rotations there cannot possibly exist non-zero vectors being mapped to multiples of themselves.

Still assuming $\omega \notin \pi\mathbb{Z}$, from $\chi_A = (X - a_+)(X - a_-) \in \mathbb{C}[X]$ where $a_+ \neq a_-$, we infer that A has the eigenvalues $\{a_\pm\} \subseteq \mathbb{C}$, where $\nu_{a_\pm}(A) = \gamma_{a_\pm}(A) = 1$, hence A is diagonalisable over $\mathbb{C}$, being similar to $\mathrm{diag}[a_+, a_-] \in \mathbb{C}^{2\times 2}$. More precisely, we have $\ker(A - a_+E_2) = \ker\left(\begin{bmatrix} -i\sin(\omega) & -\sin(\omega) \\ \sin(\omega) & -i\sin(\omega) \end{bmatrix}\right) = \ker\left(\begin{bmatrix} i & 1 \\ i & 1 \end{bmatrix}\right) =$

Table 4: Fibonacci numbers.

n	F_n	digits
1	1	
2	1	
4	3	1
8	21	2
16	987	3
32	2178309	7
64	10610209857723	14
128	251728825683549488150424261	27
256	141693817714056513234709965875411919657707794958199867	54

$\langle [i,1]^{\text{tr}} \rangle_{\mathbb{C}}$ and $\ker(A - a_- E_2) = \ker\left(\begin{bmatrix} i\sin(\omega) & -\sin(\omega) \\ \sin(\omega) & i\sin(\omega) \end{bmatrix}\right) = \ker\left(\begin{bmatrix} 1 & i \\ 1 & i \end{bmatrix}\right) = \langle [1,i]^{\text{tr}} \rangle_{\mathbb{C}}$; thus picking the vectors indicated we get the $\mathbb{C}$-basis given by $P := \begin{bmatrix} i & 1 \\ 1 & i \end{bmatrix} \in \mathrm{GL}_2(\mathbb{C})$ and $P^{-1}AP = \mathrm{diag}[a_+, a_-] \in \mathbb{C}^{2\times 2}$. Note that the latter statement also holds for $\omega \in \pi\mathbb{Z}$.

iii) Let $A := \begin{bmatrix} 1 & \cdot \\ 1 & 1 \end{bmatrix} \in \mathbb{C}^{2\times 2}$. Then we have $XE_n - A = \begin{bmatrix} X-1 & \cdot \\ -1 & X-1 \end{bmatrix} \in \mathbb{C}[X]^{2\times 2}$, thus $\chi_A = (X-1)^2 \in \mathbb{C}[X]$. Hence A has only the eigenvalue $1 \in \mathbb{C}$, where $\nu_1(A) = 2$. But we have $\ker(A - E_2) = \langle [0,1]^{\text{tr}} \rangle_{\mathbb{C}}$, thus $\gamma_1(A) = 1$, implying that A is not diagonalisable, not even over $\mathbb{C}$. $\sharp$

(2.6) Example: Fibonacci numbers. The following problem was posed in the medieval book 'Liber abbaci' [**Leonardo da Pisa 'Fibonacci', 1202**]: Any female rabbit gives birth to a couple of rabbits monthly, from its second month of life on. If there is a single couple in the first month, how many are there in month $n \in \mathbb{N}$?

Hence let $[F_n \in \mathbb{N}_0; n \in \mathbb{N}_0]$ be the **linear recurrent sequence** of **degree** 2 given by $F_0 := 0$ and $F_1 := 1$, and $F_{n+2} := F_n + F_{n+1}$ for $n \in \mathbb{N}_0$. Thus we obtain the sequence of **Fibonacci numbers**, see also Table 4:

n	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
F_n	0	1	1	2	3	5	8	13	21	34	55	89	144	233	377	610

To find a closed formula for the Fibonacci numbers, and to determine their growth behavior, we proceed as follows: Letting $A := \begin{bmatrix} \cdot & 1 \\ 1 & 1 \end{bmatrix} \in \mathbb{R}^{2\times 2}$ we have

$A \cdot [F_n, F_{n+1}]^{\text{tr}} = [F_{n+1}, F_{n+2}]^{\text{tr}}$, thus $[F_n, F_{n+1}]^{\text{tr}} = A^n \cdot [F_0, F_1]^{\text{tr}}$, for $n \in \mathbb{N}_0$. Hence we aim at determining A^n using our algebraic techniques:

We have $XE_n - A = \begin{bmatrix} X & -1 \\ -1 & X-1 \end{bmatrix} \in \mathbb{R}[X]^{2\times 2}$, thus $\chi_A = \det(XE_2 - A) = X^2 - X - 1 = (X-\rho_+)(X-\rho_-) \in \mathbb{R}[X]$, where $\rho_\pm := \frac{1}{2}(1 \pm \sqrt{5}) \in \mathbb{R}$. Hence A has the eigenvalues $\{\rho_\pm\} \subseteq \mathbb{R}$, where $\nu_{\rho_\pm}(A) = \gamma_{\rho_\pm}(A) = 1$. From $\ker(A - \rho_\pm E_2) = \langle [1, \rho_\pm]^{\text{tr}} \rangle_{\mathbb{R}}$, letting $P := \begin{bmatrix} 1 & 1 \\ \rho_+ & \rho_- \end{bmatrix} \in \mathrm{GL}_2(\mathbb{R})$, we get $P^{-1}AP = \mathrm{diag}[\rho_+, \rho_-]$. Thus we have $P^{-1}A^nP = (P^{-1}AP)^n = (\mathrm{diag}[\rho_+, \rho_-])^n = \mathrm{diag}[\rho_+^n, \rho_-^n]$, hence using $P^{-1} := \frac{1}{\rho_- - \rho_+} \cdot \begin{bmatrix} \rho_- & -1 \\ -\rho_+ & 1 \end{bmatrix}$ we get

$$A^n = P \cdot \mathrm{diag}[\rho_+^n, \rho_-^n] \cdot P^{-1} = \frac{1}{\rho_- - \rho_+} \cdot \begin{bmatrix} \rho_+^n \rho_- - \rho_+ \rho_-^n & \rho_-^n - \rho_+^n \\ \rho_+^{n+1}\rho_- - \rho_+\rho_-^{n+1} & \rho_-^{n+1} - \rho_+^{n+1} \end{bmatrix}.$$

This yields $F_n = \frac{\rho_-^n - \rho_+^n}{\rho_- - \rho_+} = \frac{1}{\sqrt{5}}(\rho_+^n - \rho_-^n)$, which since $|\rho_+| > 1 > |\rho_-|$ entails $F_n = \lfloor \frac{\rho_+^n}{\sqrt{5}} \rceil$ and $\lim_{n\to\infty} \frac{F_n \cdot \sqrt{5}}{\rho_+^n} = 1$, in particular F_n grows exponentially. ♯

The number $\rho_+ := \frac{1}{2}(1+\sqrt{5}) \in \mathbb{R}$ is called the **golden ratio**, featuring in the following classical problem: How has a line segment to be cut into two pieces, such that length ratio between the full segment and the longer piece coincides with the length ratio between the longer and the shorter piece? Assume that the line segment has length 1, and letting $\frac{1}{2} < x < 1$ be the length of the longer piece, we thus have $\frac{1}{x} = \frac{x}{1-x}$, or equivalently $x^2 + x - 1 = 0$, which yields $x = \frac{1}{2}(-1+\sqrt{5}) \in \mathbb{R}$ as the unique positive solution. Thus the above ratio indeed equals $\frac{x}{1-x} = \frac{1}{x} = \frac{2}{-1+\sqrt{5}} = \frac{1}{2}(1+\sqrt{5}) = \rho_+$.

3 Jordan normal form

(3.1) Generalised eigenspaces. a) Let K be a field and $A \in K^{n\times n}$, where $n \in \mathbb{N}_0$. For the ring homomorphism $\sigma\colon K \to K^{n\times n}\colon a \mapsto aE_n$ we have $aE_n \cdot A = A \cdot aE_n$, hence there is an evaluation map $\sigma_A\colon K[X] \to K^{n\times n}\colon f = \sum_{i\geq 0} a_i X^i \mapsto f_\sigma(A) = \sum_{i\geq 0} a_i A^i$, where for the latter we just write $f(A)$.

For $f \in K[X]$ let $T_f(A) := \ker(f(A)) = \{v \in K^{n\times 1}; f(A)v = 0\} \leq K^{n\times 1}$ be the **generalised eigenspace** of A with respect to f; note that $T_a(A) = T_{X-a}(A)$.

For $v \in T_f(A)$ we have $f(A)Av = Af(A)v = 0$, thus $T_f(A)$ is A**-invariant**, that is we have $A \cdot T_f(A) \leq T_f(A)$. Moreover, if $f = gh \in K[X]$, then for $v \in T_g(A)$ we have $f(A)v = h(A)g(A)v = 0$, thus $T_g(A) \leq T_f(A)$; in particular if $f \sim g \in K[X]$ then we have $T_f(A) = T_g(A)$.

For $P \in \mathrm{GL}_n(K)$ and $v \in T_f(A)$ we have $f(P^{-1}AP) \cdot P^{-1}v = P^{-1}f(A)P \cdot P^{-1}v = P^{-1}f(A)v = 0$, thus $P^{-1}T_f(A) \leq T_f(P^{-1}AP)$, hence replacing A by $P^{-1}AP$ yields $PT_f(P^{-1}AP) \leq T_f(A)$, thus we infer $P^{-1}T_f(A) = T_f(P^{-1}AP)$.

In particular, this implies $\dim_K(T_f(A)) = \dim_K(T_f(P^{-1}AP))$, saying that $\dim_K(T_f(A)) \in \mathbb{N}_0$ only depends on the similarity class of A.

b) Similarly, given a K-vector space V and $\varphi \in \mathrm{End}_K(V)$, since for the ring homomorphism $\sigma\colon K \to \mathrm{End}_K(V)\colon a \mapsto a \cdot \mathrm{id}$ we have $(a \cdot \mathrm{id}) \cdot \varphi = \varphi \cdot (a \cdot \mathrm{id})$, there is an evaluation map $\sigma_\varphi\colon K[X] \to \mathrm{End}_K(V)\colon f \mapsto f(\varphi) := f_\sigma(\varphi)$. Hence we analogously get **generalised eigenspaces** $T_f(\varphi) := \ker(f(\varphi)) = \{v \in V; f(\varphi)(v) = 0\} \le V$, which are **$\varphi$-invariant**, that is $\varphi(T_f(\varphi)) \le T_f(\varphi)$, and fulfill $T_g(\varphi) \le T_f(\varphi)$, for all $g \mid f \in K[X]$.

(3.2) Minimum polynomials. Let K be a field and $A \in K^{n\times n}$, where $n \in \mathbb{N}_0$. Observing that the evaluation map $\sigma_A\colon K[X] \to K^{n\times n}$ is K-linear, let $I_A := \ker(\sigma_A) = \{f \in K[X]; f(A) = 0 \in K^{n\times n}\} = \{f \in K[X]; T_f(A) = K^{n\times 1}\} = \{f \in K[X]; \dim_K(T_f(A)) = n\} \le K[X]$ be the **order ideal** of A.

Apart from being a K-subspace, $I_A \subseteq K[X]$ has the following (name-giving) closure property: For $f \in I_A$ and $g \in K[X]$ we have $K^{n\times 1} \le T_f(A) \le T_{fg}(A) \le K^{n\times 1}$, hence $fg \in I_A$ as well.

Since for any $P \in \mathrm{GL}_n(K)$ and any $f \in K[X]$ we have $\dim_K(T_f(A)) = \dim_K(T_f(P^{-1}AP))$, we infer that $I_A = I_{P^{-1}AP} \le K[X]$, in other words $I_A \le K[X]$ only depends on the similarity class of A.

We have $I_A \ne \{0\}$:

Since $\dim_K(K^{n\times n}) = n^2$, let $k \in \{0, \ldots, n^2\}$ be minimal such that $[A^i \in K^{n\times n}; i \in \{0, \ldots, k\}]$ is K-linearly dependent. Hence there are $c_0, \ldots, c_{k-1} \in K$ such that $A^k + \sum_{i=0}^{k-1} c_i A^i = 0 \in K^{n\times n}$, thus we have $0 \ne \mu := X^k + \sum_{i=0}^{k-1} c_i X^i \in I_A \le K[X]$. Moreover, since $[A^i \in K^{n\times n}; i \in \{0, \ldots, k-1\}]$ is K-linearly independent, this also shows that I_A does not contain any non-zero polynomial of degree $< k$, thus $\mu \in I_A$ is of minimal degree. $\sharp$

Hence let now $0 \ne f \in I_A$ be arbitrary of minimal degree. Then for any $g \in I_A$ quotient and remainder yields $g = qf + r$, where $q, r \in K[X]$ such that $r = 0$ or $\deg(r) < \deg(f)$. Thus we have $r(A) = g(A) - q(A)f(A) = 0 \in K^{n\times n}$, that is $r \in I_A$ as well, and minimality implies $r = 0$. Hence we infer that $f \mid g$ for all $g \in I_A$; in particular, f is uniquely determined up to associates.

Thus the unique monic polynomial $0 \ne \mu_A := \mu \in I_A$ of minimal degree is called the **minimum polynomial** of A. Hence we have $I_A = \mu_A \cdot K[X] := \{\mu_A \cdot f \in K[X]; f \in K[X]\}$, in other words $\mu_A \in \gcd(I_A)$; recall that $\deg(\mu_A) \le n^2$.

Since $I_A \le K[X]$ only depends on the similarity class of A, so does $\mu_A \in K[X]$. We have $\deg(\mu_A) = 0$ if and only if $n = 0$, in which case we have $\mu_A = 1 \in K[X]$. For example, for $n \ge 1$ and $a \in K$ we have $\mu_{aE_n} = X - a \in K[X]$.

If V is a finitely generated K-vector space and $\varphi \in \mathrm{End}_K(V)$, choosing a K-basis $B \subseteq V$ yields the **order ideal** $I_\varphi := I_{M_B^B(\varphi)} \le K[X]$ and the **minimum polynomial** $\mu_\varphi := \mu_{M_B^B(\varphi)} \in K[X]$ of φ.

(3.3) Theorem: Cayley-Hamilton. Let K be a field and let $A \in K^{n \times n}$, where $n \in \mathbb{N}_0$. Then we have $\chi_A \in I_A$, that is we have $\mu_A \mid \chi_A \in K[X]$; in particular we have $\deg \mu_A \leq n$.

Proof. For $n = 0$ we have $\mu_A = \chi_A = 1 \in K[X]$, hence we may assume $n \geq 1$. The entries of the adjoint matrix $\mathrm{adj}(XE_n - A) \in K[X]^{n \times n}$ consist of $(n-1)$-minors of the characteristic matrix $XE_n - A \in K[X]^{n \times n}$, hence are 0 or have degree at most $n-1$. Thus, essentially viewing a matrix with polynomial entries as a polynomial with matrix coefficients, there are $A_0, \ldots, A_{n-1} \in K^{n \times n}$ such that $\mathrm{adj}(XE_n - A) = \sum_{i=0}^{n-1} X^i A_i \in K[X]^{n \times n}$.

Letting $\chi_A = \det(XE_n - A) = \sum_{i=0}^{n} b_i X^i \in K[X]$ we get $\sum_{i=0}^{n} b_i X^i E_n = \det(XE_n - A) \cdot E_n = (XE_n - A) \cdot \mathrm{adj}(XE_n - A) = (XE_n - A) \cdot \sum_{i=0}^{n-1} X^i A_i = X^n A_{n-1} - AA_0 + \sum_{i=1}^{n-1} X^i (A_{i-1} - AA_i) \in K[X]^{n \times n}$. Thus, again viewing a matrix with polynomial entries as a polynomial with matrix coefficients, a comparison of coefficients yields $b_n E_n = A_{n-1}$ and $b_0 E_n = -AA_0$, as well as $b_i E_n = A_{i-1} - AA_i$ for $i \in \{1, \ldots, n-1\}$.

Hence we obtain $\chi_A(A) = \sum_{i=0}^{n} b_i A^i = \sum_{i=0}^{n} A^i (b_i E_n) = A^n A_{n-1} - AA_0 + \sum_{i=1}^{n-1} (A^i A_{i-1} - A^{i+1} A_i) = A^n A_{n-1} - AA_0 + (AA_0 - A^n A_{n-1}) = 0 \in K^{n \times n}$. $\sharp$

(3.4) Principal invariant subspaces. a) Let K be a field and let $A \in K^{n \times n}$, where $n \in \mathbb{N}_0$. Let $0 \neq f = gh \in K[X]$, where g and h are coprime, such that $\mu_A \mid f$, that is $f(A) = 0$. Then we have $V := K^{n \times 1} = T_g(A) \oplus T_h(A)$, where moreover $T_g(A) = \mathrm{im}(h(A))$ and $T_h(A) = \mathrm{im}(g(A))$:

Since $1 \in \gcd(g, h) \subseteq K[X]$, there are $g', h' \in K[X]$ such that $1 = gg' + hh' \in K[X]$. For $v = g(A)w \in \mathrm{im}(g(A))$, where $w \in V$, we get $h(A)v = h(A)g(A)w = f(A)w = 0$, implying $\mathrm{im}(g(A)) \leq T_h(A)$, similarly $\mathrm{im}(h(A)) \leq T_g(A)$. For $v \in T_g(A)$ we have $v = E_n v = E_n v - g'(A)g(A)v = h(A)h'(A)v \in \mathrm{im}(h(A))$, implying $T_g(A) \leq \mathrm{im}(h(A))$, and similarly $T_h(A) \leq \mathrm{im}(g(A))$. Hence we have $T_g(A) = \mathrm{im}(h(A))$ and $T_h(A) = \mathrm{im}(g(A))$.

For $v \in V$ we have $v = E_n v = g(A)g'(A)v + h(A)h'(A)v$, hence we have $V = \mathrm{im}(g(A)) + \mathrm{im}(h(A)) = T_g(A) + T_h(A)$. Finally, let $v \in T_g(A) \cap T_h(A)$, then $v = E_n v = g'(A)g(A)v + h'(A)h(A)v = 0$, thus we have $T_g(A) \cap T_h(A) = \{0\}$. $\sharp$

b) Since $T_g(A) \leq V$ and $T_h(A) \leq V$ are A-invariant, choosing K-bases $B \subseteq T_g(A)$ and $C \subseteq T_h(A)$ we get matrices $A_g := M_B^B(\varphi_A|_{T_g(A)}) \in K^{l \times l}$ and $A_h := M_C^C(\varphi_A|_{T_h(A)}) \in K^{m \times m}$, where $l := \dim_K(T_g(A)) \in \mathbb{N}_0$ and $m := \dim_K(T_h(A)) \in \mathbb{N}_0$. Hence $P := [B, C] \in \mathrm{GL}_n(K)$ is a K-basis of V, and A is similar to the **block diagonal matrix** $P^{-1}AP = A_g \oplus A_h \in K^{n \times n}$.

We have $\mu_{A_g} \mid g \in K[X]$ and $\mu_{A_h} \mid h \in K[X]$, as well as $\mu_A \in \mathrm{lcm}(\mu_{A_g}, \mu_{A_h}) \subseteq K[X]$, hence since μ_{A_g} and μ_{A_h} are coprime we infer that $\mu_A = \mu_{A_g}\mu_{A_h}$. In particular, since $\mu_{A_g} \mid \gcd(g, \mu_A)$, we infer that if g and μ_A are coprime then we have $\mu_{A_g} = 1$, in other words $T_g(A) = \{0\}$. Moreover, if $\mu_A \sim f$ then we have $\mu_{A_g} \sim g$ and $\mu_{A_h} \sim h$, entailing $\deg(g) = \deg(\mu_{A_g}) \leq \deg(\chi_{A_g}) =$

$\dim_K(T_g(A))$, and similarly $\deg(h) \leq \dim_K(T_h(A))$; in particular, if g is non-constant then we have $T_g(A) \neq \{0\}$.

Hence, if $\mu_A = \prod_{p\in\mathcal{P}} p^{\nu_p} \in K[X]$, where $\nu_p \in \mathbb{N}_0$ and $\mathcal{P} \subseteq K[X]$ is the set of monic irreducible polynomials, by induction we obtain the direct sum decomposition $V = \bigoplus_{p\in\mathcal{P}} T_{p^{\nu_p}}(A)$ into **principal A-invariant subspaces** $T_{p^{\nu_p}}(A) \leq V$, where the K-endomorphism of $T_{p^{\nu_p}}(A)$ induced by A has minimum polynomial $p^{\nu_p} \in K[X]$; in particular $T_{p^{\nu_p}}(A) = \{0\}$ if and only if $\nu_p = 0$.

Example. Let $A := \begin{bmatrix} . & . & 1 \\ 1 & . & . \\ . & 1 & . \end{bmatrix} \in \mathbb{Q}^{3\times 3}$. Thus $\chi_A = \det(XE_3 - A) = \det\left(\begin{bmatrix} X & . & -1 \\ -1 & X & . \\ . & -1 & X \end{bmatrix}\right) = X^3 - 1 = (X-1)(X^2+X+1) \in \mathbb{Q}[X]$, where both factors given are irreducible, and hence are coprime. We have $A^2 = \begin{bmatrix} . & 1 & . \\ . & . & 1 \\ 1 & . & . \end{bmatrix}$ and $A^3 = E_3$, hence $\{E_3, A, A^2\}$ is $\mathbb{Q}$-linearly independent, but $\{E_3, A, A^2, A^3\}$ is $\mathbb{Q}$-linearly dependent, where $A^3 = E_3$ shows that $\mu_A = X^3 - 1 = \chi_A \in \mathbb{Q}[X]$.

We have $A - E_3 = \begin{bmatrix} -1 & . & 1 \\ 1 & -1 & . \\ . & 1 & -1 \end{bmatrix}$ and $A^2 + A + 1 = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix}$, which yields $T_{X-1}(A) = \ker(A - E_3) = \langle [1,1,1]^{\mathrm{tr}} \rangle_{\mathbb{Q}} = \mathrm{im}(A^2 + A + 1)$ and $T_{X^2+X+1}(A) = \ker(A^2 + A + E_3) = \langle [1,-1,0]^{\mathrm{tr}}, [0,1,-1]^{\mathrm{tr}} \rangle_{\mathbb{Q}} = \mathrm{im}(A - E_3)$. Hence letting $P := \begin{bmatrix} 1 & 1 & 0 \\ 1 & -1 & 1 \\ 1 & 0 & -1 \end{bmatrix} \in \mathrm{GL}_3(\mathbb{Q})$ we get $P^{-1}AP = \left[\begin{array}{c|cc} 1 & . & . \\ \hline . & . & -1 \\ . & 1 & -1 \end{array}\right]$, where $\mu_{A_{X-1}} = X - 1 \in \mathbb{Q}[X]$ and $\mu_{A_{X^2+X+1}} = X^2 + X + 1 \in \mathbb{Q}[X]$. $\sharp$

(3.5) Diagonalisability again. Let K be a field and let $A \in K^{n\times n}$, where $n \in \mathbb{N}_0$. Then A is diagonalisable if and only if μ_A splits into pairwise non-associate linear factors; in this case the principal A-invariant subspaces coincide with the eigenspaces of A:

If A is diagonal, then we have $\chi_A = \prod_{i=1}^s (X - a_i)^{\nu_{a_i}(A)} \in K[X]$, for some $s \in \mathbb{N}_0$, where $\{a_1, \ldots, a_s\} \subseteq K$ are the eigenvalues of A, each occurring with multiplicity $\nu_{a_i}(A) = \gamma_{a_i}(A) \in \mathbb{N}$. Then letting $f := \prod_{i=1}^s (X - a_i)$, we have $f(A) = \prod_{i=1}^s (A - a_i E_n) = 0$, hence $\mu_A \mid f$. Moreover, the maximal proper divisors of f being $f_j := \prod_{i\neq j} (X - a_i) \in K[X]$, where $j \in \{1, \ldots, s\}$, we from $\mathrm{rk}(f_j(A)) = \nu_{a_j}(A) \geq 1$ infer that $\mu_A \nmid f_j$. Hence we have $\mu_A = \prod_{i=1}^s (X - a_i) \in K[X]$.

Conversely, let $\mu_A = \prod_{i=1}^s (X - a_i) \in K[X]$, where $s \in \mathbb{N}_0$ and $\{a_1, \ldots, a_s\} \subseteq K$ are pairwise different. Then $K^{n\times 1} = \bigoplus_{i=1}^s T_{X-a_i}(A)$ is the direct sum of the eigenspaces of A with respect to the a_i, thus A is diagonalisable. $\sharp$

(3.6) Jordan normal form. a) Let K be a field, and let $A \in K^{n\times n}$, where $n \in \mathbb{N}$; there is no point in considering the case $n = 0$. Let $p := X - a \in K[X]$, and let $\mu_A = p^l$ for some $l \in \{1, \ldots, n\}$. For $i \in \mathbb{N}_0$ we let $V_i := T_{p^i}(A) = \ker((A - aE_n)^i) \leq K^{n\times 1} =: V$. Thus we have $\{0\} = V_0 \leq V_1 \leq \cdots \leq V_{l-1} < V_l = V_{l+1} = \cdots = V$. Letting $n_i := \dim_K(V_i) - \dim_K(V_{i-1}) \in \mathbb{N}_0$ for $i \in \mathbb{N}$, we have $n_l > 0$, and $n_i = 0$ for $i > l$, where $\sum_{i=1}^{l} n_i = n$.

Then there is a K-basis $[v_{l1}, \ldots, v_{ln_l}; v_{l-1,1}, \ldots, v_{l-1,n_{l-1}}; \ldots; v_{11}, \ldots, v_{1n_1}] \subseteq V$, such that $[v_{i1}, \ldots, v_{in_i}; \ldots; v_{11}, \ldots, v_{1n_1}] \subseteq V_i$ is a K-basis, for all $i \in \{1, \ldots, l\}$, and $v_{i-1,j} = p(A)v_{ij} = (A-aE_n)v_{ij} = Av_{ij} - av_{ij}$ for all $i \in \{2, \ldots, l\}$ and $j \in \{1, \ldots, n_i\}$; thus in particular we have $n_1 \geq n_2 \geq \cdots \geq n_l > 0$:

We proceed by induction on $l \in \mathbb{N}$; the case $l = 1$ being trivial, let $l \geq 2$: Let $[v_1, \ldots, v_k; v'_{k+1}, \ldots, v'_{k+k'}; v''_{k+k'+1}, \ldots, v''_n] \subseteq V$ be a K-basis, such that $[v'_{k+1}, \ldots, v'_{k+k'}; v''_{k+k'+1}, \ldots, v''_n] \subseteq V_{l-1}$ and $[v''_{k+k'+1}, \ldots, v''_n] \subseteq V_{l-2}$ are K-bases as well, where $k := n_l$ and $k' := n_{l-1}$. Letting $w_j := p(A)v_j$ for $j \in \{1, \ldots, k\}$, we have $p^{l-1}(A)w_j = p^l(A)v_j = 0$, that is $w_j \in V_{l-1}$.

Then $[w_1, \ldots, w_k; v''_{k+k'+1}, \ldots, v''_n]$ is K-linearly independent: Let $\sum_{j=1}^{k} a_j w_j + \sum_{j=1}^{n-k-k'} b_j v''_{k+k'+j} = 0$, where $a_1, \ldots, a_k, b_1, \ldots, b_{n-k-k'} \in K$, then we get $p(A)^{l-1}(\sum_{j=1}^{k} a_j v_j) = p(A)^{l-2}(\sum_{j=1}^{k} a_j w_j) = -p(A)^{l-2}(\sum_{j=1}^{n-k-k'} b_j v''_{k+k'+j}) = 0$, thus $\sum_{j=1}^{k} a_j v_j \in V_{l-1}$. Since $[v_1, \ldots, v_k]$ extends a K-basis of V_{l-1} to one of V, we infer $a_j = 0$ for $j \in \{1, \ldots, k\}$, and thus by the K-linear independence of $[v''_{k+k'+1}, \ldots, v''_n]$ we get $b_j = 0$ for $j \in \{1, \ldots, n-k-k'\}$ as well. Thus we may assume that $v'_{k+j} = w_j$, for $j \in \{1, \ldots, k\}$, and we are done by induction. ♯

Reordering the above K-basis we obtain the **Jordan K-basis**

$$P = [P_{l1}, \ldots, P_{ln_l}; P_{l-1,n_l+1}, \ldots, P_{l-1,n_{l-1}}; \ldots; P_{1,n_2+1}, \ldots, P_{1,n_1}] \in \mathrm{GL}_n(K),$$

where $P_{ij} := [v_{ij}, v_{i-1,j}, \ldots, v_{1j}] \in K^{n\times i}$, for $i \in \{1, \ldots, l\}$ and $j \in \{n_{i+1} + 1, \ldots, n_i\}$. In particular, there are precisely $m_i := n_i - n_{i+1} \in \mathbb{N}_0$ subsets P_{ij} of cardinality $i \in \mathbb{N}$; note that $m_i = 0$ for $i > l$.

Then $Av_{ij} = p(A)v_{ij} + av_{ij} = v_{i-1,j} + av_{ij}$ implies that the column space $\mathrm{im}(P_{ij}) \leq V$ is A-invariant. Hence A is similar to the block diagonal matrix $P^{-1}AP = \bigoplus_{i=1}^{l} \bigoplus_{j=1}^{m_i} J_i(a) = \bigoplus_{i=1}^{n} \bigoplus_{j=1}^{m_i} J_i(a)$, with **Jordan matrices**

$$J_i(a) := \begin{bmatrix} a & . & . & . & \ldots & . \\ 1 & a & . & . & \ldots & . \\ . & 1 & a & . & \ldots & . \\ \vdots & \ddots & \ddots & \ddots & \ddots & \vdots \\ . & \ldots & . & 1 & a & . \\ . & \ldots & . & . & 1 & a \end{bmatrix} \in K^{i\times i}.$$

b) The multiplicities $m_1, \ldots, m_n \in \mathbb{N}_0$ are uniquely determined by A:

For a Jordan matrix $J := J_l(a) \in K^{l\times l}$ we have $\chi_J = \det(XE_l - J) = p^l \in K[X]$, that is $\nu_a(J) = l$. Moreover, we have $\mathrm{rk}(p^i(J)) = \mathrm{rk}((J - aE_l)^i) = l - i$, that is

$\dim_K(T_{p^i}(J)) = i$ for $i \in \{0, \ldots, l\}$; hence $\dim_K(T_{p^i}(J)) = l$ is constant for $i \geq l$. Thus we have $\mu_J = p^l = \chi_J \in K[X]$, and $\dim_K(T_{p^i}(J)) - \dim_K(T_{p^{i-1}}(J)) = 1$ for $i \in \{1, \ldots, l\}$; in particular $\gamma_a(J) = \dim_K(T_a(J)) = \dim_K(T_p(J)) = 1$.

Hence for any matrix $A = \bigoplus_{i=1}^n \bigoplus_{j=1}^{m_i} J_i(a) \in K^{n \times n}$, where $m_1, \ldots, m_n \in \mathbb{N}_0$ such that $\sum_{i=1}^n i m_i = n$, we have $n_i := \dim_K(T_{p^i}(A)) - \dim_K(T_{p^{i-1}}(A)) = \sum_{j=i}^n m_j$, for all $i \in \{1, \ldots, n\}$, implying that $m_i = n_i - n_{i+1}$. Hence the m_i are determined by A alone, independent of a particular choice of a Jordan form. $\sharp$

c) In practice **Jordan normal forms** can be computed combinatorially, without specifying a Jordan K-basis, if the K-dimensions of the K-subspaces $V_i = T_{p^i}(A) \leq V$ are known, for all $i \in \mathbb{N}_0$. This is best explained by an example:

Example. Let $n = 13$ and $[\dim_K(V_i) \in \mathbb{N}_0; i \in \mathbb{N}_0] = [0, 5, 8, 10, 12, 13, 13, \ldots]$, hence we have $l = 5$ and the numbers $n_i = \dim_K(V_i) - \dim_K(V_{i-1}) \in \mathbb{N}_0$, for $i \in \mathbb{N}$, are given as $[n_i \in \mathbb{N}_0; i \in \mathbb{N}] = [5, 3, 2, 2, 1, 0, \ldots]$. We depict the $n_i \in \mathbb{N}$, for $i \in \{1, \ldots, l\}$, as the rows of the following diagram, from bottom to top:

$$\begin{array}{ccccc}
\boxed{\mathbf{v_{51}}} & & & & \\
\boxed{v_{41}} & \boxed{\mathbf{v_{42}}} & & & \\
\boxed{v_{31}} & \boxed{v_{32}} & & & \\
\boxed{v_{21}} & \boxed{v_{22}} & \boxed{\mathbf{v_{23}}} & & \\
\boxed{v_{11}} & \boxed{v_{12}} & \boxed{v_{13}} & \boxed{\mathbf{v_{14}}} & \boxed{\mathbf{v_{15}}}
\end{array}$$

Then the multiplicity $m_i = n_i - n_{i+1} \in \mathbb{N}_0$ can be read off from the diagram, as the number of columns of height $i \in \mathbb{N}$; of course it suffices to consider $i \in \{1, \ldots, l\}$. Here we obtain the column heights $[5, 4, 2, 1, 1, 0, \ldots]$, and therefrom $[m_i \in \mathbb{N}_0; i \in \mathbb{N}] = [2, 1, 0, 1, 1, 0, \ldots]$, thus the Jordan normal form of the matrix A in question is $J_5(a) \oplus J_4(a) \oplus J_2(a) \oplus J_1(a) \oplus J_1(a) \in K^{13 \times 13}$.

Moreover, the vectors v_{ij} constituting the Jordan K-basis $P \subseteq V$ can be filled into the diagram as indicated above. Then the subset $P_{ij} \subseteq P$ coincides with the vectors in column i, in other words the K-subspaces generated by tbe vectors in either column are A-invariant. The construction of P can be described as follows, again by way of the above example; the vectors we are free to choose are depicted in bold face in the above diagram:

We choose $v_{51} \in V_5$, being placed on top of column 1, extending any K-basis of V_4 to a K-basis of V_5; then successively working down column 1 we get $v_{5-i,1} = p^i(A)(v_{51}) \in V_{5-i} \setminus V_{4-i}$ for $i \in \{1, \ldots, 4\}$. Then we chosse $v_{42} \in V_4$, being placed on top of column 2, so that $\{v_{41}, v_{42}\}$ extends any K-basis of V_3 to a K-basis of V_4; then successively working down column 2 we get $v_{4-i,2} = p^i(A)(v_{42}) \in V_{4-i} \setminus V_{3-i}$ for $i \in \{1, \ldots, 3\}$. Next we observe that $\{v_{31}, v_{32}\}$ already extends any K-basis of V_2 to a K-basis of V_3, so we are done for V_3. Proceeding further, we chosse $v_{23} \in V_2$, being placed on top of column 3, so that $\{v_{21}, v_{22}, v_{23}\}$ extends any K-basis of V_1 to a K-basis of V_2; then working down column 3 we get $v_{13} = p(A)(v_{23})$. Finally, we chosse $v_{14}, v_{15} \in V_1$, being placed in columns 4 and 5, extending $\{v_{11}, v_{12}, v_{13}\}$ to a K-basis of V_2; recall that we have $V_0 = \{0\}$ which has an empty K-basis. $\sharp$

Example. More explicitly, let $A := \begin{bmatrix} 1 & -1 & 1 \\ 3 & 5 & -3 \\ 2 & 2 & 0 \end{bmatrix} \in \mathbb{Q}^{3\times 3}$, thus $\chi_A = X^3 - 6X^2 + 12X - 8 = (X-2)^3 \in \mathbb{Q}[X]$. We have $A - 2E_3 = \begin{bmatrix} -1 & -1 & 1 \\ 3 & 3 & -3 \\ 2 & 2 & -2 \end{bmatrix}$, hence we get $V_1 := \ker(A - 2E_3) = \langle [1,-1,0]^{\text{tr}}, [0,1,1]^{\text{tr}} \rangle_{\mathbb{Q}}$, thus $n_1 = 2$. This already implies that $V_2 := \ker((A-2E_3)^2) = V = \mathbb{Q}^{3\times 1}$, hence $n_2 = 1$ and $l = 2$, that is $\mu_A = (X-2)^2 \in \mathbb{Q}[X]$. Thus we have $m_2 = m_1 = 2$, and the Jordan normal form of A is $J_2(2) \oplus J_1(2) = \left[\begin{array}{cc|c} 2 & . & . \\ 1 & 2 & . \\ \hline . & . & 2 \end{array}\right]$. Letting $v_{21} := [1,0,0]^{\text{tr}} \in V \setminus V_1$, we get $v_{11} := Av_{21} - 2v_{21} = [-1,3,2]^{\text{tr}} \in V_1$, and extending by $v_{12} := [1,-1,0]^{\text{tr}} \in V_1$ to the $\mathbb{Q}$-basis $\{v_{11}, v_{12}\} \subseteq V_1$, we get the $\mathbb{Q}$-basis $P := [v_{21}, v_{11}; v_{12}] \in \mathrm{GL}_3(\mathbb{Q})$ such that $P^{-1}AP = J_2(2) \oplus J_1(2)$. $\sharp$

(3.7) Triangularisability. a) Let K be a field, and let $A \in K^{n\times n}$, where $n \in \mathbb{N}_0$. Then A is triangularisable if and only if $\chi_A \in K[X]$ splits into linear factors, or equivalently if and only if $\mu_A \in K[X]$ splits into linear factors; in particular, if K is algebraically closed then A is triangularisable:

If A is triangular, then $\chi_A = \prod_{i=1}^s (X - a_i)^{\nu_{a_i}(A)} \in K[X]$, for some $s \in \mathbb{N}_0$, where $\{a_1, \ldots, a_s\} \subseteq K$ are the diagonal entries of A, each occurring with multiplicity $\nu_{a_i}(A) \in \mathbb{N}$. Hence $\chi_A \in K[X]$ splits into linear factors. Since $\mu_A \mid \chi_A$, this implies that $\mu_A \in K[X]$ splits into linear factors as well.

Hence let now $\mu_A \in K[X]$ split into linear factors, that is we have $\mu_A = \prod_{i=1}^s (X - a_i)^{l_i} \in K[X]$, for some $s \in \mathbb{N}_0$, where $\{a_1, \ldots, a_s\} \subseteq K$ are pairwise different and $l_i \in \mathbb{N}$. Letting $f_i = (X - a_i)^{l_i} \in K[X]$, we have $K^{n\times 1} = \bigoplus_{i=1}^s T_{f_i}(A)$; let $d_i := \dim_K(T_{f_i}(A)) \in \mathbb{N}$. Hence choosing a K-basis of $K^{n\times 1}$ respecting this direct sum decomposition, we infer that A is similar to a block diagonal matrix $\bigoplus_{i=1}^s A_{f_i}$, where for the matrix $A_{f_i} \in K^{d_i \times d_i}$ we have $\mu_{A_{f_i}} = f_i \in K[X]$, for $i \in \{1, \ldots, s\}$. Thus choosing Jordan K-bases $P_i \subseteq T_{f_i}(A)$, for all $i \in \{1, \ldots, s\}$, and letting $P := [P_1, \ldots, P_s] \in \mathrm{GL}_n(K)$, then A is similar to the block diagonal matrix $P^{-1}AP = \bigoplus_{i=1}^s P_i^{-1} A_{f_i} P_i \in K^{n\times n}$, where each $P_i^{-1} A_{f_i} P_i \in K^{d_i \times d_i}$ again is a block diagonal matrix, consisting of Jordan matrices with respect to the eigenvalue a_i. $\sharp$

b) Since $\mu_A \mid \chi_A \in K[X]$, the irreducible divisors of μ_A are amongst those of χ_A. Indeed, the linear factors of μ_A and of χ_A coincide: (Actually, all the irreducible divisors of μ_A and of χ_A coincide, not only the linear ones, but we are not able to prove this here.)

Assume to the contrary that $X - a \mid \chi_A$, but $X - a \nmid \mu_A$; then we have $\chi_A(a) = 0$, saying that $a \in K$ is an eigenvalue of A, that is $T_{X-a}(A) \neq \{0\}$; but since $X - a$ and μ_A are coprime we have $T_{X-a}(A) = \{0\}$, a contradiction. $\sharp$

If $\mu_A = \prod_{i=1}^s (X - a_i)^{l_i} \in K[X]$ splits into linear factors, then by the above we have $\chi_A = \prod_{i=1}^s (X - a_i)^{d_i}$, that is the algebraic multiplicity of the eigenvalue a_i is given as $\nu_{a_i}(A) = d_i = \dim_K(T_{(X-a_i)^{l_i}}(A))$, for $i \in \{1, \ldots, s\}$.

Example. We proceed to show that

$$A := \begin{bmatrix} 1 & -2 & -1 & 2 \\ 0 & -1 & -1 & 2 \\ 2 & -2 & -1 & 4 \\ 1 & -1 & 0 & 1 \end{bmatrix} \sim J_2(1) \oplus J_2(-1) = \left[\begin{array}{cc|cc} 1 & . & . & . \\ 1 & 1 & . & . \\ \hline . & . & -1 & . \\ . & . & 1 & -1 \end{array}\right] \in \mathbb{Q}^{4\times 4}:$$

We have $\chi_A = X^4 - 2X^2 + 1 = (X-1)^2(X+1)^2 \in \mathbb{Q}[X]$. This entails the direct sum decomposition $V := \mathbb{Q}^{4\times 1} = T_{(X-1)^2}(A) \oplus T_{(X+1)^2}(A)$, where the principal subspaces have dimension $\dim_{\mathbb{Q}}(T_{(X-1)^2}(A)) = 2 = \dim_{\mathbb{Q}}(T_{(X+1)^2}(A))$. Moreover, since it turns out that $\dim_{\mathbb{Q}}(T_{X-1}(A)) = 1 = \dim_{\mathbb{Q}}(T_{X+1}(A))$, we infer that the Jordan normal form of A indeed is $J_2(1) \oplus J_2(-1)$.

To obtain $P \in \mathrm{GL}_4(\mathbb{Q})$ such that $P^{-1}AP = J_2(1) \oplus J_2(-1)$ we proceed as follows: We have

$$A - E_4 = \begin{bmatrix} 0 & -2 & -1 & 2 \\ 0 & -2 & -1 & 2 \\ 2 & -2 & -2 & 4 \\ 1 & -1 & 0 & 0 \end{bmatrix} \quad \text{and} \quad (A - E_4)^2 = \begin{bmatrix} 0 & 4 & 4 & -8 \\ 0 & 4 & 4 & -8 \\ 0 & 0 & 4 & -8 \\ 0 & 0 & 0 & 0 \end{bmatrix},$$

$$A + E_4 = \begin{bmatrix} 2 & -2 & -1 & 2 \\ 0 & 0 & -1 & 2 \\ 2 & -2 & 0 & 4 \\ 1 & -1 & 0 & 2 \end{bmatrix} \quad \text{and} \quad (A - E_4)^2 = \begin{bmatrix} 4 & -4 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 8 & -8 & 0 & 8 \\ 4 & -4 & 0 & 4 \end{bmatrix},$$

from which we get $\ker(A - E_4) = \langle [0,0,2,1]^{\mathrm{tr}} \rangle_{\mathbb{Q}}$ as well as $\ker((A - E_4)^2) = \langle [0,0,2,1]^{\mathrm{tr}}, [1,0,0,0]^{\mathrm{tr}} \rangle_{\mathbb{Q}}$, and similarly $\ker(A + E_4) = \langle [1,1,0,0]^{\mathrm{tr}} \rangle_{\mathbb{Q}}$ as well as $\ker((A + E_4)^2) = \langle [1,1,0,0]^{\mathrm{tr}}, [0,0,1,0]^{\mathrm{tr}} \rangle_{\mathbb{Q}}$. Hence letting $v_{1,2} := [1,0,0,0]^{\mathrm{tr}}$ and $v_{1,1} := (A - E_4)v_{1,2} = [0,0,2,1]^{\mathrm{tr}}$, and $v_{-1,2} := [0,0,1,0]^{\mathrm{tr}}$ and $v_{-1,1} := (A + E_4)v_{-1,2} = [-1,-1,0,0]^{\mathrm{tr}}$ yields $P := [v_{1,2}, v_{1,1}; v_{-1,2}, v_{-1,1}] \in \mathrm{GL}_4(\mathbb{Q})$. $\sharp$

(3.8) Example: Damped harmonic oscillator. Let again $C^\infty(\mathbb{R}) := \{\mathbb{R} \to \mathbb{R} \colon t \mapsto x(t) \text{ smooth}\}$, where now we denote variables and maps by the letters 't' and 'x', respectively, being reminiscent of their forthcoming physical interpretation as time and place, respectively. We again use the differential operator $D := \frac{\partial}{\partial t} \in \mathrm{End}_{\mathbb{R}}(C^\infty(\mathbb{R}))$, where we abbreviate $\dot{x} := D(x) = \frac{\partial}{\partial t}(x)$.

We consider a **(single) body** of **(inert) mass** $m > 0$, being fixed to a spring. Pulling the body away from the point of equilibrium, and releasing it, it will start to oscillate. Letting $x = x(t) \in \mathbb{R}$ denote the **place** of the body at time $t \in \mathbb{R}$, its **velocity** and **acceleration** are given as $\dot{x} = \dot{x}(t) \in \mathbb{R}$ and $\ddot{x} = \ddot{x}(t) \in \mathbb{R}$, respectively. By **Newton's Law of Motion** the acceleration of the body is proportional to the force exerted to it, the proportionality factor just being its mass m. In turn, the pulling-back force exerted to the body by the spring is proportional to the distance of the place of the body to the point of equilibrium, the proportionality factor being the square of the **spring constant** $k > 0$. Assuming that the point of equilibrium is $x = 0$, we thus obtain the differential equation $m\ddot{x} = -k^2 x$ of the **(free) harmonic oscillator**.

We additionally allow for **friction**, which exerts a decelerating force to the body. The latter is proportional to its velocity, the proportionality factor being the **friction constant** $r \geq 0$; for $r = 0$ we recover the free harmonic oscillator. Hence the differential equation of the **damped** harmonic oscillator, describing the motion of the body in this **physical system**, is given as $m\ddot{x} = -r\dot{x} - k^2 x$, a **linear** differential equation of **degree** 2 with **constant coefficients**.

Hence we are looking for the $\mathbb{R}$-subspace $\mathcal{L} = \mathcal{L}_{\rho,\omega} \leq C^\infty(\mathbb{R})$ of solutions of the $\mathbb{R}$-endomorphism $D^2 + 2\rho D + \omega^2$ of $C^\infty(\mathbb{R})$, where $\rho := \frac{r}{2m} \geq 0$ and $\omega := \frac{k}{\sqrt{m}} > 0$. A consideration of **Taylor series** shows that $\dim_{\mathbb{R}}(\mathcal{L}) = 2$. More precisely, the motion of the body is uniquely described by imposing arbitrary **initial values** $x(0) \in \mathbb{R}$ and $\dot{x}(0) \in \mathbb{R}$ for the place and the velocity of the body at time $t = 0$. In particular, pulling the body away from the point of equilibrium and releasing it, amounts to letting $x(0) := 1$, say, and $\dot{x}(0) := 0$.

Since $D^2 = -2\rho D - \omega^2$ on $\mathcal{L}$, we conclude that $\mathcal{L}$ is D-invariant, and that the action of D on $\mathcal{L}$ has minimum polynomial $\mu_D \mid p = p_{\rho,\omega} := X^2 + 2\rho X + \omega^2 = (X+\rho)^2 - (\rho^2 - \omega^2) \in \mathbb{R}[X]$. We distinguish three cases with respect to the **discriminant** $\rho^2 - \omega^2 \in \mathbb{R}$ of p being positive, zero or negative, respectively:

i) Let $\rho > \omega > 0$; physically this is the 'large friction' case. Then we have $p = (X-a)(X-b) \in \mathbb{R}[X]$, where $\{a, b\} = \{-\rho \pm \sqrt{\rho^2 - \omega^2}\}$, in particular $a \neq b$ and both $a, b < 0$. We have $\mu_D \in \{X - a, X - b, p\}$, and depending on the case for μ_D we have $\chi_D \in \{(X-a)^2, (X-b)^2, p\}$. Anyway, μ_D splits into pairwise non-associate linear factors, that is D acts diagonalisably on $\mathcal{L}$.

The map $\epsilon_c \colon \mathbb{R} \to \mathbb{R} \colon t \mapsto \exp(ct)$ fulfills $\dot{\epsilon_c} = c\epsilon_c$, that is ϵ_c is an eigenvector of D on $C^\infty(\mathbb{R})$, with respect to the eigenvalue $c \in \mathbb{R}$, see (2.2). Moreover, a consideration of Taylor series shows that the corresponding eigenspace of D actually equals $\langle \epsilon_c \rangle_{\mathbb{R}}$. Hence we conclude that $T_{X-a}(D) = \langle \epsilon_a \rangle_{\mathbb{R}}$ and $T_{X-b}(D) = \langle \epsilon_b \rangle_{\mathbb{R}}$, thus we have the principal subspace decomposition $\mathcal{L} = T_{X-a}(D) \oplus T_{X-b}(D) = \langle \epsilon_a \rangle_{\mathbb{R}} \oplus \langle \epsilon_b \rangle_{\mathbb{R}}$; in particular, we have $\mu_D = p = \chi_D$.

Hence any solution is of the form $x(t) = \alpha \exp(at) + \beta \exp(bt)$, for all $t \in \mathbb{R}$, where $\alpha, \beta \in \mathbb{R}$, entailing $\dot{x}(t) = \alpha a \exp(at) + \beta b \exp(bt)$. Since both $a, b < 0$ we have $\lim_{t\to\infty} x(t) = 0$, saying that the body ultimately tends to the point of equilibrium. Since for any non-zero solution we may assume that $\beta \neq 0$, we have $\dot{x}(t) = 0$ if and only if $\exp((b-a)t) = -\frac{\alpha}{\beta} \cdot \frac{a}{b}$; hence this happens for at most one $t \in \mathbb{R}$, saying that the body changes direction at most once. In particular, letting $x(0) := 1$ and $\dot{x}(0) := 0$, we get $\alpha + \beta = x(0) = 1$ and $\alpha a + \beta b = \dot{x}(0) = 0$, yielding $\alpha = \frac{b}{b-a}$ and $\beta = \frac{a}{a-b}$, that is $x(t) = \frac{1}{b-a} \cdot (b \exp(at) - a \exp(bt))$.

ii) Let $\rho = \omega > 0$. Then we have $p = (X+\rho)^2 \in \mathbb{R}[X]$. We have $\mu_D \in \{X+\rho, p\}$, thus μ_D splits into linear factors anyway, that is D acts triangularisably on

$\mathcal{L}$, and we have $\chi_D = p$. Moreover, we have $T_{X+\rho}(D) = \langle \epsilon_{-\rho} \rangle_{\mathbb{R}}$, implying $\mu_D = p = \chi_D$, that is $\mathcal{L} = T_p(D)$ consists of a single Jordan block. Letting $\widehat{\epsilon}_c \colon \mathbb{R} \to \mathbb{R} \colon t \mapsto t \exp(ct)$, where $c \in \mathbb{R}$, we have $\dot{\widehat{\epsilon}}_c(t) = \exp(ct) + ct \exp(ct)$, for all $t \in \mathbb{R}$, hence $\dot{\widehat{\epsilon}}_c = \epsilon_c + c\widehat{\epsilon}_c$. Thus we have $(D+\rho)(\widehat{\epsilon}_{-\rho}) = \epsilon_{-\rho}$, implying that $\{\widehat{\epsilon}_{-\rho}, \epsilon_{-\rho}\}$ indeed is a Jordan $\mathbb{R}$-basis of $\mathcal{L}$.

Hence any solution is of the form $x(t) = (\alpha + \beta t) \exp(-\rho t)$, for all $t \in \mathbb{R}$, where $\alpha, \beta \in \mathbb{R}$, entailing $\dot{x}(t) = (\alpha a + \beta + \beta a t) \exp(-\rho t)$. Since $\rho > 0$ we have $\lim_{t \to \infty} x(t) = 0$, saying that the body ultimately tends to the point of equilibrium. If x is a non-zero solution, then if $\beta = 0$ we have $\dot{x}(t) = -\alpha\rho \exp(-\rho t) \neq 0$ for all $t \in \mathbb{R}$, while if $\beta \neq 0$ we have $\dot{x}(t) = 0$ if and only if $t = -\frac{\alpha}{\beta} + \frac{1}{\rho}$; hence this happens for at most one $t \in \mathbb{R}$, saying that the body changes direction at most once. In particular, letting $x(0) := 1$ and $\dot{x}(0) := 0$, we get $\alpha = x(0) = 1$ and $-\alpha\rho + \beta = \dot{x}(0) = 0$, yielding $\beta = \rho$, that is $x(t) = (1 + \rho t) \exp(-\rho t)$.

iii) Let $\omega > \rho \geq 0$; physically this is the 'small friction' case. Then $p \in \mathbb{R}[X]$ is irreducible. Hence we have $\mu_D = p = \chi_D$; in particular, does not act triangularisably on $\mathcal{L}$. To describe $\mathcal{L}$ we use **complexification**:

We have $p = (X - a)(X - \overline{a}) \in \mathbb{C}[X]$, where $\{a, \overline{a}\} = \{-\rho \pm i\varphi\} \subseteq \mathbb{C} \setminus \mathbb{R}$ and $\varphi := \sqrt{\omega^2 - \rho^2} > 0$, and where $\overline{} \colon \mathbb{C} \to \mathbb{C} \colon x + iy \mapsto x - iy$, for $x, y \in \mathbb{R}$, denotes **complex conjugation**. We consider the $\mathbb{C}$-vector space $C^\infty(\mathbb{R}, \mathbb{C}) := \{\mathbb{R} \to \mathbb{C} \colon t \mapsto z(t) = x(t) + iy(t);\, x, y \in C^\infty(\mathbb{R})\}$, and we are looking for the $\mathbb{C}$-subspace $\mathcal{L}_{\mathbb{C}} \leq C^\infty(\mathbb{R}, \mathbb{C})$ of solutions of the $\mathbb{C}$-endomorphism $D^2 + 2\rho D + \omega^2$ of $C^\infty(\mathbb{R}, \mathbb{C})$. Again a consideration of Taylor series shows that $\dim_{\mathbb{C}}(\mathcal{L}_{\mathbb{C}}) = 2$.

Similarly, for any $c \in \mathbb{C}$ the corresponding eigenspace of D on $C^\infty(\mathbb{R}, \mathbb{C})$ is seen to be equal to $\langle \epsilon_c \rangle_{\mathbb{C}}$, where $\epsilon_c \colon \mathbb{C} \to \mathbb{C} \colon t \mapsto \exp(ct)$. This yields the principal subspace decomposition $\mathcal{L}_{\mathbb{C}} = T_{X-a}(D) \oplus T_{X-\overline{a}}(D) = \langle \epsilon_a \rangle_{\mathbb{C}} \oplus \langle \epsilon_{\overline{a}} \rangle_{\mathbb{C}}$; in particular, D acts diagonalisably on $\mathcal{L}_{\mathbb{C}}$. Letting $a = -\rho + i\varphi$, we have $\epsilon_a(t) = \exp(at) = \exp(-\rho t) \cdot \big(\cos(\varphi t) + i \sin(\varphi t)\big)$ and $\epsilon_{\overline{a}}(t) = \exp(-\rho t) \cdot \big(\cos(\varphi t) - i \sin(\varphi t)\big) = \overline{\epsilon_a(t)}$, for all $t \in \mathbb{R}$. Hence with respect to the $\mathbb{C}$-basis $\{\epsilon_a, \epsilon_{\overline{a}}\} \subseteq \mathcal{L}_{\mathbb{C}}$ the map D is represented by $\mathrm{diag}[-\rho + i \cdot \sqrt{\omega^2 - \rho^2}, -\rho - i \cdot \sqrt{\omega^2 - \rho^2}] \in \mathbb{C}^{2 \times 2}$.

We are looking for solutions in $\mathcal{L} \subseteq \mathcal{L}_{\mathbb{C}}$: Letting $\tau_a := \frac{1}{2}(\epsilon_a + \epsilon_{\overline{a}})$ and $\sigma_a := \frac{1}{2i}(\epsilon_a - \epsilon_{\overline{a}})$ we have $\tau_a(t) = \exp(-\rho t) \cos(\varphi t)$ and $\sigma_a(t) = \exp(-\rho t) \sin(\varphi t)$, for all $t \in \mathbb{R}$, hence $\tau_a, \sigma_a \in \mathcal{L} \subseteq \mathcal{L}_{\mathbb{C}}$. Since $\epsilon_a, \epsilon_{\overline{a}} \in \langle \tau_a, \sigma_a \rangle_{\mathbb{C}}$ we conclude that $\langle \tau_a, \sigma_a \rangle_{\mathbb{C}} = \mathcal{L}_{\mathbb{C}}$, hence $\{\tau_a, \sigma_a\}$ is $\mathbb{C}$-linearly independent, in particular is $\mathbb{R}$-linearly independent, and thus is an $\mathbb{R}$-basis of $\mathcal{L}$; alternatively, evaluating at $t = 0$ and $t = \frac{\pi}{2}$ shows directly that $\{\tau_a, \sigma_a\}$ is $\mathbb{R}$-linearly independent. We have $\dot{\tau}_a(t) = -\rho \exp(-\rho t) \cos(\varphi t) - \varphi \exp(-\rho t) \sin(\varphi t)$ and $\dot{\sigma}_a(t) = -\rho \exp(-\rho t) \sin(\varphi t) + \varphi \exp(-\rho t) \cos(\varphi t)$, for all $t \in \mathbb{R}$, that is $\dot{\tau}_a = -\rho \tau_a - \varphi \sigma_a$ and $\dot{\sigma}_a = \varphi \tau_a - \rho \sigma_a$, hence with respect to the $\mathbb{R}$-basis $\{\tau_a, \sigma_a\} \subseteq \mathcal{L}$ the map D is represented by $\begin{bmatrix} -\rho & \varphi \\ -\varphi & -\rho \end{bmatrix} = \begin{bmatrix} -\rho & \sqrt{\omega^2 - \rho^2} \\ -\sqrt{\omega^2 - \rho^2} & -\rho \end{bmatrix} \in \mathbb{R}^{2 \times 2}$.

Hence any solution is of the form $x(t) = \exp(-\rho t) \cdot \big(\alpha \cos(\varphi t) + \beta \sin(\varphi t)\big)$, for all $t \in \mathbb{R}$, where $\alpha, \beta \in \mathbb{R}$, entailing $\dot{x}(t) = \exp(-\rho t) \cdot \big((-\alpha\rho + \beta\varphi) \cos(\varphi t) + (-\alpha\varphi -$

$\beta\rho)\sin(\varphi t)\big)$. Thus, if x is a non-zero solution, then we have $\dot{x}(t) = 0$ whenever $t = \frac{2k\pi}{\varphi} \in \mathbb{R}$ for some $k \in \mathbb{Z}$, saying that the body changes direction infinitely often. If $\rho > 0$ we have $\lim_{t\to\infty} x(t) = 0$, saying that the body ultimately tends to the point of equilibrium, in other words the body oscillates with decreasing **amplitude**; in contrast, if $\rho = 0$ the limit $\lim_{t\to\infty} x(t)$ does not exist, and the body oscillates with constant amplitude.

In particular, letting $x(0) := 1$ and $\dot{x}(0) := 0$, we get $\alpha = x(0) = 1$ and $-\alpha\rho + \beta\varphi = \dot{x}(0) = 0$, yielding $\beta = \frac{\rho}{\varphi}$, that is $x(t) = \exp(-\rho t) \cdot \big(\cos(\varphi t) + \frac{\rho}{\varphi}\sin(\varphi t)\big)$, where $\varphi = \sqrt{\omega^2 - \rho^2}$; for $\rho = 0$ we get $\varphi = \omega$ and $x(t) = \cos(\omega t)$, saying that $\frac{\omega}{2\pi} > 0$ is the **frequency** of the free harmonic oscillator.

4 Bilinear forms

(4.1) Adjoint matrices. **a)** Let K be a field, and let $\alpha\colon K \to K\colon a^\alpha$ be a **field automorphism**, that is a bijective ring homomorphism, such that $\alpha^2 = \mathrm{id}_K$. The most important examples are $K = \mathbb{R}$ together with $\mathrm{id}_\mathbb{R}\colon \mathbb{R} \to \mathbb{R}$, and $K = \mathbb{C}$ together with complex conjugation $\overline{}\colon \mathbb{C} \to \mathbb{C}\colon x + iy \mapsto x - iy$, for $x, y \in \mathbb{R}$.

Given K-vector spaces V and W, then a map $\varphi\colon V \to W$ is called **α-semilinear** if $\varphi(v + v') = \varphi(v) + \varphi(v')$ and $\varphi(av) = a^\alpha \cdot \varphi(v)$, for all $v, v' \in V$ and $a \in K$. Note that if $\alpha = \mathrm{id}_K$ then the α-semilinear maps are just the K-linear maps.

For $m, n \in \mathbb{N}_0$ we have an α-semilinear map $K^{m\times n} \to K^{m\times n}\colon A = [a_{ij}]_{ij} \mapsto [a_{ij}^\alpha]_{ij} =: A^\alpha$, called the **($\alpha$-)conjugate** matrix of A. We have $(A^\alpha)^\alpha = A$, and for $B \in K^{n\times l}$, where $l \in \mathbb{N}_0$, we have $(AB)^\alpha = A^\alpha B^\alpha \in K^{m\times l}$. For $A \in K^{n\times n}$ we have $\det(A^\alpha) = \det(A)^\alpha \in K$, and $\mathrm{adj}(A^\alpha) = \mathrm{adj}(A)^\alpha \in K^{n\times n}$ if $n \geq 1$, hence we have $\mathrm{rk}(A^\alpha) = \mathrm{rk}(A)$, in particular for $A \in \mathrm{GL}_n(K)$ we have $A^\alpha \in \mathrm{GL}_n(K)$ as well, where $(A^\alpha)^{-1} = (A^{-1})^\alpha =: A^{-\alpha}$.

We have an α-semilinear map $K^{m\times n} \to K^{n\times m}\colon A \mapsto (A^\alpha)^{\mathrm{tr}} = (A^{\mathrm{tr}})^\alpha =: A^{\alpha\mathrm{tr}} = A^*$, called the **($\alpha$-)adjoint** matrix of A. We have $(A^*)^* = A$, and for $B \in K^{n\times l}$ we have $(AB)^* = B^*A^* \in K^{m\times l}$. For $A \in K^{n\times n}$ we have $\det(A^*) = \det(A)^\alpha \in K$, and $\mathrm{adj}(A^*) = \mathrm{adj}(A)^* \in K^{n\times n}$ if $n \geq 1$, hence we have $\mathrm{rk}(A^*) = \mathrm{rk}(A)$, in particular for $A \in \mathrm{GL}_n(K)$ we have $A^* \in \mathrm{GL}_n(K)$ as well, where $(A^*)^{-1} = (A^{-1})^* =: A^{-*} = A^{-\alpha\mathrm{tr}}$.

b) Then $A \in K^{n\times n}$ is called **normal** if $AA^* = A^*A$. In particular, A is called **hermitian** or **self-adjoint** if $A^* = A$, it is called **skew-hermitian** if $A^* = -A$, and $A \in \mathrm{GL}_n(K)$ is called **unitary** if $A^* = A^{-1}$; note that each of the latter conditions implies normality. Moreover, if $\alpha = \mathrm{id}_K$ then the latter conditions become $A^{\mathrm{tr}} = A$ and $A^{\mathrm{tr}} = -A$ and $A^{\mathrm{tr}} = A^{-1}$, respectively, and A is called **symmetric** and **symplectic** and **orthogonal**, respectively.

Example. We consider the matrices in (2.5) again: For the reflection $A := \begin{bmatrix} . & 1 \\ 1 & . \end{bmatrix} \in \mathrm{GL}_2(\mathbb{R})$ we have $A^2 = E_2$, hence we get $A^{-1} = A = A^{\mathrm{tr}}$, that is A is both symmetric and orthogonal.

For the rotation $A_\omega := \begin{bmatrix} \cos(\omega) & -\sin(\omega) \\ \sin(\omega) & \cos(\omega) \end{bmatrix} \in \mathrm{GL}_2(\mathbb{R})$, with respect to the angle $\omega \in \mathbb{R}$, we have $A_\omega^{-1} = A_{-\omega} = A_\omega^{\mathrm{tr}} = \begin{bmatrix} \cos(\omega) & \sin(\omega) \\ -\sin(\omega) & \cos(\omega) \end{bmatrix}$, that is A_ω is an orthogonal matrix. Moreover, for $B_\omega := \mathrm{diag}[\exp(i\omega), \exp(-i\omega)] \in \mathrm{GL}_2(\mathbb{C})$, where $\omega \in \mathbb{R}$, we have $B_\omega^{-1} = B_{-\omega} = \overline{B}_\omega = B_\omega^* = \mathrm{diag}[\exp(-i\omega), \exp(i\omega)]$, that is B_ω is an orthogonal matrix; recall that $A_\omega, B_\omega \in \mathbb{C}^{2\times 2}$ are similar. $\sharp$

(4.2) Sesquilinear forms. a) Let K be a field, and let $\alpha \colon K \to K$ be a field automorphism such that $\alpha^2 = \mathrm{id}_K$. Given a K-vector space V, a map $\Phi = \langle \cdot, \cdot \rangle \colon V \times V \to K \colon [v, w] \mapsto \langle v, w \rangle$ being K-linear in the second component, that is $\langle v, w + w' \rangle = \langle v, w \rangle + \langle v, w' \rangle$ and $\langle v, aw \rangle = a \langle v, w \rangle$, and α-semilinear in the first component, that is $\langle v + v', w \rangle = \langle v, w \rangle + \langle v', w \rangle$ and $\langle av, w \rangle = a^\alpha \cdot \langle v, w \rangle$, for all $v, v', w, w' \in V$ and $a \in K$, is called an **α-sesquilinear form** on V. In particular, if $\alpha = \mathrm{id}_K$ then Φ is K-linear in the first component as well, and thus is also called a **K-bilinear** form.

An α-sesquilinear form Φ is called **hermitian** if $\langle w, v \rangle = \langle v, w \rangle^\alpha$ holds, and called **skew-hermitian** if $\langle w, v \rangle = -\langle v, w \rangle^\alpha$ holds, for all $v, w \in V$. If $\alpha = \mathrm{id}_K$ the latter conditions become $\langle w, v \rangle = \langle v, w \rangle$ and $\langle w, v \rangle = -\langle v, w \rangle$, respectively, and Φ is called **symmetric** and **symplectic**, respectively.

b) Given $w \in V$, a vector $v \in V$ is called **right** and **left orthogonal** to w if $\langle w, v \rangle = 0$ and $\langle v, w \rangle = 0$, respectively; we write $w \perp v$ and $v \perp w$, respectively. If Φ is (skew-)hermitian then we have $w \perp v$ if and only if $v \perp w$, for all $v, w \in V$. Moreover, a vector $v \in V$ is called **normed** if $\langle v, v \rangle = 1$.

Given $S \subseteq V$, then $S^\perp := \{v \in V ; \langle w, v \rangle = 0 \text{ for all } w \in S\} \leq V$ and ${}^\perp S := \{v \in V ; \langle v, w \rangle = 0 \text{ for all } w \in S\} \leq V$ are called the **right** and **left orthogonal** spaces of S, respectively; note that due to K-linearity and α-semilinearity, respectively, the latter indeed are K-subspaces of V.

Hence $\emptyset^\perp = {}^\perp\emptyset = V$, and due to α-semilinearity and K-linearity, respectively, we have $S^\perp = \langle S \rangle_K^\perp$ and ${}^\perp S = {}^\perp \langle S \rangle_K$. If Φ is (skew-)hermitian then we have $S^\perp = {}^\perp S$. In particular, $V^\perp$ and ${}^\perp V$ are called the **right** and **left radical** of Φ, respectively, and Φ is called **non-degenerate** if $V^\perp = \{0\} = {}^\perp V$.

c) If $0 \neq v \in V$ such that $v \perp v$, that is $\langle v, v \rangle = 0$, or in other words $v \in \langle v \rangle_K^\perp \cap {}^\perp \langle v \rangle_K$, then v is called **isotropic**; if there are no isotropic vectors then Φ is called **anisotropic**. Note that any anisotropic form fulfills $V^\perp = V \cap V^\perp = \{0\} = V \cap {}^\perp V = {}^\perp V$, hence is non-degenerate.

We show that for any hermitian α-sesquilinear form $\Phi \neq 0$ there indeed is a non-isotropic vector, unless $2 = 0 \in K$ and $\alpha = \mathrm{id}_K$; we will show below by way of an example that the exception is indeed necessary:

Assume that Φ is **totally isotropic**, that is $\langle v, v \rangle = 0$ for all $v \in V$. Since $V^\perp < V$, there are $v, w \in V$ such that $\langle v, w \rangle = 1$. Hence for all $a \in K$ we have $0 = \langle v + aw, v + aw \rangle = \langle v, v \rangle + a \langle v, w \rangle + a^\alpha \langle w, v \rangle + aa^\alpha \langle w, w \rangle = a + a^\alpha$, and thus $\alpha = -\mathrm{id}_K$, from which $1 = 1^\alpha = -1 \in K$ shows $2 = 0 \in K$ and $\alpha = \mathrm{id}_K$. $\sharp$

Example. We present a few examples:

i) The **standard** α-sesquilinear form $\Gamma\colon K^{n\times 1}\times K^{n\times 1}\to K$ is defined as $\langle [a_1,\ldots,a_n]^{\mathrm{tr}},[b_1,\ldots,b_n]^{\mathrm{tr}}\rangle := [a_1,\ldots,a_n]^\alpha\cdot[b_1,\ldots,b_n]^{\mathrm{tr}} = \sum_{i=1}^n a_i^\alpha b_i$, for $n\in\mathbb{N}_0$. Then $\langle [b_1,\ldots,b_n]^{\mathrm{tr}},[a_1,\ldots,a_n]^{\mathrm{tr}}\rangle = \sum_{i=1}^n b_i^\alpha a_i = \sum_{i=1}^n b_i^\alpha a_i^{\alpha^2} = (\sum_{i=1}^n a_i^\alpha b_i)^\alpha = \langle [a_1,\ldots,a_n]^{\mathrm{tr}},[b_1,\ldots,b_n]^{\mathrm{tr}}\rangle^\alpha$ shows that Γ is hermitian. Since for $[a_1,\ldots,a_n]^{\mathrm{tr}}\in {}^\perp K^{n\times 1}$ we get $0=\langle e_i,[a_1,\ldots,a_n]^{\mathrm{tr}}\rangle = a_i$, where $e_i\in K^{n\times 1}$ denotes the i-th **unit vector**, for $i\in\{1,\ldots,n\}$, we infer that Γ is non-degenerate. We have $\langle e_i,e_j\rangle = 0$ for $i\neq j$, that is the **standard** K-basis $\{e_1,\ldots,e_n\}\subseteq K^{n\times 1}$ is an **orthogonal** K-basis, and since $\langle e_i,e_i\rangle = 1$ for $i\in\{1,\ldots,n\}$ it is even an **orthonormal** K-basis.

Moreover, in the particular case of $K=\mathbb{R}$ and $\alpha=\mathrm{id}_{\mathbb{R}}$, for any $[a_1,\ldots,a_n]^{\mathrm{tr}}\neq 0$ we get $\langle [a_1,\ldots,a_n]^{\mathrm{tr}},[a_1,\ldots,a_n]^{\mathrm{tr}}\rangle = \sum_{i=1}^n a_i^2\neq 0$, hence Γ is anisotropic.

ii) Let $\Gamma^{(n-1,1)}$ be the **Minkowski** α-sesquilinear form on $K^{n\times 1}$, for $n\in\mathbb{N}$, defined by $\langle [a_0,a_1,\ldots,a_{n-1}]^{\mathrm{tr}},[b_0,b_1,\ldots,b_{n-1}]^{\mathrm{tr}}\rangle := -a_0^\alpha b_0+\sum_{i=1}^{n-1} a_i^\alpha b_i$. Then we have $\langle [a_0,\ldots,a_{n-1}]^{\mathrm{tr}},[b_0,\ldots,b_{n-1}]^{\mathrm{tr}}\rangle = \langle [b_0,\ldots,b_{n-1}]^{\mathrm{tr}},[a_0,\ldots,a_{n-1}]^{\mathrm{tr}}\rangle^\alpha$, hence $\Gamma^{(n-1,1)}$ is hermitian, and from $[a_0,\ldots,a_{n-1}]^{\mathrm{tr}}\in {}^\perp\mathbb{R}^{n\times 1}$ we get $0 = \langle e_i,[a_0,\ldots,a_{n-1}]^{\mathrm{tr}}\rangle = a_i$, for $i\in\{1,\ldots,n-1\}$, and $0=\langle e_0,[a_0,\ldots,a_{n-1}]^{\mathrm{tr}}\rangle = -a_0$, hence $\Gamma^{(n-1,1)}$ is non-degenerate. We have $\langle e_i,e_j\rangle = 0$ for $i\neq j$, hence the standard K-basis $\{e_0,\ldots,e_{n-1}\}\subseteq K^{n\times 1}$ is an orthogonal K-basis, where $\langle e_i,e_i\rangle = 1$ for $i\in\{1,\ldots,n\}$, but $\langle e_0,e_0\rangle = -1$. Thus for $n\geq 2$ there are isotropic vectors; for example $\langle [1,0,\ldots,0,1]^{\mathrm{tr}},[1,0,\ldots,0,1]^{\mathrm{tr}}\rangle = -1+1=0$.

iii) The set $\mathbb{F}_2 := \{0,1\}$ becomes a field with respect to the following addition and multiplication, where $1+1:=0$ is the only non-trivial entry:

$+$	0	1
0	0	1
1	1	0

and

$\cdot$	0	1
0	0	0
1	0	1

We consider the symmetric **hyperbolic** $\mathbb{F}_2$-bilinear form H on $\mathbb{F}_2^{2\times 1}$ given by $\langle [a,b]^{\mathrm{tr}},[c,d]^{\mathrm{tr}}\rangle := ad+bc$, for all $a,b,c,d\in\mathbb{F}_2$. Then for $[a,b]^{\mathrm{tr}}\in {}^\perp\mathbb{F}_2^{2\times 1}$ from $0=\langle [a,b]^{\mathrm{tr}},[0,1]^{\mathrm{tr}}\rangle = a$ and $0=\langle [a,b]^{\mathrm{tr}},[1,0]^{\mathrm{tr}}\rangle = b$ we conclude that H is non-degenerate, but from $\langle [a,b]^{\mathrm{tr}},[a,b]^{\mathrm{tr}}\rangle = ab+ba=0$, for all $a,b\in\mathbb{F}_2$, we infer that H is totally isotropic. $\sharp$

(4.3) Gram matrices. a) Let K be a field, let $\alpha\colon K\to K$ be a field automorphism such that $\alpha^2=\mathrm{id}_K$. Moreover, let V be a finitely generated K-vector space with K-bases $B:=[v_1,\ldots,v_n]$ and $C:=[w_1,\ldots,w_n]$, where $n:=\dim_K(V)\in\mathbb{N}_0$, and let $\Phi=\langle\cdot,\cdot\rangle$ be an α-sesquilinear form on V.

Then for $v=\sum_{i=1}^n a_iv_i\in V$ and $w=\sum_{j=1}^n b_jw_j$, where $a_i,b_j\in K$, we have $\langle v,w\rangle = \langle\sum_{i=1}^n a_iv_i,\sum_{j=1}^n b_jw_j\rangle = \sum_{i=1}^n\sum_{j=1}^n a_i^\alpha b_j\langle v_i,w_j\rangle\in K$. Thus letting $G_B^C(\Phi) := [\langle v_i,w_j\rangle]_{ij}\in K^{n\times n}$ be the **Gram matrix** of Φ with respect to the K-bases B and C, using the coordinate tuples $M_B(v)=[a_1,\ldots,a_n]^{\mathrm{tr}}\in K^{n\times 1}$ and $M_C(w)=[b_1,\ldots,b_n]^{\mathrm{tr}}\in K^{n\times 1}$ we get $\langle v,w\rangle = M_B(v)^*\cdot G_B^C(\Phi)\cdot M_C(w)\in K$.

Hence Φ is uniquely determined by $G_B^C(\Phi)$. Conversely, for any $G \in K^{n\times n}$ letting $\langle v,w\rangle_G := M_B(v)^* \cdot G \cdot M_C(w) \in K$, for all $v,w \in V$, defines an α-sesquilinear form on V, with Gram matrix G with respect to the K-bases B and C. Thus the set of all α-sesquilinear forms on V, being a K-vector space with respect to pointwise addition and scalar multiplication, is isomorphic to the K-vector space $K^{n\times n}$ via $\Phi \mapsto G_B^C(\Phi)$.

In particular, Φ is hermitian if and only if $G_B^B(\Phi) = [\langle v_i, v_j\rangle]_{ij} = [\langle v_j, v_i\rangle^\alpha]_{ij} = [\langle v_i, v_j\rangle]_{ji}^\alpha = G_B^B(\Phi)^* \in K^{n\times n}$, that is $G_B^B(\Phi)$ is hermitian; similarly, Φ is skew-hermitian if and only if $G_B^B(\Phi)$ is skew-hermitian, and Φ is (skew-)symmetric if and only if $G_B^B(\Phi)$ is (skew-)symmetric. Here are a few hermitian examples:

Example. i) For the standard α-sesquilinear form Γ on $K^{n\times 1}$ with respect to the standard K-basis $B \subseteq K^{n\times 1}$, which is orthonormal, we get $G_B^B(\Gamma) = \mathrm{diag}[1,\ldots,1] = E_n \in K^{n\times n}$.

ii) For the Minkowski α-sesquilinear form $\Gamma^{(n-1,1)}$ on $K^{n\times 1}$ with respect to the standard K-basis $B \subseteq K^{n\times 1}$, which is orthogonal but not orthonormal, we get $G_B^B(\Gamma^{(n-1,1)}) = \mathrm{diag}[-1,1,\ldots,1] \in K^{n\times n}$.

iii) For the hyperbolic bilinear form H on $\mathbb{F}_2^{2\times 1}$, which is totally isotropic, with respect to the standard $\mathbb{F}_2$-basis $B \subseteq \mathbb{F}_2^{2\times 1}$ we get $G_B^B(H) = \begin{bmatrix} . & 1 \\ 1 & . \end{bmatrix} \in \mathbb{F}_2^{2\times 2}$.

b) We examine how the Gram matrix of Φ changes if the K-bases of V are changed: If $B' := [v_1',\ldots,v_n']$ and $C' := [w_1',\ldots,w_n']$ are also K-bases of V, then for $i,j \in \{1,\ldots,n\}$ we have $\langle v_i', w_j'\rangle = M_B(v_i')^* \cdot G_B^C(\Phi) \cdot M_C(w_j') \in K$, where $M_C(w_j') \in K^{n\times 1}$ is column j of the base change matrix $M_C^{C'}(\mathrm{id}) \in \mathrm{GL}_n(K)$, and $M_B(v_i') \in K^{n\times 1}$ is column i of the base change matrix $M_B^{B'}(\mathrm{id}) \in \mathrm{GL}_n(K)$, thus $G_{B'}^{C'}(\Phi) := [\langle v_i', w_j'\rangle]_{ij} = M_B^{B'}(\mathrm{id})^* \cdot G_B^C(\Phi) \cdot M_C^{C'}(\mathrm{id}) \in K^{n\times n}$.

In particular, for Gram matrices with respect to pairs of coinciding K-bases we have the base change formula $G_C^C(\Phi) = M_B^C(\mathrm{id})^* \cdot G_B^B(\Phi) \cdot M_B^C(\mathrm{id}) \in K^{n\times n}$.

Hence, if B is an orthonormal K-basis with respect to Φ, that is $G_B^B(\Phi) = E_n$, then C is an orthonormal K-basis with respect to Φ if and only if for $P := M_B^C(\mathrm{id}) \in \mathrm{GL}_n(K)$ we have $E_n = G_C^C(\Phi) = P^* \cdot G_B^B(\Phi) \cdot P = P^*P$, which holds if and only if $P^* = P^{-1}$, that is P is unitary. Note that it is not yet clear under which circumstances orthonormal bases exist at all.

Moreover, this leads to the following notion: If Φ' also is an α-sesquilinear form on V, then Φ and Φ' are called **equivalent**, if there is a K-basis $B' \subseteq V$ such that $G_{B'}^{B'}(\Phi') = G_B^B(\Phi)$, in other words if and only if there is $P \in \mathrm{GL}_n(K)$ such that $G_B^B(\Phi') = P^* \cdot G_B^B(\Phi) \cdot P$; note that this is an equivalence relation on $K^{n\times n}$.

(4.4) Orthogonal spaces. a) Let K be a field, let $\alpha\colon K \to K$ be a field automorphism such that $\alpha^2 = \mathrm{id}_K$. Moreover, let V be a K-vector space such that $n := \dim_K(V) \in \mathbb{N}_0$, and let $\Phi = \langle\cdot,\cdot\rangle$ be an α-sesquilinear form on V. We proceed to consider left and right orthogonal spaces of K-subspaces of V, in particular the left and right radical of Φ:

To this end, by the above identifications, we may assume that $V = K^{n\times 1}$, and that Φ has Gram matrix $G := G_B^B(\Phi) \in K^{n\times n}$ with respect to the standard K-basis $B \subseteq V$; hence we have $\langle v, w\rangle = v^*Gw \in K$, for all $v, w \in V$. Now let the K-subspace $U \leq V$ be given as the column space of the matrix $P \in K^{n\times m}$, where $m := \dim_K(U) \in \mathbb{N}_0$, and let $U^\perp \leq V$ and ${}^\perp U \leq V$ be given as the column spaces of $Q' \in K^{n\times m'}$ and $Q'' \in K^{n\times m''}$, respectively, where $m' := \dim_K(U^\perp) \in \mathbb{N}_0$ and $m'' := \dim_K({}^\perp U) \in \mathbb{N}_0$.

Then we have $U^\perp = \ker(P^*G) \leq V$, thus the columns of Q' consist of a K-basis of the (column) kernel of $P^*G \in K^{m\times n}$. Similarly we have $({}^\perp U)^\alpha = \ker((GP)^{\mathrm{tr}}) \leq V$, equivalently ${}^\perp U = \ker((GP)^{\mathrm{tr}})^\alpha = \ker((GP)^*) = \ker(P^*G^*)$, thus the columns of Q'' consist of a K-basis of the (column) kernel of $P^*G^* \in K^{m\times n}$; recall that $\ker((GP)^{\mathrm{tr}})^{\mathrm{tr}} \leq K^n$ is the row kernel of $GP \in K^{n\times m}$.

In particular, we have $V^\perp = \ker(G)$ and ${}^\perp V = \ker(G^*)$, thus from $\mathrm{rk}(G) = \mathrm{rk}(G^*)$ we infer that $\dim_K(V^\perp) = \dim_K(\ker(G)) = n - \mathrm{rk}(G) = n - \mathrm{rk}(G^*) = \ker(G^*) = \dim_K({}^\perp V) \in \mathbb{N}_0$. Hence Φ is non-degenerate if and only if $V^\perp = \{0\}$, if and only if ${}^\perp V = \{0\}$, which holds if and only if $G \in \mathrm{GL}_n(K)$.

b) Considering the associated maps $\varphi_G \in \mathrm{End}_K(V)$ and $\varphi_{G^*} \in \mathrm{End}_K(V)$, we have $\ker(GP) = \ker(\varphi_G|_U) = U \cap V^\perp$ and $\ker(G^*P) = \ker(\varphi_{G^*}|_U) = U \cap {}^\perp V$.

This yields $m' = \dim_K(\ker(P^*G)) = n - \mathrm{rk}(P^*G) = n - \mathrm{rk}((P^*G)^*) = n - \mathrm{rk}(G^*P) = n - (m - \dim_K(\ker(G^*P))) = n - m + \dim_K(U \cap {}^\perp V)$, or equivalently $\dim_K(U) + \dim_K(U^\perp) = \dim_K(V) + \dim_K(U \cap {}^\perp V)$.

Similarly, $m'' = \dim_K(\ker(P^*G^*)) = n - \mathrm{rk}(P^*G^*) = n - \mathrm{rk}((P^*G^*)^*) = n - \mathrm{rk}(GP) = n - (m - \dim_K(\ker(GP))) = n - m + \dim_K(U \cap V^\perp)$, or equivalently $\dim_K(U) + \dim_K({}^\perp U) = \dim_K(V) + \dim_K(U \cap V^\perp)$.

In particular, if Φ is non-degenerate, then we get $m + m' = n = m + m''$, thus $m' = n - m = m''$, and from $m = \dim_K({}^\perp(U^\perp)) = \dim_K(({}^\perp U)^\perp)$ and $U \leq {}^\perp(U^\perp) \cap ({}^\perp U)^\perp$ we infer $U = {}^\perp(U^\perp) = ({}^\perp U)^\perp$, that is U is **saturated**.

Moreover, if Φ is even anisotropic, hence in particular non-degenerate, then we additionally have $U \cap U^\perp = \{0\} = U \cap {}^\perp U$. Hence from $m + m' = n = m + m''$ we infer that we have the direct sum decompositions $V = U \oplus U^\perp = U \oplus {}^\perp U$, that is U has both a **right orthogonal** and a **left orthogonal** complement.

Example. We consider $V := \mathbb{R}^{2\times 1}$ equipped with the standard $\mathbb{R}$-bilinear form Γ, which is symmetric and anisotropic. With respect to the standard $\mathbb{R}$-basis $B \subseteq V$ the associated Gram matrix is given as $G := G_B^B(\Gamma) = E_2 \in \mathbb{R}^{2\times 2}$, reflecting the orthonormality of B; moreover, from $G = G^{\mathrm{tr}}$ and $\mathrm{rk}(G) = 2$ we recover the facts that Γ is symmetric and non-degenerate.

Let $v := [1, 1]^{\mathrm{tr}} \in V$ and $U := \langle v\rangle_{\mathbb{R}}$. Then from $V = U \oplus U^\perp$ we get $\dim_{\mathbb{R}}(U^\perp) = 1$ and $U \cap U^\perp = \{0\}$. Indeed, letting $P := [v] \in \mathbb{R}^{2\times 1}$ we have $U^\perp = \ker(P^*G) = \ker(P^{\mathrm{tr}}G) = \ker([[1, 1]] \cdot E_2) = \ker([[1, 1]]) = \langle w\rangle_{\mathbb{R}}$, where $w := [-1, 1]^{\mathrm{tr}} \in V$. Thus we infer that $C := [v, w] \subseteq V$ is an orthogonal $\mathbb{R}$-basis.

Letting $Q := M_B^C(\mathrm{id}) = [v,w] \in \mathbb{R}^{2\times 2}$ be the associated base change matrix, we get $G_C^C(\Gamma) = Q^* G Q = Q^{\mathrm{tr}} G Q = Q^{\mathrm{tr}} Q = \begin{bmatrix} 1 & 1 \\ -1 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & -1 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} 2 & . \\ . & 2 \end{bmatrix} \in \mathbb{R}^{2\times 2}$, where the diagonality of the latter matrix reflects the orthogonality of C, and the diagonal entries say that $\langle v,v\rangle = 2 = \langle w,w\rangle$.

Going over to normed vectors $v' := \frac{1}{\sqrt{2}} \cdot v \in V$ and $w' := \frac{1}{\sqrt{2}} \cdot w \in V$ yields the orthonormal $\mathbb{R}$-basis $C' := [v',w'] \subseteq V$, with associated base change matrix $Q' := M_B^{C'}(\mathrm{id}) = [v',w'] = \frac{1}{\sqrt{2}} \cdot Q \in \mathbb{R}^{2\times 2}$. From this we get $G_{C'}^{C'}(\Gamma) = Q'^{\mathrm{tr}} G Q' = Q'^{\mathrm{tr}} Q' = \frac{1}{2} \cdot Q^{\mathrm{tr}} Q = E_2 \in \mathbb{R}^{2\times 2}$, saying again that C' is orthonormal, and that Q' indeed is an orthogonal matrix; note that in order to go over to normed vectors we have to extract square roots. $\sharp$

(4.5) Orthogonalisation. Let K be a field, let $\alpha\colon K \to K$ be a field automorphism such that $\alpha^2 = \mathrm{id}_K$, let V be finitely generated K-vector space, and let Φ be a hermitian α-sesquilinear form on V, where if $\alpha = \mathrm{id}_K$ we additionally assume that $2 \neq 0 \in K$. Then V actually has an orthogonal K-basis; note that orthogonal K-bases possibly exist only if Φ is hermitian:

We proceed by induction on $n := \dim_K(V) \in \mathbb{N}_0$, where the case $n = 0$ is trivial; hence we assume that $n \geq 1$. We may also assume that $\Phi \neq 0$, since otherwise we are done anyway. By our general assumption there is a non-isotropic vector $v \in V$, that is we have $\langle v,v\rangle \neq 0$. Letting $U := \langle v\rangle_K \leq V$, then $v \notin U^\perp$ shows $U \cap U^\perp = \{0\}$, thus we have $U \cap V^\perp = \{0\}$ as well, implying $\dim_K(U^\perp) = n - \dim_K(U) = n-1$, and hence $V = U \oplus U^\perp = \langle v\rangle_K \oplus U^\perp$. Thus $U^\perp$ by induction has an orthogonal K-basis, which joined with v yields an orthogonal K-basis of V. $\sharp$

Hence, if $0 \neq v \in V$ is non-isotropic, a K-basis reflecting the direct sum decomposition $V = \langle v\rangle_K \oplus U^\perp$ is found as follows: Let $B := [v, v_1, \ldots, v_{n-1}] \subseteq V$ be any K-basis containing v, and for $i \in \{1,\ldots,n-1\}$ let $w_i := v_i - \frac{\langle v,v_i\rangle}{\langle v,v\rangle} \cdot v \in V$. Then $C := [v, w_1, \ldots, w_{n-1}] \subseteq V$ is a K-basis as well, where $\langle v,w_i\rangle = \langle v,v_i\rangle - \frac{\langle v,v_i\rangle}{\langle v,v\rangle} \cdot \langle v,v\rangle = 0$ shows that $C' := [w_1,\ldots,w_{n-1}]$ is a K-basis of $U^\perp$.

In other words, letting $P := M_B^C(\mathrm{id}) = E_n - \sum_{i=1}^{n-1} \frac{\langle v,v_i\rangle}{\langle v,v\rangle} \cdot E_{1i} \in K^{n\times n}$ we have $G_C^C(\Phi) = P^* \cdot G_B^B(\Phi) \cdot P = [\langle v,v\rangle] \oplus G_{C'}^{C'}(\Phi|_{U^\perp}) \in K^{n\times n}$. Thus $G_C^C(\Phi)$ is found from $G_B^B(\Phi)$ by subtracting the $\frac{\langle v,v_i\rangle}{\langle v,v\rangle}$-fold of column 1 from column i, and subtracting the $\frac{\langle v,v_i\rangle}{\langle v,v\rangle}$-fold of row 1 from row i, for all $i \in \{1,\ldots,n-1\}$.

Before addressing the question when we have orthonormal K-bases, we present an example, which in particular exhibits obstructions to their existence even in the geometric case, where the extraction of square roots is always possible:

Example. Let $K := \mathbb{R}$ and $\alpha = \mathrm{id}$, and let Φ be given with respect to some $\mathbb{R}$-basis $B \subseteq \mathbb{R}^{3\times 1}$ by $G = G_B^B(\Phi) := \begin{bmatrix} 0 & -2 & 4 \\ -2 & 1 & -1 \\ 4 & -1 & 0 \end{bmatrix} \in \mathbb{R}^{3\times 3}$. Hence we may choose the second basis vector as a non-isotropic vector to begin with, and letting $P_1 := \begin{bmatrix} . & 1 & . \\ 1 & . & . \\ . & . & 1 \end{bmatrix} \in \mathrm{GL}_3(\mathbb{R})$ we get $G_1 = P_1^{\mathrm{tr}} G P_1 = \begin{bmatrix} 1 & -2 & -1 \\ -2 & 0 & 4 \\ -1 & 4 & 0 \end{bmatrix}$. Then, letting $P_2 := \begin{bmatrix} 1 & 2 & 1 \\ . & 1 & . \\ . & . & 1 \end{bmatrix} \in \mathrm{GL}_3(\mathbb{R})$ yields $G_2 = P_2^{\mathrm{tr}} G_1 P_2 = \begin{bmatrix} 1 & . & . \\ . & -4 & 2 \\ . & 2 & -1 \end{bmatrix}$. Next, letting $P_3 := \begin{bmatrix} 1 & . & . \\ . & 1 & \frac{1}{2} \\ . & . & 1 \end{bmatrix} \in \mathrm{GL}_3(\mathbb{R})$ we get $G_3 = P_3^{\mathrm{tr}} G_2 P_3 = \begin{bmatrix} 1 & . & . \\ . & -4 & . \\ . & . & . \end{bmatrix}$. Finally, rescaling with $P_4 := \begin{bmatrix} 1 & . & . \\ . & \frac{1}{2} & . \\ . & . & 1 \end{bmatrix} \in \mathrm{GL}_3(\mathbb{R})$ yields $G' = P_4^{\mathrm{tr}} G_3 P_4 = \begin{bmatrix} 1 & . & . \\ . & -1 & . \\ . & . & . \end{bmatrix}$. Hence we have $G_C^C(\Phi) = G' = P^{\mathrm{tr}} G P \in \mathbb{R}^{3\times 3}$, where the $\mathbb{R}$-basis $C \subseteq V$ is given as $M_B^C(\mathrm{id}) = P := P_1 P_2 P_3 P_4 = \begin{bmatrix} 0 & \frac{1}{2} & \frac{1}{2} \\ 1 & 1 & 2 \\ 0 & 0 & 1 \end{bmatrix} \in \mathrm{GL}_3(\mathbb{R})$. ♯

(4.6) Signature. a) Let $[K, \alpha] \in \{[\mathbb{R}, \mathrm{id}_{\mathbb{R}}], [\mathbb{C}, \overline{}]\}$, and let $\Phi = \langle\cdot,\cdot\rangle$ be a hermitian α-sesquilinear form on a K-vector space V such that $n := \dim_K(V) \in \mathbb{N}_0$. Then we have **Sylvester's Theorem of Inertia**, saying that there is an orthogonal K-basis $B \subseteq V$ such that $G_B^B(\Phi) = E_k \oplus (-E_l) \oplus (0 \cdot E_{n-k-l})$, where $k, l \in \mathbb{N}_0$ are independent of the particular choice of B:

The existence of B follows by replacing the non-isotropic elements v of an orthogonal K-basis, which exists by (4.5), by $v' := \frac{1}{\sqrt{|\langle v,v\rangle|}} \cdot v$; then we have $\langle v', v'\rangle = \frac{1}{|\langle v,v\rangle|}\langle v, v\rangle \in \{\pm 1\}$, depending on whether $\langle v, v\rangle > 0$ or $\langle v, v\rangle < 0$.

To show uniqueness, for $\epsilon \in \{0, \pm 1\}$ let $B_\epsilon := \{v \in B, \langle v, v\rangle = \epsilon\}$ and $V_\epsilon := \langle B_\epsilon\rangle_K \leq V$, thus we have $V = V_1 \oplus V_{-1} \oplus V_0$ with pairwise orthogonal direct summands, where $k = \dim_K(V_1)$ and $l = \dim_K(V_{-1})$. We have $V^\perp = \ker(G_B^B(\Phi)) = V_0$, thus $m := n - k - l = \dim_K(V_0) \in \mathbb{N}_0$ is uniquely determined by Φ. Moreover, for $w = \sum_{v \in B_\epsilon} a_v v \in V_\epsilon$ we have $\langle w, w\rangle = \epsilon \cdot \sum_{v \in B_\epsilon} |a_v|^2$, thus $\langle w, w\rangle > 0$ for $0 \neq w \in V_1$, and $\langle w, w\rangle < 0$ for $0 \neq w \in V_{-1}$.

Let now $C \subseteq V$ be a K-basis such that $G_C^C(\Phi) = E_{k'} \oplus (-E_{l'}) \oplus (0 \cdot E_m)$, where $k', l' \in \mathbb{N}_0$, with associated K-subspaces $V'_{\pm 1}$, but $V'_0 = V_0$. Then we have $V_1 \cap (V'_{-1} \oplus V'_0) = \{0\}$, implying $k + l' + m = \dim_K(V_1 + V'_{-1} + V'_0) \leq n = k' + l' + m$, thus $k \leq k'$; similarly, interchanging the roles of B and C we get $k' \leq k$. ♯

The pair $[k, l]$ is called the **signature** of Φ. Hence the equivalence classes of hermitian α-sesquilinear forms on V are described by the signatures $[k, l]$, where $k, l \geq 0$ such that $k + l \leq n = \dim_K(V)$. In particular, $(-\Phi)$ has signature $[l, k]$.

In particular, Φ has signature $[n, 0]$, in other words V has an orthonormal K-

basis, if and only if Φ is equivalent to the standard α-sesquilinear form Γ; this is the genuinely geometric case discussed in some more detail below. Moreover, Φ has signature $[n-1,1]$ if and only if Φ is equivalent to the Minkowski α-sesquilinear form $\Gamma^{(n-1,1)}$; in this case V is called a **Minkowski space**.

b) Let $q\colon V \to K\colon v \mapsto \langle v,v\rangle$ be the **quadratic form** associated with Φ; note that $\langle v,v\rangle = \overline{\langle v,v\rangle} \in K$ implies that q has values in $\mathbb{R}$. For $a \in K$ and $v \in V$ we have $q(av) = a\overline{a}\langle v,v\rangle = |a|^2 q(v) \in \mathbb{R}$, where $q(0) = 0$.

If $q(v) > 0$ for all $0 \neq v \in V$, then q is called **positive definite**; if $q(v) \geq 0$ for all $v \in V$, then q is called **positive semi-definite**; if $q(v) < 0$ for all $0 \neq v \in V$, then q is called **negative definite**; if $q(v) \leq 0$ for all $v \in V$, then q is called **negative semi-definite**; otherwise q is called **indefinite**. In particular, if q is positive or negative definite then Φ is anisotropic.

These notions are related to the signature $[k,l]$ of Φ as follows: If $B \subseteq V$ is an orthogonal K-basis as in Sylvester's Theorem, then we have $q(x_1,\ldots,x_n) = [\overline{x}_1,\ldots,\overline{x}_n] \cdot G_B^B(\Phi) \cdot [x_1,\ldots,x_n]^{\text{tr}} = (\sum_{i=1}^k |x_i|^2) - (\sum_{j=1}^l |x_{k+j}|^2) \in \mathbb{R}$, where $[x_1,\ldots,x_n]^{\text{tr}} \in K^{n\times 1}$ is the coordinate tuple with respect to B. Hence q is positive definite if and only if $k = n$; and q is positive semi-definite if and only if $l = 0$; while q is negative definite if and only if $l = n$; and q is negative semi-definite if and only if $k = 0$; thus q is indefinite in all the cases $\{k,l\} \neq \{0,n\}$.

If q is positive definite, then Φ is called a **scalar product**, where V is called **Euclidean** if $K = \mathbb{R}$, and **unitary** if $K = \mathbb{C}$. In particular, for the standard α-sesquilinear form Γ on $K^{n\times 1}$, where $n \in \mathbb{N}_0$, we have $q([a_1,\ldots,a_n]^{\text{tr}}) = \langle [a_1,\ldots,a_n]^{\text{tr}}, [a_1,\ldots,a_n]^{\text{tr}}\rangle = \sum_{i=1}^n |a_i|^2 > 0$, for all $0 \neq [a_1,\ldots,a_n]^{\text{tr}} \in K^{n\times 1}$, thus Γ is also called the **standard** scalar product on $K^{n\times 1}$.

(4.7) Hurwitz-Sylvester criterion. a) Let $[K,\alpha] \in \{[\mathbb{R},\text{id}_{\mathbb{R}}],[\mathbb{C},\overline{}]\}$, and let $\Phi = \langle\cdot,\cdot\rangle$ be a hermitian α-sesquilinear form on a finitely generated K-vector space V. We give a characterisation of the associated quadratic form q being positive or negative definite in terms of the **leading principal minors** of the Gram matrix of Φ:

To this end, let $B = [v_1,\ldots,v_n] \subseteq V$ be any K-basis, where $n := \dim_K(V) \in \mathbb{N}_0$, and let $G := G_B^B(\Phi) \in K^{n\times n}$. Moreover, for $k \in \{0,\ldots,n\}$ let $B_k := [v_1,\ldots,v_k]$ and $V_k := \langle B_k\rangle_K \leq V$ and $G_k := G_{B_k}^{B_k}(\Phi|_{V_k}) \in K^{k\times k}$; hence we have $G_n = G$.

Let q be positive or negative definite, and let $\epsilon := 1$ and $\epsilon := -1$, respectively. Then letting $C \subseteq V$ be an orthogonal K-basis as in Sylvester's Theorem, and $P := M_B^C(\text{id}) \in \text{GL}_n(K)$, we have $P^*GP = G_C^C(\Phi) = \epsilon E_n \in K^{n\times n}$, implying that $|\det(P)|^2 \cdot \det(G) = \det(G_C^C(\Phi)) = \epsilon^n$, hence $\epsilon^n \cdot \det(G) > 0$. Moreover, since definiteness is inherited to K-subspaces, we infer that $\epsilon^k \cdot \det(G_k) > 0$, for all $k \in \{0,\ldots,n\}$; note that $\det(G_k)$ is the k-th leading principal minor of G, and that since G is hermitian we have $\det(G_k) \in \mathbb{R}$ indeed.

Conversely, let $\epsilon \in \{\pm 1\}$, and assume that $\epsilon^k \cdot \det(G_k) > 0$ for all $k \in \{0,\ldots,n\}$. We proceed by induction on $k \in \mathbb{N}_0$, where for $k \geq 1$ we may assume that

$\Phi|_{V_{k-1}}$ is positive or negative definite, respectively; the case $k=0$ being trivial: Let $[w_1,\ldots,w_{k-1}] \subseteq V_{k-1}$ be a K-basis as in Sylvester's Theorem, that is $\langle w_j, w_j\rangle = \epsilon$ for $j \in \{1,\ldots,k-1\}$. Then letting $w := v_k - \epsilon \cdot \sum_{j=1}^{k-1} \langle w_j, v_k\rangle w_j \in V_k$, we have $\langle w_i, w\rangle = \langle w_i, v_k\rangle - \langle w_i, v_k\rangle = 0$, for $i \in \{1,\ldots,k-1\}$, hence $w \in V_k \cap V_{k-1}^\perp$. Thus $C := [w_1,\ldots,w_{k-1},w] \subseteq V_k$ is an orthogonal K-basis such that $G_C^C(\Phi|_{V_k}) = \epsilon E_{k-1} \oplus [\langle w,w\rangle]$; note that $V_{k-1} \cap V_{k-1}^\perp = \{0\}$. Hence from $\epsilon\langle w,w\rangle = \epsilon^k \cdot \det(G_C^C(\Phi|_{V_k})) = |\det(M_{B_k}^C(\mathrm{id}))|^2 \cdot \epsilon^k \cdot \det(G_k) > 0$ we infer that $\langle w,w\rangle = \epsilon$, that is $\Phi|_{V_k}$ is positive or negative definite, respectively. ♯

b) We now give a characterisation of the quadratic form q associated with Φ being positive or negative semi-definite in terms of all **principal minors** of the Gram matrix of Φ: To this end, for $S \subseteq \{1,\ldots,n\}$ let $G_S \in K^{|S|\times|S|}$ be the submatrix of $G = G_B^B(\Phi)$ consisting of the columns and rows in S; hence we have $G_{\{1,\ldots,k\}} = G_k$, for $k \in \{0,\ldots,n\}$.

Let q be positive or negative semi-definite, and let $\epsilon := 1$ and $\epsilon := -1$, respectively. Then letting $C \subseteq V$ be an orthogonal K-basis as in Sylvester's Theorem, and $P := M_B^C(\mathrm{id}) \in \mathrm{GL}_n(K)$, we have $P^*GP = G_C^C(\Phi) = \epsilon E_r \oplus (0 \cdot E_{n-r}) \in K^{n\times n}$, for some $r \in \{0,\ldots,n\}$, implying that $|\det(P)|^2 \cdot \det(G) = \det(G_C^C(\Phi)) \in \{\epsilon^n, 0\}$, hence $\epsilon^n \cdot \det(G) \geq 0$. Moreover, since semi-definiteness is inherited to K-subspaces, we infer $\epsilon^{|S|} \cdot \det(G_S) \geq 0$, for all $S \subseteq \{1,\ldots,n\}$; note that $\det(G_S)$ is a principal minor of G, and that since G is hermitian we have $\det(G_S) \in \mathbb{R}$.

Conversely, let $\epsilon \in \{\pm 1\}$, and assume that $\epsilon^{|S|} \cdot \det(G_S) \geq 0$, for all $S \subseteq \{1,\ldots,n\}$. We consider the hermitian α-sesquilinear form $\Phi + \epsilon\xi\Gamma$, where $\xi > 0$ and Γ denotes the standard α-sesquilinear form with respect to the K-basis $B \subseteq V$, whose Gram matrix is given as $G_B^B(\Phi + \epsilon\xi\Gamma) = G + \epsilon\xi E_n \in K^{n\times n}$, and whose associated quadratic form is given as $q_\xi(v) = q(v) + \epsilon\xi\Gamma(v,v)$, for all $v \in V$: For $k \in \{0,\ldots,n\}$ the characteristic polynomial of G_k equals $\chi_{G_k} = \det(XE_k - G_k) = X^k + \sum_{j=1}^k (-1)^j \cdot \big(\sum_{S\subseteq\{1,\ldots,k\},\,|S|=j} \det(G_S)\big) \cdot X^{k-j} \in \mathbb{R}[X]$. This yields $\det(G_k + XE_k) = (-1)^k \cdot \det((-X)E_k - G_k) = X^k + \sum_{j=1}^k \big(\sum_{S\subseteq\{1,\ldots,k\},\,|S|=j} \det(G_S)\big) \cdot X^{k-j}$. Hence we get $\epsilon^k \cdot \det(G_k + \epsilon\xi E_k) = \xi^k + \sum_{j=1}^k \epsilon^j \cdot \big(\sum_{S\subseteq\{1,\ldots,k\},\,|S|=j} \det(G_S)\big) \cdot \xi^{k-j} > 0$. Thus q_ξ is positive or negative definite, respectively, and hence $\epsilon q(v) = \lim_{\xi\to 0^+}(\epsilon q_\xi(v)) \geq 0$, for all $0 \neq v \in V$, showing that q is positive or negative semi-definite, respectively. ♯

Note that the straightforward generalisation of the definite case, namely that $\epsilon^k \cdot \det(G_k) \geq 0$, for all $k \subseteq \{0,\ldots,n\}$, already entails semi-definiteness, does not hold, as the example $G := \begin{bmatrix} . & . \\ . & -1 \end{bmatrix}$, for $\epsilon = 1$, shows.

(4.8) Orthonormalisation. a) Let $[K,\alpha] \in \{[\mathbb{R}, \mathrm{id}_\mathbb{R}], [\mathbb{C}, \overline{}]\}$, let $\Phi = \langle\cdot,\cdot\rangle$ be a scalar product on a K-vector space V, and let $B = [v_1,\ldots,v_n] \subseteq V$ be a K-basis, where $n := \dim_K(V) \in \mathbb{N}_0$. Then V has a unique orthonormal K-basis C such that $M_B^C(\mathrm{id}) \in \mathrm{GL}_n(K)$ is an upper triangular matrix having positive diagonal entries, called the **Gram-Schmidt** K-basis associated with B; recall that orthonormal K-bases possibly exist only if Φ is a scalar product:

The existence of C follows from the orthogonalisation procedure in (4.5), using that Φ is anisotropic. To show uniqueness, let $C = [w_1, \ldots, w_n] \subseteq V$ be a K-basis having the desired properties, implying $V_k := \langle v_1, \ldots, v_k \rangle_K = \langle w_1, \ldots, w_k \rangle_K = \langle w_1, \ldots, w_{k-1}, v_k \rangle_K \leq V$, for $k \in \{0, \ldots, n\}$. Now we proceed by induction on $k \in \mathbb{N}_0$, the case $k = 0$ being trivial, we assume $k \geq 1$. We have $w_k = av_k + \sum_{j=1}^{k-1} a_j w_j \in V_k \cap V_{k-1}^{\perp}$, for $a, a_1, \ldots, a_{k-1} \in K$, where a equals the k-th diagonal entry of $M_B^C(\mathrm{id})$. From $0 = \langle w_i, w_k \rangle = a\langle w_i, v_k \rangle + \sum_{j=1}^{k-1} a_j \langle w_i, w_j \rangle = a\langle w_i, v_k \rangle + a_i$, for all $i \in \{1, \ldots, k-1\}$, we get $w_k = aw_k'$, where $w_k' := v_k - \sum_{j=1}^{k-1} \langle w_j, v_k \rangle w_j \in V_k$, which by induction is determined uniquely. Finally, from $1 = \langle w_k, w_k \rangle = |a|^2 \langle w_k', w_k' \rangle$ we get $|a| = \frac{1}{\sqrt{\langle w_k', w_k' \rangle}} \in K$, where by assumption we have $a = |a|$. ♯

In particular any orthonormal subset of V can be extended to an orthonormal K-basis of V; recall that orthogonal sets consisting of non-isotropic vectors are K-linearly independent anyway.

b) If we are given a Gram matrix $G = G_B^B(\Phi)$ of some hermitian α-sesquilinear form Φ with respect to some K-basis $B \subseteq V$, the question arises how we may decide whether Φ is a scalar product. This can be done in various ways:

i) The associated quadratic form is given as $q(x_1, \ldots, x_n) = [\overline{x}_1, \ldots, \overline{x}_n] \cdot G \cdot [x_1, \ldots, x_n]^{\mathrm{tr}}$, where $[x_1, \ldots, x_n]^{\mathrm{tr}} \in \mathbb{R}^{n \times 1}$ is the coordinate tuple with respect to B, and we may try and decide whether q is positive definite. **ii)** We may apply the Hurwitz-Sylvester criterion. **iii)** We may run the orthogonalisation procedure, regardless of whether or not Φ is a scalar product, which yields an orthonormal K-basis if Φ is a scalar product, and otherwise at a certain stage necessarily produces a vector $0 \neq v \in V$ such that $\Phi(v, v) \leq 0$. **iv)** Yet another criterion will be given in (5.6).

Example. Let Γ be the standard scalar product on $V := \mathbb{R}^{2 \times 1}$, let $A \subseteq V$ be the standard $\mathbb{R}$-basis, and let the $\mathbb{R}$-basis $B \subseteq V$ be given as $Q = M_A^B(\mathrm{id}) := \begin{bmatrix} 1 & -\frac{1}{2} \\ 0 & \frac{\sqrt{3}}{2} \end{bmatrix} \in \mathrm{GL}_2(\mathbb{R})$, hence we get $G := G_B^B(\Gamma) = Q^{\mathrm{tr}} Q = \begin{bmatrix} 1 & -\frac{1}{2} \\ -\frac{1}{2} & 1 \end{bmatrix} \in \mathbb{R}^{2 \times 2}$.

By construction G is the Gram matrix of a scalar product. But if we are just given the matrix G then this information is lost. Still, the associated quadratic form is given as $q(x, y) = [x, y] \cdot G \cdot [x, y]^{\mathrm{tr}} = x^2 - xy + y^2 = (x - \frac{1}{2}y)^2 + \frac{3}{4}y^2$, hence $q(x, y) > 0$ for all $0 \neq [x, y] \in \mathbb{R}^2$; alternatively, we have $\det([1]) = 1 > 0$ and $\det(G) = \frac{3}{4} > 0$, hence the Hurwitz-Sylvester criterion implies that G describes a scalar product. We aim to find an orthonormal $\mathbb{R}$-basis of V from G:

Letting $P_1 := \begin{bmatrix} 1 & \frac{1}{2} \\ 0 & 1 \end{bmatrix}$ yields $P_1^{\mathrm{tr}} G P_1 = \mathrm{diag}[1, \frac{3}{4}]$, thus letting $P_2 := \mathrm{diag}[1, \frac{2}{\sqrt{3}}]$ and $P := P_1 P_2 = \begin{bmatrix} 1 & \frac{1}{\sqrt{3}} \\ 0 & \frac{2}{\sqrt{3}} \end{bmatrix} \in \mathrm{GL}_2(\mathbb{R})$ yields $P^{\mathrm{tr}} G P = E_2$, hence we get the orthonormal $\mathbb{R}$-basis $C \subseteq V$ defined by $M_B^C(\mathrm{id}) := P$; indeed we have $M_A^C(\mathrm{id}) = M_A^B(\mathrm{id}) \cdot M_B^C(\mathrm{id}) = QP = E_2$, thus C is just the standard $\mathbb{R}$-basis. ♯

(4.9) Euclidean and unitary geometry. a) Let $[K, \alpha] \in \{[\mathbb{R}, \mathrm{id}_{\mathbb{R}}], [\mathbb{C}, \overline{}]\}$, and let $\Phi = \langle \cdot, \cdot \rangle$ be a scalar product on a finitely generated K-vector space V, with associated quadratic form q. Let $\|v\| := \sqrt{q(v)} = \sqrt{\langle v, v \rangle} \in \mathbb{R}_{\geq 0}$ be the **length** or **norm** of $v \in V$.

Then we have $\|av\| = |a| \cdot \|v\|$, for $a \in K$, that is **linearity** with respect to absolute values, and $\|v\| = 0$ if and only if and only if $v = 0$, that is **definiteness**. For any vector $0 \neq v \in V$ there is an associated normed vector $\frac{1}{\|v\|} \cdot v \in V$.

For $v, w \in V$ we have the **Cauchy-Schwarz inequality** $|\langle v, w \rangle| \leq \|v\| \cdot \|w\|$, where equality holds if and only if $[v, w]$ is K-linearly dependent:

We may assume that $v \neq 0$. For any $u := av + bw \in V$, where $a, b \in K$, we have $\langle u, u \rangle = |a|^2 \langle v, v \rangle + \overline{a} b \langle v, w \rangle + a \overline{b} \langle w, v \rangle + |b|^2 \langle w, w \rangle$. Hence letting $a := -\overline{\langle v, w \rangle}$ and $b := \langle v, v \rangle$ we get $\langle u, u \rangle = |\langle v, w \rangle|^2 \langle v, v \rangle - \overline{\langle v, w \rangle} \langle v, v \rangle \langle v, w \rangle - \langle v, w \rangle \overline{\langle v, v \rangle} \langle w, v \rangle + |\langle v, v \rangle|^2 \langle w, w \rangle = \langle v, v \rangle \big(\langle v, v \rangle \langle w, w \rangle - |\langle v, w \rangle|^2 \big)$. Since we have $\langle u, u \rangle \geq 0$ and $\langle v, v \rangle > 0$ we conclude that $|\langle v, w \rangle|^2 \leq \langle v, v \rangle \cdot \langle w, w \rangle$.

Moreover, if equality holds then $\langle u, u \rangle = 0$, that is $u = 0$, thus $b = \langle v, v \rangle \neq 0$ implies that $[v, w]$ is K-linearly dependent. Conversely, if $[v, w]$ is K-linearly dependent, then there is $a \in K$ such that $w = av$, and hence $|\langle v, w \rangle|^2 = |\langle v, av \rangle|^2 = |a|^2 |\langle v, v \rangle|^2 = \langle v, v \rangle \langle av, av \rangle = \langle v, v \rangle \langle w, w \rangle$. ♯

This yields the **Minkowski** or **triangle inequality** $\|v + w\| \leq \|v\| + \|w\|$:

We have $\|v + w\|^2 = \langle v, v \rangle + \langle v, w \rangle + \overline{\langle v, w \rangle} + \langle w, w \rangle = \langle v, v \rangle + 2\mathrm{Re}(\langle v, w \rangle) + \langle w, w \rangle \leq \langle v, v \rangle + 2|\langle v, w \rangle| + \langle w, w \rangle \leq \|v\|^2 + 2\|v\|\|w\| + \|w\|^2 = (\|v\| + \|w\|)^2$. ♯

Thus V together with the norm $\|\cdot\|$, where the latter fulfills linearity, definiteness and the triangle inequality, becomes a **normed vector space**; since the norm is induced by a scalar product, V even is a **(pre-)Hilbert space**.

Moreover, for $K = \mathbb{R}$ we have the following geometric interpretation: For $0 \neq v, w \in V$ we have $-1 \leq \frac{\langle v, w \rangle}{\|v\| \cdot \|w\|} \leq 1$. Thus there is a unique $0 \leq \omega \leq \pi$ such that $\cos(\omega) = \frac{\langle v, w \rangle}{\|v\| \cdot \|w\|}$, called the **angle** between the normed vectors $\frac{1}{\|v\|} \cdot v$ and $\frac{1}{\|w\|} \cdot w$; the latter are **perpendicular**, that is we have $\omega = \frac{\pi}{2}$, if and only if $\cos(\omega) = 0$, which holds if and only if $\langle v, w \rangle = 0$, that is $v \perp w$.

b) Let $\{v_1, \ldots, v_n\} \subseteq V$ be an orthonormal K-basis, that is $\langle v_i, v_j \rangle = 0$ and $\langle v_i, v_i \rangle = 1$, for all $i \neq j \in \{1, \ldots, n\}$, where $n := \dim_K(V) \in \mathbb{N}_0$.

Then for any $v \in V$ we have the **Fourier expansion** $v = \sum_{i=1}^n \langle v_i, v \rangle v_i$: Letting $v' := \sum_{i=1}^n \langle v_i, v \rangle v_i \in V$, we have $\langle v_j, v' \rangle = \sum_{i=1}^n \langle v_i, v \rangle \langle v_j, v_i \rangle = \langle v_j, v \rangle$, thus $\langle v_j, v - v' \rangle = 0$, for all $j \in \{1, \ldots, n\}$, implying $v - v' \in V^\perp = \{0\}$.

Moreover, Fourier expansion yields **Pythagoras's Theorem** $\|v\|^2 = \langle v, v \rangle = \sum_{i=1}^n \sum_{j=1}^n \langle v_i, v \rangle \overline{\langle v_j, v \rangle} \langle v_i, v_j \rangle = \sum_{i=1}^n |\langle v_i, v \rangle|^2$.

c) Let $U \leq V$ be a K-subspace with orthonormal K-basis $\{u_1, \ldots, u_m\} \subseteq U$, where $m := \dim_K(U)$. Then for $a_1, \ldots, a_m \in K$ we have $\|v - \sum_{i=1}^m a_i u_i\|^2 = \langle v, v \rangle - \sum_{i=1}^m (a_i \overline{\langle u_i, v \rangle} + \overline{a}_i \langle u_i, v \rangle) + \sum_{i=1}^m |a_i|^2 = \langle v, v \rangle - \sum_{i=1}^m |\langle u_i, v \rangle|^2 +$

$\sum_{i=1}^m (a_i - \langle u_i, v\rangle)(\overline{a}_i - \overline{\langle u_i, v\rangle}) = \langle v, v\rangle - \sum_{i=1}^m |\langle u_i, v\rangle|^2 + \sum_{i=1}^m |a_i - \langle u_i, v\rangle|^2$, thus the **Bessel inequality** $\min\{\|v-u\|^2; u \in U\} = \|v\|^2 - \sum_{i=1}^m |\langle u_i, v\rangle|^2 \geq 0$.

Indeed, the minimum is attained precisely for the **best approximation** $u_0 := \sum_{i=1}^m \langle u_i, v\rangle u_i \in U$. We have $\langle v - u_0, u_j\rangle = \langle v, u_j\rangle - \sum_{i=1}^m \langle u_i, v\rangle\langle u_i, u_j\rangle = \langle v, u_j\rangle - \langle u_j, v\rangle = 0$, for all $j \in \{1, \ldots, m\}$, hence $v - u_0 \in U^\perp$, saying that u_0 is the U-component of v with respect to the direct sum decomposition $V = U \oplus U^\perp$, in other words we have $U \cap (v + U^\perp) = \{u_0\}$.

5 Adjoint maps

(5.1) Adjoint maps. a) Let K be a field, let $\alpha\colon K \to K$ be a field automorphism such that $\alpha^2 = \mathrm{id}_K$, and let V be finitely generated K-vector space with a non-degenerate α-sesquilinear form Φ. For any $\varphi \in \mathrm{End}_K(V)$ there is a unique **adjoint map** $\varphi^* \in \mathrm{End}_K(V)$ such that $\langle v, \varphi(w)\rangle = \langle \varphi^*(v), w\rangle$ for all $v, w \in V$:

Let $B := [v_1, \ldots, v_n] \subseteq V$ be a K-basis, where $n := \dim_K(V) \in \mathbb{N}_0$, and let $G := G_B^B(\Phi) \in \mathrm{GL}_n(K)$ and $A = [a_{ij}]_{ij} := M_B^B(\varphi) \in K^{n\times n}$. Then for the α-sesquilinear form $\Psi\colon V \times V \to K\colon [v, w] \mapsto \langle v, \varphi(w)\rangle$ we have $\Psi(v_i, v_j) = \langle v_i, \varphi(v_j)\rangle = \sum_{k=1}^n a_{kj}\langle v_i, v_k\rangle = (GA)_{ij}$, for $i, j \in \{1, \ldots, n\}$, implying that $G_B^B(\Psi) = GA$. Similarly, for the α-sesquilinear form $\Psi'\colon V \times V \to K\colon [v, w] \mapsto \langle \varphi(v), w\rangle$ we have $\Psi'(v_i, v_j) = \langle \varphi(v_i), v_j\rangle = \sum_{k=1}^n a_{ki}^\alpha \langle v_k, v_j\rangle = (A^*G)_{ij}$, for $i, j \in \{1, \ldots, n\}$, implying that $G_B^B(\Psi') = A^*G$.

Hence letting $A' := (GAG^{-1})^* \in K^{n\times n}$, we let $\varphi^* \in \mathrm{End}_K(V)$ be defined by $M_B^B(\varphi^*) = A'$. Then we have $GA = A'^*G$, implying that $\langle v, \varphi(w)\rangle = \langle \varphi^*(v), w\rangle$, for all $v, w \in V$. If $\varphi' \in \mathrm{End}_K(V)$ such that $\langle \varphi'(v), w\rangle = \langle \varphi^*(v), w\rangle$, for all $v, w \in V$, then we have $(\varphi' - \varphi^*)(v) \in {}^\perp V = \{0\}$, that is $\varphi' = \varphi^*$. ♯

In particular, if B is orthonormal then we have $M_B^B(\varphi^*) = A^* = M_B^B(\varphi)^*$.

b) We collect a few properties: From $(G \cdot aA \cdot G^{-1})^* = a^\alpha (GAG^{-1})^*$, for all $a \in K$, we conclude that the additive map ${}^*\colon \mathrm{End}_K(V) \to \mathrm{End}_K(V)\colon \varphi \mapsto \varphi^*$ is α-semilinear. Moreover, for $\varphi' \in \mathrm{End}_K(V)$, letting $A' := M_B^B(\varphi') \in K^{n\times n}$, we get $(GA'AG^{-1})^* = (GAG^{-1})^*(GA'G^{-1})^*$, thus $(\varphi'\varphi)^* = \varphi^*\varphi'^*$.

We have $\mathrm{id}^* = \mathrm{id}$, as well as $\det(\varphi^*) = \det((GAG^{-1})^*) = \det(A)^\alpha = \det(\varphi)^\alpha$, and $\mathrm{rk}(\varphi^*) = \mathrm{rk}((GAG^{-1})^*) = \mathrm{rk}(A) = \mathrm{rk}(\varphi)$. In particular, we have $\varphi \in \mathrm{GL}(V)$ if and only if $\varphi^* \in \mathrm{GL}(V)$, and in this case from $((GAG^{-1})^*)^{-1} = (GA^{-1}G^{-1})^*$ we get $(\varphi^*)^{-1} = (\varphi^{-1})^*$.

Since ${}^\perp V = \{0\}$, for $v \in V$ we have $v \in \ker(\varphi^*)$ if and only if $0 = \langle \varphi^*(v), w\rangle = \langle v, \varphi(w)\rangle$ for all $w \in V$, implying that $\ker(\varphi^*) = {}^\perp\mathrm{im}(\varphi)$. Similarly, since $V^\perp = \{0\}$, for $w \in V$ we have $w \in \ker(\varphi)$ if and only if $0 = \langle v, \varphi(w)\rangle = \langle \varphi^*(v), w\rangle$ for all $v \in V$, implying that $\ker(\varphi) = \mathrm{im}(\varphi^*)^\perp$.

If $U \leq V$ is φ-invariant, then from $\langle \varphi^*(v), w\rangle = \langle v, \varphi(w)\rangle = 0$ for all $v \in {}^\perp U$ and $w \in U$ we infer that ${}^\perp U$ is φ^*-invariant. Similarly, if $U \leq V$ is φ^*-invariant then from $\langle v, \varphi(w)\rangle = \langle \varphi^*(v), w\rangle = 0$ for all $v \in U$ and $w \in U^\perp$ we infer that $U^\perp$ is φ-invariant.

If Φ is hermitian then $\langle v, \varphi^*(w)\rangle = \langle \varphi^*(w), v\rangle^\alpha = \langle w, \varphi(v)\rangle^\alpha = \langle \varphi(v), w\rangle$, for all $v, w \in V$, hence we get $\varphi^{**} = \varphi$. We argue similarly if Φ is skew-hermitian.

(5.2) Normal maps. a) Let K be a field, let $\alpha\colon K \to K$ be a field automorphism such that $\alpha^2 = \mathrm{id}_K$, and let V be finitely generated K-vector space with a non-degenerate hermitian form Φ.

A map $\varphi \in \mathrm{End}_K(V)$ is called **normal** if $\varphi\varphi^* = \varphi^*\varphi$. In particular, if $\varphi^* = \varphi$ then φ is called **hermitian** or **self-adjoint**; if $\varphi \in \mathrm{GL}(V)$ such that $\varphi^* = \varphi^{-1}$ then φ is called **unitary** or an **isometry**; if $\alpha = \mathrm{id}_K$ then in the above cases φ is also called **symmetric** and **orthogonal**, respectively. Hence if $B \subseteq V$ is an orthonormal K-basis, then these properties are translated into the respective properties of the matrix $M_B^B(\varphi)$.

We proceed to characterise normal maps: The map φ is normal if and only if $\langle \varphi(v), \varphi(w)\rangle = \langle \varphi^*(v), \varphi^*(w)\rangle$, for all $v, w \in V$:

If φ is normal, then we have $\langle \varphi(v), \varphi(w)\rangle = \langle \varphi^*\varphi(v), w\rangle = \langle \varphi\varphi^*(v), w\rangle = \langle \varphi^*(v), \varphi^*(w)\rangle$, for all $v, w \in V$. Conversely, $\langle \varphi^*\varphi(v), w\rangle = \langle \varphi(v), \varphi(w)\rangle = \langle \varphi^*(v), \varphi^*(w)\rangle = \langle \varphi\varphi^*(v), w\rangle$, for all $w \in V$, shows $(\varphi^*\varphi - \varphi\varphi^*)(v) \in V^\perp = \{0\}$ for all $v \in V$, hence we have $\varphi^*\varphi = \varphi\varphi^*$. $\sharp$

b) Let Φ be a scalar product. Then the map φ is normal if and only if $\|\varphi(v)\| = \|\varphi^*(v)\|$, for all $v \in V$:

If φ is normal, then $\|\varphi(v)\|^2 = \langle \varphi(v), \varphi(v)\rangle = \langle \varphi^*(v), \varphi^*(v)\rangle = \|\varphi^*(v)\|^2$, for all $v \in V$. Conversely, from $\langle \varphi(v), \varphi(v)\rangle = \langle \varphi^*(v), \varphi^*(v)\rangle$ and $\langle \varphi(v+aw), \varphi(v+aw)\rangle = \langle \varphi^*(v+aw), \varphi^*(v+aw)\rangle$, for all $v, w \in V$ and $a \in K$, we obtain $a\langle \varphi(v), \varphi(w)\rangle + \overline{a}\langle \varphi(w), \varphi(v)\rangle = a\langle \varphi^*(v), \varphi^*(w)\rangle + \overline{a}\langle \varphi^*(w), \varphi^*(v)\rangle$, which since Φ is hermitian entails $\mathrm{Re}\big(a\langle \varphi(v), \varphi(w)\rangle\big) = \mathrm{Re}\big(a\langle \varphi^*(v), \varphi^*(w)\rangle\big)$, hence letting $a := 1$ and $a := -i$ shows that $\langle \varphi(v), \varphi(w)\rangle = \langle \varphi^*(v), \varphi^*(w)\rangle$. $\sharp$

In particular, if φ is normal then we have $\ker(\varphi) = \ker(\varphi^*)$. Moreover, if φ is normal then for any φ-invariant K-subspace $U \leq V$ the K-subspace $U^\perp \leq V$ is φ-invariant as well:

Let $B := [v_1, \ldots, v_n] \subseteq V$ be an orthonormal K-basis, where we assume that $B' := [v_1, \ldots, v_m] \subseteq U$ and $B'' := [v_{m+1}, \ldots, v_n] \subseteq U^\perp$, where $n := \dim_K(V) \in \mathbb{N}_0$ and $m := \dim_K(U) \in \mathbb{N}_0$; recall that $V = U \oplus U^\perp$. Then $A := M_B^B(\varphi) \in K^{n\times n}$ is an upper **block triangular** matrix of shape $A = \left[\begin{array}{c|c} A' & C \\ \hline . & A'' \end{array}\right]$, where $A' \in K^{m\times m}$ and $A'' \in K^{(n-m)\times(n-m)}$ and $C = [c_{ij}]_{ij} \in K^{m\times(n-m)}$. We have $A^* = \left[\begin{array}{c|c} A'^* & . \\ \hline C^* & A''^* \end{array}\right]$, hence normality, that is $AA^* = A^*A$, implies $A'^*A' = A'A'^* + CC^*$. Since $\mathrm{Tr}(A'^*A') = \mathrm{Tr}(A'A'^*)$, this entails $0 = \mathrm{Tr}(CC^*) = \sum_{i=1}^m \sum_{j=1}^{n-m} c_{ij}\overline{c_{ij}} = \sum_{i=1}^m \sum_{j=1}^{n-m} |c_{ij}|^2$, thus $C = 0$; that is $A = A' \oplus A'' = M_{B'}^{B'}(\varphi|_U) \oplus M_{B''}^{B''}(\varphi|_{U^\perp})$ is a block diagonal matrix. $\sharp$

(5.3) Unitary maps. **a)** Let K be a field, let $\alpha\colon K \to K$ be a field automorphism such that $\alpha^2 = \mathrm{id}_K$, let V be finitely generated K-vector space with a non-degenerate hermitian form Φ, and let $\varphi \in \mathrm{End}_K(V)$.

Then φ is unitary if and only if $\langle \varphi(v), \varphi(w)\rangle = \langle v, w\rangle$, for all $v, w \in V$:

If φ is unitary, then $\langle \varphi(v), \varphi(w)\rangle = \langle \varphi^*\varphi(v), w\rangle = \langle \varphi^{-1}\varphi(v), w\rangle = \langle v, w\rangle$, for all $v, w \in V$. Conversely, $\langle \varphi^*\varphi(v), w\rangle = \langle \varphi(v), \varphi(w)\rangle = \langle v, w\rangle$, for all $w \in V$, shows that $\varphi^*\varphi(v) - v \in V^\perp = \{0\}$, for all $v \in V$, that is $\varphi^*\varphi = \mathrm{id}$. ♯

If φ is unitary, then we have $\det(\varphi)^{1+\alpha} = \det(\varphi\varphi^*) = \det(\mathrm{id}) = 1$; in particular, if $[K, \alpha] = [\mathbb{C}, \overline{\ }]$ then $|\det(\varphi)| = 1$, and if $\alpha = \mathrm{id}_K$ then $\det(\varphi) \in \{\pm 1\}$.

It follows from the above characterisation of unitary maps that $\varphi\varphi'$ and φ^{-1} are unitary, whenever φ and φ' are. Hence $\mathrm{GU}(V) := \{\varphi \in \mathrm{GL}(V); \varphi \text{ unitary}\} \leq \mathrm{GL}(V)$ is a subgroup, being called the **general unitary group**; moreover, $\mathrm{SU}(V) := \mathrm{GU}(V) \cap \mathrm{SL}(V) = \{\varphi \in \mathrm{GU}(V); \det(\varphi) = 1\} \leq \mathrm{GL}(V)$ is called the **special unitary group**. If $\alpha = \mathrm{id}_K$ the latter are also called the **general** and **special orthogonal groups**, denoted by $\mathrm{GO}(V)$ and $\mathrm{SO}(V)$, respectively; orthogonal maps of determinant 1 are called **rotations**.

b) Let Φ be a scalar product. Then φ is unitary if and only if $\|\varphi(v)\| = \|v\|$, for all $v \in V$; this is the reason why unitary maps are also called isometries:

If φ is unitary, then we have $\|\varphi(v)\|^2 = \langle \varphi(v), \varphi(v)\rangle = \langle v, v\rangle = \|v\|^2$, for all $v \in V$. Conversely, from $\langle \varphi(v), \varphi(v)\rangle = \langle v, v\rangle$ and $\langle \varphi(v+aw), \varphi(v+aw)\rangle = \langle v+aw, v+aw\rangle$, for all $v, w \in V$ and $a \in K$, we get $a\langle \varphi(v), \varphi(w)\rangle + \overline{a}\langle \varphi(w), \varphi(v)\rangle = a\langle v, w\rangle + \overline{a}\langle w, v\rangle$, which since Φ is hermitian entails $\mathrm{Re}\big(a\langle \varphi(v), \varphi(w)\rangle\big) = \mathrm{Re}\big(a\langle v, w\rangle\big)$, hence letting $a := 1$ and $a := -i$ shows that $\langle \varphi(v), \varphi(w)\rangle = \langle v, w\rangle$. ♯

In particular, if φ is unitary then for any eigenvalue $a \in K$, with associated eigenvector $v \in V$, we get $\|v\| = \|\varphi(v)\| = \|av\| = |a| \cdot \|v\|$, hence $|a| = 1$.

If φ is unitary, then for $0 \neq v, w \in V$ we have $\frac{\langle \varphi(v), \varphi(w)\rangle}{\|\varphi(v)\| \cdot \|\varphi(w)\|} = \frac{\langle v, w\rangle}{\|v\| \cdot \|w\|}$. Hence, next to the length of vectors, unitary maps also leave the angle between vectors invariant In particular, we recover the fact that unitary maps map orthonormal bases to orthonormal bases; recall that conversely a K-linear map mapping an orthonormal basis to an orthonormal basis is unitary.

(5.4) Theorem: Spectral theorem. Let $[K, \alpha] \in \{[\mathbb{R}, \mathrm{id}_\mathbb{R}], [\mathbb{C}, \overline{\ }]\}$, let Φ be a scalar product on a finitely generated K-vector space V, and let $\varphi \in \mathrm{End}_K(V)$. Then there is an orthonormal K-basis of V consisting of eigenvectors of φ if and only if φ is normal and $\chi_\varphi \in K[X]$ splits into linear factors.

In particular, these conditions are fulfilled if
i) $K = \mathbb{C}$ and φ is normal, or **ii)** $K = \mathbb{R}$ and φ is symmetric.

Using standard scalar products, in terms of matrices this reads as follows: Given a matrix $A \in K^{n \times n}$, where $n \in \mathbb{N}_0$, then there is a unitary matrix $P \in \mathrm{GL}_n(K)$ such that $P^{-1}AP = P^*AP \in K^{n \times n}$ is a diagonal matrix, provided
i) $K = \mathbb{C}$ and A is normal, or **ii)** $K = \mathbb{R}$ and A is symmetric.

Proof. Let $B \subseteq V$ be an orthonormal K-basis consisting of eigenvectors of φ. Then φ is diagonalisable, hence $\chi_\varphi \in K[X]$ splits into linear factors. Moreover, $A := M_B^B(\varphi) \in K^{n\times n}$, where $n := \dim_K(V) \in \mathbb{N}_0$, is a diagonal matrix, hence from $M_B^B(\varphi^*) = A^*$ we infer $AA^* = A^*A$, that is $\varphi\varphi^* = \varphi^*\varphi$.

Conversely, we proceed by induction on $n \in \mathbb{N}_0$, the case $n = 0$ being trivial: Let $n \geq 1$, and since $\chi_\varphi \in K[X]$ splits into linear factors, let $v \in V$ be an eigenvector of φ, where we may assume that $\|v\| = 1$, and let $U := \langle v\rangle_K$. Hence we have $V = U \oplus U^\perp$. Since U is φ-invariant, we conclude that $U^\perp$ is φ^*-invariant, and since φ is normal, we infer that $U^\perp$ is also φ-invariant. Since $\Phi|_{U^\perp}$ is a scalar product, in particular is non-degenerate, by the definition of adjoint maps we get $(\varphi|_{U^\perp})^* = \varphi^*|_{U^\perp}$. Hence $\varphi|_{U^\perp}$ is normal, and since $\chi_\varphi = \chi_{\varphi|_U} \cdot \chi_{\varphi|_{U^\perp}} \in K[X]$ we are done by induction.

The assertion in (i) follows from $\mathbb{C}$ being algebraically closed.

To show (ii), we more generally allow for $K = \mathbb{C}$ or $K = \mathbb{R}$, and that φ is hermitian. Let $A := M_B^B(\varphi) \in K^{n\times n}$, where $B \subseteq V$ be an orthonormal K-basis. We have to show that $\chi_A \in K[X]$ splits into linear factors. Since $\chi_A \in \mathbb{C}[X]$ splits into linear factors anyway, we proceed to show that all complex eigenvalues of $A \in \mathbb{C}^{n\times n}$ actually belong to $\mathbb{R}$:

For all $a \in \mathbb{C}$ we have $(A - aE_n)^* = A^* - \overline{a}E_n \in \mathbb{C}^{n\times n}$. Since A is normal, that is $AA^* = A^*A$, we conclude that $A - aE_n$ is normal as well. Hence we have $T_a(A) = \ker(A - aE_n) = \ker((A - aE_n)^*) = \ker(A^* - \overline{a}E_n) = T_{\overline{a}}(A^*)$. Since $A = A^*$, this implies that all eigenvalues a of A fulfill $\overline{a} = a$; recall that eigenvectors with respect to distinct eigenvalues are linearly independent. ♯

(5.5) Corollary: Unitary and hermitian maps. a) If $K = \mathbb{C}$, then φ is unitary if and only if φ is normal with all eigenvalues having absolute value 1.

b) The map φ is hermitian if and only if φ is normal and $\chi_\varphi \in K[X]$ splits into linear factors over $\mathbb{R}$.

Proof. a) We have seen that unitary maps have the desired properties. Conversely, let $B := [v_1, \ldots, v_n] \subseteq V$ be an orthonormal $\mathbb{C}$-basis such that $\varphi(v_i) = a_iv_i$, where $|a_i| = 1$, for all $i \in \{1, \ldots, n\}$. Then for $v = \sum_{i=1}^n b_iv_i \in V$, where $b_1, \ldots, b_n \in \mathbb{C}$, we have $\|\varphi(v)\|^2 = \|\sum_{i=1}^n a_ib_iv_i\|^2 = \sum_{i=1}^n \langle a_ib_iv_i, a_ib_iv_i\rangle = \sum_{i=1}^n |a_i|^2|b_i|^2 = \sum_{i=1}^n |b_i|^2 = \sum_{i=1}^n \langle b_iv_i, b_iv_i\rangle = \|v\|^2$, hence φ is unitary.

b) We have seen that hermitian maps have the desired properties. Conversely, let $B := [v_1, \ldots, v_n] \subseteq V$ be an orthonormal K-basis such that $\varphi(v_i) = a_iv_i$, where $a_i \in \mathbb{R}$, for all $i \in \{1, \ldots, n\}$. Then $M_B^B(\varphi)^* = (\mathrm{diag}[a_1, \ldots, a_n])^* = \mathrm{diag}[\overline{a}_1, \ldots, \overline{a}_n] = \mathrm{diag}[a_1, \ldots, a_n] = M_B^B(\varphi)$ says that φ is hermitian. ♯

(5.6) Principal axes transformation. Let $[K, \alpha] \in \{[\mathbb{R}, \mathrm{id}_\mathbb{R}], [\mathbb{C}, \overline{}]\}$, let Φ be a hermitian α-sesquilinear form on a K-vector space V, and let $G := G_B^B(\Phi) \in K^{n\times n}$ with respect to any K-basis $B \subseteq V$, where $n := \dim_K(V) \in \mathbb{N}_0$.

Then we have $\sum_{a\in\mathbb{R}} \nu_a(G) = n$, and Φ has signature $[\sum_{a>0} \nu_a(G), \sum_{a<0} \nu_a(G)]$:

Since G is hermitian, there is a unitary matrix $P \in \mathrm{GL}_n(K)$ such that $G' := P^{-1}GP = P^*GP = \mathrm{diag}[a_1, \ldots, a_n] \in K^{n\times n}$, where $a_i \in \mathbb{R}$, for all $i \in \{1, \ldots, n\}$. Hence on the one hand we have $\nu_a(G) = \nu_a(G')$ for all $a \in K$, where $\nu_a(G) > 0$ only if $a \in \mathbb{R}$, and on the other hand $G' = G_C^C(\Phi)$ is the Gram matrix of Φ with respect to the K-basis $C \subseteq V$, where $M_B^C(\mathrm{id}) = P$. Hence replacing all non-isotropic vectors $v \in C$ by normed scalar multiples $v' := \frac{1}{\sqrt{|\Phi(v,v)|}} \cdot v$ yields a K-basis $C' \subseteq V$ such that $G_{C'}^{C'}(\Phi) = E_k \oplus (-E_l) \oplus (0 \cdot E_m)$, where $k = \sum_{a>0} \nu_a(G)$ and $l = \sum_{a<0} \nu_a(G)$; note that $m = \dim_K(V^\perp) = \nu_0(G)$. ♯

The 1-dimensional K-subspaces of the eigenspace $T_a(G) \leq V$ are called **principal axes** of Φ with respect to $a \in \mathbb{R}$; recall that $T_0(G) = V^\perp \leq V$. In particular, if $\dim_K(T_a(G)) = 1$ then the latter are uniquely determined.

Example. For $K := \mathbb{R}$ and $\alpha = \mathrm{id}$, let Φ be given with respect to some $\mathbb{R}$-basis $B \subseteq \mathbb{R}^{3\times 1}$ by $G = G_B^B(\Phi) := \begin{bmatrix} 0 & -2 & 4 \\ -2 & 1 & -1 \\ 4 & -1 & 0 \end{bmatrix} \in \mathbb{R}^{3\times 3}$. We have $\chi_G = X^3 - X^2 - 21X = X(X - a_+)(X - a_-) \in \mathbb{R}[X]$, hence we get the eigenvalues $a_0 := 0$ and $a_\pm := \frac{1}{2}(1 \pm \sqrt{85}) \in \mathbb{R}$. Hence we conclude that Φ has signature $[1, 1]$, as we have already observed in (4.5); note that is suffices to observe that $a_+a_- = -21 < 0$ to conclude that $a_- < 0 < a_+$.

Moreover, we get the principal axes $T_0(G) = \langle v_0 \rangle_{\mathbb{R}}$ and $T_{a_\pm}(G) = \langle v_\pm \rangle_{\mathbb{R}}$, where $v_0 := [1, 4, 2]^{\mathrm{tr}} \in \mathbb{R}^{3\times 1}$ and $v_\pm := [\pm 4\sqrt{85}, -17 \mp \sqrt{85}, 34]^{\mathrm{tr}} \in \mathbb{R}^{3\times 1}$. Letting $\Gamma = \langle \cdot, \cdot \rangle$ denote the standard scalar product on $\mathbb{R}^{3\times 1}$, we indeed have $\langle v_0, v_\pm \rangle = 0 = \langle v_+, v_- \rangle$, as well as $\|v_0\|^2 = 21$ and $\|v_\pm\|^2 = 2890 \pm 34\sqrt{85}$. Hence $P := [v_+, v_-, v_0] \cdot \mathrm{diag}[\frac{1}{\|v_+\|}, \frac{1}{\|v_-\|}, \frac{1}{\|v_0\|}] \in \mathrm{GL}_3(\mathbb{R})$ is orthogonal, that is fulfills $P^{-1} = P^{\mathrm{tr}}$, and thus we get $P^{\mathrm{tr}}GP = P^{-1}GP = \mathrm{diag}[a_+, a_-, 0] \in \mathbb{R}^{3\times 3}$. ♯