

Linear Algebra 2

Lecture notes, University (of Technology) Graz
based on the lecture by Franz Lehner

Lukas Prokop

May 10, 2018

Contents

0.1	Lecture	2
1	Linear algebra 1	2
2	Determinants	3
2.1	Definition	3
2.2	Properties	3
2.3	Determinant form	7
2.4	Permutations and transpositions	9
2.5	Leibniz formula for determinants	15
2.6	On determinants, invertibility and linear independence	20
2.7	Laplace expansion	30
3	Inner products	35
3.1	Law of cosines	39
3.2	Outer product	39
3.3	Inner products and positive definiteness	42
3.4	Cauchy-Bunyakovskii-Schwarz inequality	46
3.5	Congruence of matrices	50
3.6	Gram-Schmidt process	82
3.7	Riesz representation theorem	86
3.8	Quaternions	100

This lecture took place on 2018/03/05.

0.1 Lecture

- Mon, 08:15–09:45, lecture
- Wed, 08:15–09:45, lecture
- Mon, 16:00–18:00, tutorial, AE01
- Mon, 13:15–14:00, conversatorium (BE01)

1 Linear algebra 1

Gottfried Wilhelm von Leibniz (1646–1716). Results from 1693:

- Vector spaces (first definition in 1880)
- Matrices and linear maps

From now, it will be more specific (matrices). In general, we discuss “when is a matrix invertible”?

$$\begin{aligned} ax + by &= e \\ cx + dy &= f \end{aligned}$$

We need to invert the matrix

Assuming $a \neq 0$. We multiply the first row with $\frac{1}{a} \cdot (-c)$.

$$\begin{array}{cc|cc} a & b & 1 & 0 \\ c & d & 0 & 1 \\ \hline 0 & d - \frac{c}{a} \cdot b & -\frac{c}{a} & 1 \end{array}$$

We then divide by $d - \frac{c}{a}b$ if $\neq 0$.

If $a = 0$ and $c = 0$, rank is certainly not 2.

If $a = 0$ and $c \neq 0$, we multiply with $\frac{1}{c}(-a)$.

$$\begin{array}{cc|cc} a & b & 1 & 0 \\ c & d & 0 & 1 \\ \hline 0 & b - \frac{ad}{c} & \frac{a}{c} & \frac{1}{c} \end{array}$$

we divide $b - \frac{ad}{c}$ if $c \neq 0$.

When does such a system have a non-trivial solution? There is a non-trivial solution iff $ad - bc \neq 0$.

$ad - bc \neq 0$ iff $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ is invertible.

Leibniz was not the first discovering it. The result was found before 1685 by Seki Takahazu.

2 Determinants

2.1 Definition

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

is called *determinant of matrix* $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$.

2.2 Properties

- The determinant is linear in every row and every column. For fixed b, d , it is

$$\begin{pmatrix} x \\ y \end{pmatrix} \mapsto \det \begin{pmatrix} x & b \\ y & d \end{pmatrix} = dx - by \quad \text{is linear}$$

$$\mathbb{K}^2 \rightarrow \mathbb{K}$$

$$\begin{aligned} \det \begin{pmatrix} \lambda x + \mu x' & b \\ \lambda y + \mu y' & d \end{pmatrix} &= d(\lambda x + \mu x') - b(\lambda y + \mu y') \\ &= \lambda(dx - by) + \mu(dx' - by') \\ &= \lambda \det \begin{pmatrix} x & b \\ y & d \end{pmatrix} + \mu \det \begin{pmatrix} x' & b \\ y' & d \end{pmatrix} \end{aligned}$$

The determinant is bilinear in rows and columns.

$$\det(\lambda v + \mu v', w) = \lambda \det(v, w) + \mu \det(v', w)$$

$$\text{Let } v = \begin{pmatrix} a \\ c \end{pmatrix}.$$

$$\det(v, \lambda w + \mu w') = \lambda \det(v, w) + \mu \det(v, w')$$

$$\text{Let } w = \begin{pmatrix} b \\ d \end{pmatrix}. \text{ Follows analogously.}$$

- If two rows are the same, then $\det(M) = 0$.

$$\det \begin{pmatrix} a & b \\ c & d \end{pmatrix} = ab - ba = 0$$

$$\det \begin{pmatrix} a & a \\ c & c \end{pmatrix} = ac - ca = 0$$

- The determinant of the unit matrix is one.

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

Theorem 2.1. *The properties 1–3 characterize the determinant. If $\varphi : \mathbb{K}^2 \times \mathbb{K}^2 \rightarrow \mathbb{K}$.*

bilinear¹

$$\varphi(\lambda v + \mu v', w) = \lambda \varphi(v, w) + \mu \varphi(v', w)$$

$$\forall v, w, v', w' : \mu(v, \lambda w + \mu w') = \lambda \varphi(v, w) + \mu \varphi(v, w')$$

$$\forall v : \varphi(v, v) = 0$$

$$\implies \varphi = \det$$

$$\varphi(e_1, e_2) = 1$$

Proof.

$$v = \begin{pmatrix} a \\ c \end{pmatrix} = a \cdot e_1 + c \cdot e_2$$

$$w = \begin{pmatrix} d \\ b \end{pmatrix} = b \cdot e_1 + d \cdot e_2$$

$$\begin{aligned} \varphi(v, w) &= \varphi(a \cdot e_1 + c \cdot e_2, b \cdot e_1 + d \cdot e_2) \\ &= a \cdot \varphi(e_1, b \cdot e_1 + d \cdot e_2) + c \cdot \varphi(e_2, b \cdot e_1 + d \cdot e_2) \\ &= ab \cdot \underbrace{\varphi(e_1, e_1)}_{=0} + ad \cdot \varphi(e_1, e_2) + cb \cdot \varphi(e_2, e_1) + cd \cdot \underbrace{\varphi(e_2, e_2)}_{=0} \end{aligned}$$

Is zero, because of property 3.

$$= ad \cdot \underbrace{\varphi(e_1, e_2)}_{=1} + cb \cdot \varphi(e_2, e_1)$$

$$\begin{aligned} 0 = \varphi(e_1 + e_2, e_1 + e_2) &= \underbrace{\varphi(e_1, e_1)}_{=0} + \underbrace{\varphi(e_1, e_2)}_{=1} + \varphi(e_2, e_1) + \underbrace{\varphi(e_2, e_2)}_{=0} \\ &\implies \varphi(e_2, e_2) = -1 \end{aligned}$$

□

Corollary.

$$\varphi(v, w) = -\varphi(w, v) \forall v, w$$

Corollary (Geometrical interpretation).

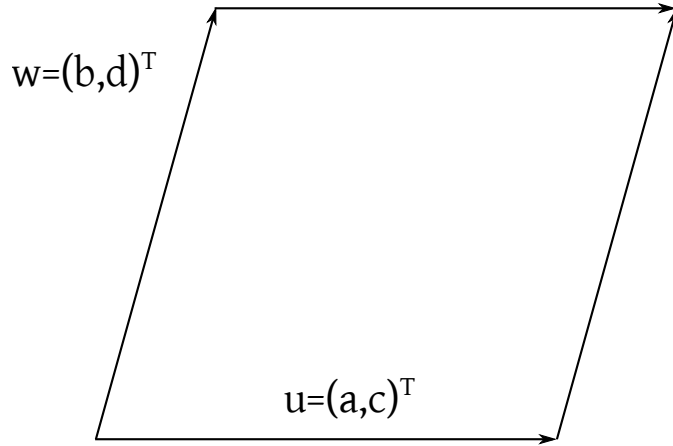


Figure 1: Geometric interpretation of determinants

See Figure 1. The determinant $\det(v, w)$ is the area of the spanned parallelogram. We denote F as the function returning the area of a geometric object.

Proof. $\text{area}(v, w)$ satisfies properties (i) – (iii).

Consider orthogonal e_1 and e_2 . $F = 1 = \det(e_1, e_2)$. $\det(e_2, e_1) = -1$.

The sign indicates the orientation of the area. □

By property 2, if $v = w$, then $F = 0$. By property 1,

1. If v and w are *linear dependent*², then

$$\lambda v + \mu w = 0 \quad (\lambda, \mu) \neq (0, 0)$$

Without loss of generality, $\mu \neq 0 \implies w = -\frac{\lambda}{\mu} \cdot v$.

2. To show:

$$F(\lambda v, w) = \lambda \cdot F(v, w)$$

²Hence, one vector is a multiple of the other

$$F(v + v', w) = F(v, w) + F(v', w)$$

Let $\lambda \in \mathbb{N}$. We multiply the area n times.

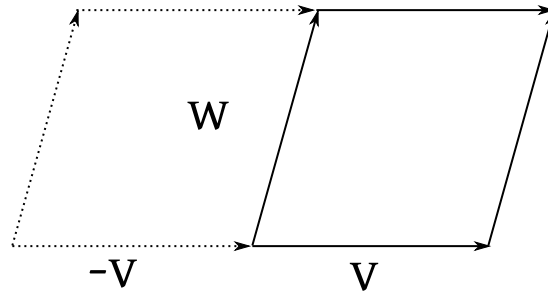
$$F(n \cdot v, w) = n \cdot F(v, w)$$

3.

$$F\left(\frac{1}{n} \cdot v, w\right) = \frac{1}{n} F(v, w)$$

follows from $F(\lambda v, w) = \lambda \cdot F(v, w)$, because $v = n \cdot \left(\frac{1}{n}v\right)$:

$$F\left(n\left(\frac{1}{n}v\right), w\right) = n \cdot F\left(\frac{1}{n}v, w\right)$$



4.

Figure 2: The sign changes if the orientation changes

If we combine (2) and (3),

$$F\left(\frac{m}{n}v, w\right) = \frac{m}{n} F(v, w)$$

See Figure 2.

5. By continuity, $F(\lambda v, w) = \lambda F(v, w) \forall \lambda \in \mathbb{R}_+^3$. If the orientation changes, the sign changes. By this property, this actually holds for \mathbb{R} , not only \mathbb{R}_+ .

Analogously:

$$F(v, \lambda w) = \lambda F(v, w) \forall \lambda \in \mathbb{R} \forall v, w \in \mathbb{R}^2$$

6. To show: $F(v + v', w) = F(v, w) + F(v', w)$

If v and w are linear independent, then $F(v + w, w) = F(v, w)$. In general, for a parallelogram of height h and vector w , it holds that

$$F = |w| \cdot h$$

³By the way, how are real numbers defined?

The height of the parallelogram stays the same.

$$F(v, w) = F(v + w, w)$$

7.

$$F(\lambda v + \mu w, w) = \lambda F(v, w)$$

Case $\mu = 0$ Already shown, $F(\lambda v, w) = \lambda F(v, w) \forall \lambda \in \mathbb{R}$.

Case $\mu \neq 0$ $F(\lambda v + \mu w, w) = \frac{1}{\mu} F(\lambda v + \mu w, \mu w) = \frac{1}{\mu} F(\lambda v, \mu w) = F(\lambda v, w) = \lambda F(v, w)$

8. Let v and w be linear independent, then they define a basis of \mathbb{R}^2 .

$$v_1 = \lambda_1 v + \mu_1 w$$

$$v_2 = \lambda_2 v + \mu_2 w$$

$$\begin{aligned} \rightarrow F(v_1 + v_2, w) &= F(\lambda_1 v + \mu_1 w + \lambda_2 v + \mu_2 w, w) \\ &= F((\lambda_1 + \lambda_2)v + (\mu_1 + \mu_2)w, w) \\ &= F((\lambda_1 + \lambda_2)v, w) \\ &= (\lambda_1 + \lambda_2)F(v, w) \\ &= \lambda_1 F(v, w) + \lambda_2 F(v, w) \\ &= F(\lambda_1 v, w) + F(\lambda_2 v, w) \\ &= F(\lambda_1 v + \mu_1 w, w) + F(\lambda_2 v + \mu_2 w, w) \\ &= F(v_1, w) + F(v_2, w) \end{aligned}$$

This shows that additivity is given.

2.3 Determinant form

Definition 2.1. Let V be an n -dimensional vector space over \mathbb{K} . A determinant form is a map

$$\Delta : V^n \rightarrow \mathbb{K}$$

$$(a_1, \dots, a_n) \mapsto \Delta(a_1, \dots, a_n)$$

Let $n = 2$.

$$\Delta : \left(\begin{pmatrix} a \\ c \end{pmatrix}, \begin{pmatrix} b \\ d \end{pmatrix} \right) \mapsto \begin{vmatrix} a & b \\ c & d \end{vmatrix} = ad - bc$$

It satisfies the properties of *multilinearity*:

1. $\Delta(a_1, \dots, \lambda a_k, \dots, a_n) = \lambda \Delta(a_1, \dots, a_n)$
2. $\Delta(a_1, \dots, a_k + v, \dots, a_n) = \Delta(a_1, \dots, a_k, \dots, a_n) + \Delta(a_1, \dots, a_{k-1}, v, a_{k+1}, \dots, a_n)$

Multilinearity is given, if linearity is given in every component. Hence, if $a_1, \dots, a_{k-1}, a_{k+1}, \dots, a_n$ are fixed, then

$$V \rightarrow \mathbb{K}$$

$$v \mapsto \Delta(a_1, \dots, a_{k-1}, v, a_{k+1}, \dots, a_n) \text{ linear}$$

Furthermore, it satisfies the following property:

$$\Delta(a_1, \dots, a_n) = 0$$

if $\exists k \neq l : a_k = a_l$. If $\Delta \neq 0$, then Δ is called *non-trivial*.

Corollary.

$$\Delta(a_1, \dots, a_k + \lambda a_i, \dots, a_n) = \Delta(a_1, \dots, a_k, \dots, a_n) \forall \lambda \in \mathbb{K}, \forall i \neq k$$

$$\Delta(a_1, \dots, a_i, \dots, a_j, \dots, a_n) = -\Delta(a_1, \dots, a_j, \dots, a_i, \dots, a_n)$$

Proof.

$$\begin{aligned} \Delta(a_1, \dots, a_k + \lambda a_i, \dots, a_n) &= \Delta(a_1, \dots, a_k, \dots, a_n) + \Delta(a_1, \dots, a_{k-1}, \lambda a_i, a_{k+1}, \dots, a_n) \\ &= \Delta(a_1, \dots, a_n) + \lambda \Delta(a_1, \dots, a_{k-1}, a_i, a_{k+1}, \dots, a_n) \\ &= 0 \quad \text{because } a_i \text{ occurs twice} \end{aligned}$$

□

$$\begin{aligned} 0 &= \Delta(a_1, \dots, a_i + a_j, \dots, a_i + a_j, \dots, a_n) \\ &= \Delta(a_1, \dots, a_i, \dots, a_i, \dots, a_n) \\ &\quad + \Delta(a_1, \dots, a_i, \dots, a_j, \dots, a_n) \\ &\quad + \Delta(a_1, \dots, a_j, \dots, a_i, \dots, a_n) \\ &\quad + \Delta(a_1, \dots, a_j, \dots, a_j, \dots, a_n) \end{aligned}$$

The first and last term are zero. Multilinearity is given:

$$\lambda(a_1, \dots, \lambda a_k, \dots, a_n) = \lambda \Delta(a_1, \dots, a_n)$$

$$\lambda(a_1, \dots, \lambda a_k + v, \dots, a_n) = \lambda \Delta(a_1, \dots, a_n) + \Delta(a_1, \dots, a_{k-1}, v, a_{k+1}, \dots, a_n)$$

This lecture took place on 2018/03/07.

Determinant form: $\dim V = n$

$$\Delta : V^n \rightarrow \mathbb{K}$$

1. $\Delta(a_1, \dots, a_{k-1}, \lambda a_k, a_{k+1}, \dots, a_n) = \lambda \Delta(a_1, \dots, a_n)$
2. $\Delta(a_1, \dots, a_{k-1}, a_k + v, a_{k+1}, \dots, a_n) = \Delta(a_1, \dots, a_k, \dots, a_n) + \Delta(a_1, \dots, v, \dots, a_n)$
3. $\Delta(a_1, \dots, a_n) = 0$ if $\exists i \neq j : a_i = a_j$

Multilinearity is given by the first two properties.

$\Delta \neq 0$

Then the fourth property follows:

4. $\Delta(a_1, \dots, a_k + \lambda a_i, \dots, a_n) = \Delta(a_1, \dots, a_n) \forall i \neq k \forall \lambda \in \mathbb{K}$
1. $\Delta(a_1, \dots, a_i, \dots, a_j, \dots, a_n) = -\Delta(a_1, \dots, a_j, \dots, a_i, \dots, a_n)$

Example 2.1. Let $n = 2$, $V = \mathbb{K}^2$.

$$\Delta\left(\begin{pmatrix} a \\ c \end{pmatrix}, \begin{pmatrix} b \\ d \end{pmatrix}\right) = ad - bc = \det\begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

2.4 Permutations and transpositions

Definition 2.2. A permutation is a bijective map $\sigma : \{1, \dots, n\} \rightarrow \{1, \dots, n\}$. σ_n is the set of all permutations.

$$|\sigma_n| = n!$$

Remark 2.1. σ_n in regards of composition defines a group with neutral element id and is called symmetric group.

Remark 2.2. For $n \geq 3$, it is non-commutative.

Example 2.2. Permutations:

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

So, e.g. 2 is mapped to 3 (right side of \circ) and 3 is mapped to 3 (left side of \circ). Hence 2 is mapped to 3 (right-hand side of $=$).

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 3 & 2 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix}$$

Definition 2.3. A transposition is a permutation exchanging exactly 2 elements.

$$\tau_{ij} : \begin{cases} i \mapsto j \\ j \mapsto i \\ k \mapsto k \forall k \notin \{i, j\} \end{cases}$$

$$\tau_{ij}^{-1} = \tau_{ij}$$

Remark 2.3. Every permutation $\sigma \in \sigma_n$ with $\sigma \neq \text{id}$ can be denoted as product of transpositions.

Proof.

$$\sigma = \begin{pmatrix} 1 & 2 & \dots & n \\ \sigma(1) & \sigma(2) & \dots & \sigma(n) \end{pmatrix}$$

Example:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 3 & 5 & 4 & 7 & 6 & 2 \end{pmatrix}$$

□

Find transpositions τ_1, \dots, τ_k such that $\sigma = \tau_1 \circ \tau_2 \circ \dots \circ \tau_k$.

If $\sigma = \text{id}$, then $k = 0$.

If $\sigma \neq \text{id}$,

$$k_1 = \min \{i \mid \sigma(i) \neq i\} \neq \emptyset$$

$$\tau_1 = \tau_{k_1 \sigma(k_1)}$$

$$\sigma_1 = \tau_1 \circ \sigma$$

if $\sigma_i = \text{id}$, then $\tau_1 \circ \sigma = \text{id}$. Then $\sigma = \tau_1^{-1} = \tau_1$.

$$k_2 = \min \{i \mid \sigma_1(i) \neq i\}$$

$$\tau_2 = \tau_{k_2 \sigma_1(k_2)}$$

$$\sigma_2 = \tau_2 \circ \sigma_1$$

Example 2.3. Let $k_1 = 2$.

$$\tau_1 = \tau_{23}$$

$$\begin{aligned} \sigma_1 &= \tau_{23} \circ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 3 & 5 & 4 & 7 & 6 & 2 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 2 & 5 & 4 & 7 & 6 & 3 \end{pmatrix} \end{aligned}$$

$k_2 = 3$.

$$\tau_2 = \tau_{35}$$

$$\sigma_2 = \tau_2 \circ \sigma_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 2 & 3 & 4 & 7 & 6 & 5 \end{pmatrix}$$

$k_3 = 5$.

$$T_3 = T_{57}$$

$$\sigma_3 = \tau_3 \circ \sigma_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 \end{pmatrix} \\ = \text{id}$$

$$\tau_3 \circ \tau_2 \circ \tau_1 \circ \sigma = \text{id} \\ \implies \tau_2 \circ \tau_1 \circ \sigma = T_3^{-1} \circ \text{id} = \tau_3 \\ \tau_1 \circ \sigma = \tau_2^{-1} \circ T_3 = \tau_2 \circ \tau_3 \\ \sigma = \tau_1 \circ \tau_2 \circ \tau_3$$

and so on and so forth.

$$\tau_k \\ \sigma_k = \tau_k \circ \tau_{k-1} \circ \dots \circ \tau_i \circ \sigma = \text{id} \\ \implies \sigma = \tau_1 \circ \tau_2 \circ \dots \circ \tau_k$$

Remark 2.4. This decomposition is not unique.

Definition 2.4. Let $\pi \in \sigma_n$ be a permutation. A malposition of π is a pair (i, j) such that $i < j$ and $\pi(i) > \pi(j)$.

$$f_\pi := \left| \left\{ (i, j) \mid (i, j) \text{ is malposition of } \pi \right\} \right|$$

$$\text{sign}(\pi) := (-1)^{f_\pi} =: (-1)^\pi$$

is called signature of π

Example 2.4.

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 3 & 5 & 4 & 7 & 6 & 2 \end{pmatrix}$$

Malpositions:

$$\{(2, 7), (3, 4), (3, 7), (5, 6), (5, 7), (4, 7), (6, 7)\}$$

$$2 < 7$$

$$\pi(2) - 3 > 2 = \pi(7)$$

$$f_\pi = 7$$

Theorem 2.2.

$$\text{sign}(\pi) = \prod_{\substack{i, j \\ i < j}} \frac{\pi(j) - \pi(i)}{j - i}$$

- $\binom{n}{2}$ factors
- for transposition, $\text{sign } \tau = -1$.

Proof.

$$\prod_{i < j} \frac{\pi(j) - \pi(i)}{j - i} = \frac{\prod_{i < j} (\pi(j) - \pi(i))}{\prod_{i < j} (j - i)}$$

π is bijective in $\{1, \dots, n\}$ Hence, every difference $j - i$ occurs exactly one time in the numerator and the denominator with sign ± 1 depending on whether (i, j) is a malposition or not.

$$\text{sign}(\pi(j) - \pi(i)) = \begin{cases} +1 & \pi(j) > \pi(i) \\ -1 & \pi(j) < \pi(i) \text{ hence malposition} \end{cases}$$

□

Example 2.5.

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 3 & 5 & 4 & 7 & 6 & 2 \end{pmatrix}$$

Malposition:

$$\{(2, 7), (3, 4), (3, 7), (5, 6), (5, 7), (4, 7), (6, 7)\}$$

$$2 < 7$$

$$\pi(2) - 3 > 2 = \pi(7)$$

$$f_\pi = 7$$

$$\frac{\prod_{i < j} (\pi(j) - \pi(i))}{\prod_{i < j} (j - i)} = \frac{\prod_{i < j} (j - i) \cdot (-1)^{f_\pi}}{\prod_{i < j} (j - i)} = \text{sign } \pi$$

$$\pi = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

$$\begin{aligned} \prod_{i < j} \frac{\pi(j) - \pi(i)}{j - i} &= \frac{\pi(2) - \pi(1)}{2 - 1} \cdot \frac{\pi(3) - \pi(1)}{3 - 1} \cdot \frac{\pi(3) - \pi(2)}{3 - 2} \\ &= \frac{(2 - 3) \cdot (1 - 3) \cdot (1 - 2)}{(2 - 1)(3 - 1)(3 - 2)} \\ &= (-1)^3 = -1 \end{aligned}$$

Malpositions:

1. (1, 2)
2. (1, 3)
3. (2, 3)

Transposition: Let $k < \tau(k)$.

$$\tau = \begin{pmatrix} 1 & 2 & \dots & k-1 & k & k+1 & \dots & \tau(k) & \tau(k+1) & \dots & n \\ 1 & 2 & \dots & k-1 & \tau(k) & k+1 & \dots & k & \tau(k+1) & \dots & n \end{pmatrix}$$

Malpositions (denoted F_τ):

$$F_\tau = \begin{cases} (k, k+1), \dots, (k, \tau(k)) \\ (k+1, \tau(k)), (k+2, \tau(k)), \dots, (\tau(k)-1, \tau(k)) \end{cases}$$

Let us count on a specific example:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 2 & 6 & 4 & 5 & 3 & 7 \end{pmatrix}$$

$$\begin{cases} (3, 4), (3, 5), (3, 6) \\ (4, 6), (5, 6) \end{cases}$$

$$|F_\tau| = (\tau(k) - k) + ((\tau(k) - 1) - k) = 2\tau(k) - 2k - 1 = 2(\tau(k) - k) - 1 \text{ even}$$

Theorem 2.3. 1. $\text{sign}(\text{id}) = 1$

2. $\text{sign}(\pi \circ \sigma) = \text{sign}(\pi) \circ \text{sign}(\sigma)$
Hence, $\text{sign} \sigma_n \rightarrow \{\pm 1\}$ is a homomorphism.
 $(\{+1, -1\}, \cdot)$ is a group $\cong (\mathbb{Z}_2, +)$

$$+1 \rightarrow [0]_2$$

$$-1 \rightarrow [1]_2$$

3. $\text{sign}(\pi^{-1}) = \text{sign}(\pi)$

Proof. 1. obvious, because there are no malpositions

2.

$$\text{sign}(\pi \circ \sigma) = \prod_{i < j} \frac{(\pi \circ \sigma(j) - \pi \circ \sigma(i))}{j - i} \prod_{i < j} \frac{\sigma(j) - \sigma(i)}{\sigma(j) - \sigma(i)}$$

because of bijectivity

$$= \underbrace{\prod_{i < j} \frac{\pi(\sigma(j)) - \pi(\sigma(i))}{\sigma(j) - \sigma(i)}}_{\text{sign } \pi} \cdot \underbrace{\prod_{i < j} \frac{\sigma(j) - \sigma(i)}{j - i}}_{\text{sign } \pi}$$

3. Homomorphism

$$\text{sign}(\pi^{-1}) = \text{sign}(\pi)^{-1} = \text{sign}(\pi)$$

□

Remark 2.5. Recall that the kernel of a homomorphism defines a subgroup.

Corollary. 1. If $\pi = \tau_1 \circ \dots \circ \tau_k$ is a product of transpositions, then $\text{sign}(\pi) = (-1)^k$

2. $\mathfrak{a}_n = \{\pi \in \sigma_n \mid \text{sign}(\pi) = +1\} = \ker(\text{sign} : \sigma_n \rightarrow \{\pm 1\})$ is a subgroup of σ_n , the so-called alternating group

$$|\mathfrak{a}_n| = \frac{n!}{2}$$

Corollary.

$$\dim V = n$$

$$\Delta : V^n \rightarrow \mathbb{K} \quad \text{determinant form}$$

then it holds that $\forall \sigma \in \sigma_n : \Delta(a_{\sigma(1)}, \dots, a_{\sigma(n)}) = \text{sign}(\sigma) \cdot \Delta(a_1, \dots, a_n)$

Proof. If $\sigma = \tau$ is a transposition, the fourth property:

$$\Delta(a_{\tau(1)}, \dots, a_{\tau(n)}) = -\Delta(a_1, \dots, a_n)$$

and $\text{sign}(\tau) = -1$.

The general case: $\sigma = \tau_1 \circ \dots \circ \tau_k$ and $\sigma = \tau_1 \circ \sigma_1$.

$$\begin{aligned} \Delta(a_{\sigma(1)}, \dots, a_{\sigma(n)}) &= \Delta(a_{\tau_1(\sigma_1(1))}, \dots, a_{\tau_1(\sigma_1(n))}) \\ &= -\Delta(a_{\sigma_1(1)}, \dots, a_{\sigma_1(n)}) \end{aligned}$$

$$\sigma_1 = \tau_2 \circ \sigma_2$$

= and so on and so forth

$$= (-1)^2 \Delta(a_{\sigma_2(1)}, \dots, a_{\sigma_2(n)})$$

$$= (-1)^k \Delta(a_1, \dots, a_n)$$

$$= \text{sign } \sigma \Delta(a_1, \dots, a_n)$$

□

2.5 Leibniz formula for determinants

Definition 2.5. Let $\dim V = n$. Let $B = (b_1, \dots, b_n)$ be a basis of V . $a_1, \dots, a_n \in V$ with coordinates

$$\psi_B(a_j) = \begin{pmatrix} a_{1j} \\ a_{2j} \\ \vdots \\ a_{nj} \end{pmatrix} \quad A := \begin{bmatrix} a_{11} & \dots & a_{1n} \\ \vdots & & \vdots \\ a_{n1} & \dots & a_{nn} \end{bmatrix}$$

Then $\Delta(a_1, \dots, a_n) = \det(A) \cdot \Delta(b_1, \dots, b_n)$ where

$$\det(A) := \sum_{\pi \in \sigma_n} \text{sign}(\pi) a_{1\pi(1)} a_{2\pi(2)} \dots a_{n\pi(n)}$$

is called determinant of A

This formula was discovered by Leibniz.

Example 2.6. Consider $n = 2$.

$$\begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix} = \underbrace{a_{11}a_{22}}_{\pi=\text{id}} - \underbrace{a_{12}a_{21}}_{\pi=\begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}}$$

Proof.

$$a_j = \sum_{i=1}^n a_{ij} b_i$$

$$\Delta(a_1, \dots, a_n) = \Delta \left(\sum_{i_1=1}^n a_{i_1,1} b_{i_1}, \sum_{i_2=1}^n a_{i_2,2} b_{i_2}, \dots, \sum_{i_n=1}^n a_{i_n,n} b_{i_n} \right)$$

because it is multilinear

$$= \sum_{i_1=1}^n \sum_{i_2=1}^n \dots \sum_{i_n=1}^n a_{i_1,1} a_{i_2,2} \dots a_{i_n,n} \cdot \Delta(b_{i_1}, b_{i_2}, \dots, b_{i_n})$$

where $\Delta = 0$ is two indices equate.

$$\implies i_1, \dots, i_n \text{ are all difference } \in \{1, \dots, n\}$$

$$\implies \text{every occurs exactly once}$$

$$i_1, \dots, i_n \text{ is permutation of } 1, \dots, n$$

$$\exists \sigma \in \sigma_n : i_1 = \sigma(1), \dots, i_n = \sigma(n)$$

$$\begin{aligned}
&= \sum_{\sigma \in \sigma_n} a_{\sigma(1)1} a_{\sigma(2)2} \dots a_{\sigma(n)n} \underbrace{\Delta(b_{\sigma(1)} \dots b_{\sigma(n)})}_{\text{sign } \sigma \Delta(b_1, \dots, b_n) \text{ because of Corollary 2.4}} \\
&= \sum_{\pi \in \sigma_n} a_{1\pi(1)} \dots a_{n\pi(n)} \cdot \text{sign}(\pi) \Delta(b_1, \dots, b_n)
\end{aligned}$$

□

Corollary. A determinant form is uniquely defined by the value $\Delta(b_1, \dots, b_n)$ on a basis.

Especially, $\Delta \neq 0 \iff \Delta(b_1, \dots, b_n) \neq 0$ [for any basis] $\iff \Delta(b_1, \dots, b_n) \neq 0$ [for every basis].

Assume $\Delta(b_1, \dots, b_n) = 0$ for any basis. Every other basis can be expressed by b_1, \dots, b_n and the formula gives $\Delta(a_1, \dots, a_n) = 0 \forall a_1, \dots, a_n$.

This lecture took place on 2018/03/12.

Theorem 2.4.

$$\Delta \text{ non-trivial} \iff \Delta(b_1, \dots, b_n) \neq 0 \text{ for every basis}$$

Theorem 2.5. Define determinant of matrix A .

$$\Delta(a_1, \dots, a_n) = \Delta(b_1, \dots, b_n) \cdot \det A$$

if $a_j = \sum_{i=1}^n a_{ij} b_i$. Hence

$$\begin{pmatrix} a_{1j} \\ a_{2j} \\ \vdots \\ a_{nj} \end{pmatrix} = \Phi_B(a_j)$$

Theorem 2.6. Inverse of Theorem 2.5. Given basis $B = (b_1, \dots, b_n)$.

$$\Delta(a_1, \dots, a_n) := \det[\Phi_B(a_1), \dots, \Phi_B(a_n)]$$

defines a non-trivial determinant form such that $\Delta(b_1, \dots, b_n) = 1$

Corollary. Let Δ be a non-trivial determinant form. Then v_1, \dots, v_n is linearly independent.

$$\iff \Delta(v_1, \dots, v_n) \neq 0$$

Direction \Rightarrow : Immediate, because v_1, \dots, v_n is a basis.

Direction \Leftarrow : Assume v_1, \dots, v_n is linearly independent. Without loss of generality, $v_n = \sum_{k=1}^{n-1} \lambda_k v_k$.

$$\begin{aligned}\Delta(v_1, \dots, v_n) &= \Delta(v_1, \dots, v_{n-1}, \sum_{k=1}^{n-1} \lambda_k v_k) \\ &= \sum_{k=1}^{n-1} \lambda_k \Delta(\underbrace{v_1, \dots, v_{n-1}, v_k}_{=0 \text{ because } v_k \text{ occurs twice}}) \\ &= 0\end{aligned}$$

Remark 2.6 (Summary). 1. The determinant form defines a 1-dimensional vector space.

2. There exists a non-trivial determinant form. Given a basis b_1, \dots, b_n

$$\Delta(b_1, \dots, b_n) = \mathbf{1}$$

By Theorem 2.6, $\Delta(a_1, \dots, a_n) = \det(\Phi_B(a_1), \dots, \Phi_B(a_n))$.

Proof of Theorem 2.6. 1.

$$\begin{aligned}\Delta(a_1, \dots, \lambda a_k, \dots, a_n) &= \sum_{\pi \in \sigma_n} (-1)^\pi a_{\pi(1)1} \lambda a_{\pi(k)k} a_{\pi(n)n} \\ &= \lambda \cdot \sum_{\pi \in \sigma_n} (-1)^\pi a_{\pi(1)1} \dots a_{\pi(n)n} \\ &= \lambda \cdot \Delta(a_1, \dots, a_n)\end{aligned}$$

2.

$$\begin{aligned}\Delta(a_1, \dots, a_k + v, \dots, a_n) &= \sum_{\pi \in \sigma_n} (-1)^\pi a_{\pi(1)1} \dots (a_{\pi(k)k} + v_{\pi(k)}) \cdot a_{\pi(n)n} \\ &= \sum_{\pi \in \sigma_n} (-1)^\pi a_{\pi(1)1} \dots a_{\pi(k)k} \dots a_{\pi(n)n} \\ &\quad + \sum_{\pi \in \sigma_n} (-1)^\pi a_{\pi(1)1} \dots v_{\pi(k)} \dots a_{\pi(n)n} \\ &= \Delta(a_1, \dots, a_k, \dots, a_n) + \Delta(a_1, \dots, v, \dots, a_n)\end{aligned}$$

This proves multilinearity.

3. Let $a_k = a_l, a_{ik} = a_{il} \forall i = 1, \dots, n$. Without loss of generality, $k < l$.

$$\begin{aligned}\Delta(a_1, \dots, a_k) &= \sum_{\pi \in \sigma_n} (-1)^\pi a_{\pi(1)1} \dots a_{\pi(k)k} \dots a_{\pi(l)l} \dots a_{\pi(n)n} \\ &\quad \tau \cdot \pi = (\text{reference } *)\end{aligned}$$

Let $\tau = \tau_{kl}$, exchange of k and l .

Claim.

$$\sigma_n = \underbrace{\mathcal{A}_n}_{\substack{\text{alternating group} \\ = \{ \pi \mid \text{sign}(\pi)=+1 \}}} \cup \underbrace{\mathcal{A}_n \cdot \tau}_{= \{ \pi \circ \tau \mid \pi \in \mathcal{A}_n \}}$$

Proof. Direction \Leftarrow . Let $\text{sign}(\pi) = -1$.

$$\Rightarrow \pi = (\pi \circ \tau) \circ \tau$$

$\underbrace{\quad}_{=\text{id}}$

$\sigma = \pi \circ \tau$ has $\text{sign}(\sigma) = \text{sign}(\pi \circ \tau) = \text{sign}(\pi) \cdot \text{sign}(\tau) = (-1) \cdot (-1) = 1$.

$$\sigma \in \mathcal{A}_n \text{ and } \pi = \sigma \circ \tau$$

$$\begin{aligned} \text{reference}^* &= \sum_{\pi \in \mathcal{A}_n} \underbrace{(-1)^\pi}_{=+1} a_{\pi(1)1} \dots a_{\pi(n)n} \\ &+ \sum_{\substack{\pi \in \mathcal{A}_n \tau \\ \pi = \sigma \circ \tau}} \underbrace{(-1)^{\text{sign}(\pi)}}_{=-1} a_{\pi(1)1} \dots a_{\pi(n)n} \\ &= \sum_{\pi \in \mathcal{A}_n} a_{\pi(1)1} \dots a_{\pi(n)n} - \sum_{\sigma \in \mathcal{A}_n} \underbrace{a_{\sigma \circ \tau(1)1} \dots a_{\sigma \circ \tau(k)2} \dots a_{\sigma \circ \tau(l)l} \dots a_{\sigma \circ \tau(n)n}}_{\substack{a_{\sigma(1)1} \dots \underbrace{a_{\sigma(l)k} \dots a_{\sigma(k)l}}_{=a_{\sigma(l)l}} \dots a_{\sigma(n)n} \\ =a_{\sigma(k)k}}} = 0 \end{aligned}$$

□

□

This previous part, beginning with the reference from 2018/03/12, was actually added on 2018/03/14, because we skipped it by accident.

$$\Delta(a_1, \dots, a_n)$$

Determinant form \Longleftrightarrow

multilinear $\Delta(a_1, \dots, \lambda a_k + \mu a'_k, \dots, a_n) = \lambda \Delta(a_1, \dots, a_k, \dots, a_n) + \mu \Delta(a_1, \dots, a'_k, \dots, a_n)$

anti-symmetrical $\Delta(a_1, \dots, a_k, \dots, a_l, \dots, a_n) = -\Delta(a_1, \dots, a_l, \dots, a_k, \dots, a_n)$

$$\Delta(a_{\pi(1)}, \dots, a_{\pi(n)}) = (-1)^\pi \Delta(a_1, \dots, a_n)$$

where $(-1)^\pi := \text{sign}(\pi) = (-1)^{F(\pi)}$

$$F(\pi) = \left\{ (i, j) \mid i < j \wedge \pi(i) > \pi(j) \right\}$$

$$\text{sign}(\pi \circ \sigma) = \text{sign}(\pi) \cdot \text{sign}(\sigma)$$

Basis b_1, \dots, b_n .

$$\Delta\left(\sum_{i=1}^n a_{i1}b_i, \dots, \sum_{i=1}^n a_{in}b_i\right) = \det A \cdot \Delta(b_1, \dots, b_n)$$

$$\det(A) = \sum_{\pi \in \sigma_n} (-1)^\pi a_{1\pi(1)} \dots a_{n\pi(n)} = \sum_{\pi \in \sigma_n} (-1)^\pi a_{\pi(1)1} \dots a_{\pi(n)n}$$

Lemma 2.1. Let V, W be vector spaces over \mathbb{K} with $\dim V = \dim W = n$. Let $\Delta : W^n \rightarrow \mathbb{K}$ be a determinant form and $f : V \rightarrow W$ linear.

$$V \xrightarrow{f} W$$

$$V^n \xrightarrow{f^{(n)}} W^n \xrightarrow{\Delta} \mathbb{K}$$

$$(v_1, \dots, v_n) \mapsto (f(v_1), \dots, f(v_n))$$

$$\implies \Delta^f : V^n \rightarrow \mathbb{K}$$

$$\Delta^f(v_1, \dots, v_n) = \Delta(f(v_1), \dots, f(v_n))$$

is a determinant form on V .

Proof. 1. Multilinear

$$\begin{aligned} & \Delta^f(v_1, \dots, \lambda v_k + \mu v'_k, \dots, v_n) \\ &= \Delta(f(v_1), \dots, f(\lambda v_k + \mu v'_k), \dots, f(v_n)) \\ &= \Delta(f(v_1), \dots, \lambda f(v_k) + \mu f(v'_k), \dots, f(v_n)) \\ &= \lambda \Delta(f(v_1), \dots, f(v_k), \dots, f(v_n)) + \mu \Delta(f(v_1), \dots, f(v'_k), \dots, f(v_n)) \\ &= \lambda \Delta^f(v_1, \dots, v_k, \dots, v_n) + \mu \Delta^f(v_1, \dots, v'_k, \dots, v_n) \end{aligned}$$

□

Corollary. Let $V = W$, $\Delta : V^n \rightarrow \mathbb{K}$ determinant form.

$$f : V \rightarrow V \text{ linear}$$

$$\implies \Delta^f \text{ is determinant form}$$

Because there is (except for one factor) only one determinant form:

$$\exists C_f \in \mathbb{K} : \Delta^f(v_1, \dots, v_n) = C_f \cdot \Delta(v_1, \dots, v_n) \forall v_1, \dots, v_n \in V$$

$$\det(f) := C_f \text{ is called determinant on } f$$

Proof. Let Δ_1, Δ_2 be two determinant forms.

$$\Delta_1(v_1, \dots, v_n) = \det A \cdot \Delta_1(b_1, \dots, b_n)$$

$$\Delta_2(v_1, \dots, v_n) = \det A \cdot \Delta_2(b_1, \dots, b_n)$$

if b_1, \dots, b_n is basis and

$$v_j = \sum_{i=1}^n a_{ij} b_i$$

$$\implies \Delta_2(v_1, \dots, v_n) = \frac{\Delta_2(b_1, \dots, b_n)}{\Delta_1(b_1, \dots, b_n)} \cdot \Delta_1(v_1, \dots, v_n)$$

$$\implies C_f = \frac{\Delta^f(b_1, \dots, b_n)}{\Delta(b_1, \dots, b_n)} = \det(f)$$

□

2.6 On determinants, invertibility and linear independence

Corollary. $B = (b_1, \dots, b_n)$ is basis of V . $\phi_B^B(f)$ is matrix representation of f and $\det(f) = \det \phi_B^B(f)$ (LHS by Corollary 2.5, RHS by Definition 2.5 $\sum_{\pi} (-1)^{\pi} \dots$)

Proof.

$$\det(f) = \frac{\Delta(f(b_1), \dots, \Delta(f(b_n)))}{\Delta(b_1, \dots, b_n)}$$

$$\begin{aligned} f(b_j) &= \sum_{i=1}^n \phi_B(f(b_i))_i \cdot b_i \\ &= \sum_{i=1}^n (\phi_B^B(f))_{ij} b_i \end{aligned}$$

with $\phi_B^B(f)_{ij} = \phi_B(f(b_j))_i$.

$$\det f = \frac{\det \phi_B^B(f) \cdot \Delta(b_1, \dots, b_n)}{\Delta(b_1, \dots, b_n)}$$

□

Theorem 2.7. $f : V \rightarrow V$ is invertible $\iff \det(f) \neq 0$.

Proof. Let Δ be a non-trivial determinant form.

$$B = (b_1, \dots, b_n) \text{ is a basis } \implies \Delta(b_1, \dots, b_n) \neq 0$$

$$\det(f) = \frac{\Delta(f(b_1), \dots, f(b_n))}{\Delta(b_1, \dots, b_n)}$$

$(f(b_1), \dots, f(b_n))$ is basis $\iff f$ is invertible.

If f is invertible, then $(f(b_1), \dots, f(b_n))$ is basis.

$$\implies \Delta(f(b_1), \dots, f(b_n)) \neq 0 \implies \det(f) \neq 0$$

If f is not invertible, then

$$\implies f(b_1) \dots f(b_n) \text{ is linear dependent}$$

$$\exists k : f(b_k) = \sum_{i \neq k} \lambda_i f(b_i)$$

Without loss of generality: $k = n$

$$\begin{aligned} \Delta(f(b_1), \dots, f(b_n)) &= \Delta(f(b_1), \dots, f(b_{n-1}), \sum_{i=1}^{n-1} \lambda_i f(b_i)) \\ &= \sum_{i=1}^n \lambda_i \underbrace{\Delta(f(b_1), \dots, f(b_{n-1}), f(b_i))}_{=0 \forall i \in \{1, \dots, n-1\}} \\ &= 0 \end{aligned}$$

□

Corollary. For a matrix $A \in \mathbb{K}^{n \times n}$ it holds that $\det A \neq 0 \iff A$ has full rank.

Theorem 2.8. $f, g : V \rightarrow V$ linear.

$$\implies \det(f \circ g) = \det(f) \cdot \det(g)$$

for a matrix: $\det(A \cdot B) = \det(A) \cdot \det(B)$

Proof. Case 1: f and g are invertible.

$$\det(f) = \frac{\Delta(f(b_1), \dots, f(b_n))}{\Delta(b_1, \dots, b_n)}$$

for arbitrary bases (b_1, \dots, b_n) of V .

$$\begin{aligned} \det(f \circ g) &= \frac{\Delta(f(g(b_1)), \dots, f(g(b_n)))}{\Delta(b_1, \dots, b_n)} \cdot \frac{\Delta(g(b_1), \dots, g(b_n))}{\Delta(g(b_1), \dots, g(b_n))} \\ &= \underbrace{\frac{\Delta(f(g(b_1)), \dots, f(g(b_n)))}{\Delta(g(b_1), \dots, g(b_n))}}_{0 \neq \det(f)} \cdot \underbrace{\frac{\Delta(g(b_1), \dots, g(b_n))}{\Delta(b_1, \dots, b_n)}}_{\det(g) \neq 0} \end{aligned}$$

g invertible

$$\implies g(b_1), \dots, g(b_n) \text{ is basis}$$

□

Claim. $f \circ g$ invertible $\iff f$ invertible and g invertible.

$f \circ g$ invertible $\implies f \circ g$ surjective $\implies f$ surjective $\implies (\dim V < \infty)$ f is bijective.

$f \circ g$ invertible $\implies f \circ g$ injective $\implies g$ injective $\implies g$ bijective.

Case 2: $\neg(f \text{ bijective} \wedge g \text{ bijective}) \implies f \circ g$ not bijective

f is not bijective or g is not bijective.

$$\det(f) = 0 \vee \det(g) = 0 \iff \det(f) \circ \det(g) = 0 = \det(f \circ g)$$

Corollary. For $A, B \in \mathbb{K}^{n \times n}$ it holds that

1. $\det(A \cdot B) = \det(A) \cdot \det(B)$
2. $\det(A^{-1}) = \frac{1}{\det(A)}$ if invertible
3. $\det(A) = 0 \iff \text{rank}(A) < n$
4. $\det(A^t) = \det(A)$

Proof of Corollary 2.6. 1. $\det(A \cdot B) = \det(f_A \circ f_B) = \det(f_A) \cdot \det(f_B) = \det(A) \cdot \det(B)$

2. $A \cdot A^{-1} = I$ and $1 = \det(A \cdot A^{-1}) = \det(A) \cdot \det(A^{-1})$

Remark 2.7 (From the practicals).

$$\det(A) = \det(f_A)$$

Shown so far:

$$\det f = \det(\phi_B^B(f))$$

$$A = \phi_B^B(f_A)$$

for $B = (e_1, \dots, e_n)$

□

Direct proof of Corollary 2.6 (1).

$$A = \begin{bmatrix} s_1 & \dots & s_n \\ \vdots & & \vdots \end{bmatrix}$$

s_i are column vectors of A . Let Δ be the uniquely defined determinant form by $\Delta(e_1, \dots, e_n) = 1$.

$$A \cdot B = \begin{bmatrix} s_1 & \dots & s_n \\ \vdots & & \vdots \end{bmatrix} \cdot \begin{bmatrix} b_{11} & b_{12} & \dots & b_{1n} \\ \vdots & & & \vdots \\ b_{n1} & & & b_{nn} \end{bmatrix}$$

$$\begin{aligned}
&= \begin{bmatrix} s_1 b_{11} + s_2 b_{21} + \dots + s_n b_{n1} & s_1 b_{12} + s_2 b_{22} + \dots + s_n b_{n2} & \dots & s_1 b_{1n} + s_2 b_{2n} + \dots + s_n b_{nn} \\ \vdots & \vdots & & \vdots \end{bmatrix} \\
\det(A \cdot B) &= \frac{\Delta(s_1(A \cdot B), \dots, s_n(A \cdot B))}{\Delta(e_1, \dots, e_n)} = \Delta\left(\sum_{i_1=1}^n s_{i_1} b_{i_1 1}, \sum_{i_2=1}^n s_{i_2} b_{i_2 2}, \dots, \sum_{i_n=1}^n s_{i_n} b_{i_n n}\right) \\
&= \sum_{i_1=1}^n \dots \sum_{i_n=1}^n b_{i_1 1} b_{i_2 2} \dots b_{i_n n} \underbrace{\Delta(s_{i_1}, \dots, s_{i_n})}_{=0}
\end{aligned}$$

if one index occurs twice. It suffices to consider \sum_{i_1, \dots, i_n} such that all ij are difference. If all are difference, then all occur exactly once. Hence, i_1, \dots, i_n is permutation of $1, \dots, n$.

$$\begin{aligned}
&= \sum_{\pi \in \sigma_n} b_{\pi(1)1} \dots b_{\pi(n)n} \Delta(s_{\pi(1)} \dots s_{\pi(n)}) \\
&= \sum_{\pi \in \sigma_n} \underbrace{(-1)^\pi b_{\pi(1)1} \dots b_{\pi(n)n}}_{\det B} \underbrace{\Delta(s_1, \dots, s_n)}_{=\det(A)} = \det(B) \cdot \det(A)
\end{aligned}$$

□

Proof of Corollary 2.6 (4).

$$\begin{aligned}
\det(A^t) &= \sum_{\pi \in \sigma_n} (-1)^\pi (A^t)_{\pi(1)1} \dots (A^t)_{\pi(n)n} \\
&= \sum_{\pi \in \sigma_n} (-1)^\pi a_{1\pi(1)} \dots a_{n\pi(n)}
\end{aligned}$$

Remark 2.8.

$$\begin{aligned}
\sigma_n &\rightarrow \sigma_n \\
\pi &\mapsto \pi^{-1}
\end{aligned}$$

is bijective.

$$\begin{aligned}
\text{injective: } \pi^{-1} = \sigma^{-1} &\implies \pi = \sigma \\
\text{surjective: } \pi &= (\pi^{-1})^{-1}
\end{aligned}$$

$$= \sum_{\pi \in \sigma_n} (-1)^{\pi^{-1}} a_{1\pi^{-1}(1)} \dots a_{n\pi^{-1}(n)}$$

Every index i occurs once on the left side and once on the right side. i occurs right

$$\pi^{-1}(j) = i \iff j = \pi(i)$$

$$= \sum_{\pi \in \sigma_n} (-1)^\pi a_{\pi(1)1} \dots a_{\pi(n)n}$$

$$\begin{aligned}\text{sign}(\pi \circ \pi^{-1}) &= 1 \\ &= \text{sign}(\pi) \cdot \text{sign}(\pi^{-1})\end{aligned}$$

Remark 2.9 (A small exercise).

$$\begin{aligned}\det(A) &= \det(f_A) \\ \prod_{j=1}^n a_{j, \pi^{-1}(j)} &= \prod_{i=1}^n a_{\pi(i), \pi^{-1}(\pi(i))} = \prod_{i=1}^n a_{\pi(i), i} \\ j &= \pi(i)\end{aligned}$$

□

Definition 2.6.

$$\text{perm}(A) := \sum_{\pi \in \sigma_n} a_{\pi(1)1} \dots a_{\pi(n)n}$$

is called permanent of A .

Open problem: for which matrix does $\text{perm}(A) = 0$ hold?

Example 2.7 (Computation of the determinant).

$$\dim \leq 3$$

$$n = 2 : \begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix} = a_{11}a_{22} - a_{12}a_{21}$$

$$n = 3 : \begin{vmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{vmatrix} = \sum_{\sigma \in \sigma_n} (-1)^\pi a_{\pi(1)1} a_{\pi(2)2} a_{\pi(3)3}$$

TODO drawing cayley graph

By the Cayley-Graph of group σ_3 we can see that $\sigma_3 = \left\langle \underline{(12)}, \underline{(23)} \right\rangle = -1$.

$$= a_{11}a_{22}a_{33} + a_{21}a_{32}a_{13} + a_{31}a_{12}a_{23}$$

TODO drawing tic tac toe

$$-a_{21}a_{12}a_{33} - a_{11}a_{32}a_{23} - a_{31}a_{22}a_{13}$$

TODO drawing tic tac toe

$$\begin{array}{ccc|cc} a_{11} & a_{12} & a_{13} & a_{11} & a_{12} \\ a_{21} & a_{22} & a_{23} & a_{21} & a_{22} \\ a_{31} & a_{32} & a_{33} & a_{31} & a_{32} \end{array}$$

Rule by Sarrus only holds for $n = 2$ or $n = 3$.

This lecture took place on 2018/03/14.

Example 2.8 (Rule by Sarrus). Let $n = 2$:

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

Let $n = 3$:

$$\begin{vmatrix} 1 & 2 & 5 & 1 & 2 \\ 2 & 5 & 14 & 2 & 5 \\ 5 & 14 & 42 & 5 & 14 \end{vmatrix} = 1$$

$$\begin{aligned} & 1 \cdot 5 \cdot 42 + 2 \cdot 14 \cdot 5 + 5 \cdot 2 \cdot 14 - 5 \cdot 5 \cdot 5 - 1 \cdot 14 \cdot 14 - 2 \cdot 2 \cdot 42 \\ &= 14 \cdot (1 \cdot 5 \cdot 3 + 2 \cdot 5 + 5 \cdot 2) - 125 - 14 \cdot (14 + 2 \cdot 2 \cdot 3) \\ &= 14 \cdot 35 - 125 - 14 \cdot 26 \\ &= 14 \cdot 9 - 125 = 1 \end{aligned}$$

An error in the computation will be enhanced.

Let $n = 4$. $|\sigma_n| = 24$ makes consideration of all permutations impractical.

Lemma 2.2. Let A be an upper triangular matrix, hence $a_{ij} = 0$ if $i > j$.

$$\implies \det(A) = a_{11}a_{22} \dots a_{nn}$$

Proof.

$$\det(A) = \sum_{\pi \in \sigma_n} (-1)^\pi a_{\pi(1)1} \dots a_{\pi(n)n}$$

such that $\pi(j) \leq j \forall j$.

$$\implies \text{id}$$

$$\pi(j) \leq j \forall j \implies \pi(1) \leq 1 \implies \pi(1) = 1$$

$$\pi(2) \leq 2 \implies \pi(2) = 2$$

$$\pi(3) \leq 3 \implies \pi(3) = 3$$

...

$$\pi(n) \leq n \implies \pi(n) = n$$

□

Theorem 2.9. Let $A = (a_{ij})$ be a $n \times n$ matrix.

1. Let z_1, \dots, z_n be row vectors of A . Then

$$\det \begin{bmatrix} z_1 & \dots \\ \vdots & \\ z_n & \dots \end{bmatrix} = \det \begin{bmatrix} z_1 & \dots \\ z_i + \lambda z_j & \dots \\ \vdots & \\ z_n & \dots \end{bmatrix} \forall i \neq j, \lambda \in \mathbb{K}$$

2. Let S_1, \dots, S_n be columns of A . Then,

$$\det \begin{pmatrix} S_1 & \dots & S_n \\ \vdots & & \vdots \end{pmatrix} = \det \begin{pmatrix} S_1 & \dots & S_i + \lambda S_j & \dots & S_j & \dots & S_n \\ \vdots & & \vdots & & \vdots & & \vdots \end{pmatrix}$$

Proof for column i.

$$\begin{aligned} \Delta(s_1, \dots, s_n) &= \Delta(s_1, \dots, s_i + \lambda s_j, \dots, s_n) \\ &= \Delta(s_1, \dots, s_i, \dots, s_n) + \underbrace{\lambda \Delta(s_1, \dots, s_j, \dots, s_j, \dots, s_n)}_{=0} \end{aligned}$$

□

Second proof. Row form is multiplication from left with matrix of structure

$$\begin{aligned} &I + \lambda E_{ij} \\ \det((I + \lambda E_{ij})A) &= \underbrace{\det(I + \lambda E_{ij})}_{\text{triangular matrix}=1} \cdot \det(A) \end{aligned}$$

□

Example 2.9.

$$\begin{vmatrix} 1 & 2 & 5 \\ 2 & 5 & 14 \\ 5 & 14 & 42 \end{vmatrix} = \begin{vmatrix} 1 & 2 & 5 \\ 0 & 1 & 4 \\ 0 & 4 & 17 \end{vmatrix} = \begin{vmatrix} 1 & 2 & 5 \\ 0 & 1 & 4 \\ 0 & 0 & 1 \end{vmatrix} = 1$$

Example 2.10.

$$\begin{aligned} &\begin{vmatrix} 1 & 0 & 3 & -2 \\ 2 & 6 & 4 & 1 \\ 3 & 3 & -1 & -1 \\ -1 & 2 & 4 & 1 \end{vmatrix} = \begin{vmatrix} 1 & 0 & 3 & -2 \\ 0 & 6 & -2 & 5 \\ 0 & 3 & -10 & 5 \\ 0 & 2 & 7 & -1 \end{vmatrix} \\ &= \frac{1}{3} \frac{1}{2} \begin{vmatrix} 1 & 0 & 3 & -2 \\ 0 & 6 & -2 & 5 \\ 0 & 6 & -20 & 10 \\ 0 & 6 & 21 & -3 \end{vmatrix} = \frac{1}{6} \begin{vmatrix} 1 & 0 & 3 & -2 \\ 0 & 6 & -2 & 5 \\ 0 & 0 & -18 & 5 \\ 0 & 0 & 23 & -8 \end{vmatrix} = \frac{1}{6} \cdot 6 \begin{vmatrix} 1 & 0 & 3 & -2 \\ 0 & 1 & -2 & 5 \\ 0 & 0 & -18 & 5 \\ 0 & 0 & 23 & -8 \end{vmatrix} \\ &= \begin{vmatrix} 1 & 0 & -1 & -2 \\ 0 & 1 & 8 & 5 \\ 0 & 0 & -8 & 5 \\ 0 & 0 & 7 & -8 \end{vmatrix} = \begin{vmatrix} 1 & 0 & -1 & -2 \\ 0 & 1 & 8 & 5 \\ 0 & 0 & -8 & 5 \\ 0 & 0 & -1 & -3 \end{vmatrix} = \begin{vmatrix} 1 & 0 & -1 & -2 \\ 0 & 1 & 8 & 5 \\ 0 & 0 & 0 & 29 \\ 0 & 0 & -1 & -3 \end{vmatrix} \\ &= \begin{vmatrix} 1 & 0 & -1 & -2 \\ 0 & 1 & 8 & 5 \\ 0 & 0 & -1 & -3 \\ 0 & 0 & 0 & 29 \end{vmatrix} = 29 \end{aligned}$$

Remark 2.10 (Laws, discussed so far).

$$\begin{vmatrix} z_1 & \dots \\ \lambda \cdot z_1 & \dots \\ z_n & \dots \end{vmatrix} = \lambda \begin{vmatrix} z_1 & \dots \\ \vdots & \\ z_k & \dots \\ \vdots & \\ z_n & \dots \end{vmatrix}$$

$$\begin{vmatrix} z_1 & \dots \\ z_1 + \lambda z_j & \dots \\ z_n & \dots \end{vmatrix} = \begin{vmatrix} z_1 & \dots \\ \vdots & \\ z_i & \dots \\ \vdots & \\ z_n & \dots \end{vmatrix} \quad (i \neq j)$$

$$\begin{vmatrix} z_1 & \dots \\ \vdots & \\ z_i & \dots \\ z_j & \dots \\ \vdots & \\ z_n & \dots \end{vmatrix} = - \begin{vmatrix} z_1 & \dots \\ \vdots & \\ z_j & \dots \\ \vdots & \\ z_i & \dots \\ \vdots & \\ z_n & \dots \end{vmatrix}$$

$$\begin{vmatrix} a_{11} & \dots & & \\ & a_{22} & \dots & \\ & & a_{33} & \dots \\ & & & \ddots \\ 0 & & & & a_{nn} \end{vmatrix} = a_{11} \cdot a_{nn}$$

(iii) If there are individual square matrices (A_1, A_2, \dots, A_k) along the diagonal of a matrix, the determinant of the matrix is the product of the determinant of the submatrices.

$$\det(A) = \det(A_1) \cdot \det(A_2) \cdot \dots \cdot \det(A_k)$$

Proof. Proof of (ii)

$$\begin{aligned} \begin{vmatrix} B & \begin{matrix} 0 \\ \vdots \\ 0 \end{matrix} \\ a_{n,1} & \dots & a_{n,n-1} & a_{n,n} \end{vmatrix} &= \sum_{\pi \in \sigma_n} (-1)^\pi a_{\pi(1)1} \dots a_{\pi(n)n} \\ &= \sum_{\pi' \in \sigma_{n-1}} (-1)^{\pi'} a_{\pi'(1)1} \dots a_{\pi'(n-1)n-1} \cdot a_{nn} \\ &= \det(B) \cdot a_{nn} \end{aligned}$$

$$\{\pi \in \sigma_n \mid \pi(n) = n\}$$

$$\pi(n) = n$$

$$B = \begin{pmatrix} a_{11} & \dots & a_{1,n-1} \\ \vdots & & \\ a_{n-1,1} & \dots & a_{n,n-1} \end{pmatrix}$$

Same idea: If

$$A = \begin{bmatrix} \vdots & 0 & \vdots \\ & \vdots & \\ & 0 & \\ & a_{ij} & \\ & 0 & \\ & \vdots & \\ & 0 & \end{bmatrix}$$

Exchange the i -th row with the last row.

$$= \pm 1 \begin{bmatrix} \vdots & 0 & \vdots \\ & \vdots & \\ & 0 & \\ & 0 & 0 \\ & \vdots & \\ & a_{ij} & \end{bmatrix}$$

□

Definition 2.7.

$$A \in \mathbb{K}^{n \times n}$$

$A_{k,l}$ is an $(n-1) \times (n-1)$ matrix, that is created by omitting the k -th row and l -th column.

$$\begin{bmatrix} a_{1,1} & \dots & a_{1,l-1} & a_{1,l+1} & \dots & a_{1,n} \\ \vdots & & & & & \vdots \\ a_{k-1,1} & \dots & a_{k-1,l-1} & a_{k-1,l+1} & \dots & a_{k-1,n} \\ a_{k+1,1} & \dots & a_{k+1,l-1} & a_{k+1,l+1} & \dots & a_{k+1,n} \\ \vdots & & & & & \vdots \\ a_{n,1} & \dots & a_{n,l-1} & a_{n,l+1} & \dots & a_{n,n} \end{bmatrix}$$

Pierre-Simon Laplace (1749–1827)

Definition 2.8 (Laplace expansion). *In German, this theorem is called Entwicklungssatz von Laplace*

Let l be fixed.

$$\det(A) = \sum_{k=1}^n a_{kl}(-1)^{k+l} \det(A_{kl})$$

“Expansion along column l ”.

Let k be fixed.

$$\det(A) = \sum_{l=1}^n a_{kl}(-1)^{k+l} \det(A_{kl})$$

“Expansion along row k ”.

Example 2.11.

$$\begin{aligned} \begin{vmatrix} 1 & 2 & 5 \\ 2 & 5 & 14 \\ 5 & 14 & 42 \end{vmatrix} &= \sum_{l=1}^3 (-1)^{1+l} \det(A_{1l}) \quad \text{for } k=1 \text{ fixed} \\ &= 1 \begin{vmatrix} 5 & 14 \\ 14 & 42 \end{vmatrix} - 2 \begin{vmatrix} 2 & 14 \\ 5 & 42 \end{vmatrix} + 5 \begin{vmatrix} 2 & 5 \\ 5 & 14 \end{vmatrix} \\ &= 1 \cdot \begin{pmatrix} 5 \cdot 42 - 14 \cdot 14 \\ 5 \cdot 3 \cdot 14 - 14 \cdot 14 \end{pmatrix} - 2 \begin{pmatrix} 2 \cdot 42 - 5 \cdot 14 \\ 2 \cdot 3 \cdot 13 - 5 \cdot 14 \end{pmatrix} + 5 \begin{pmatrix} 2 \cdot 14 - 5 \cdot 9 \\ 2 \cdot 14 - 5 \cdot 9 \end{pmatrix} = 14 - 2 \cdot 14 + 5 \cdot 15 = 1 \end{aligned}$$

$$TODO = -2 \cdot TODO$$

This lecture took place on 2018/03/19.

Review:

- Determinants are multilinear (in rows and columns)
- Determinants switches its sign if two rows or row columns are exchanged
- $\Delta(s_1, \dots, s_n) = (-1)^\pi \Delta(s_{\pi(1)}, \dots, s_{\pi(n)})$ where s_i are column vectors
-

$$\begin{vmatrix} a_{11} & 0 & \dots & 0 \\ * & & & \\ \vdots & & B & \\ * & & & \end{vmatrix} = a_{11} \cdot \det B$$

$$B = A_{11}$$

where A_{kl} is the $(n-1) \times (n-1)$ matrix created by removal of the k -th row and l -th column. This is a special case of Laplace expansion.

2.7 Laplace expansion

$$\begin{aligned}\det A &= \sum_{k=1}^n (-1)^{k+l} a_{kl} \cdot \det A_{kl} && \text{for fixed } l \in \{1, \dots, n\} \\ &= \sum_{l=1}^n (-1)^{k+l} a_{kl} \cdot \det A_{kl} && \text{for fixed } k \in \{1, \dots, n\}\end{aligned}$$

So in the case of (a very classic example)

$$\begin{vmatrix} a_{11} & 0 & \dots & 0 \\ * & & & \\ \vdots & & B & \\ * & & & \end{vmatrix} = a_{11} \cdot (-1)^{1+1} \cdot \det A_{11}$$

for fixed $k = 1$:

$$\sum_{l=1}^n (-1)^{1+l} \underbrace{a_{1l}}_{=0 \text{ for } l>1} \det A_{1l}$$

Proof. Let $l \in \{1, \dots, n\}$ be fixed. For the l -th column,

$$s_l = \sum_{k=1}^n a_{kl} e_k = \begin{pmatrix} a_{1l} \\ a_{2l} \\ \vdots \\ a_{nl} \end{pmatrix}$$

where e_k is a unit vector.

$$\begin{aligned}
\det(A) &= \Delta(s_1, s_2, \dots, s_{l-1}, \sum_{k=1}^n a_{kl} e_k, s_{l+1}, \dots, s_n) \\
&= \sum_{k=1}^n a_{kl} \Delta(s_1, \dots, s_{l-1}, e_k, s_{l+1}, \dots, s_n) \\
&= \sum_{k=1}^n a_{kl} \begin{vmatrix} a_{11} & a_{12} & \vdots & a_{1,l-1} & 0 & a_{1,l+1} & \dots & a_{1n} \\ a_{21} & a_{22} & \vdots & a_{2,l-1} & \vdots & \vdots & & \vdots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & & \vdots \\ \vdots & \vdots & \vdots & \vdots & 0 & \vdots & & \vdots \\ \vdots & \vdots & \vdots & \vdots & 1 & \vdots & & \vdots \\ \vdots & \vdots & \vdots & \vdots & 0 & \vdots & & \vdots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & & \vdots \\ a_{n1} & a_{n2} & \vdots & a_{n,l-1} & 0 & a_{n,l+1} & \dots & a_{nn} \end{vmatrix}
\end{aligned}$$

Recognize the one in row k . We consecutively exchange row k with the row above until it becomes row 1. This gives $k-1$ exchanges. Hence a cycle $(1 \dots k)$. This gives sign $= (-1)^{k-1}$.

$$= \sum_{k=1}^n a_{kl} (-1)^{k-1} \begin{vmatrix} a_{k1} & a_{k2} & \dots & a_{k,l-1} & 1 & a_{k,l+1} & \dots & a_{kn} \\ a_{11} & a_{12} & \dots & & 0 & & & a_{1n} \\ \vdots & \vdots & \dots & & 0 & & & \vdots \\ a_{k-1,1} & a_{k-1,2} & \dots & & 0 & & & a_{k-1,n} \\ a_{k+1,1} & a_{k+1,2} & \dots & & 0 & & & a_{k+1,n} \\ \vdots & \vdots & \dots & & 0 & & & \vdots \\ a_{n1} & a_{n2} & \dots & & 0 & & & a_{nn} \end{vmatrix}$$

Now we can do $l-1$ column exchange to move the one into the first column. This gives a cycle $(1, 2, \dots, l)$ and sign $= (-1)^{l-1}$

$$= \sum_{k=1}^n a_{kl} (-1)^{k-1} (-1)^l \begin{vmatrix} 1 & a_{k1} & a_{k2} & \dots & a_{k,l-1} & a_{k,l+1} & \dots & a_{kn} \\ 0 & a_{11} & a_{12} & \dots & a_{1,l-1} & a_{1,l+1} & \dots & a_{1n} \\ 0 & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & a_{2,n} \\ 0 & a_{k-1,1} & a_{k-1,2} & \dots & a_{k-1,l-1} & a_{k-1,l+1} & \dots & a_{k-1,n} \\ 0 & a_{k+1,1} & a_{k+1,2} & \dots & a_{k+1,l-1} & a_{k+1,l+1} & \dots & a_{k+1,n} \\ 0 & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & a_{2,n} \\ 0 & a_{n1} & a_{n2} & \dots & a_{n,l-1} & a_{n,l+1} & \dots & a_{nn} \end{vmatrix}$$

where the k -th row and l -th column is removed

$$= \sum_{k=1}^n (-1)^{k+l} a_{kl} \det A_{kl}$$

□

Example 2.12. $\begin{matrix} + & - & + & - & + & - \\ - & + & - & + & - & + \end{matrix}$

$$(-1)^{k+l}$$

Theorem 2.10. $\hat{a}_{kl} = (-1)^{k+l} \det A_{lk}$ is called cofactor.

$$\hat{A} = [\hat{a}_{kl}]_{k,l=1}^n$$

is called complementary matrix or adjugate matrix of A .

$$\begin{aligned} \hat{a}_{kl} &= (-1)^{k+l} \det (\text{the matrix without row } l \text{ and column } k) \\ &= (-1)^{k+l} \det A_{lk} = \frac{\partial}{\partial a_{lk}} \det A \end{aligned}$$

Then it holds that

$$A^{-1} = \frac{1}{\det A} \hat{A}$$

Proof. Show that $\hat{A} \cdot A = I \cdot \det(A)$. Let $B = \hat{A} \cdot A$.

$$b_{kl} = \sum_{i=1}^n \hat{a}_{ki} \cdot a_{il} = \sum_{i=1}^n (-1)^{k+i} \det A_{ik} \cdot a_{il}$$

Case 1: $k = l$

$$\begin{aligned} b_{ll} &= \sum_{i=1}^n (-1)^{l+i} \det A_{il} \cdot a_{il} \\ &= \det A \end{aligned}$$

Laplace expansion with l -th column

Case 2: $k \neq l$ (without loss of generality, $k < l$)

$$\begin{aligned} b_{kl} &= \sum_{i=1}^n \det(A_{ik}) (-1)^{k+i} a_{il} \\ &= \det \begin{bmatrix} a_{11} & \dots & a_{1l} & \dots & a_{1l} & \dots & a_{1n} \\ \vdots & & \vdots & & \vdots & & \vdots \\ a_{n1} & \dots & a_{nl} & & a_{nl} & & a_{nn} \end{bmatrix} \\ &= 0 \end{aligned}$$

two equal columns

(i.e. matrix A with k -th column replaced by l -th column) expanded by k -th row.

$$\det A = \sum_{i=1}^n (-1)^{k+i} \det(A_{ik}) \cdot a_{ik}$$

$$\tilde{A} = (\text{matrix } A \text{ replacing } k\text{-th column with } l\text{-th column})$$

$$\det \tilde{A} = \sum_{i=1}^n (-1)^{k+i} \det(A_{ik}) \cdot a_{il}$$

□

Example 2.13 (Small inverse matrices). Let $n = 2$.

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} = \frac{1}{ad - bc} \cdot \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$$

$$\hat{a}_{11} = (-1)^{1+1} \cdot \det A_{11} \quad \hat{a}_{21} = (-1)^{2+1} \cdot \det A_{12}$$

$$\hat{a}_{12} = (-1)^{1+2} \cdot \det A_{21} \quad \hat{a}_{22} = (-1)^{2+2} \cdot \det A_{22}$$

Remark 2.11 (Cayley 1855).

$$A^{-1} = \frac{1}{\nabla} \begin{bmatrix} \partial_a \nabla & \partial_c \nabla \\ \partial_b \nabla & \partial_d \nabla \end{bmatrix}$$

$$\nabla f = \begin{bmatrix} \frac{\partial f}{\partial x_1} \\ \vdots \\ \frac{\partial f}{\partial x_n} \end{bmatrix}$$

Example 2.14. Let $n = 3$.

$$\begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{bmatrix}^{-1} = \frac{1}{\det(A)} \begin{bmatrix} \begin{vmatrix} a_{22} & a_{23} \\ a_{32} & a_{33} \end{vmatrix} & -\begin{vmatrix} a_{12} & a_{13} \\ a_{32} & a_{33} \end{vmatrix} & \begin{vmatrix} a_{12} & a_{13} \\ a_{22} & a_{23} \end{vmatrix} \\ -\begin{vmatrix} a_{21} & a_{23} \\ a_{31} & a_{33} \end{vmatrix} & \begin{vmatrix} a_{11} & a_{13} \\ a_{31} & a_{33} \end{vmatrix} & -\begin{vmatrix} a_{11} & a_{13} \\ a_{21} & a_{23} \end{vmatrix} \\ \begin{vmatrix} a_{21} & a_{22} \\ a_{31} & a_{32} \end{vmatrix} & -\begin{vmatrix} a_{11} & a_{12} \\ a_{31} & a_{32} \end{vmatrix} & \begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix} \end{bmatrix}$$

Corollary. Let $A \in \mathbb{Z}^{n \times n}$. If $\det A = 1 \implies A^{-1} \in \mathbb{Z}^{n \times n}$.

Let $A \in \mathbb{Z}^{n \times n}$ and $\det A = 1$. Let $B \in \mathbb{Z}^{n \times n}$ and $\det B = 1$.

$$\implies \det(A \cdot B) = 1 \quad \implies \det(A^{-1}) = 1$$

Definition 2.9. Integer matrices with $\det = 1$ define a group called special linear group.

$$\text{SL}(n, \mathbb{Z}) = \{A \in \mathbb{Z}^{n \times n} \mid \det A = 1\}$$

Or in general for a ring R :

$$\text{SL}(n, R) = \{A \in R^{n \times n} \mid \det A = 1\}$$

Theorem 2.11 (Cramer's Rule). *Gabriel Cramer (1704–1752)*

Show by Cramer in 1750, by McLaurin 1748 for $n \leq 3$.

Let A be a regular matrix with column vectors a_1, \dots, a_n . Then the solution $Ax = b$ ($\implies x = A^{-1}b$ has a unique solution) is given by

$$x_i = \frac{\Delta(a_1, \dots, a_{i-1}, b, a_{i+1}, \dots, a_n)}{\Delta(a_1, \dots, a_n)}$$

$$= \frac{\det \begin{pmatrix} a_1 & \dots & a_{i-1} & b & a_{i+1} & \dots & a_n \\ \vdots & & \vdots & \vdots & \vdots & & \vdots \end{pmatrix}}{\det A}$$

$n + 1$ determinants of form $n \times n$. In practice infeasible except for small matrices.

Geometrical proof for $n = 2$.

$$A = \begin{pmatrix} a_1 & a_2 \\ \vdots & \vdots \end{pmatrix}$$

$$Ax = b \quad a_1 \cdot x + a_2 \cdot x_2 = b$$

$$\Delta(a_1, a_2) = A(a_1, a_2)$$

where A is the area function.

TODO drawing parallelogram

$$\Delta(b, a_2) = A(b, a_2) = \Delta(x_1 \cdot a_1, a_2) = x_1 \cdot \Delta(a_1, a_2)$$

$$\implies x_1 = \frac{\Delta(b, a_2)}{\Delta(a_1, a_2)}$$

□

Generic proof. Let $x = A^{-1} \cdot b = \frac{1}{\det A} \cdot \hat{A} \cdot b$.

$$x_i = \frac{1}{\det A} \cdot \sum_{k=1}^n \hat{a}_{ik} b_k$$

$$= \frac{1}{\det A} \sum_{k=1}^n (-1)^{i+k} \det A_{ki} \cdot b_k$$

$$\underbrace{=}_{\substack{\text{see proof of} \\ \text{Laplace expansion}}} \frac{1}{\det A} \sum_{k=1}^n \Delta(a_1, \dots, a_{i-1}, e_k, a_{i+1}, \dots, a_n) b_k$$

$$= \frac{\Delta(a_1, \dots, a_{i-1}, b, a_{i+1}, \dots, a_n)}{\det A}$$

□

Example 2.15.

$$\begin{aligned} 2x_1 + x_2 &= 7 \\ x_1 - 3x_2 &= 0 \end{aligned}$$

$$A = \begin{bmatrix} 2 & 1 \\ 1 & -3 \end{bmatrix}$$

$$\det(A) = 2 \cdot (-3) - 1 = -7$$

$$x_1 = -\frac{1}{7} \begin{vmatrix} 7 & 1 \\ 0 & -3 \end{vmatrix} = 3$$

$$x_2 = -\frac{1}{7} \begin{vmatrix} 2 & 7 \\ 1 & 0 \end{vmatrix} = 1$$

Remark 2.12. For large n (hence $n \geq 4$), Cramer's Rule is impractical (tiresome and unstable). But it helps with theoretical considerations.

1. The map $A \mapsto \det A$ is continuous and differentiable.
2. if $\det A \neq 0 \implies$ the set of invertible matrices is open⁴
3. The solution of system $Ax = b$ depends continuously on a_{ij} and b_i ⁵

3 Inner products

Definition 3.1.

$$\mathbb{R}^3 : \left\| \begin{pmatrix} a_1 \\ a_2 \\ a_3 \end{pmatrix} \right\| = \sqrt{a_1^2 + a_2^2 + a_3^2}$$

By Pythagorem Theorem

Pythagorem Theorem. Claim: $a^2 + b^2 = c^2$

TODO

□

⁴Hence for all invertible A , there exists some neighborhood such that all matrices in this neighborhood are invertible.

$$\text{e.g. } d(A, B) = \max_{i,j} |a_{ij} - b_{ij}|$$

⁵ This justifies why Computational Mathematics (dt. Numerik) is practical and interesting

$$\forall \varepsilon \exists \delta : d(b, b') < \delta \implies d(x, x') < \varepsilon$$

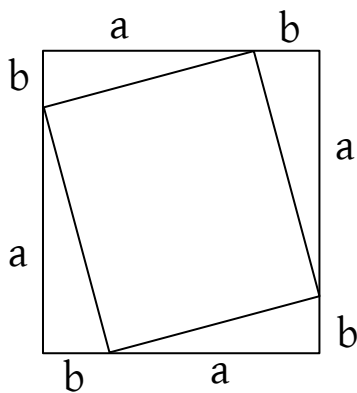


Figure 3: Proof construction of the Pythagorem Theorem

This lecture took place on 2018/03/21.

The norm is given by

$$\left\| \begin{pmatrix} a_1 \\ a_2 \\ a_3 \end{pmatrix} \right\| = \sqrt{a_1^2 + a_2^2 + a_3^2}$$

Definition 3.2 (Scalar product in $\mathbb{R}^2/\mathbb{R}^3$).

$$\langle a, b \rangle = \|a\| \cdot \|b\| \cdot \cos \theta$$

where θ is the angle between vector a and b .

Theorem 3.1.

$$\langle a, a \rangle = \|a\|^2$$

Recall that

$$\cos 0 = 1 \quad \cos \frac{\pi}{2} = 0 \quad \cos \pi = -1 \quad \cos \frac{3}{2}\pi = 0$$

$$\sin 0 = 0 \quad \sin \frac{\pi}{2} = 1 \quad \sin \pi = 0 \quad \sin \frac{3}{2}\pi = -1$$

$$\sin \theta = \cos(\theta - \frac{\pi}{2})$$

$$\cos(\pi - \theta) = -\cos(\theta)$$

$$\sin(-\theta) = -\sin(\theta)$$

$$\sin(\pi - \theta) = \sin(\theta)$$

$$\sin(-\theta) = -\sin(\theta)$$

Theorem 3.2. 1. $\langle a, a \rangle = \|a\|^2$

2. $\langle a, a \rangle = 0 \iff a = 0$

3. $\langle a, b \rangle = 0 \iff a = 0 \vee b = 0 \vee \theta = \frac{\pi}{2} \vee \theta = \frac{3}{2}\pi$, hence orthogonal

4. $\langle a, b \rangle > 0 \iff$ acute angle

5. $\langle a, b \rangle < 0 \iff$ obtuse angle

Theorem 3.3. 1. $\langle a, b \rangle = \langle b, a \rangle$

2. $\langle \lambda a, b \rangle = \lambda \cdot \langle a, b \rangle = \langle a, \lambda \cdot b \rangle$

3. $\langle a + b, c \rangle = \langle a, c \rangle + \langle b, c \rangle$

Thus, linear in a and b . Thus, bilinear.

Proof. 2. Assume $\lambda > 0$. Angle stays the same.

$$\langle \lambda a, b \rangle = \|\lambda a\| \cdot \|b\| \cdot \cos \theta = \lambda \cdot \|a\| \cdot \|b\| \cdot \cos \theta$$

Assume $\lambda < 0$. θ becomes $\pi - \theta$.

$$\langle \lambda a, b \rangle = \|\lambda a\| \cdot \|b\| \cdot \cos(\pi - \theta) = |\lambda| \cdot \|a\| \cdot \|b\| \cdot (-\cos(\theta)) = \lambda \cdot \|a\| \cdot \|b\|$$

3. Let $\|c\| = 1$. $\langle a, c \rangle = \|a\| \cdot \cos \theta$.

$$\langle a + b, c \rangle = \langle a, c \rangle + \langle b, c \rangle$$

Projections will add up.

In the generic case:

$$\begin{aligned} \langle a + b, c \rangle &= \left\langle a + b, \|c\| \cdot \frac{c}{\|c\|} \right\rangle \\ &= \underbrace{\|c\|}_{\text{by (2.)}} \left\langle a + b, \frac{c}{\|c\|} \right\rangle \end{aligned}$$

□

Theorem 3.4.

$$\left\langle \begin{pmatrix} a_1 \\ a_2 \\ a_3 \end{pmatrix}, \begin{pmatrix} b_1 \\ b_2 \\ b_3 \end{pmatrix} \right\rangle = a_1 b_1 + a_2 b_2 + a_3 b_3$$

Proof.

$$\begin{aligned}
\langle a \rangle b &= \langle a_1 e_1 + a_2 e_2 + a_3 e_3, b \rangle \\
&= a_1 \langle e_1, b \rangle + a_2 \langle e_2, b \rangle + a_3 \langle e_3, b \rangle \\
&= a_1 b_1 + a_2 b_2 + a_3 b_3 \\
\langle e_i, b \rangle &= \langle e_i, b_1 e_1 + b_2 e_2 + b_3 e_3 \rangle \\
&= b_1 \langle e_i, e_1 \rangle + b_2 \langle e_i, e_2 \rangle + b_3 \langle e_i, e_3 \rangle \\
&= b_1 \delta_{i1} + b_2 \delta_{i2} + b_3 \delta_{i3} \\
&= b_i
\end{aligned}$$

□

In this chapter, we will talk about vector spaces in which we will discuss scalar products with properties 1–3 from Theorem 3.3.

$$\text{in } \mathbb{R}^n : \quad \langle x, y \rangle = \sum_{i=1}^n x_i y_i$$

$$\text{in } V \subseteq \mathbb{R}^\infty : \quad \langle x, y \rangle = \sum_{i=1}^{\infty} x_i y_i$$

if convergent! For this space, $(e_i)_{i \in \mathbb{N}}$ is a basis.

$$\text{in } C[a, b] \quad \langle f, g \rangle = \int f(x)g(x) dx$$

is the Delta function.

Or better: $(\sin nx)_{n \in \mathbb{N}} \cup (\cos nx)_{n \in \mathbb{N}}$.

$$\begin{aligned}
\int_0^{2\pi} \sin(nx) \cos(mx) dx &= 0 \forall m, n \\
\int_0^{2\pi} \sin(nx) \sin(mx) dx &= 0 \text{ if } m \neq n
\end{aligned}$$

1768/03/21 J. Fourier

Theorem 3.5 (1822 Fourier). *Every function f in $[0, 2\pi]$ can be denoted as*

$$\begin{aligned}
f(x) &= \sum_{n=0}^{\infty} a_n \cos(nx) + \sum_{n=1}^{\infty} b_n \sin(nx) \\
a_n &= \langle f, \cos(nx) \rangle = \int_0^{2\pi} f(x) \cos(nx) dx \\
b_n &= \langle f, \sin(nx) \rangle = \int_0^{2\pi} f(x) \sin(nx) dx
\end{aligned}$$

This theorem cannot be proven, because it depends on the definition of “function”. The answer to the question, which functions satisfy this theorem, is an open research topic.

3.1 Law of cosines

Theorem 3.6 (Law of cosines). *In German, “Kosinussatz”.*

$$c^2 = a^2 + b^2 - 2ab \cos \gamma$$

$$\begin{aligned} \|\vec{c}\|^2 &= \|\vec{b} - \vec{a}\|^2 \\ &= \langle \vec{b} - \vec{a}, \vec{b} - \vec{a} \rangle \\ &= \langle \vec{b}, \vec{b} \rangle - \langle \vec{a}, \vec{b} \rangle - \langle \vec{b} - \vec{a}, \vec{a} \rangle + \langle \vec{a}, \vec{a} \rangle \\ &= \|b\|^2 - 2\|a\| \|b\| \cos \gamma + \|a\|^2 \end{aligned}$$

$$\|a\| \cdot \|b\| \cdot \sin \theta = \text{area of the spanned parallelogram}$$

How to find an orthogonal vector?

Remark 3.1 (Orthogonal vector in \mathbb{R}^2). Find \vec{b} such that $\langle \vec{a}, \vec{b} \rangle = 0$, $a_1 b_1 + a_2 b_2 = 0$. For example, $b_1 = a_2$ and $b_2 = -a_1$.

$$\vec{a} = \begin{pmatrix} a_1 \\ a_2 \end{pmatrix} \quad \vec{b} = \begin{pmatrix} a_2 \\ -a_1 \end{pmatrix}$$

3.2 Outer product

Definition 3.3. Called outer product (only in \mathbb{R}^3) or cross product.

Let $a, b \in \mathbb{R}^3$ and $a \times b$ is the vector which

1. $\|a \times b\| = \|a\| \cdot \|b\| \cdot \sin \theta$ is the area of the spanned parallelogram.
2. $a \times b \perp a$ and b
 $\langle a \times b, a \rangle = 0$ and $\langle a \times b, b \rangle = 0$
3. $(a, b, a \times b)$ is clockwise.

When does $a \times b = 0$ hold? $a = 0, b = 0, \sin \theta = 0$, hence $\theta = 0 \vee \theta = \pi$

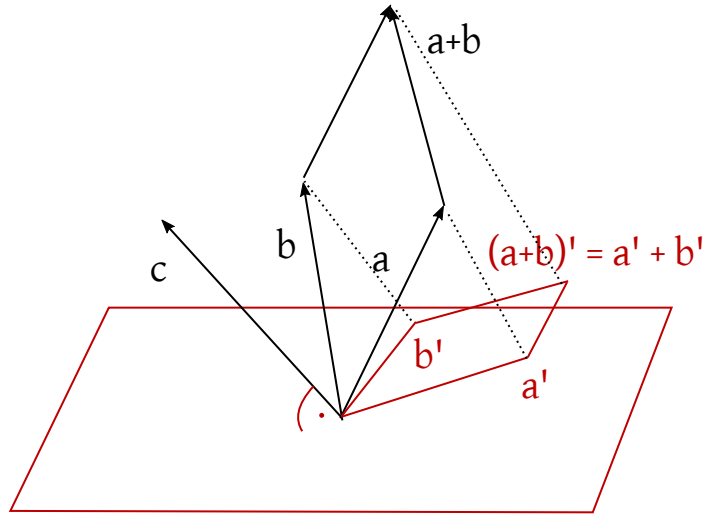
$$\iff a, b \text{ are linear independent}$$

Theorem 3.7. • $b \times a = -a \times b$

- $(\lambda a) \times b = \lambda(a \times b) = a \times (\lambda b)$
- $(a + b) \times c = a \times c + b \times c$

Proof. • Orientation swaps.

- If $\lambda > 0$, it follows immediate. If $\lambda < 0$, lengths stay the same, but orientation swaps.
- If $c = 0$, it is trivial. If $c \neq 0$, E is the plane orthogonal to c . a' and b' are



projections of a and b to E .

1. $(a + b)' = a' + b'$
2. $a \times c = a' \times c$.

$$\begin{aligned} \|a \times c\| &= \|a\| \|c\| \cdot \sin \theta \\ &= \|a'\| \cdot \|c\| \\ &= \|a' \times c\| \end{aligned}$$

- Orientation of $a \times c$ and $a' \times c$ is the same
- The plane, spanned by c and a , is also spanned by c and a'

$$\|a'\| = \|a\| \cdot \underbrace{\cos\left(\frac{\pi}{2} - \theta\right)}_{=\sin \theta}$$

Hence,

$$(a + b) \times c = (a + b)' \times c = (a' + b') \times c \stackrel{!}{=} a' \times c + b' \times c = a \times c + b \times c$$

$$(a' + b') \times c = a' \times c + b' \times c$$

rotated by 90° multiplied by $\|c\|$

$$a' \times c = a'$$

rotated by 90° multiplied by $\|c\|$

$$a' \times c + b' \times c = (a' + b') \times c$$

The relation $u + v = w$ will be preserved under rotation by 90° and multiplication with λ .

□

Corollary. The cross product is a map of $\mathbb{R}^3 \times \mathbb{R}^3 \rightarrow \mathbb{R}^3$ such that

- bilinear
- antisymmetrical, $a \times b = -b \times a$
- $e_1 \times e_2 = e_3, e_2 \times e_3 = e_1, e_3 \times e_1 = e_2$

$$e_i \times e_j = e_k \cdot \text{sign } \pi \quad \pi = \begin{pmatrix} 1 & 2 & 3 \\ i & j & k \end{pmatrix}$$

Corollary.

$$\begin{pmatrix} a_1 \\ a_2 \\ a_3 \end{pmatrix} \times \begin{pmatrix} b_1 \\ b_2 \\ b_3 \end{pmatrix} = \begin{bmatrix} a_2 b_3 - a_3 b_2 \\ a_3 b_1 - a_1 b_3 \\ a_1 b_2 - a_2 b_1 \end{bmatrix} = \begin{bmatrix} \begin{vmatrix} a_2 & b_2 \\ a_3 & b_3 \end{vmatrix} \\ - \begin{vmatrix} a_1 & b_1 \\ a_3 & b_3 \end{vmatrix} \\ \begin{vmatrix} a_1 & b_1 \\ a_2 & b_2 \end{vmatrix} \end{bmatrix} \underbrace{=}_{\text{by Laplace expansion along the third column}^6} \begin{vmatrix} a_1 & b_1 & e_1 \\ a_2 & b_2 & e_2 \\ a_3 & b_3 & e_3 \end{vmatrix}$$

Proof.

$$\begin{aligned} & (a_1 e_1 + a_2 e_2 + a_3 e_3) \times (b_1 e_1 + b_2 e_2 + b_3 e_3) \\ &= a_1 b_1 e_1 \times e_1 + a_1 b_2 e_1 \times e_2 + a_1 b_3 e_1 \times e_3 \\ &+ a_2 b_1 e_2 \times e_1 + a_2 b_2 e_2 \times e_2 + a_2 b_3 e_2 \times e_3 \\ &= a_3 b_1 e_3 \times e_1 + a_3 b_2 e_3 \times e_2 + a_3 b_3 e_3 \times e_3 \\ &= a_1 b_2 e_3 - a_1 b_3 e_2 - a_2 b_1 e_3 + a_2 b_3 e_1 + a_3 b_1 e_2 - a_3 b_2 e_1 \\ &= (a_2 b_3 - a_3 b_2) e_1 + (a_3 b_1 - a_1 b_3) e_2 + (a_1 b_2 - a_2 b_1) e_3 \end{aligned}$$

□

Theorem 3.8.

$$\langle a \times b, c \rangle = \begin{vmatrix} a_1 & b_1 & c_1 \\ a_2 & b_2 & c_2 \\ a_3 & b_3 & c_3 \end{vmatrix}$$

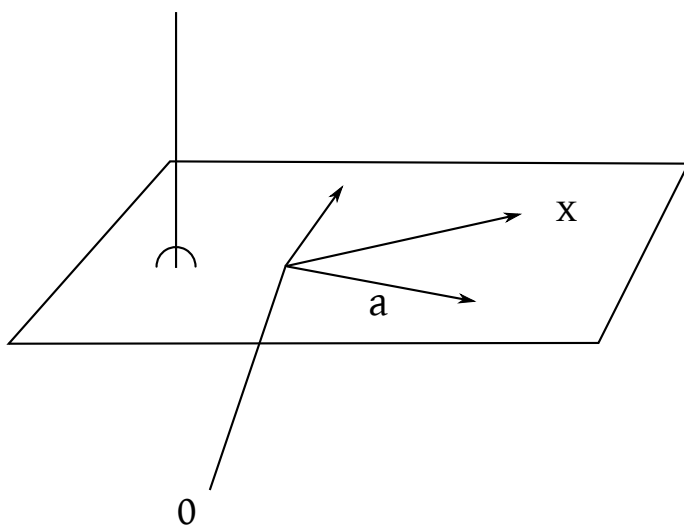
This corresponds to the volume of the spanned parallelepiped (dt. "Spat"). $\|a \times b\|$ is the area of the parallelogram and $\|c\|$ its height.

Equivalently, $\begin{vmatrix} a_1 & a_2 \\ b_1 & b_2 \end{vmatrix}$ is the area of the parallelogram.

Example 3.1. Let planes in \mathbb{R}^3 be given.

$$E = \{x_0 + \lambda a + \mu b \mid \lambda, \mu \in \mathbb{R}\}$$

$$c = a \times b = \{x \in \mathbb{R}^3 \mid x - x_0 \perp c\} = \{x \in \mathbb{R}^3 \mid \langle x - x_0, c \rangle = 0\}$$



3.3 Inner products and positive definiteness

From now on \mathbb{K} will be \mathbb{R} or \mathbb{C} .

Definition 3.4. An inner product on a vector space V is a map

$$V \times V \rightarrow \mathbb{K}$$

$$(x, y) \mapsto \langle x, y \rangle$$

1. $\langle x + y, z \rangle = \langle x, z \rangle + \langle y, z \rangle \forall x, y, z \in V$
2. $\langle \lambda x, y \rangle = \lambda \langle x, y \rangle \forall \lambda \in \mathbb{K} \forall x, y \in V$
3. $\langle y, x \rangle = \overline{\langle x, y \rangle} \forall x, y \in V$

where $\overline{\langle x, y \rangle}$ denotes the complex conjugate.

$$\underbrace{\langle x, \lambda y \rangle}_{\text{by (3)}} = \overline{\langle \lambda y, x \rangle} \underbrace{=}_{\text{by (2)}} \overline{\lambda \langle y, x \rangle} = \bar{\lambda} \overline{\langle y, x \rangle} = \bar{\lambda} \langle x, y \rangle$$

Linear in x , semi-linear in y . Sesquilinear⁷.

In physics, the notation is different:

$$\begin{array}{ccc} \langle x|y \rangle & \langle \lambda x|y \rangle = \bar{\lambda} \langle x|y \rangle & \langle x|\lambda y \rangle = \lambda \langle x|y \rangle \\ |y \rangle \dots \text{ket} & & \langle x| \dots \text{bra} \\ \langle x|y \rangle & & \text{bracket} \end{array}$$

The inner product is called positive-semidefinite, if

$$\langle x, x \rangle \geq 0 \forall x \in X$$

if additionally $\langle x, x \rangle = 0 \iff x = 0$, then \langle, \rangle is called positive definite.

This lecture took place on 2018/04/09. Easter holidays finished..

Lemma 3.1. 1. $\langle x, y + z \rangle = \langle x, y \rangle + \langle x, z \rangle$

$$2. \langle x, \lambda y \rangle = \bar{\lambda} \cdot \langle x, y \rangle$$

$$3. \langle x, 0 \rangle = 0$$

Definition 3.5. An inner product is positive semidefinite, if $\langle x, x \rangle \geq 0$. Is positive definite, if $\langle x, x \rangle > 0$ for all $x \neq 0$. Is negative definite, if $\langle x, x \rangle < 0$ for all $x \neq 0$. Is indefinite, if neither positive nor negative semidefinite.

A positive definite product is called scalar product. A positive definite product is in Hermitian form, if $\mathbb{K} = \mathbb{C}$. A positive definite product is also called unitary product, if $\mathbb{K} = \mathbb{C}$.

So quadratic form over \mathbb{R} and Hermitian form over \mathbb{C} .

⁷In Latin, sesqui means 1.5

Example 3.2. • Let $V = \mathbb{R}^n$.

$$\left\langle \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}, \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} \right\rangle = \sum_{i=1}^n x_i y_i$$

Let $V = \mathbb{C}^n$.

$$\left\langle \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}, \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} \right\rangle = \sum_{i=1}^n x_i \overline{y_i} \implies \langle x, x \rangle = \sum_{i=1}^n x_i \overline{x_i} = \sum_{i=1}^n |x_i|^2 \geq 0$$

\rightarrow positive definite.

• Another example: let $A \in \mathbb{R}^{n \times n}$. Let $x, y \in \mathbb{R}^n$.

$$\begin{aligned} \langle x, y \rangle_A &= x^t \cdot A \cdot y \quad \text{is bilinear} \\ &= \sum_{i=1}^n x_i \sum_{j=1}^n a_{ij} y_j = \sum_{i,j=1}^n a_{ij} x_i y_j \end{aligned}$$

hence $\langle x, y \rangle_A = \langle y, x \rangle_A$. It must hold that

$$\sum_{i,j=1}^n a_{ij} x_i y_j = \sum_{i,j=1}^n a_{ij} y_i x_j \quad \forall x, y$$

We let $x = e_k$ and $y = e_l$.

$$\implies a_{kl} = a_{lk} \quad \forall k, l$$

Hence $A = A^T$. A is symmetrical.

Let $A \in \mathbb{C}^{n \times n}$. Let $x, y \in \mathbb{C}^n$.

$$\langle x, y \rangle_A = \sum_{i=1}^n \sum_{j=1}^n x_i a_{ij} - i j \overline{y_j}$$

$$\langle x, y \rangle_A = \langle y, x \rangle_A \quad \forall x, y$$

$$\iff A^T = \overline{A} \quad \text{is in Hermitian form}$$

$$a_{ji} = \overline{a_{ij}} \quad \forall i, j$$

•

$$V = C[a, b] = \{f : [a, b] \rightarrow \mathbb{K} \text{ continuous}\}$$

$$\langle f, g \rangle = \int_a^b f(t) \overline{g(t)} dt \quad \text{is a scalar product}$$

$$\langle f, f \rangle = \int_a^b |f(t)|^2 dt \geq 0$$

- Consider $V = l_2(\mathbb{R}^\infty \text{ would be too large})$ where $l_2 = \{(x_n)_{n \in \mathbb{N}} \mid x_n \in \mathbb{R}, \sum_{n=1}^{\infty} x_n^2 < \infty\}$.

$$\langle x, y \rangle = \sum_{n=1}^{\infty} x_n y_n \quad \text{is a scalar product}$$

Does it converge? This is not obvious.

Fourier claimed that this example (4) and example (3) are the same. He claimed every function can be written as $f(x) = \sum_{n=0}^{\infty} a_n e^{inx}$.

$$x \cdot x = \langle x, x \rangle = \sum_{i=1}^n x_i^2 = \|x\|^2$$

Definition 3.6. Let V be a vector space. A norm on V is a map $\|\cdot\| : V \rightarrow [0, \infty[$ such that

1. $\|x\| \geq 0$ and $\|x\| = 0 \iff x = 0$
2. $\|\lambda \cdot x\| = |\lambda| \cdot \|x\| \quad \forall \lambda \in K, \forall x \in V$
3. $\|x + y\| \leq \|x\| + \|y\|$ is the triangle inequality

Remark 3.2. Every norm is a metric with $d(x, y) = \|x - y\|$.

d is translation invariant. $d(x + x_0, y + x_0) = d(x, y)$. This is compatible to a vector space.

In a black hole (\rightarrow physics), you have a different metric in every point (Riemannian geometry): $\langle x, y \rangle_{A(x,y)}$.

Example 3.3. Let $V = \mathbb{R}^n$.

- $\|x\|_2 = \left(\sum_{i=1}^n x_i^2\right)^{1/2}$ is called euclidean norm.
- $\|x\|_1 = \sum_{i=1}^n |x_i|$ is called l^1 norm or Manhattan norm.
- $\|x\|_\infty = \max \{|x_i| \mid i = 1, \dots, n\}$

Let $V = C[a, b]$.

•

$$\|f\|_1 = \int_a^b |f(t)| dt$$

L^1 -norm, gives rise to the Lebesgue integral.

•

$$\|f\|_\infty = \max_{t \in [\bar{a}, b]} |f(t)| \quad \text{is a } L^\infty\text{-norm}$$

•

$$\|f\|_2 = \left(\int |f(t)|^2 dt \right)^{\frac{1}{2}}$$

Theorem 3.9. Let \langle, \rangle be a scalar product in V (hence, positive-definite inner product). Then $\|x\| = \sqrt{\langle x, x \rangle}$ is a norm on V .

Proof. • $\|x\| \geq 0, \|x\| = 0 \iff \langle x, x \rangle = 0 \iff x = 0$

$$\bullet \| \lambda x \| = \sqrt{\langle \lambda x, \lambda x \rangle} = \sqrt{\lambda \cdot \bar{\lambda} \cdot \langle x, x \rangle} = \sqrt{\lambda^2 \cdot \langle x, x \rangle} = |\lambda| \cdot \sqrt{\langle x, x \rangle}$$

• Triangle inequality

□

3.4 Cauchy-Bunyakovskii-Schwarz inequality

Lemma 3.2 (Cauchy-Bunyakovskii-Schwarz inequality). *Cauchy (1789–1857) for \mathbb{R}^n , Bunyakovskii (1804–1889) for $C[a, b]$, Schwarz (1843–1921) generically.*

$$|\langle x, y \rangle| \leq \|x\| \cdot \|y\|$$

Hence, l^2 if $\sum_{n=1}^{\infty} x_n^2 < \infty$ and $\sum_{n=1}^{\infty} y_n^2 < \infty$. $\langle x, x \rangle < \infty$ and $\langle y, y \rangle < \infty$.

$$\implies \sum x_n y_n \leq \sqrt{\sum x_n^2} \sqrt{\sum y_n^2}$$

If $|\langle x, y \rangle| = \|x\| \cdot \|y\| \iff x, y$ are linear dependent.

Proof. Now we can continue with part 3 of the proof of Theorem 3.9. Triangle inequality:

$$\begin{aligned} \|x + y\|^2 &= \langle x + y, x + y \rangle \\ &= \langle x, x \rangle + \langle x, y \rangle + \langle y, x \rangle + \langle y, y \rangle \\ &\leq \|x\|^2 + 2|\langle x, y \rangle| + \|y\|^2 \\ &\leq \|x\|^2 + 2\|x\|\|y\| + \|y\|^2 \\ &= (\|x\| + \|y\|)^2 \end{aligned}$$

□

Proof of CBS inequality, Lemma 3.2. Case 1: $y = 0$ trivial

Case 2: $y \neq 0$ Let $\lambda \in \mathbb{K}$ be arbitrary.

$$\begin{aligned} 0 &\leq \langle x - \lambda y, x - \lambda y \rangle \\ &= \langle x, x \rangle - \langle x, \lambda y \rangle - \langle \lambda y, x \rangle + \langle \lambda y, \lambda y \rangle \\ &= \langle x, x \rangle - \bar{\lambda} \langle x, y \rangle - \lambda \langle y, x \rangle + |\lambda|^2 \langle y, y \rangle \end{aligned}$$

This holds for all λ , hence also for $\lambda = \frac{\langle x, y \rangle}{\langle y, y \rangle}$. Because $y \neq 0 \implies \langle y, y \rangle > 0$, we can divide.

$$\begin{aligned} &= \langle x, x \rangle - \frac{\overline{\langle x, y \rangle}}{\langle y, y \rangle} \cdot \langle x, y \rangle - \frac{\langle x, y \rangle}{\langle y, y \rangle} \cdot \langle y, x \rangle + \frac{|\langle x, y \rangle|^2}{\langle y, y \rangle^2} \cdot \langle y, y \rangle \\ &= \langle x, x \rangle - \frac{|\langle x, y \rangle|^2}{\langle y, y \rangle} - \frac{|\langle x, y \rangle|^2}{\langle y, y \rangle} + \frac{|\langle x, y \rangle|^2}{\langle y, y \rangle} \\ &= \|x\|^2 - \frac{|\langle x, y \rangle|^2}{\|y\|^2} \\ &\implies \|x\|^2 \cdot \|y\|^2 - |\langle x, y \rangle|^2 \geq 0 \end{aligned}$$

□

Alternative proof of CBS inequality in \mathbb{R}^n .

$$\begin{aligned} 0 &\leq \sum_{i=1}^n \sum_{j=1}^n (x_i y_j - x_j y_i)^2 \\ &= \sum_{i,j=1}^n (x_i^2 y_j^2 - 2x_i y_j x_j y_i + x_j^2 y_i^2) \\ &= \sum_{i,j} x_i^2 y_j^2 - 2 \sum_{i,j} x_i x_j y_i y_j + \sum_{i,j} x_j^2 y_i^2 \\ &= 2 \sum_i x_i^2 \sum_j y_j^2 - 2 \sum_i x_i y_i \sum_j x_j y_j \\ &= 2 \|x\|^2 \|y\|^2 - 2 \langle x, y \rangle^2 \\ &\leadsto \|x\|^2 \|y\|^2 = \langle x, y \rangle^2 + \frac{1}{2} \sum_i \sum_j (x_i y_j - x_j y_i)^2 \end{aligned}$$

So for $n = 3$, $\|x\|^2 \|y\|^2 = \langle x, y \rangle^2 + \|x \times y\|^2$. Hence, equality is given iff x and y are linear dependent.

In the general case: If $|\langle x, y \rangle| = \|x\| \cdot \|y\|$. From the proof, it follows that $\exists \lambda : \langle x - \lambda y, x - \lambda y \rangle = 0$

$$\implies x - \lambda y = 0 \implies x, y \text{ are linear independent}$$

□

Theorem 3.10. Let V be a vector space over $\mathbb{K} = \mathbb{R}$ or \mathbb{C} . Let $B = \{b_1, \dots, b_n\}$ is a basis. \langle, \rangle is an inner product. What does \langle, \rangle look like in regards of the coordinate?

There exists a unique matrix A in Hermitian form (hence, $a_{ij} = \overline{a_{ji}}$, $A = \overline{A^T}$) such that $\forall x, y \in V : \langle x, y \rangle = \Phi_B(x)^T \cdot A \cdot \overline{\Phi_B(y)}$. If \langle, \rangle is positive definite, A is regular.

Remark 3.3.

$$\langle x, y \rangle = \sum x_i \overline{y_i}$$

corresponds to $A = I$.

$$x^T \cdot I \cdot \overline{y} = x^T \cdot \overline{y}$$

How about $A = -I$.

$$\langle x, y \rangle_A = - \sum x_i \overline{y_i}$$

This is not a scalar product (because of negative definiteness).

Proof. Let $x = \sum_{i=1}^n \xi_i b_i$, $y = \sum_{j=1}^n \eta_j b_j$.

$$\begin{aligned} \langle x, y \rangle &= \left\langle \sum_{i=1}^n \xi_i b_i, \sum_{j=1}^n \eta_j b_j \right\rangle \\ &= \sum_{i=1}^n \xi_i \sum_{j=1}^n \overline{\eta_j} \underbrace{\langle b_i, b_j \rangle}_{=: a_{ij} \text{ is unique } a_{ij} = \langle b_i, b_j \rangle} \\ &= \sum_{i=1}^n \sum_{j=1}^n \xi_i a_{ij} \overline{\eta_j} \\ &= \xi^T \cdot A \cdot \overline{\eta} \\ &= \Phi_B(x)^T \cdot A \cdot \overline{\Phi_B(y)} \\ a_{ji} &= \langle b_j, b_i \rangle = \overline{\langle b_i, b_j \rangle} = \overline{a_{ij}} \end{aligned}$$

Show: If \langle, \rangle is positive definite, then A is regular. It suffices to show that $\ker A = \{0\}$.

Assume: $A \cdot \xi = 0 \implies \xi^T \cdot A \cdot \xi = 0$. Let $x = \sum_{i=1}^n \xi_i b_i \implies \langle x, x \rangle = 0 \implies x = 0 \implies \xi = \Phi_B(x) = 0$ □

Definition 3.7. Let $A \in \mathbb{C}^{n \times n}$. The matrix $A^* := \overline{A^T}$ ($(A^*)_{ij} = \overline{a_{ji}}$) is called conjugate transpose.

A is called self-adjoint if $A = A^*$. A is called symmetrical if $A = \overline{A}$ and $\mathbb{K} = \mathbb{R}$ or A is called Hermitian if $A = A^*$ and $\mathbb{K} = \mathbb{C}$.

$A = A^*$ is called (positive/negative) (semidefinite/definite) if the corresponding sesquilinear form

$$\langle \xi, \eta \rangle_A = \xi^T \cdot A \cdot \bar{\eta}$$

Hence, $\xi^T A \bar{\xi} \geq 0 \forall \xi \neq 0$ is positive definite, has the corresponding property or $\xi^T A \bar{\xi} > 0 \forall \xi \neq 0$ is positive semidefinite, has the corresponding property.

$\xi^T A \bar{\xi} \leq 0 \forall \xi \neq 0$ is negative definite or $\xi^T A \bar{\xi} < 0 \forall \xi \neq 0$ is negative semidefinite.

If $\exists \xi : \xi^T A \bar{\xi} > 0$ and $\exists \eta : \eta^T A \bar{\eta} < 0$, then A is called indefinite.

This lecture took place on 2018/04/11.

Inner product: $\langle x, y \rangle$

- $\forall x : \langle x, x \rangle \geq 0$ positive semi-definite
- $\forall x \neq 0 : \langle x, x \rangle > 0$ positive definite

in regards of basis b_1, \dots, b_n .

$$\begin{aligned} \langle x, y \rangle &= \sum a_{ij} \xi_i \bar{\eta}_j \\ a_{ij} &= \langle b_i, b_j \rangle \end{aligned}$$

Remark 3.4. $A = A^*$ is called positive semidefinite if $A \geq 0$ if $\forall \xi : \xi^T A \bar{\xi} \geq 0$.

$A = A^*$ is called positive definite if $A > 0$ if $\forall \xi \in \mathbb{K}^n \setminus \{0\} : \xi^T A \bar{\xi} > 0$ with $\xi^T A \bar{\xi} = \sum_{i=1}^n \sum_{j=1}^n$ TODO.

Example 3.4.

$$A = I > 0$$

$$\xi^T I \bar{\xi} = \sum_{i=1}^n \xi_i \bar{\xi}_i = \sum |\xi_i|^2 > 0 \quad \text{if } \xi \neq 0$$

$A = -I < 0$ is negative definite

$$A = \begin{bmatrix} 1 & & & & \\ & \ddots & & & \\ & & 1 & & \\ & & & -1 & \\ & & & & \ddots \\ & & & & & -1 \end{bmatrix}$$

is indefinite:

$$e_1^T A e_1 > 0 \quad e_n^T A e_n < 0$$

Remark 3.5. For a diagonal matrix

$$A = \begin{bmatrix} a_1 & & 0 \\ & \ddots & \\ 0 & & a_n \end{bmatrix}$$

$A = A^* \iff a_i = \bar{a}_i$, hence for all $a_i \in \mathbb{R}$.

For a diagonal matrix it holds that

$$A > 0 \text{ if all } a_i > 0 : \xi^T A \bar{\xi} = \sum_{i=1}^n a_i |\xi_i|^2 \geq 0$$

$$A \leq 0 \text{ if all } a_i \geq 0 \text{ if } \xi^T A \bar{\xi} = 0 \implies \text{all } a_i \cdot |\xi_i|^2 = 0$$

$$A < 0 \text{ if all } a_i < 0$$

$$A \leq 0 \text{ if all } a_i \leq 0$$

$$\text{indefinite if } \exists i : a_i > 0 \exists j : a_j < 0$$

Remark 3.6. Remember, that the rank of matrix satisfies:

$$\exists P, Q \in \text{GL}(n) : PAQ = \begin{pmatrix} 1 & & & \\ & 1 & & \\ & & \ddots & \\ & & & 0 \end{pmatrix}$$

$A \sim PAQ$ is equivalent

3.5 Congruence of matrices

Definition 3.8 (Congruence). Consider two self-adjoint matrices $A, B \in \mathbb{K}^{n \times n}$ are called congruent (denoted $A \cong B$) if $\exists C \in \text{GL}(n, \mathbb{K})$ such that $C^* A C = B$.

Remark 3.7. C is invertible, hence C^T is invertible.

$$(C^T)^{-1} = (C^{-1})^T \quad (C^{-1})^T \cdot C^T = (C \cdot C^{-1})^T = I^T = I$$

$$(\bar{A}^{-1}) = \overline{A^{-1}}$$

$$(AB)^* = \overline{(AB)^T} = \overline{B^T A^T} = \overline{B^T} \overline{A^T} = B^* \cdot A^*$$

$C^* A C$ is self-adjoint.

$$(C^* A C)^* = C^* \cdot A^* \cdot (C^*)^* = C^* \cdot A \cdot C$$

Theorem 3.11. Every Hermitian matrix is congruent to a diagonal matrix of structure:

$$\begin{bmatrix} 1 & & & & & & & & \\ & 1 & & & & & & & \\ & & \ddots & & & & & & \\ & & & 1 & & & & & \\ & & & & -1 & & & & \\ & & & & & \ddots & & & \\ & & & & & & -1 & & \\ & & & & & & & 0 & \\ & & & & & & & & \ddots & \\ & & & & & & & & & 0 \end{bmatrix}$$

Proof. The proof is given by an algorithm.

We construct matrix C inductively such that

$$C^*AC = \text{diag}(\pm 1, \dots, 0)$$

Consider $n = 1$.

$$A = [a_{11}]$$

If $a_{11} = 0$ where $a_{11} \in \mathbb{R}$, we don't have to do anything. If $a_{11} \neq 0$,

$$C = \left[\frac{1}{\sqrt{|a_{11}|}} \right]$$

$$C^*AC = \left[\frac{1}{\sqrt{|a_{11}|}} \cdot a_{11} \cdot \frac{1}{\sqrt{|a_{11}|}} \right] = [\text{sign}(a_{11})]$$

Example 3.5.

$$A = \begin{bmatrix} 0 & 1 & i \\ 1 & 0 & 1 \\ -i & 1 & 0 \end{bmatrix}$$

Then $n - 1 \rightarrow n$:

Case 1: $A = 0$ nothing to do.

Case 2: $a_{11} = 0$ **Case 2a:**

$$\exists j : a_{jj} \neq 0 : \begin{bmatrix} 0 & & \\ & a_{jj} & \\ & & \end{bmatrix}$$

$$T_{(1,j)} = \begin{bmatrix} 0 & & & & & 1 \\ & 1 & & & & \\ & & \ddots & & & \\ & & & 1 & & \\ & & & & 0 & \\ & & & & & 1 \\ 1 & & & & & & 1 \end{bmatrix} = T_{(ij)}^*$$

Permutation matrix that swaps 1 with j .

$$T_{(1j)}^* A T_{(1j)} = \begin{bmatrix} a_{ji} & \dots & \dots \\ \vdots & \ddots & \\ \vdots & & 0 \end{bmatrix}$$

where $T_{(1j)}^*$ exchanges j -th and first row and $T_{(1j)}$ exchanges j -th and first column.

Case 2b : all $a_{jj} = 0$. Choose i, j such that $a_{ij} \neq 0$.

$$C = I + E_{ij}e^{i\theta}$$

where θ such that $a_{ij} = e^{i\theta} |a_{ij}|$.

Example 3.6. $a_{12} \neq 0$

$$C_1 = \begin{bmatrix} 1 & 1 & \\ & 1 & \\ & & 1 \end{bmatrix}$$

$$C_1^* A C_1 = \begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 0 & 1 & i \\ 1 & 0 & 1 \\ -i & 1 & 0 \end{bmatrix} \cdot \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

$$\begin{bmatrix} 0 & 1 & i \\ 1 & 1 & 1+i \\ -i & 1 & 0 \end{bmatrix} \cdot \begin{bmatrix} 0 & 1 & i \\ 1 & 2 & 1+i \\ -i & 1-i & 0 \end{bmatrix}$$

In the general case:

$$C^* A C = (I + E_{ji}e^{-i\theta})A(I + E_{ij}e^{i\theta})$$

$$\begin{aligned} (C^* A C)_{jj} &= (A + E_{ji}e^{-i\theta}A + AE_{ij}e^{i\theta} + E_{ji}AE_{ij})_{jj} \\ &= \underbrace{a_{jj}}_{=0} + \underbrace{(E_{ji}e^{-i\theta}A)_{jj}}_{e^{-i\theta}a_{jj}=|a_{ij}|} + \underbrace{(AE_{ij}e^{i\theta})_{jj}}_{a_{ji}e^{i\theta}=\overline{a_{ij}}e^{i\theta}=|a_{ij}|} + \underbrace{a_{ii}}_{=0} \\ &= 2|a_{ij}| \end{aligned}$$

Case 2a is shown.

Example 3.7.

$$C_2 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \\ & & 1 \end{bmatrix} = T_{(12)}$$

$$A_2 = C_2^* A_1 C_2 = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 0 & 1 & i \\ 1 & 2 & i+1 \\ -i & 1-i & 0 \end{bmatrix} \cdot \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 2 & i+1 \\ 0 & 1 & i \\ -i & 1-i & 0 \end{bmatrix} \cdot \begin{bmatrix} 2 & 1 & 1+i \\ 1 & 0 & i \\ 1-i & -i & 0 \end{bmatrix}$$

Case 3 $a_{11} \neq 0$

$$C = \begin{bmatrix} 1 & -\frac{a_{12}}{a_{11}} & -\frac{a_{13}}{a_{11}} & \dots & -\frac{a_{1n}}{a_{11}} \\ & 1 & \dots & 0 & 0 \\ & \vdots & 1 & & 0 \\ & 0 & & \ddots & \\ & 0 & 0 & \dots & 1 \end{bmatrix}$$

Example 3.8.

$$C_3 = \begin{bmatrix} 1 & -\frac{1}{2} & -\frac{1+i}{2} \\ & 1 & \\ & & 1 \end{bmatrix}$$

$$A_3 = C_3^* A_2 C_3 = \begin{bmatrix} 1 & 0 & 0 \\ -\frac{1}{2} & 1 & 0 \\ -\frac{1-i}{2} & 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 2 & 1 & 1+i \\ 1 & 0 & i \\ 1-i & -i & 0 \end{bmatrix} \cdot \begin{bmatrix} 1 & -\frac{1}{2} & -\frac{1+i}{2} \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

$$\begin{bmatrix} 2 & 1 & 1+i \\ 0 & -\frac{1}{2} & \frac{1}{2}(-i+i) \\ 0 & \frac{1}{2}(-1-i) & -1 \end{bmatrix} \cdot \begin{bmatrix} 2 & 0 & 0 \\ 0 & -\frac{1}{2} & \frac{-1+i}{2} \\ 0 & \frac{-1-i}{2} & -1 \end{bmatrix}$$

$$C^* A C = \begin{bmatrix} a_{11} & 0 & \dots & 0 \\ 0 & & & \\ \vdots & & & \\ 0 & & & \tilde{A} \end{bmatrix}$$

$$\tilde{A} \in \mathbb{K}^{(n-1) \times (n-1)}$$

$$\tilde{A} = \tilde{A}^*$$

$$C' = \begin{bmatrix} \frac{1}{\sqrt{|a_{11}|}} & & & 0 \\ & 1 & & \\ & & \ddots & \\ 0 & & & 1 \end{bmatrix}$$

$$(C')^*(C^*AC)C' = \begin{bmatrix} \frac{a_{11}}{|a_{11}|} & 0 & 0 \\ 0 & & \\ \vdots & & \\ 0 & & \tilde{A} \end{bmatrix} \text{ where } \frac{a_{11}}{|a_{11}|} = \pm 1$$

Apply this algorithm to \tilde{A} .

Example 3.9 (Part 4).

$$C_4 = \begin{bmatrix} \frac{1}{\sqrt{2}} & & \\ & 1 & \\ & & 1 \end{bmatrix}$$

$$A_4 = C_4^* A_3 C_4 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & -\frac{1}{2} & \frac{-1+i}{2} \\ 0 & \frac{-1-i}{2} & -1 \end{bmatrix}$$

$$\tilde{A} = \begin{bmatrix} -\frac{1}{2} & \frac{-1+i}{2} \\ \frac{-1-i}{2} & -1 \end{bmatrix}$$

$$C_5 = \begin{bmatrix} 1 & & \\ & 1 & -1+i \\ & 0 & 1 \end{bmatrix}$$

$$A_5 = C_5^* A_4 C_5 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & -1-i & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 & 0 \\ 0 & -\frac{1}{2} & \frac{-1+i}{2} \\ 0 & \frac{-1-i}{2} & -1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & -1+i \\ 0 & 0 & 1 \end{bmatrix}$$

$$A_5 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & -\frac{1}{2} & \frac{-1+i}{2} \\ 0 & 0 & 0 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & -1+i \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & -\frac{1}{2} & 0 \\ 0 & 0 & 0 \end{bmatrix}$$

$$C_6 = \begin{bmatrix} 1 & & \\ & \sqrt{2} & \\ & & 1 \end{bmatrix}$$

$$\sqrt{2} = \frac{1}{\sqrt{\frac{1}{2}}}$$

$$C_6^* A_5 C_6 = \begin{bmatrix} 1 & & \\ & -1 & \\ & & 0 \end{bmatrix}$$

$$C_6^* \dots C_2^* C_1^* A C_1 C_2 \dots C_6 = \begin{bmatrix} 1 & & \\ & -1 & \\ & & 0 \end{bmatrix} \Rightarrow \text{indefinite}$$

$$C = C_1 C_2 \dots C_6$$

$$C^* = C_6^* C_5^* \dots C_1^*$$

□

Example 3.10. 1. If $A \geq 0$, C arbitrary $\implies C^*AC \geq 0$.

$$\xi^T (C^*AC) \bar{\xi} = \underbrace{(\xi^T C^*)}_{\xi^T C^T = \bar{\xi}^T C^T = \overline{(C \bar{\xi})}^T = \bar{\eta}^T} A \underbrace{(C \bar{\xi})}_{\eta} = \bar{\eta}^T A \bar{\eta} \geq 0$$

2. If $A > 0$, C invertible

$$\implies C^*AC > 0$$

$$\text{if } \xi^T C^*AC \bar{\xi} = 0 \implies \eta = C \bar{\xi} = 0 \text{ because } A > 0$$

$$\implies \bar{\xi} = 0 \text{ because } C \text{ is invertible}$$

Corollary. If we apply the example 3.5 to $A > 0$,

$$C^*AC = \begin{bmatrix} \pm 1 & & & & \\ & \ddots & & & \\ & & \pm 1 & & \\ & & & \ddots & \\ & & & & 0 \\ & & & & & \ddots \end{bmatrix} \text{ is still positive definite } \implies C^*AC = I$$

Theorem 3.12 (Sylvester's law of inertia). J. J. Sylvester (1814–1897)

Let $A \in \mathbb{C}^{n \times n}$ be Hermitian. $C \in \text{GL}(n, \mathbb{C})$ by the algorithm such that

$$C^*AC = \begin{bmatrix} \pm 1 & & & & & \\ & \ddots & & & & \\ & & \pm 1 & & & \\ & & & -1 & & \\ & & & & \ddots & \\ & & & & & -1 \\ & & & & & & 0 \\ & & & & & & & \ddots \\ & & & & & & & & 0 \end{bmatrix}$$

Then the number of $+1$, -1 and zeros is uniquely determined (it does not depend on the order to the operands).

Proof. C is invertible, hence

$$\text{rank}(A) = \text{rank} \begin{bmatrix} +1 & & & & & & & \\ & \ddots & & & & & & \\ & & +1 & & & & & \\ & & & -1 & & & & \\ & & & & \ddots & & & \\ & & & & & -1 & & \\ & & & & & & 0 & \\ & & & & & & & \ddots \\ & & & & & & & & 0 \end{bmatrix}$$

Let r be the number of $+1$ and s be the number of -1 . The number of $+1$ and -1 is uniquely determined.

Hence, it suffices to show that the number r of $+1$ is uniquely defined.

Let \tilde{C} be another matrix such that

$$\tilde{C}^* A \tilde{C} = \begin{bmatrix} \pm 1 & & & & & & & \\ & \ddots & & & & & & \\ & & \pm 1 & & & & & \\ & & & -1 & & & & \\ & & & & \ddots & & & \\ & & & & & -1 & & \\ & & & & & & 0 & \\ & & & & & & & \ddots \\ & & & & & & & & 0 \end{bmatrix}$$

with \tilde{r} ones and \tilde{s} minus ones.

It suffices to show that $r \leq \tilde{r}$. We know $r + s = \tilde{r} + \tilde{s}$.

C is an invertible matrix, hence a basis change. In this new basis $B' = \{b_1, \dots, b_n\}$, it holds that

$$x^* A x = \overline{x^T} A x = \overline{\Phi_B(x)^T} \cdot D \cdot \Phi_B(x)$$

$$\begin{aligned} A &= (C^*)^{-1} D C^{-1} \\ \overline{x^T} A x &= \overline{x^T} (C^*)^{-1} D \underbrace{C^{-1} x}_{\tilde{C}^{-1} x} \end{aligned}$$

Equivalently, \tilde{C} is a basis change to basis \tilde{B} such that $x^* A x = \Phi_{\tilde{B}}(x)^* \tilde{D} \Phi_{\tilde{B}}(x)$. For

$$x \in \mathcal{L}(\{b_1, \dots, b_r\}) \setminus \{0\},$$

$$\Phi_B(x) = \begin{pmatrix} \xi_1 \\ \vdots \\ \xi_r \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

$$\implies x^*Ax = \Phi_B(x)^*D\Phi_B(x)$$

$$= (\bar{\xi}_1, \dots, \bar{\xi}_r, 0, \dots, 0) \begin{bmatrix} +1 & & & & & & \\ & \ddots & & & & & \\ & & +1 & & & & \\ & & & -1 & & & \\ & & & & \ddots & & \\ & & & & & -1 & \\ & & & & & & 0 \\ & & & & & & & \ddots \\ & & & & & & & & 0 \end{bmatrix} \begin{pmatrix} \xi_1 \\ \vdots \\ \xi_r \\ 0 \\ \vdots \\ 0 \end{pmatrix} = \sum_{i=1}^r |\xi_i|^2 > 0$$

$$\text{On the other hand, } \forall x \in \mathcal{L}(\tilde{b}_{\tilde{r}+1}, \dots, \tilde{b}_n).$$

$$\Phi_{\tilde{B}}(x) = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ \tilde{\xi}_{\tilde{r}+1} \\ \vdots \\ \tilde{\xi}_n \end{pmatrix}$$

$$x^*Ax = \Phi_{\tilde{B}}(x)^*\tilde{D}\Phi_{\tilde{B}}(x)$$

$$= (0, \dots, 0, \tilde{\xi}_{\tilde{r}+1}, \dots, \tilde{\xi}_n) \begin{bmatrix} +1 & & & & & & \\ & \ddots & & & & & \\ & & +1 & & & & \\ & & & -1 & & & \\ & & & & \ddots & & \\ & & & & & -1 & \\ & & & & & & 0 \\ & & & & & & & \ddots \\ & & & & & & & & 0 \end{bmatrix} \begin{pmatrix} 0 \\ \vdots \\ 0 \\ \tilde{\xi}_{\tilde{r}+1} \\ \vdots \\ \tilde{\xi}_n \end{pmatrix} \leq 0$$

$$\implies \mathcal{L}(b_1, \dots, b_r) \cap \mathcal{L}(\tilde{b}_{\tilde{r}+1}, \dots, \tilde{b}_n) = \{0\}$$

$$\text{dimension } r + (n - \tilde{r}) \leq n \implies r \leq \tilde{r}$$

□

This lecture took place on 2018/04/16.

$$A = A^*$$

Conjugate complex. The important question: When does it hold that

$$A > 0$$

Hence

$$\forall x \in \mathbb{C}^n : x^* A x \geq 0$$

$$A > 0 \text{ if } x^* A x > 0 \forall x \neq 0$$

$$(x^*)_i = \bar{x}_i$$

$$\exists C \in GL(n, \mathbb{C}) \text{ such that}$$

$$C^* A C \underset{\text{congruence}}{=} \begin{bmatrix} +1 & & & & & & \\ & \ddots & & & & & \\ & & +1 & & & & \\ & & & -1 & & & \\ & & & & \ddots & & \\ & & & & & -1 & \\ & & & & & & 0 & \ddots \\ & & & & & & & & 0 \end{bmatrix}$$

where the number of +1 is r (see Sylvester's Law of inertia).

Definition 3.9. If $A = A^*$ is congruent to

$$\begin{bmatrix} +1 & & & & & & \\ & \ddots & & & & & \\ & & +1 & & & & \\ & & & -1 & & & \\ & & & & \ddots & & \\ & & & & & -1 & \\ & & & & & & 0 & \ddots \\ & & & & & & & & 0 \end{bmatrix}$$

with r occurring +1s and s occurring -1s.

Then $\text{ind}(A) := r$ is called index of A . $\text{sign}(A) := r - s$ is called signature of A .

Corollary. 1. $A > 0 \iff A \hat{=} I \iff \text{ind}(A) = n$

$$2. A \geq 0 \iff \text{ind}(A) = \text{sign}(A) = \text{rank}(A)$$

$$3. A \hat{=} B \iff \text{ind}(A) = \text{ind}(B) \wedge \text{sign}(A) = \text{sign}(B)$$

It is left as an exercise to the reader that congruence is an equivalence relation.

$$1. I \cdot A \cdot I = A$$

$$2. A \hat{=} B \implies C^*AC = B \implies A = (C^*)^{-1}BC^{-1} = (C^{-1})^*BC^{-1} \implies B \hat{=} A$$

$$3. C_1^*A_1C_1 = A_2 \wedge C_2^*A_2C_2 = A_3 \implies \underbrace{C_2^*C_1^*A_1C_1C_2}_{=(C_1C_2)^*A_1(C_1C_2)} = A_3 \implies A_1 \hat{=} A_3$$

Furthermore it will be shown in the practicals that $A > 0 \iff \exists CA = C^*C$

Remark 3.8 (Idea).

$$\det(C^*AC) = \det \begin{bmatrix} +1 & & & & & & & \\ & \ddots & & & & & & \\ & & +1 & & & & & \\ & & & -1 & & & & \\ & & & & \ddots & & & \\ & & & & & -1 & & \\ & & & & & & 0 & \\ & & & & & & & \ddots \\ & & & & & & & & 0 \end{bmatrix}$$

$$\det(C^*) \det(A) \det(C) = \begin{cases} 0 & \text{if } \text{rank}(A) < n \\ (-1)^{\text{number of } -1} & \end{cases}$$

$$\overline{\det(C)} \det(A) \det(C)$$

If $A > 0$,

$$|\det(C)|^2 \cdot \det(A) = 1 \implies \det(A) > 0$$

Lemma 3.3. 1.

$$\det(C^*) = \overline{\det(C)}$$

2.

$$A = A^* \implies \det(A) \in \mathbb{R}$$

3.

$$A = A^*, B = B^*, A \hat{=} B \implies \text{sign } \det(A) = \text{sign } \det(B)$$

4.

$$A > 0 \implies \det(A) > 0$$

but not the other way around:

$$\det \begin{bmatrix} -1 & \\ & -1 \end{bmatrix} = 1$$

Proof. 1.

$$\begin{aligned} \det(C^*) &= \sum_{\sigma \in \Sigma_n} (-1)^\sigma \underbrace{(C^*)_{1\sigma(1)} \dots (C^*)_{n\sigma(n)}}_{\overline{C_{\sigma(1)1}} \quad \overline{C_{\sigma(n)n}}} \\ &= \sum_{\sigma} (-1)^\sigma C_{\sigma(1)1} \dots C_{\sigma(n)n} = \overline{\det(C)} \end{aligned}$$

2. immediate

$$3. A\hat{B} \implies C^*AC = B$$

$$\begin{aligned} \det(C^*AC) &= \det(B) \\ \underbrace{|\det(C)|^2}_{>0} \cdot \det(A) &= \det(B) \end{aligned}$$

$$4. A \hat{=} I \implies \text{sign } \det(A) = \text{sign } \det(I) = 1$$

□

Definition 3.10. Let $A \in \mathbb{K}^{m \times n}$, $r \leq \min\{m, n\}$.

$$I = \underbrace{\{i_1 < \dots < i_r\}}_{\subseteq \{1, \dots, m\}} \quad J = \underbrace{\{j_1 < \dots < j_r\}}_{\subseteq \{1, \dots, n\}}$$

Then

$$[A]_{I,J} = \begin{bmatrix} a_{i_1 j_1} & a_{i_1 j_2} & \dots & a_{i_1 j_r} \\ a_{i_2 j_1} & a_{i_2 j_2} & \dots & a_{i_2 j_r} \\ \vdots & \vdots & \ddots & \vdots \\ a_{i_r j_1} & a_{i_r j_2} & \dots & a_{i_r j_r} \end{bmatrix}$$

is called minor of A.

Example 3.11. Let $r = 1$, $I = \{i_1\}$, $J = \{j_1\}$, $[A]_{\{i_1\}, \{j_1\}} = a_{i_1 j_1}$.

Definition 3.11. If $m = n$ with $I = \{1, \dots, r\}$ and $J = \{1, \dots, r\}$, then

$$\begin{bmatrix} a_{11} & a_{12} & \dots & a_{1r} \\ \vdots & \vdots & \ddots & \vdots \\ a_{r1} & a_{r2} & \dots & a_{rr} \end{bmatrix}$$

the first minor of A (Hauptminoren).

$$A < 0 \iff (-A) > 0$$

$$\det(\lambda A) = \lambda^n \det(A)$$

Theorem 3.13. Let $A = A^*$, then it holds that

1. $A > 0 \iff$ all first minors satisfy $\det(A_r) > 0$
2. $A < 0 \iff (-1)^r \det(A_r) > 0 \forall r \in \{1, \dots, n\}$

Proof. Direction \implies

For $r = n$: $\det(A_r) = \det(A) > 0$. It suffices to show: the submatrices

$$A_r = \begin{bmatrix} a_{11} & a_{12} & \dots & a_{1r} \\ \vdots & & & \\ a_{r1} & & & a_{rr} \end{bmatrix}$$

are positive definite. Hence, $\forall x \in \mathbb{C}^r$ with $x \neq 0$: $x^* A_r x > 0$.

$$\begin{aligned} x \in \mathbb{C}^r \setminus \{0\} : x^* A_r x &= \begin{bmatrix} x^* & 0 \\ \underbrace{ 0}_{n-r} \end{bmatrix} \cdot A \cdot \begin{bmatrix} x \\ 0 \end{bmatrix} > 0 \\ &= [x^* 0] \begin{bmatrix} A_r & * \\ \vdots & \vdots \\ * & \dots * \end{bmatrix} \begin{bmatrix} x \\ 0 \end{bmatrix} \end{aligned}$$

Remark: every submatrix $\begin{bmatrix} a_{i_1 i_1} & \dots & a_{i_1 i_r} \\ \vdots & \ddots & \vdots \\ a_{i_r i_1} & \dots & a_{i_r i_r} \end{bmatrix}$ of a positive definite matrix is positive definite.

Direction \impliedby

Assume all first minors $\det(A_r) > 0$.

We use complete induction:

Let $n = 1$ and $r = 1$ $A = [a_{11}]$ and $\det(A_1) = a_{11}$. $A > 0 \iff a_{11} > 0$.

Consider $n \rightarrow n + 1$ Assume all first minors are greater 0. Then all first minors of matrix A_{n-1} are greater 0.

□

$$\begin{aligned}
A' &= \begin{bmatrix} C & \vdots 0 \vdots \\ \dots 0 \dots & 1 \end{bmatrix} A \begin{bmatrix} C & \\ & 1 \end{bmatrix} \\
&= \begin{bmatrix} C^* & \vdots 0 \vdots \\ \dots 0 \dots & 1 \end{bmatrix} \begin{bmatrix} A_{n-1} & a_{1,n} \\ & a_{2,n} \\ & \vdots \\ & a_{n-1,n} \\ \overline{a_{n,1}} & \overline{a_{n,2}} & \dots & a_{nn} \end{bmatrix} \begin{bmatrix} C & \vdots 0 \vdots \\ \dots 0 \dots & 1 \end{bmatrix} \\
&= \begin{bmatrix} I & a_{1,n} \\ & a_{2,n} \\ & \vdots \\ \overline{a_{1,n}} & \overline{a_{2,n}} & \dots & \overline{a_{n-1,n}} & a_{n,n} \end{bmatrix} \\
C' &= \begin{bmatrix} 1 & 0 & -a_{1,n} \\ & \ddots & -a_{2,n} \\ & & \vdots \\ & & -a_{n-1,n} \\ 0 & & 1 \end{bmatrix} = \left[\begin{array}{c|c} I & -b \\ \hline 0 & 1 \end{array} \right]
\end{aligned}$$

with

$$b = \begin{bmatrix} a_{11} \\ a_{21} \\ \vdots \\ a_{n-1,n} \end{bmatrix}$$

$$(C')^* A' C' = \left[\begin{array}{c|c} I & 0 \\ \hline -b^* & 1 \end{array} \right] \left[\begin{array}{c|c} I & b \\ \hline b^* & a_{n,n} \end{array} \right] \text{TODO}$$

$$\Rightarrow A \hat{=} A' \hat{=} \begin{bmatrix} I & 0 \\ 0 & -b^* b + a_n \end{bmatrix}$$

$$\exists C'' = C \cdot C'$$

such that

$$(C'')^* A C'' = \left[\begin{array}{c|c} I & 0 \\ \hline 0 & a_{n,n} - b^* b \end{array} \right]$$

$$\det(A) \cdot |\det(C'')|^2 = \det \begin{bmatrix} I & 0 \\ 0 & a_{n,n} - b^* b \end{bmatrix} = a_{n,n} - b^* b > 0 \Rightarrow \begin{bmatrix} I & 0 \end{bmatrix}$$

Back to the scalar product:

Definition 3.12. 1. (a) A vector space with a positive definite inner product is called Euclidean space ($K = \mathbb{R}, \dim < \infty$) or unitary space ($K = \mathbb{C}$)
(b) Hilbert space if $\dim = \infty$.
David Hilbert (1862–1943)

$$\|v\| = \sqrt{\langle v, v \rangle}$$

$$\|\lambda v\| = |\lambda| \cdot \|v\|$$

$$\text{in } \mathbb{R}^2: \langle a, b \rangle = \|a\| \|b\| \cos \varphi$$

2. An element $v \in V$ is called **normed** if $\|v\| = 1$ (if not, then $\frac{v}{\|v\|}$ is normed)
3. Let $v, w \in V \setminus \{0\}$. Then the angle spanned between v and w is the angled $\varphi \in [0, \phi]$ such that $\cos \varphi = \frac{\Re \langle v, w \rangle}{\|v\| \|w\|}$
4. Two vectors $v, w \in V$ are **orthogonal** ($v \perp w$) if $\langle v, w \rangle = 0$ (hence $\varphi = \frac{\pi}{2}$)

Theorem 3.14. 1. $\|v + w\|^2 = \|v\|^2 + \|w\|^2 + 2 \|v\| \|w\| \cos \varphi$ (Law of cosines)
2. if $v \perp w$: $\|v + w\|^2 = \|v\|^2 + \|w\|^2$ (Pythagorean Theorem)
3. $\|v + w\|^2 + \|v - w\|^2 = 2(\|v\|^2 + \|w\|^2)$ (Parallelogram Law)

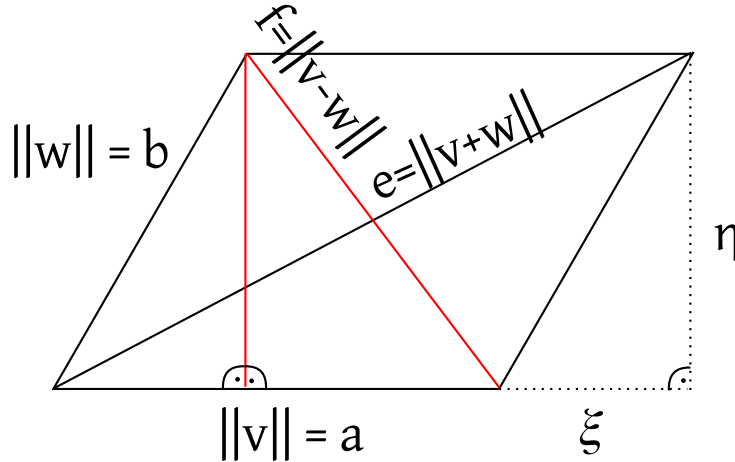


Figure 4: Geometrical proof of Theorem 3.14

$$\begin{aligned}
e^2 + f^2 &= 2(a^2 + b^2) \\
e^2 &= (a + \xi)^2 + \eta^2 \\
f^2 &= (a - \xi)^2 + \eta^2 \\
e^2 + f^2 &= (a + \xi)^2 + (a - \xi)^2 + 2\eta^2 \\
&= a^2 + \xi^2 + a^2 + \xi^2 + 2\eta^2 = 2a^2 + 2b^2
\end{aligned}$$

Proof. 1.

$$\begin{aligned}
\|v + w\|^2 &= \langle v + w, v + w \rangle = \langle v, v \rangle + \langle v, w \rangle + \langle w, v \rangle + \langle w, w \rangle \\
&= \|v\|^2 + \langle v, w \rangle + \overline{\langle v, w \rangle} + \|w\|^2 \\
&= \|v\|^2 + 2 \underbrace{\Re \langle v, w \rangle}_{\cos \varphi \cdot \|v\| \cdot \|w\|} + \|w\|^2
\end{aligned}$$

2. immediate, $\langle v, w \rangle = 0$

3.

$$\begin{aligned}
\|v + w\|^2 + \|v - w\|^2 &= \|v\|^2 + \|w\|^2 + 2\Re \langle v, w \rangle + \|v\|^2 + \|-w\|^2 + 2\Re \langle v, -w \rangle \\
&= 2\|v\|^2 + 2\|w\|^2 + 0
\end{aligned}$$

Other norms:

$$\begin{aligned}
\left\| \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} \right\|_1 &= \sum_1^n |x_i| \\
\left\| \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} \right\|_\infty &= \max |x_i|
\end{aligned}$$

□

Remark 3.9. You can show (von Neumann did): A norm on \mathbb{R}^n satisfies the Parallel-ogram Law iff \exists a scalar product on \mathbb{R}^n such that $\|v\| = \sqrt{\langle v, v \rangle}$

Definition 3.13. Let (v, \langle, \rangle) be a vector space with scalar product. A family $(v_i)_{i \in I} \subseteq V$ is called

orthogonal if $\forall i \neq j : \langle v_i, v_j \rangle = 0$

orthonormal if additionally $\|v_i\| = 1 \forall i$

hence $\forall i, j : \langle v_i, v_j \rangle = \delta_{ij}$

orthonormal basis if they are orthonormal and give a basis of V .

Example 3.12. 1. Canonical basis in \mathbb{R}^n in regards of the standard scalar product

$$\langle e_i, e_j \rangle = \delta_{ij}$$

2. Fourier $\left\{ \sqrt{2} \sin 2\pi x, \sqrt{2} \sin 4\pi x, \dots, \sqrt{2} \sin(2k\pi x), \dots \right\}$ with $k \in \mathbb{N}$ union with $\left\{ \sqrt{2} \cos 2\pi x, \sqrt{2} \cos 4\pi x, \dots \right\} \cup \{g\}$ on $C[0, 1]$.

$$\langle f, g \rangle = \int_0^1 f(x)g(x) dx$$

And this is wrong unless we redefine the term basis (not every function is built using the sine/cosine). A basis here is every function:

$$f(x) = \sum_{k=0}^{\infty} a_k \cos 2k\pi x + \sum_{k=1}^{\infty} b_k \sin 2k\pi x$$

And this is wrong as well unless we define equality more precisely (in the usual sense, it is wrong). Lebesgue did this later.

Remark 3.10. For JPEG compression, Fourier transformation is applied. Hence, we consider the music (amplitudes) as f and

$$f(x) = \sum_{k=0}^n a_k \cos 2k\pi x + \sum_{k=1}^n b_k \sin 2k\pi x$$

with n finite.

Theorem 3.15. Let $(v_i)_{i \in I} \subseteq V$, $v_i \neq 0 \forall i$

1. $(v_i)_{i \in I}$ orthogonal $\iff \left(\frac{v_i}{\|v_i\|} \right)_{i \in I}$ is orthonormal
2. $(v_i)_{i \in I}$ is orthogonal, then $(v_i)_{i \in I}$ is linear independent.

This lecture took place on 2018/04/18.

$$\cos \varphi = \frac{\langle v, w \rangle}{\|v\| \|w\|}$$

$$v \perp w \iff \langle v, w \rangle = 0$$

$(v_i)_{i \in I}$ orthogonal if $\langle v_i, v_j \rangle = 0 \forall i \neq j$

orthonormal: $\langle v_i, v_j \rangle = \delta_{ij}$.

Proof of Theorem 3.15. Let $\sum_{k=1}^n \lambda_k v_{i_k} = 0$.

$$\implies 0 = \left\langle \sum_{k=1}^n \lambda \cdot v_{i_k}, v_i \right\rangle = \sum_{k=1}^n \lambda_k \langle v_{i_k}, v_i \rangle$$

$\forall l \in \{1, \dots, n\} : \text{Let } i = i_l.$

$$\begin{aligned} i_l &= \sum_{k=1}^n \lambda_k \left\langle \underbrace{v_{i_k}, v_{i_l}} \right\rangle \\ &= \begin{cases} 0 & i_k \neq i_l \\ \|v_{i_l}\|^2 & i_k = i_l \end{cases} \\ &= \lambda_l \cdot \|v_{i_l}\|^2 \implies \lambda_l = 0 \end{aligned}$$

□

Theorem 3.16. Let $B = (b_1, \dots, b_n)$ is an orthonormal basis of a finite dimensional vector space over \mathbb{K} . For $v \in V$, let $\Phi_B(v) = \begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_n \end{pmatrix}$. For $w \in V$, let $\Phi_B(w) = \begin{pmatrix} \mu_1 \\ \vdots \\ \mu_n \end{pmatrix}$.

1. $\lambda_i = \langle v, b_i \rangle$
2. $\langle v, w \rangle = \sum_{i=1}^n \lambda_i \overline{\mu_i}$

Proof. 1.

$$\begin{aligned} \langle v, b_i \rangle &= \left\langle \sum_{j=1}^n \lambda_j b_j, b_i \right\rangle \\ &= \sum_{j=1}^n \lambda_j \cdot \underbrace{\langle b_j, b_i \rangle}_{=\delta_{ji}} \\ &= \lambda_i \end{aligned}$$

2.

$$\begin{aligned} \langle v, w \rangle &= \left\langle \sum_{i=1}^n \lambda_i b_i, \sum_{j=1}^n \mu_j b_j \right\rangle \\ &= \sum_{i=1}^n \lambda_i \sum_{j=1}^n \overline{\mu_j} \underbrace{\langle b_i, b_j \rangle}_{\delta_{ij}} \\ &= \sum_{i=1}^n \lambda_i \cdot \overline{\mu_i} \end{aligned}$$

Compare: B is an arbitrary basis:

$$\langle v, w \rangle = \Phi_B(v)^T \cdot A \cdot \overline{\Phi_B(w)}$$

$$a_{ij} = \langle b_i, b_j \rangle = \delta_{ij}$$

$$A = I$$

$$\rightarrow \langle v, w \rangle = \Phi_B(v)^T \cdot \overline{\Phi_B(w)}$$

□

Definition 3.14. Let V be a vector space with a scalar product. Let $v \in V$, then

$$v^\perp = \{w \in V \mid \langle v, w \rangle = 0\}$$

For $M \subseteq V : M^\perp = \{w \in V \mid \forall u \in M : \langle u, w \rangle = 0\}$ is called orthogonal complement of v or orthogonal complement of M

Compare with Figure 5

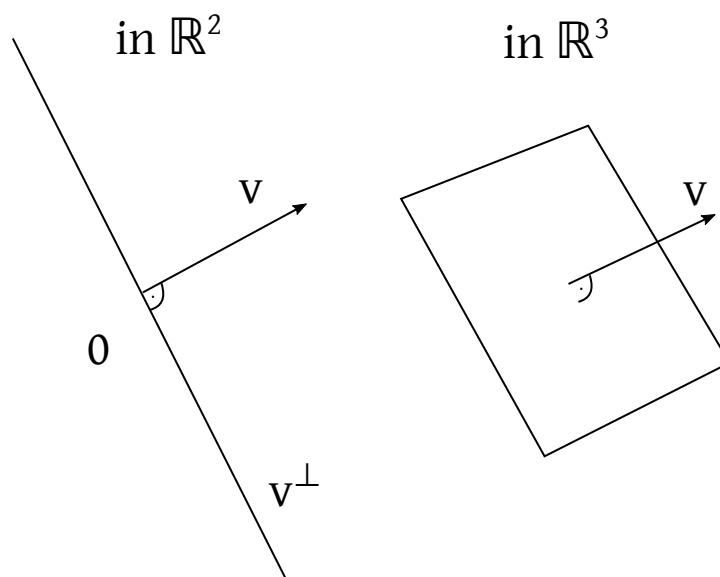


Figure 5: Orthogonal complement

in \mathbb{R}^n :

$$\{w \mid \langle v, w \rangle = 0\}$$

$$= \left\{ \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \middle| \sum_1^n a_i x_i = 0 \right\}$$

$$\text{if } v = \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix}.$$

Theorem 3.17. *Let V be a vector with scalar product. $M, N \subseteq V$ are partitions.*

1. M^\perp is a subspace.
2. $M \subseteq N \implies N^\perp \subseteq M^\perp$
 $(M_1 \cup M_2)^\perp = M_1^\perp \cap M_2^\perp$
3. $\{0\}^\perp = V$
4. $V^\perp = \{0\}$
5. $M \cap M^\perp \subseteq \{0\}$
6. $M^\perp = \mathcal{L}(M)^\perp$
7. $M \subseteq (M^\perp)^\perp$

Proof. 1.

$$v^\perp = \{w \in V \mid \langle v, w \rangle = 0\}$$

$$T_v : V \rightarrow \mathbb{K} \text{ (linear functional)}$$

$$w \mapsto \langle w, v \rangle$$

$$v^\perp = \{w \mid T_v(w) = 0\} = \ker T_v$$

is a subspace.

$$\begin{aligned} M^\perp &= \bigcap_{v \in M} v^\perp \\ &= \bigcap_{v \in M} \ker(T_v) \end{aligned}$$

is a subspace.

2. $M \subseteq N \implies N^\perp \subseteq M^\perp$

$$\begin{aligned} (M_1 \cup M_2)^\perp &= \{w \mid \forall v \in M_1 : \langle w, v \rangle = 0 \wedge \forall v \in M_2 : \langle w, v \rangle = 0\} \\ &= M_1^\perp \cap M_2^\perp \end{aligned}$$

3. trivial: $\forall v \in V : \langle v, 0 \rangle = 0$

4. Let $w \in V$ such that $\langle w, v \rangle = 0 \forall v \in V$. Especially for $v = w$.

$$\begin{aligned} \implies \underbrace{\langle w, w \rangle}_{\|w\|^2} = 0 &\implies w = 0 \\ \implies V^\perp &= \{0\} \end{aligned}$$

5. Let $w \in M \cap M^\perp$, hence

$$\begin{aligned} \forall v \in M : \langle w, v \rangle &= 0 \\ w \in M &\implies \langle w, w \rangle = 0 \\ &\implies w = 0 \\ \text{or } M \cap M^\perp &= \varphi \end{aligned}$$

6.

$$M \subseteq \mathcal{L}(M) \underbrace{\implies}_{\text{by point (2.)}} \mathcal{L}(M)^\perp \subseteq M^\perp$$

Show that: $M^\perp \subseteq \mathcal{L}(M)^\perp$. Hence, $\forall v \in M^\perp \implies v \in \mathcal{L}(M)^\perp$. Let $v \in M^\perp$, $w \in \mathcal{L}(M)$.

$$\exists w_1, \dots, w_n \in M : \exists \lambda_1, \dots, \lambda_n \in \mathbb{K} : w = \sum_{i=1}^n \lambda_i w_i$$

$$\begin{aligned} \langle w, v \rangle &= \left\langle \sum_{i=1}^n \lambda_i w_i, v \right\rangle \\ &\underbrace{=}_{\text{by linearity in 1st argument}} \sum_{i=1}^n \lambda_i \underbrace{\left\langle \underbrace{w_i}_{\in M}, \underbrace{v}_{\in M^\perp} \right\rangle}_{=0} = 0 \\ \implies v &\perp w \quad \forall w \in \mathcal{L}(M) \end{aligned}$$

7. Show that $\forall v \in M : v \in (M^\perp)^\perp$. Hence, $\forall w \in M^\perp : v \perp w$

$$\begin{aligned} M^\perp &= \{w \mid \forall v \in M : v \perp w\} \\ \implies \forall v \in M \forall w \in M^\perp : v &\perp w \implies \forall w \in M^\perp \forall v \in M, v \in W^\perp \\ \implies \forall v \in M : v &\in \bigcap_{w \in M^\perp} w^\perp = (M^\perp)^\perp \end{aligned}$$

□

Corollary. Let $U \subseteq V$ be a subspace. By Theorem 3.17 (1), U^\perp is a subspace and $U \cap U^\perp = \{0\}$ because of Theorem 3.17 (5),

$$U + U^\perp \text{ is direct sum}$$

in \mathbb{R}^n : $U + U^\perp = \mathbb{R}^n$.

Remark 3.11. If $\dim(V) = \infty$, it must not hold that $U + U^\perp = V$.

Example 3.13.

$$V = l^2 = \left\{ (x_n)_{n \in \mathbb{N}} \mid \sum |x_n|^2 < \infty \right\}$$

$$\begin{aligned} U &= \mathcal{L}((e_i)_{i \in \mathbb{N}}) \\ &= \{ (x_n)_{n \in \mathbb{N}} \mid x_n = 0 \text{ except for finite many } n \} \end{aligned}$$

$$U^\perp = \{ e_i \mid i \in \mathbb{N} \}^\perp = \left\{ (x_n)_{n \in \mathbb{N}} \mid \underbrace{\langle (x_n)_{n \in \mathbb{N}}, e_i \rangle}_{= \langle (x_n)_{n \in \mathbb{N}} \mid \forall i \in \mathbb{N} : x_i = 0 \rangle = \langle 0 \rangle} = 0 \forall i \in \mathbb{N} \right\}$$

$$\langle (x_n)_n, (y_n)_n \rangle = \sum_{n=1}^{\infty} x_n \overline{y_n}$$

$$\implies U^\perp = \{0\}$$

$$\text{but } U + U^\perp \neq l_2$$

$U + U^\perp$ is a direct sum.

$$v \in U + U^\perp$$

$$U \xrightarrow{\pi_U} U$$

$$U^\perp \xrightarrow{\pi_{U^\perp}} U^\perp$$

Every $v \in U + U^\perp$ has a unique decomposition:

$$v = u + w \quad u \in U, w \in U^\perp$$

Definition 3.15. Let V be a vector space. A subset $K \subseteq V$ is called convex⁸ if

$$\forall \lambda \in [0, 1] : \forall x, y \in K : \lambda x + (1 - \lambda)y \in K$$

Example 3.14. Subspaces are convex.

1.

$$U \subseteq V : \forall x, y \in U \forall \lambda, \mu : \lambda x + \mu y \in U$$

$$\text{Especially: } \lambda \in [0, 1], \mu = 1 - \lambda$$

⁸Wide-sighted people with glasses use a glass with convex curvature.

2. Let $(V, \|\cdot\|)$ be a normed space.

$$B_{\|\cdot\|}(0, 1) = \left\{ x \in V \mid \underbrace{\|x\|}_{\text{unit circle}} < 1 \right\}$$

We discussed three different norms so far. In \mathbb{R}^2 with $\|\cdot\|_2$ (Euclidean norm), the unit circle is a circle of radius 1. In \mathbb{R}^2 with $\left\| \begin{pmatrix} x \\ y \end{pmatrix} \right\|_\infty = \max(|x|, |y|)$ (infinity norm), the unit circle is a square from $(-1, -1)$ to $(1, 1)$. This square contains the circle of radius 1. In \mathbb{R}^2 with $\left\| \begin{pmatrix} x \\ y \end{pmatrix} \right\|_1 = |x| + |y|$ (Manhattan norm), the unit circle is a square rotated by 45 degrees from $(-1, 0)$ to $(1, 0)$. It also contains the circle of radius 1.

Let $x, y \in B(0, 1)$, hence $\|x\| < 1, \|y\| < 1$.

$$\begin{aligned} \|\lambda x + (1 - \lambda)y\| &\stackrel{\text{by triangle ineq.}}{\leq} \lambda \|x\| + (1 - \lambda)\|y\| \\ &< \lambda + (1 - \lambda) \\ &= 1 \\ &\implies \lambda x + (1 - \lambda)y \in \mathcal{B}(0, 1) \end{aligned}$$

3. Translation in a convex set gives a convex set. Let K be convex. $K' = x_0 + K = \{x_0 + z \mid z \in K\}$ Let $x', y' \in K' \implies x' = x_0 + x$ and $y' = x_0 + y$.

$$\begin{aligned} \implies \lambda x' + (1 - \lambda)y' &= \lambda \cdot (x_0 + x) + (1 - \lambda)(x_0 + y) \\ &= x_0 + \underbrace{\lambda x + (1 - \lambda)y}_{\in K} \end{aligned}$$

Especially: linear manifolds are convex. $B(x_0, 1)$ is convex.

4. $K \subseteq V$ convex. $f : V \rightarrow W$ is linear. $\implies f(K)$ is convex.

Optimization: Given a set M and a function $f : M \rightarrow \mathbb{R}$. Find $y \in M$ such that $f(y)$ is minimal.

Find $y \in M$ such that $d(x_0, y)$ is minimal. Compare with Figure 6.

Now if M is convex (consider M convex in $(\mathbb{R}^n, \|\cdot\|_2)$), there exists a unique element $y \in M$ such that $\|x_0 - y\|$ is minimal.

Finite elements (in computational mathematics) is the same idea.

Theorem 3.18. $(V, \langle \cdot, \cdot \rangle)$ is a vector space with scalar product. $K \subseteq V$ is convex. Let $x \in V$ be given. Let $y_0 \in K$. Then the following statements are equivalent:

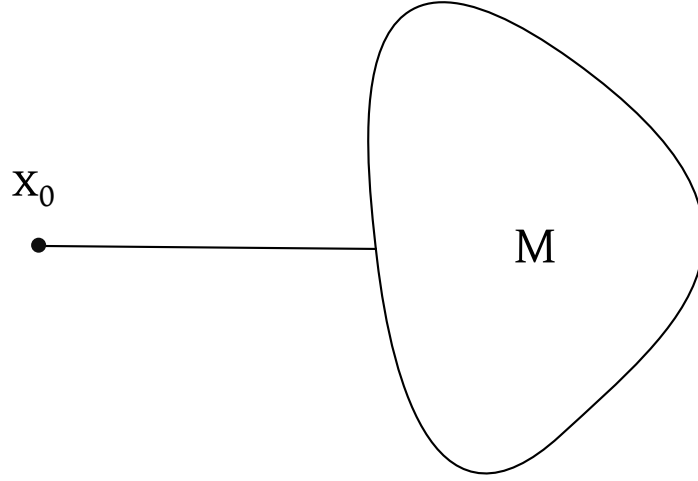


Figure 6: A generic optimization problem

1. $\forall y \in K : \|x - y_0\| \leq \|x - y\|$
2. $\forall y \in K : \Re \langle x - y_0, y - y_0 \rangle \leq 0$
3. $\forall y \in K \setminus \{y_0\} : \|x - y_0\| < \|x - y\|$

Compare with Figure 7. In the special case if $K = U$ is a subspace, then the following statement is given (equivalent to statement 2)

$$2'. \forall y \in U : \langle x - y_0, y - y_0 \rangle = 0$$

Proof $1 \rightarrow 2$. Let $y \in K : 1 > \varepsilon > 0$.

$$y_\varepsilon = \underbrace{y_0 + \varepsilon(y - y_0)}_{\varepsilon y + (1-\varepsilon)y_0 \text{ because of convexity}} \in K$$

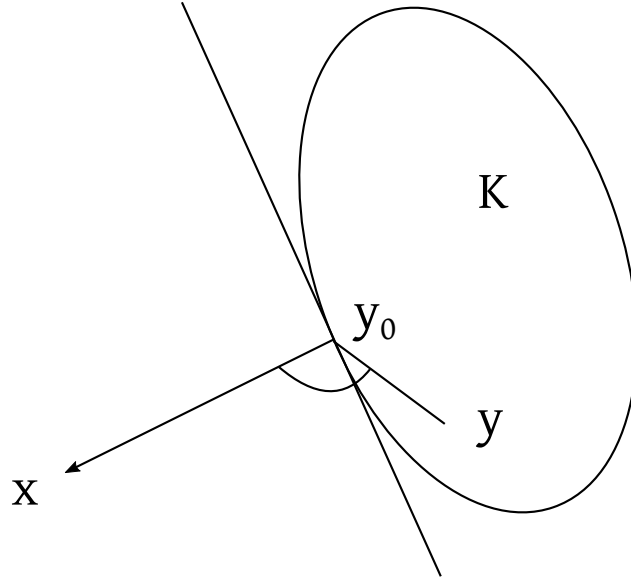


Figure 7: Optimization on a convex set

$$\begin{aligned}
\forall \varepsilon \in]0, 1[: \quad & \|x - y_0\|^2 \leq \|x - y_\varepsilon\|^2 \\
& = \|x - (y_0 + \varepsilon(y - y_0))\|^2 \\
& = \|(x - y_0) - \varepsilon(y - y_0)\|^2 \\
& = \|x - y_0\|^2 - 2\varepsilon \Re \langle x - y_0, y - y_0 \rangle + \varepsilon^2 \|y - y_0\|^2 \\
\Rightarrow \quad & \forall 0 < \varepsilon < 1 : 0 \leq -2\varepsilon \Re \langle x - y_0, y - y_0 \rangle + \varepsilon^2 \|y - y_0\|^2 \\
& = \varepsilon \cdot \left(-2\Re \langle x - y_0, y - y_0 \rangle + \varepsilon \|y - y_0\|^2 \right) \\
& \xRightarrow{\varepsilon \rightarrow 0} 0 \leq -2\Re \langle x - y_0, y - y_0 \rangle
\end{aligned}$$

2 \rightarrow 3.

$$\begin{aligned}
\|x - y\|^2 &= \|(x - y_0) + (y_0 - y)\|^2 \\
&= \|(x - y_0) - (y - y_0)\|^2 \\
&= \|x - y_0\|^2 + \|y - y_0\|^2 - \underbrace{2\Re \langle x - y_0, y - y_0 \rangle}_{\geq 0} \\
&\geq \|x - y_0\|^2 + \|y - y_0\|^2 \\
&> \|x - y_0\|^2 \\
&y \neq y_0
\end{aligned}$$

3 \rightarrow 1. trivial.

2 \rightarrow 2'. Consider $K = U$ is subspace.

$$\forall y \in Y : \Re \langle x - y_0, y - y_0 \rangle \leq 0$$

U is a subspace.

$$\{y - y_0 \mid y \in U\} = \{z \mid z \in U\} = U - y_0$$

$$\left. \begin{array}{l} \forall z \in U : \Re \langle x - y_0, z \rangle \leq 0 \\ \forall z \in U : \Re \langle x - y_0, -z \rangle \leq 0 \end{array} \right\} \implies \forall z \in U : \Re \langle x - y_0, z \rangle = 0$$

Case $K = \mathbb{C}$:

$$\begin{aligned}
&i \cdot U = U \\
\implies &z \in U : \Re \langle x - y_0, iz \rangle = 0 \\
&\Re i \langle x - y_0, z \rangle = \Im \langle x - y_0, z \rangle
\end{aligned}$$

□

Corollary. Let (V, \langle, \rangle) be a vector space.

1. $K \subseteq V$ is convex, $x \in V$. Then the optimization problem

$$\left\{ \begin{array}{l} \|x - y\| = \min! \\ y \in K \end{array} \right.$$

has at most one solution.

2. If $K = U$ subspace, then there exists at most one $y_0 \in U$ such that $x - y_0 \in U^\perp$.

This lecture took place on 2018/04/23.

Orthonormalbasis:

$$\langle b_i, b_j \rangle = \delta_{ij}$$

$$v = \sum \lambda_i b_i \rightsquigarrow \langle v, b_i \rangle = \lambda_i$$

Given: an arbitrary basis of a subspace

Find: orthonormal basis of the subspace

TODO sketch drawing (projection and convexity)

$$K \subseteq V \text{ convex}$$

V with scalar product.

Then the optimization problem

$$\|x - y\| = \min_{Y \in K}$$

has at most one solution.

y is the solution.

$$\iff \Re \langle x - y_0, y - y_0 \rangle \leq 0 \forall y \in K$$

If K is the subspace U ($x - y_0 \perp U$), then

$$\Re \langle x - y_0, y \rangle = 0 \forall y \in K$$

$$U^\perp = \{ y \mid y \perp U \}$$

is subspace.

$$U \cap U^\perp = \{0\}$$

If $x \in U \cap U^\perp$, then $x \perp x = \langle x, x \rangle = \|x\|^2 = 0$.

Orthogonal complement: $U + U^\perp$ is direct sum.

Every $x \in U + U^\perp$ has a unique decomposition.

$$x = u + v \quad u \in U, v \in U^\perp$$

The maps $x \mapsto u$ and $x \mapsto v$ are linear.

Definition 3.16. Assume $U + U^\perp = V$. Then the projection maps

$$\pi_U : V \rightarrow V \quad \pi_{U^\perp} : V \rightarrow V$$

such that $\pi_U(x) \in U$ and $\pi_{U^\perp}(x) \in U^\perp$ and $x = \pi_U(x) + \pi_{U^\perp}(x)$ are orthogonality projections.

Remark 3.12. 1. $x \in U \iff \pi_U(x) = x \iff \pi_{U^\perp}(x) = 0$

2. $x \in U^\perp \iff \pi_U(x) = 0 \iff \pi_{U^\perp}(x) = x$
3. $\pi_{U^\perp} = \text{id} - \pi_U$

$$\begin{aligned} \pi_U(x) &\in U \\ \implies \text{remark (4): } \pi_U(\pi_U(x)) &= \pi_U(x) \\ (\sim): \pi_U \circ \pi_U &= \pi_U \text{ idempotent} \\ \pi_U \text{ is linear: } \pi_U \circ \pi_{U^\perp} &= 0 \end{aligned}$$

Theorem 3.19. Let $V = U \dot{+} U^\perp$.

1. $\forall x, y \in V : \langle x, \pi_{U(y)} \rangle = \langle \pi_U(x), y \rangle = \langle \pi_U(x), \pi_U(y) \rangle$
2. Compare with Figure 8.

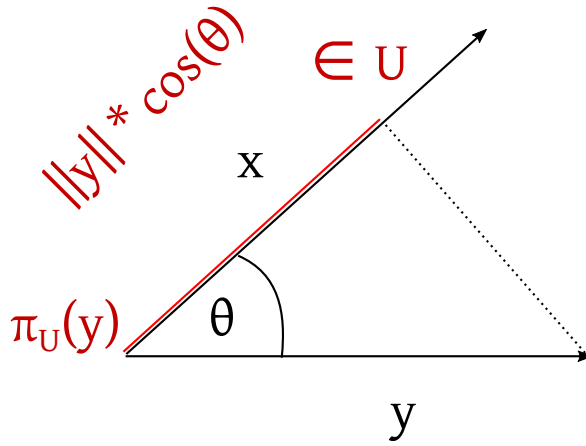


Figure 8: Projection

$$\|\pi_U(x)\| \leq \|x\| \wedge \|\pi_U(x)\| = \|x\| \iff x \in U$$

Proof:

(a)

$$x = \pi_U(x) + \pi_{U^\perp}(x) \quad y = \pi_U(y) + \pi_{U^\perp}(y)$$

$$\langle x, \pi_U(y) \rangle = \langle \pi_U(x) + \pi_{U^\perp}(x), \pi_U(y) \rangle = \langle \pi_U(x), \pi_U(y) \rangle + \underbrace{\left\langle \underbrace{\pi_U(x)}_{\in U^\perp}, \underbrace{\pi_U(y)}_{\in U} \right\rangle}_{=0}$$

$$\langle \pi_U(x), y \rangle = \langle \pi_U(x), \pi_U(y) \rangle + \langle \pi_U(x), \pi_{U^\perp}(y) \rangle$$

(b)

$$x = \pi_U(x) + \pi_{U^\perp}(x)$$

$$\implies \|x\|^2 = \|\pi_U(x)\|^2 + \|\pi_{U^\perp}(x)\|^2 \geq \|\pi_U(x)\|^2$$

$$\text{By equality} \iff \|\pi_{U^\perp}(x)\| = 0 \iff x = \pi_U(x) \iff x \in U$$

Definition 3.17. Jørgen Pedison Gram (1850–1916)

Let $v_1, v_2, \dots \in V$.

$$\text{Gram}(v_1, \dots, v_m) = \begin{bmatrix} \langle v_1, v_1 \rangle & \langle v_1, v_2 \rangle & \dots & \langle v_1, v_m \rangle \\ \langle v_2, v_1 \rangle & \langle v_2, v_2 \rangle & \dots & \langle v_2, v_m \rangle \\ \vdots & \vdots & \ddots & \vdots \\ \langle v_m, v_1 \rangle & \langle v_m, v_2 \rangle & \dots & \langle v_m, v_m \rangle \end{bmatrix}$$

is called Gram matrix of tuple v_1, v_2, \dots, v_m

Remark 3.13. In case $V = \mathbb{C}^n$.

$$\langle v, w \rangle = \overline{w}^T \cdot v = \sum_1^n \lambda_i \overline{\mu_i} = (\overline{\mu_1}, \dots, \overline{\mu_n}) \begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_n \end{pmatrix}$$

$$v = \begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_n \end{pmatrix} \quad w = \begin{pmatrix} \mu_1 \\ \vdots \\ \mu_n \end{pmatrix}$$

Hence, if

$$v_i = \begin{pmatrix} \beta_{1i} \\ \vdots \\ \beta_{ni} \end{pmatrix} \quad i = 1, \dots, m$$

$$\begin{aligned}
V &= \begin{pmatrix} v_1 & v_2 & \dots & v_m \\ \vdots & \vdots & & \vdots \end{pmatrix} \in \mathbb{C}^{n \times m} \\
&= \begin{pmatrix} \beta_{11} & \beta_{12} & \dots & \beta_{1m} \\ \vdots & \vdots & & \vdots \\ \beta_{n1} & \beta_{n2} & \dots & \beta_{nm} \end{pmatrix} \\
(V^* V)_{ij} &= \sum_{k=1}^n (v^*)_{ik} v_{kj} = \sum_{k=1}^n \overline{\beta_{ki}} \beta_{kj} = \overline{\langle v_i, v_j \rangle} \\
&= \begin{pmatrix} v_1^* & \dots \\ \vdots & \\ v_m^* & \dots \end{pmatrix} \begin{pmatrix} v_1 & \dots & v_m \\ \vdots & & \vdots \end{pmatrix} \\
V^* V &= \overline{\text{Gram}(v_1, \dots, v_m)}
\end{aligned}$$

Theorem 3.20. Let $v_1, \dots, v_m \in V$. $G = \text{Gram}(v_1, \dots, v_m)$.

1. $G = G^*$ is Hermitian, positive semidefinite.

$$\xi^T \cdot G \cdot \bar{\xi} = \left\| \sum_{i=1}^m \xi_i v_i \right\|^2 \geq 0$$

2. $\xi \in \ker G \iff \sum_{i=1}^m \bar{\xi}_i v_i = 0$
3. G is positive definite iff (v_1, \dots, v_m) are linear independent.

Proof. 1. $g_{ij} = \langle v_i, v_j \rangle = \overline{\langle v_j, v_i \rangle} = \overline{g_{ji}}$

$$\xi^T \cdot G \cdot \bar{\xi} = \sum_{i=1}^n \sum_{j=1}^n \xi_i g_{ij} \bar{\xi}_j = \sum_{i=1}^n \sum_{j=1}^n \xi_i \bar{\xi}_j \langle v_i, v_j \rangle = \left\langle \sum_{i=1}^n \xi_i v_i, \sum_{j=1}^n \bar{\xi}_j v_j \right\rangle = \left\| \sum_{i=1}^n \xi_i v_i \right\|^2$$

2. Direction \implies . $\xi \in \ker G \implies G\xi = 0 \implies \xi^T \cdot G \cdot \xi = 0$

$$\xi^T \cdot G \cdot \xi = \xi^T \cdot G \cdot \bar{\xi} \underbrace{=}_{(1)} \left\| \sum_{i=1}^m \bar{\xi}_i v_i \right\|^2$$

Direction \longleftarrow . If $\left\| \sum_{i=1}^m \bar{\xi}_i v_i \right\| = 0$

$$\begin{aligned}
(G \cdot \xi)_i &= \sum_{j=1}^n \langle v_i, v_j \rangle \xi_j = \sum_{j=1}^n \langle v_i, \bar{\xi}_j v_j \rangle = \left\langle v_i, \underbrace{\sum_{j=1}^n \bar{\xi}_j v_j}_{=0} \right\rangle \\
&\implies G \cdot \xi = 0
\end{aligned}$$

3. G is positive definite

$$\begin{aligned}
&\iff \forall \xi \neq 0 : \xi^T \cdot G \cdot \xi > 0 \\
&\iff \forall \xi \neq 0 : \left\| \sum_{i=1}^m \xi_i \cdot v_i \right\|^2 > 0 \\
&\iff \forall \xi \neq 0 : \sum_{i=1}^m \xi_i v_i \neq 0 \\
&\iff (v_1, \dots, v_m) \text{ is linear independent} \\
&\iff \ker G = \{0\} \\
&\iff G \text{ is regular}
\end{aligned}$$

□

Theorem 3.21. Let $U \subseteq V$ be a subspace. V is a vector space with scalar product.

(u_1, \dots, u_m) is basis of U

$$G = \text{Gram}(u_1, \dots, u_m) = \left[\langle u_i, u_j \rangle \right]_{i,j=1,\dots,m}$$

Then the projection $\pi_U(x) = \sum_{j=1}^m \eta_j u_j$ where

$$\eta = \overline{G}^{-1} \cdot \begin{pmatrix} \langle x, u_1 \rangle \\ \vdots \\ \langle x, u_m \rangle \end{pmatrix}$$

If u_1, \dots, u_m would be an orthonormal basis, then

$$\begin{pmatrix} \langle x, u_1 \rangle \\ \vdots \\ \langle x, u_m \rangle \end{pmatrix}$$

would be the coordinate of x .

Let $u = \sum_{j=1}^m \eta_j u_j$. Compare with Figure 9. Show that $x - u \in U^\perp = \mathcal{L}(u_1, \dots, u_m)^\perp = \{u_1, \dots, u_m\}^\perp = \bigcap_{i=1}^m u_i^\perp$

Hence, show that $x - u \perp u_i \forall i \in \{1, \dots, m\}$.

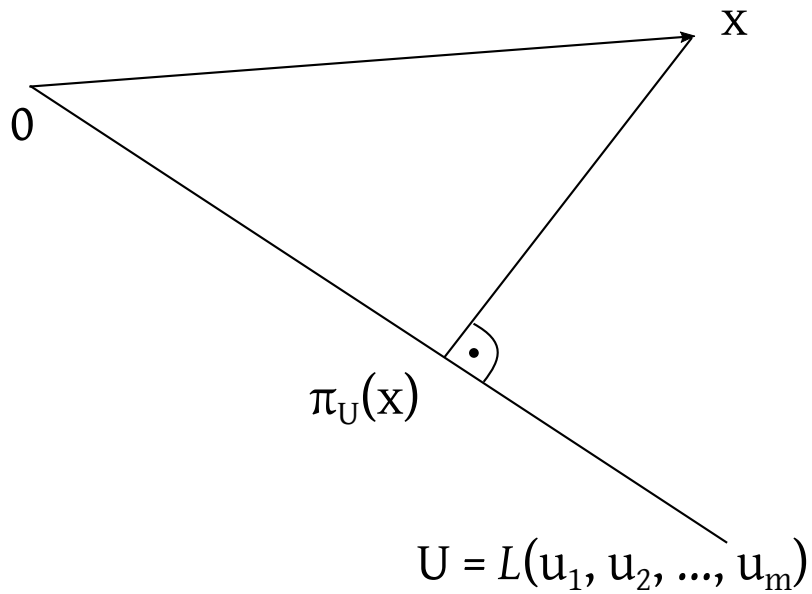


Figure 9: Projection

$$\begin{aligned}
 \langle u_i, u \rangle &= \left\langle u_i, \sum_{j=1}^m \eta_j u_j \right\rangle \\
 &= \sum_{j=1}^m \langle u_i, u_j \rangle \cdot \overline{\eta_j} \\
 &= \sum_{j=1}^m g_{ij} \overline{\eta_j} \\
 &= (G\overline{\eta})_i &= \langle u_i, x \rangle
 \end{aligned}$$

because

$$\begin{aligned}
 \overline{G} \cdot \eta &= \begin{pmatrix} \langle x, u_1 \rangle \\ \vdots \\ \langle x, u_m \rangle \end{pmatrix} \\
 G \cdot \overline{\eta} &= \begin{pmatrix} \langle x, u_1 \rangle \\ \vdots \\ \overline{\langle x, u_m \rangle} \end{pmatrix} = \begin{pmatrix} \langle u_1, x \rangle \\ \vdots \\ \langle u_m, x \rangle \end{pmatrix}
 \end{aligned}$$

Hence, $\forall i \in \{1, \dots, m\}$:

$$\langle u_i, u \rangle = \langle u_i, x \rangle \implies \forall i \in \{1, \dots, m\} : \langle u_i, x - u \rangle = 0 \implies x - u \in \{u_1, \dots, u_m\}^\perp$$

Example 3.15. Find polynomial $p(t)$ of degree 2 such that

$$\int_0^1 |t^3 - p(t)|^2 dt \stackrel{!}{=} \min$$

$V = C[0, 1]$, scalar product

$$\langle f, g \rangle = \int_0^1 f(t) \overline{g(t)} dt$$

$U =$ polynomial function of degree ≤ 2

$$x = t \mapsto t^3 \notin U$$

Find $p \in U$ such that $\|x - p\|^2 \stackrel{!}{=} \min$

$$\|x - p\|^2 = \int |x(t) - p(t)|^2 dt$$

Basis of $U = \mathcal{L}(\{1, t, t^2\})$

$$u_i(t) = t^{i-1} \quad i = 1, 2, 3$$

Gram matrix:

$$g_{ij} = \langle u_i, u_j \rangle = \int_0^1 t^{i-1} t^{j-1} dt = \int_0^1 t^{i+j-2} dt = \frac{t^{i+j-1}}{i+j-1} \Big|_0^1 = \frac{1}{i+j-1}$$

$$G = \begin{bmatrix} 1 & \frac{1}{2} & \frac{1}{3} \\ \frac{1}{2} & \frac{1}{3} & \frac{1}{4} \\ \frac{1}{3} & \frac{1}{4} & \frac{1}{5} \end{bmatrix}$$

Hilbert matrix:

$$\left[\frac{1}{i+j-1} \right]_{i,j=1,\dots,k}$$

This matrix is very unstable (in the equation system $Gx = b$) and therefore a very important test matrix in computational mathematics (ie. Numerics).

$$u = \sum_{j=1}^3 \eta_j u_j$$

$$\eta = \overline{G}^{-1} \cdot \begin{pmatrix} \langle x, u_1 \rangle \\ \langle x, u_2 \rangle \\ \langle x, u_3 \rangle \end{pmatrix}$$

$$\langle x, u_j \rangle = \int_0^1 x(t)u_j(t) dt = \int_0^1 t^3 \cdot t^{j-1} dt = \int_0^1 t^{2+j} dt = \frac{1}{3+j}$$

$$\eta = \begin{bmatrix} 1 & \frac{1}{2} & \frac{1}{3} \\ \frac{1}{2} & \frac{1}{3} & \frac{1}{4} \\ \frac{1}{3} & \frac{1}{4} & \frac{1}{5} \end{bmatrix}^{-1} \begin{pmatrix} \frac{1}{4} \\ \frac{1}{5} \\ \frac{1}{6} \end{pmatrix} = \begin{bmatrix} 9 & -36 & 30 \\ -36 & 192 & -180 \\ 30 & -180 & 180 \end{bmatrix} \begin{bmatrix} \frac{1}{4} \\ \frac{1}{5} \\ \frac{1}{6} \end{bmatrix} = \begin{bmatrix} \frac{1}{20} \\ -\frac{3}{5} \\ \frac{3}{2} \end{bmatrix}$$

(Assume that we don't know 180 in the bottom-right corner precisely. Consider $180 + \varepsilon$, then this error ε explodes tremendously in the solution).

Corollary. Special case u_i is orthonormal basis of U ($\rightarrow G = I$) Then it holds that

$$1. \forall v \in V : \pi_U(v) = \sum_{i=1}^m \langle v, u_i \rangle \cdot u_i$$

2.

$$\|v\|^2 \geq \sum_{i=1}^m |\langle v, u_i \rangle|^2 \quad (\text{Bessel's inequality})$$

$$\|v\|^2 = \sum_{i=1}^m |\langle v, u_i \rangle|^2 \iff v \in U \quad (\text{Parseval's identity})$$

$$\eta_j = \overline{G}^{-1} \begin{pmatrix} \langle v, u_1 \rangle \\ \vdots \\ \langle v, u_m \rangle \end{pmatrix}$$

F. Bessel (1784–1846)

M. A. Parseval (1755–1836)

Proof. Gram's matrix = I .

$$\eta_j = \langle v, u_j \rangle$$

□

3.6 Gram-Schmidt process

Given: $U = \mathcal{L}(v_1, \dots, v_m)$

Find: orthonormal basis of U .

Theorem 3.22 (Gram–Schmidt process for orthogonalization). *Let $(v_1, \dots, v_m) \subseteq V$ be linear independent. Then $\exists u_1, \dots, u_m$ is orthonormal basis of $\mathcal{L}(v_1, \dots, v_m)$, specifically inductive*

$$u_1 = \frac{v_1}{\|v_1\|}$$

and for $k = 2, \dots, m$:

$$\tilde{u}_k = v_k - \sum_{j=1}^{k-1} \langle v_k, u_j \rangle \cdot u_j$$

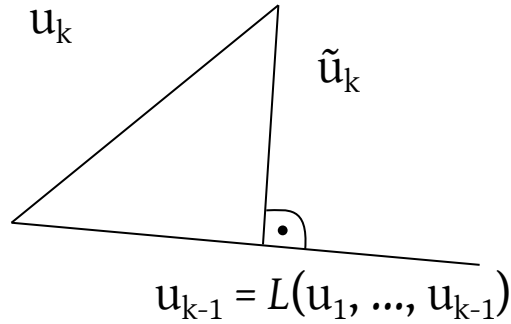


Figure 10: Projection used in the Gram-Schmidt process

$$u_k = \frac{\tilde{u}_k}{\|\tilde{u}_k\|}$$

Proof. **Induction base** $k = 1$ is trivial

Induction step $k - 1 \rightarrow k$. Assume

$$\mathcal{L}(u_1, \dots, u_{k-1}) = \mathcal{L}(v_1, \dots, v_{k-1}) =: U_{k-1}$$

$$\tilde{u}_k = v_k - \pi_{U_{k-1}}(v_k) \in U_{k-1}^\perp \text{ because of Theorem 3.5}$$

$$\implies \tilde{u}_k \perp u_1, \dots, u_{k-1} \implies (u_1, \dots, u_{k-1}, \frac{\tilde{u}_k}{\|\tilde{u}_k\|})$$

is an orthonormal basis.

$$\mathcal{L}(u_1, \dots, u_{k-1}, \frac{\tilde{u}_k}{\|\tilde{u}_k\|}) = \mathcal{L}(u_1, \dots, u_{k-1}, v_k)$$

then $\tilde{u}_k - v_k \in \mathcal{L}(u_1, \dots, u_{k-1})$

□

This lecture took place on 2018/04/25.

Gram-Schmidt process:

$$\mathcal{L}(v_1, v_2) = \mathcal{L}(v_2 - p(v_2), v_1) \quad v_2 - p(v_2) \perp v_1$$

Given: v_1, \dots, v_m

$$u_i = \frac{v_i}{\|v_i\|}$$

$$\tilde{u}_k = v_k - \sum_{i=1}^{k-1} \langle v_k, u_i \rangle \cdot u_i$$

$$u_k = \frac{\tilde{u}_k}{\|\tilde{u}_k\|} \quad \frac{\langle v_k, \tilde{u}_i \rangle \tilde{u}_i}{\|\tilde{u}_i\|^2}$$

Example 3.16. Let $V = \mathbb{R}^3$.

$$\langle x, y \rangle = x^t A y$$

$$A = \begin{bmatrix} 1 & -1 & 1 \\ -1 & 3 & -1 \\ 1 & -1 & 2 \end{bmatrix}$$

$$v_i = \text{standard basis } e_i$$

$$\|v_1\|^2 = \langle v_1, v_1 \rangle = v_1^T A v_1 = a_{11} = 1$$

$$\|v_2\|^2 = \langle v_2, v_2 \rangle = a_{22} = 3$$

$$u_1 = \frac{v_1}{\|v_1\|} = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$$

$$\tilde{u}_2 = v_2 - u_1 \langle v_2, u_1 \rangle = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} - \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} \cdot (0 \ 1 \ 0) A \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} + \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix}$$

$$u_2 = \frac{\tilde{u}_2}{\|\tilde{u}_2\|} \quad \|\tilde{u}_2\|^2 = \langle \tilde{u}_2, \tilde{u}_2 \rangle = (1 \ 1 \ 0) \cdot A \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix} = 2 \quad u_2 = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix}$$

$$\tilde{u}_3 = v_3 - u_1 \langle v_3, u_1 \rangle - u_2 \langle v_3, u_2 \rangle$$

$$= \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} - \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} \cdot (0 \ 0 \ 1) \cdot A \cdot \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} - \underbrace{\frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix} \cdot (0 \ 0 \ 1) \cdot A \cdot \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix}}_{a_{31}+a_{32}=0} \cdot \frac{1}{\sqrt{2}} = \begin{pmatrix} -1 \\ 0 \\ 1 \end{pmatrix}$$

$a_{31}=1$ $a_{31}+a_{32}=0$

$$\|\tilde{u}_3\|^2 = (-1 \ 0 \ 1) \cdot A \cdot \begin{pmatrix} -1 \\ 0 \\ 1 \end{pmatrix} = 1 - 1 - 1 + 2 = 1 \quad u_3 = \begin{pmatrix} -1 \\ 0 \\ 1 \end{pmatrix}$$

Remark 3.14. This is an alternative method to build orthogonal projection on subspace $U \subseteq \mathbb{C}^n$ with standard scalar product.

1. Determine an orthonormal basis of U : $u_1, \dots, u_m \in \mathbb{C}^{n \times 1}$
2. $P = \sum_{i=1}^m u_i \cdot u_i^*$

$$P \cdot v = \sum_{i=1}^m u_i \underbrace{u_i^* \cdot v}_{\langle v, v_i \rangle} = \sum_{i=1}^m u_i \langle v, v_i \rangle$$

Gram matrix = I

Example 3.17 (Example 3.15 again).

$$V = C[0, 1] \quad U = \mathcal{L}(1, x, x^2) =: \mathcal{L}(v_1, v_2, v_3)$$

$$\langle f, g \rangle = \int_0^1 f(t) \overline{g(t)} dt$$

Orthonormal basis:

$$\|v_1\|^2 = \int_0^1 1^2 dt = 1$$

$$u_1 = 1$$

$$\tilde{u}_2 = v_2 - u_1 \cdot \underbrace{\langle v_2, u_1 \rangle}_{=\frac{1}{2}} = x - 1 \cdot \int_0^1 t \cdot 1 dt = x - \frac{1}{2}$$

$$\|\tilde{u}_2\|^2 = \int_0^1 (t - \frac{1}{2})^2 dt = \left. \frac{(t - \frac{1}{2})^3}{3} \right|_0^1 = \frac{(\frac{1}{2})^3 - (-\frac{1}{2})^2}{3} = \frac{1}{12}$$

$$u_2 = \frac{\tilde{u}_2}{\|\tilde{u}_2\|} = \sqrt{12} \cdot (x - \frac{1}{2})$$

$$\begin{aligned} \tilde{u}_3 &= v_3 - u_1 \langle v_3, u_1 \rangle - u_2 \cdot \langle v_3, u_2 \rangle \\ &= x^2 - 1 \cdot \underbrace{\int_0^1 t^2 \cdot 1 dt}_{=\frac{1}{3}} - \sqrt{12}(x - \frac{1}{2}) \int_0^1 t^2 \sqrt{12}(t - \frac{1}{2}) dt \\ &= x^2 - \frac{1}{3} - 12(x - \frac{1}{2}) \cdot \frac{1}{12} \\ &= x^2 - x + \frac{1}{6} \end{aligned}$$

Side note:

$$\int_0^1 t^2(t - \frac{1}{2}) dt = \int_0^1 (t^3 - \frac{1}{2}t^2) dt = \frac{1}{4} - \frac{1}{6} = \frac{1}{12}$$

$$\|\tilde{u}_3\|^2 = \int_0^1 (t^2 - t + \frac{1}{6})^2 dt = \frac{1}{180}$$

$$\implies u_3 = \sqrt{180} \cdot (x^2 - x + \frac{1}{6})$$

Projection:

$$\int_0^1 (t^3 - p(t))^2 dt = \min!$$

Solution: $\pi_U(x^3) \quad U = \mathcal{L}(1, x, x^2)$

$$\begin{aligned} \pi_U(x^3) &= u_1 \langle x^3, u_1 \rangle + u_2 \langle x^3, u_2 \rangle + u_3 \langle x^3, u_3 \rangle \\ &= 1 \cdot \int_0^1 t^3 \cdot 1 dt + \sqrt{12}(x - \frac{1}{2}) \int_0^1 t^3 \sqrt{12}(t - \frac{1}{2}) dt \\ &\quad + \sqrt{180}(x^2 - x + \frac{1}{6}) \int_0^1 t^3 \sqrt{180}(t^2 - t + \frac{1}{6}) dt \end{aligned}$$

Consider $\langle f, g \rangle := \int_{-1}^1 \sqrt{1-t^2} f(t) \overline{g(t)} dt$. Take $1, x, x^2, \dots$ and apply Gram schmidt process to retrieve the Chebyshev polynomials.

$$\begin{aligned} \int_0^1 f(t)g(t) dt & \quad \text{Laguerre} \\ \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{\infty} e^{-\frac{t^2}{2}} f(t)g(t) dt & \quad \text{Hermite polynomials} \end{aligned}$$

3.7 Riesz representation theorem

Frigyies Riesz (1880–1956)

Let $(V, \langle \cdot, \cdot \rangle)$ be a vector space with scalar product $\dim V < \infty$.

V^* is the dual space $= \text{Hom}(V, \mathbb{K}) =$ space of linear functionals. For fixed $y \in V$ the map $T_y(x) = \langle x, y \rangle$ is linear in x , hence $T_y \in V^*$.

Then the map $V \rightarrow V^*$ with $y \mapsto T_y : V \rightarrow \mathbb{K}$ with $x \mapsto \langle x, y \rangle$ is an antilinear isomorphism (antiisomorphism).

This is trivial in \mathbb{R} , but in \mathbb{C} is much more complex (pun intended).

Hence,

1. For every y it holds that $T_y \in V^*$
2. For every linear functional $f \in V^*$

$$\exists! y \in V : f = T_y$$

3. Let $y \mapsto T_y$ is an antilinear map.

$$T_{\lambda y_1 + \mu y_2} = \bar{\lambda} T_{y_1} + \bar{\mu} T_{y_2}$$

Example 3.18 (For point 2).

$$V = C[0, 1]$$

Scalar product: $\langle f, g \rangle = \int f(t)g(t) dt$. Let $F : C[0, 1] \rightarrow \mathbb{R}$ linear. Then by the Riesz representation theorem, there exists $g \in C[0, 1] : F(f) = \int f(t)g(t) dt$.

For example $f \rightarrow f(1)$

$$\exists g(t) : f(1) = \int_0^1 f(t)g(t) dt$$

In physics, e.g. the Dirac delta function.

Proof of point 3. We show linearity.

$$Ty(x) = \langle x, y \rangle \text{ is linear in } X \implies T_y \in V^*$$

$$\begin{aligned} \forall x \in V : T_{\lambda y_1 + \mu y_2}(x) &= \langle x, \lambda y_1 + \mu y_2 \rangle = \bar{\lambda} \langle x, y_1 \rangle + \bar{\mu} \langle x, y_2 \rangle \\ &= \bar{\lambda} Ty_1(x) + \bar{\mu} Ty_2(x) = (\bar{\lambda} Ty_1 + \bar{\mu} Ty_2)(x) \\ &\implies T_{\lambda y_1 + \mu y_2} = \bar{\lambda} Ty_1 + \bar{\mu} Ty_2 \end{aligned}$$

We show injectivity: the map $y \mapsto Ty$ is injective.

Assume: $Ty = 0$ (zero functional). Show $y = 0$. $Ty = 0$ means $\forall x \in V : Ty(x) = 0$, especially for $x = y$, $T_y(y) = \langle y, y \rangle = 0 \implies y = 0$.

We show surjectivity: the map $y \mapsto Ty$ is surjective.

Let u_1, \dots, u_n is an orthonormal basis (exists because of Gram-Schmidt).

Given: $f \in V^*$. Find: y such that $f = Ty$.

$$\text{Hence, } \forall x \in V : f(x) = \langle x, y \rangle \quad \underbrace{\iff}_{\text{by Fortsetzungssatz}} \quad f(u_i) = \langle u_i, y \rangle$$

$$\text{Let } y = \sum_{j=1}^n \overline{f(u_j)} \cdot u_j.$$

$$\implies \langle u_i, y \rangle = \left\langle u_i, \sum_{j=1}^n \overline{f(u_j)} u_j \right\rangle = \sum_{j=1}^n f(u_j) \underbrace{\langle u_i, u_j \rangle}_{\delta_{ij}} = f(u_i)$$

Hence, y satisfies the condition. □

Remark 3.15. The Riesz representation theorem also holds in infinite dimensions in the case of Hilbert spaces. In those spaces, there exists some Hilbert base:

$$(u_i)_{i \in I} : x = \sum_{i \in I} \langle x, u_i \rangle \cdot u_i \forall x$$

So every x has such a representation and in infinite dimensions, this representation is a series.

Corollary. 1. $v = 0 \iff \forall w \in V : \langle v, w \rangle = 0$

$$2. \|v\| = \sup \{ |\langle v, w \rangle| \mid \|w\| \leq 1 \}$$

Equivalently in the dual space:

$$1. v = 0 \iff \forall f \in V^* : f(v) = 0$$

$$2. \|v\| = \sup \{ |f(v)| \mid f \in V^* \quad \|f\| \leq 1 \}$$

holds in general in a normed space.

Remark 3.16. We make a small revision: dual space $V^* = \text{Hom}(V, \mathbb{K})$

$$W \xrightarrow{T} V \xrightarrow{f} \mathbb{K}$$

$$\implies f \circ T : W \rightarrow \mathbb{K} \in W^*$$

is a linear functional on W . Hence, the map $\text{Hom}(V, \mathbb{K}) \rightarrow \text{Hom}(W, \mathbb{K})$ and $f \mapsto f \cdot T$ is linear.

$$(\lambda f + \mu g) \circ T = \lambda \cdot f \circ T + \mu g \circ T \quad \text{“transposed map”}$$

Linear map: $T^* : V^* \rightarrow W^*$.

Let V, W be spaces with a scalar product. Then $V \simeq V^*$ and $W \simeq W^*$ where \simeq means anti-isomorphic. $T : W \rightarrow V \implies T^* : V \rightarrow W$.

Definition 3.18 (Theorem and definition). Let $(V, \langle \cdot, \cdot \rangle_V)$ and $(W, \langle \cdot, \cdot \rangle_W)$ be spaces with a scalar product. $\dim V, \dim W < \infty$.

$T \in \text{Hom}(W, V)$ hence, $T : W \rightarrow V$ linear

1. For every $v \in V$ is the map

$$w \mapsto \langle T(w), v \rangle_V \quad \text{linear}$$

2. $\forall v \in V \exists! u \in W \forall w \in W : \langle T(w), v \rangle_V = \langle w, u \rangle_W$ and $T^*(v) = u$.

Hence,

$$\langle T(w), v \rangle_V = \langle w, T^*(v) \rangle_W \quad \forall w \in W \quad \forall v \in V$$

3. The map $T^* : V \rightarrow W$ with $v \mapsto u$ is linear, hence $T^* \in \text{Hom}(V, W)$ and is called adjoint map.

4. The map $\text{Hom}(W, V) \mapsto \text{Hom}(V, W)$ with $T \mapsto T^*$ is antilinear and $T^{**} = T$.

Proof. 1. $\langle T(w), v \rangle = T_V(T(w)) = T_v \circ T(w)$
Composition of linear maps is linear.

2. $T_V \circ T \in W^*$. By Riesz representation theorem, $\exists! u \in W : T_V \circ T(w) = \langle w, u \rangle \forall w \in W = \langle T(w), v \rangle = \langle w, u \rangle$

3. Show that,

$$\forall v_1, v_2 \in V \forall \lambda, \mu : T^*(\lambda v_1 + \mu v_2) = \lambda T^*(v_1) + \mu T^*(v_2)$$

It suffices to show that

$$\langle w, T^*(\lambda v_1 + \mu v_2) \rangle = \langle w, \lambda T^*(v_1) + \mu T^*(v_2) \rangle \forall w \in W$$

Compare with corollary: $w_1 = w_2$ in $W \iff \forall w : \langle w, w_1 \rangle = \langle w, w_2 \rangle$.

$$\begin{aligned} \langle w, T^*(\lambda v_1 + \mu v_2) \rangle &= \langle T(w), \lambda v_1 + \mu v_2 \rangle \\ &= \bar{\lambda} \langle T(w), v_1 \rangle + \bar{\mu} \langle T(w), v_2 \rangle \\ &= \bar{\lambda} \langle w, T^*(v_1) \rangle + \bar{\mu} \langle w, T^*(v_2) \rangle \\ &= \langle w, \lambda T^*(v_1) \rangle + \langle w, \mu T^*(v_2) \rangle \\ &= \langle w, \lambda T^*(v_1) + \mu T^*(v_2) \rangle \end{aligned}$$

4. Show $(\lambda T_1 + \mu T_2)^* = \bar{\lambda} T_1^* + \bar{\mu} T_2^*$.

$$\iff \forall v \in V : (\lambda T_1 + \mu T_2)^* v = (\bar{\lambda} T_1^* + \bar{\mu} T_2^*)(v)$$

$$\forall v \in V \forall w \in W : \langle w, (\lambda T_1 + \mu T_2)^*(v) \rangle = \langle w, (\bar{\lambda} T_1^* + \bar{\mu} T_2^*)(v) \rangle$$

Hence,

$$\begin{aligned} \langle w, (\lambda T_1 + \mu T_2)^*(v) \rangle &= \langle (\lambda T_1 + \mu T_2)(w), v \rangle \\ &= \lambda \langle T_1(w), v \rangle + \mu \langle T_2(w), v \rangle \\ &= \lambda \langle w, T_1^*(v) \rangle + \mu \langle w, T_2^*(v) \rangle \\ &= \langle w, \bar{\lambda} T_1^*(v) \rangle + \langle w, \bar{\mu} T_2^*(v) \rangle \\ &= \langle w, \bar{\lambda} T_1^*(v) + \bar{\mu} T_2^*(v) \rangle \\ &= \langle w, (\bar{\lambda} T_1^* + \bar{\mu} T_2^*)(v) \rangle \end{aligned}$$

$$T : W \rightarrow V \quad T^* : V \rightarrow W \quad T^{**} : W \rightarrow V$$

Show that $\forall w \in W : T^{**}(w) = T(w)$. Hence $\forall w \in W \forall v \in V : \langle T^{**}(w), v \rangle_V = \langle T(w), v \rangle_V$

$$\begin{aligned} \langle T^{**}(w), v \rangle_V &= \overline{\langle v, T^{**}(w) \rangle} = \overline{\langle T^*(v), w \rangle} = \langle w, T^*(v) \rangle \\ &= \langle T(w), v \rangle \\ \langle T(w), v \rangle &= \langle w, T^* v \rangle \end{aligned}$$

If $V = W$, then $T = T^*$.

5. Assume $u = D^*(x)$ exists $\in \mathbb{R}[x]$

$$\begin{aligned} &\implies M := \max_{t \in [0,1]} |u(t)| < \infty \\ \|x^n\| D^*(x) &= \left| \int_0^1 t^n \cdot u(t) dt \right| \leq \int_0^1 t^n \cdot M dt = \frac{M}{n+1} \\ &\implies \frac{n}{n+1} \leq \frac{M}{n+1} \forall n \in \mathbb{N} \\ &\implies u(x) \notin \mathbb{R}[x] \end{aligned}$$

□

Example 3.19 (For Definition 3.18, point 3). If $\dim V = \infty$, then not every linear map has an adjoint map!

$$\begin{aligned} V &= \mathbb{R}[x]_1 \\ \langle f, g \rangle &= \int_0^1 f(t)g'(t) dt \\ D : V &\rightarrow V \quad p(x) \mapsto p'(x) \end{aligned}$$

Recall: The derivative of a linear combination is the linear combination of derivatives. Assume D has an adjoint D^* .

$$\implies \langle x^n, D^*(x) \rangle = \langle D(x^n), x \rangle = \int_0^1 nt^{n-1}t dt = \frac{n}{n+1}$$

This lecture took place on 2018/05/02.

Riesz representation theorem
 V with scalar product
 $\text{Hom}(V, \mathbb{K}) \simeq V$ where \simeq is antilinear
 $\forall f \in \text{Hom}(V, \mathbb{K}) : \exists! y \in V : f = T_y$

$$\begin{aligned} T_y(x) &= \langle x, y \rangle \\ T_{\lambda x + \mu y} &= \bar{\lambda} T_x + \bar{\mu} T_y \end{aligned}$$

For $f \in \text{Hom}(V, W)$, the map $x \mapsto \langle f(x), y \rangle \in \text{Hom}(V, \mathbb{K})$

$$\implies \exists! z \in V : \forall x \in V : \langle f(x), y \rangle = \langle x, z \rangle$$

$z =: f^*(y) \dots$ adjoint map

$f^* : W \rightarrow V$ is linear

$\text{Hom}(V, W) \rightarrow \text{Hom}(W, V)$

$$f \mapsto f^*$$

is an antilinear *involution*.

$$f^{**} = f$$

Theorem 3.23. Let $B \subseteq V, C \subseteq W$ be orthonormal bases. $f \in \text{Hom}(V, W)$.

$$\Phi_B^C(f^*) = \Phi_C^B(f)^* = \overline{\Phi_C^B(f)}^T$$

Proof.

$$A = \Phi_C^B(f)$$

Column $s_j(A)$ is the coordinate of $b_j \in B$ in regards of basis C .

$$\begin{aligned} a_{ij} &= \text{i-th coordinate of } f(b_j) \\ &= \Phi_C(f(b_j))_i = \langle f(b_j), c_i \rangle \\ &= \langle b_j, f^*(c_i) \rangle = \overline{\langle f^*(c_i), b_j \rangle} \\ &= \text{j-th coordinate of } f^*(c_i) \\ &= \overline{\Phi_B^C(f^*)_{ji}} = \overline{\tilde{a}_{ji}} \end{aligned}$$

if $\tilde{A} = \Phi_B^C(f^*)$

□

Theorem 3.24. Let U, V, W be finite-dimensional.

$$U \xrightarrow{f} V \xrightarrow{g} W$$

1. $(g \circ f)^* = f^* \circ g^*$
2. $f^{**} = f$
3. $\ker f = (\text{image } f^*)^\perp$
4. $\text{image } f = (\ker f^*)^\perp$
5. $f \text{ injective} \iff f^* \text{ surjective}$
6. $f \text{ surjective} \iff f^* \text{ injective}$

Proof. 1. Let $u \in V, w \in W$

$$\begin{aligned} \langle (g \circ f)(u), w \rangle_W &= \langle g(f(u)), w \rangle_W \\ &= \langle f(u), g^*(w) \rangle_V \\ &= \langle u, f^*(g^*(w)) \rangle_U \end{aligned}$$

holds $\forall u \in U \forall w \in W$. By definition

$$\langle (g \circ f)(u), w \rangle_W = \langle u, (g \circ f)^*(w) \rangle$$

Hence,

$$\implies (g \circ f)^* = f^* \circ g^*$$

3. Show that

- $\text{kern } f \subseteq (\text{image } f^*)^\perp$
- $(\text{image } f^*)^\perp \subseteq \text{kern } f$

Proof:

- Let $u \in \text{kern } f$. Show that $\forall y \in \text{image } f^* : \langle u, y \rangle = 0$

$$y \in \text{image } f^* \implies \exists v \in V : y = f^*(v)$$

$$\langle u, y \rangle_U = \langle u, f^*(v) \rangle_U = \underbrace{\langle f(u), v \rangle}_V = 0$$

- Let $u \in (\text{image } f^*)^\perp$, hence $\forall v \in V : u \perp f^*(v)$. Hence $\forall v \in V : \langle u, f^*(v) \rangle_U = 0$.

$$\forall v \in V : \langle f(u), v \rangle_V = 0$$

$$\implies f(u) \in V^\perp = \{0\}$$

$$\implies u \in \text{kern } f$$

4. Apply (3) to f^* .

$$\text{kern } f^* = (\text{image } f^{**})^\perp = (\text{image } f)^\perp$$

$$\implies (\text{kern } f^*)^\perp = (\text{image } f)^{\perp\perp} \underbrace{=}_{\dim < \infty} \text{image } f$$

□

Remark 3.17 (Addition to Theorem 3.17). So, if subspace $U \subseteq V$. Then $U^{\perp\perp} = U$.

Proof: It holds that $U + U^\perp = V$ and $U^\perp + U^{\perp\perp} = V$. $U \subseteq U^{\perp\perp}$ and $\dim U = \dim U^{\perp\perp} \implies U = U^{\perp\perp}$.

Definition 3.19. Let V be a vector space with scalar product.

1. $f : V \rightarrow V$ is called self-adjoint, if $f = f^*$. Hence $\forall x, y \in V : \langle f(x), y \rangle = \langle x, f(y) \rangle \iff \Phi_B^B(f) = \Phi_B^B(f)^*$ if B is orthonormal basis of V .
2. $f \in \text{Hom}(V, W)$ is called unitary transformation or linear isometry if

$$\forall x, y \in V : \langle f(x), f(y) \rangle = \langle x, y \rangle$$

esp. $\|f(x)\| = \|x\|$, hence lengths (and also angles) are preserved.
mostly it is additionally required that f is invertible.

Remark 3.18. 1. Unitary transformations are injective.

2. If $\dim V = \dim W < \infty$ and $f : V \rightarrow W$ is linear and unitary, then f is regular and $f^{-1} = f^*$.

3. If $\dim V = \infty$, $f : V \rightarrow V$ is isometry, it does not imply that f is invertible.

Proof. 1. Immediate: $f(v) = 0 \implies \|f(v)\| = \|v\| = 0 \implies v = 0$
 $\text{kern } f = \{0\}$

2. f unitary $\xrightarrow{(1.)} f$ injective $\implies f$ surjective.

$$\begin{aligned}\forall x, y \in V : \langle x, y \rangle &= \langle f(x), f(y) \rangle \\ &= \langle x, f^* \circ f(y) \rangle\end{aligned}$$

hence for fixed y , it holds that

$$\begin{aligned}\forall x \in V : \langle x, y \rangle &= \langle x, f^* \circ f(y) \rangle \\ \implies y &= f^* \circ f(y) \text{ for all } y \implies f^* \circ f = \text{id}\end{aligned}$$

3. $V = l^2 = \{(x_n)_n \mid \sum |x_n|^2 < \infty\}$

$$S : l^2 \rightarrow l^2$$

$$(x_1, x_2, \dots) = (0, x_1, x_2, \dots)$$

$$\|S(x)\| = \|x\|$$

$$\langle S(x), S(y) \rangle = \langle (0, x_1, x_2, \dots), (y_1, y_2, \dots) \rangle$$

$$= 0 + \sum_{i=1}^{\infty} x_i \overline{y_i}$$

$$= \langle x, y \rangle$$

$$\langle x, S^* y \rangle = \langle Sx, y \rangle$$

$$= \langle (0, x_1, x_2, \dots), (y_1, y_2, \dots) \rangle$$

$$= 0 \cdot \overline{y_1} + x_1 \cdot \overline{y_2} + x_2 \cdot \overline{y_3} + \dots$$

$$= \langle (x_1, x_2, \dots), (y_1, y_2, \dots) \rangle$$

$$S^*(y_1, y_2, \dots) = (y_2, y_3, \dots)$$

$$\langle S_x, S_y \rangle = \langle x, S^* S y \rangle \forall x, y$$

$$\implies S^* \circ S = \text{id}$$

$$\text{but } S \circ S^*(x_1, x_2, \dots) = S(x_2, x_3, \dots)$$

$$= (0, x_2, x_3, \dots)$$

$$\implies S \circ S^* \neq \text{id}$$

S is not invertible

This shifting of indices works in a finite number of dimensions, but does not work in infinity (in this case you miss one dimension).

□

Definition 3.20. 1. A matrix U is called unitary if $U^*U = I$

2. A matrix $U \in \mathbb{R}^{n \times n}$ is called orthogonal if $U^T U = I$

Theorem 3.25. For a matrix $T \in \mathbb{C}^{n \times n}$ it holds equivalently:

1. T is unitary ($T^* \cdot T = I$)
2. $\forall x \in \mathbb{C}^n : \|Tx\| = \|x\|$ (isometry)
3. $\forall x, y \in \mathbb{C}^n : \Re \langle Tx, Ty \rangle = \Re \langle x, y \rangle$
4. $\forall x, y \in \mathbb{C}^n : \langle Tx, Ty \rangle = \langle x, y \rangle$
5. The columns of T define an orthonormal basis of \mathbb{C}^n

Proof. 1. \rightarrow 2.

$$\|Tx\|^2 = \langle Tx, Tx \rangle = \langle x, T^*Tx \rangle = \langle x, Ix \rangle = \|x\|^2$$

2. \rightarrow 3.

$$\begin{aligned} \|T(x+y)\|^2 &= \|x+y\|^2 \\ \|T(x-y)\|^2 &= \|x-y\|^2 \\ \|Tx+Ty\|^2 &= \|Tx\|^2 + 2\Re \langle Tx, Ty \rangle + \|Ty\|^2 \\ \|Tx-Ty\|^2 &= \|Tx\|^2 - 2\Re \langle Tx, Ty \rangle + \|Ty\|^2 \\ \hline \|Tx+Ty\|^2 - \|Tx-Ty\|^2 &= 4\Re \langle Tx, Ty \rangle \\ \text{analogously, } \|x+y\|^2 - \|x-y\|^2 &= 4\Re \langle x, y \rangle \\ \hline \implies \Re \langle Tx, Ty \rangle &= \Re \langle x, y \rangle \end{aligned}$$

3. \rightarrow 4.

$$\Re \langle Tx, Ty \rangle = \Re \langle x, y \rangle \quad \forall x, y \in \mathbb{C}^n$$

also holds for $i \cdot y$ instead of y

$$\Re \langle Tx, iTy \rangle = \Re \langle x, iy \rangle \quad \forall x, y \in \mathbb{C}^n$$

$$\Re(-i \langle Tx, Ty \rangle) = \Re(-i \langle x, y \rangle)$$

$$\Re(-i(a+ib)) = \Re(-ia+b) = b$$

$$\Re(-i \cdot z) = \Im(z)$$

$$\Im \langle Tx, Ty \rangle = \Im \langle x, y \rangle \quad \forall x, y \in \mathbb{C}^n$$

\Re and \Im are equivalent.

$$\implies \langle Tx, Ty \rangle = \langle x, y \rangle \quad \forall x, y$$

(this is a common proof pattern, that you only show it for \Re and \Im follows immediately)

4. \rightarrow 5. e_1, \dots, e_n define some orthonormal basis.

$\Rightarrow (Te_1, \dots, Te_n)$ is orthonormal basis

$u_i = Te_i =$ i-th column of T

$$\langle u_i, u_j \rangle = \langle Te_i, Te_j \rangle = \langle e_i, e_j \rangle = \delta_{ij}$$

5. \rightarrow 4. $(T^*T)_{ij}$ is the i -th column vector of T^* times the j -th column vector of T .

$$u_j^* \cdot u_j = \langle u_j, u_i \rangle = \delta_{ji}$$

$$\Rightarrow T^*T = \begin{bmatrix} 1 & \dots & 0 \\ & \ddots & \\ 0 & \dots & 1 \end{bmatrix} = I$$

□

What do isometries of \mathbb{R}^n or \mathbb{C}^n look like?

Definition 3.21. An isometry between two metric spaces (M_1, d_1) and (M_2, d_2) . Metric d :

$$d(x, y) \geq 0$$

$$d(x, y) = 0 \iff x = y$$

$$d(x, y) \leq d(x, z) + d(z, y)$$

is a map $f : M_1 \rightarrow M_2$ such that

$$d_2(f(x), f(y)) = d_1(x, y)$$

Every normed space has metric $d(x, y) = \|x - y\|$. An isometry between two spaces is a (not necessarily linear) map $f : V \rightarrow W$ such that $\|f(x) - f(y)\| = \|x - y\|$.

Example 3.20 (Translation).

$$x_0 \in V \quad T_{x_0} : V \rightarrow V \quad x \mapsto x + x_0$$

is isometry, but is not unitary because non-linear⁹

$$\|T_{x_0}(x) - T_{x_0}(y)\| = \|x + x_0 - (y + x_0)\| = \|x - y\|$$

Other examples in \mathbb{R}^n :

1. rotation

⁹0 is not mapped to 0, but x_0

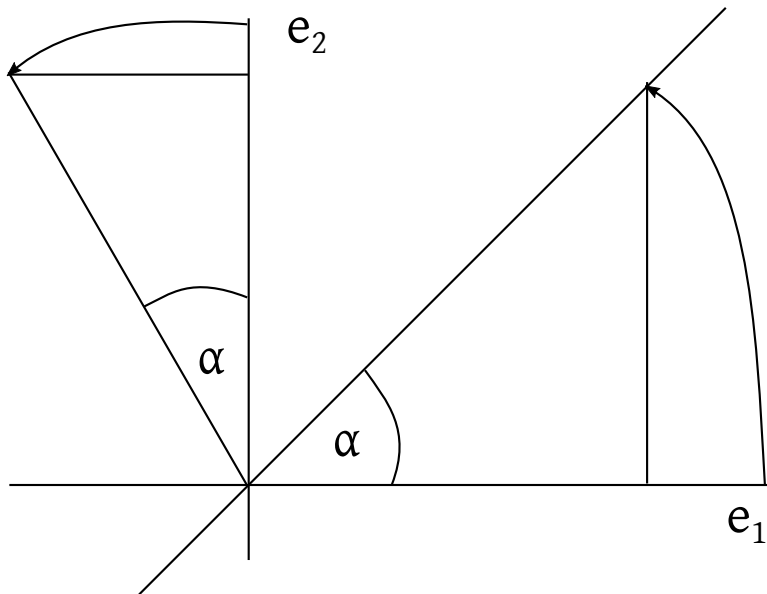


Figure 11: Rotation in \mathbb{R}^2

2. reflection

3. unitary/orthogonal map

Example 3.21 (Rotation in \mathbb{R}^2).

$$U(e_1) = \begin{pmatrix} \cos \alpha \\ \sin \alpha \end{pmatrix}$$

$$U(e_2) = \begin{pmatrix} -\sin \alpha \\ \cos \alpha \end{pmatrix}$$

Compare with Figure 11.

$$U_\alpha = \begin{bmatrix} \cos \alpha & \dots & -\sin \alpha \\ & \ddots & \\ \sin \alpha & \dots & \cos \alpha \end{bmatrix} = \begin{bmatrix} 1 & \\ & 1 \end{bmatrix} \cdot \cos \alpha + \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \cdot \sin \alpha$$

Tangent a :

$$\begin{pmatrix} x(t) \\ y(t) \end{pmatrix} = \begin{pmatrix} \dot{x}(t) \\ \dot{y}(t) \end{pmatrix}$$

Example 3.22 (Rotation considered as motion).

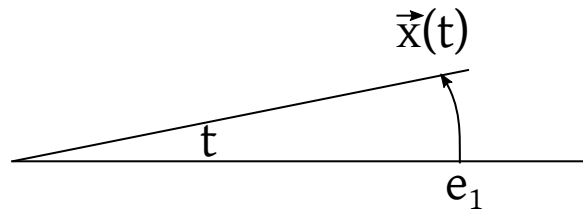


Figure 12: Rotation in \mathbb{R}^2 considered as motion. Commonly done by physicists.

$$\begin{aligned}\dot{\vec{x}}(t) &= \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \vec{x}(t) \\ \vec{x}(t) &= e^{\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} t} \cdot \vec{x}_0\end{aligned}$$

Compare with Figure 12.

$$x'(t) = a \cdot x(t) \implies x(t) = c \cdot e^{at}$$

$$\frac{dx}{dt} = ax$$

$$dx = ax \cdot dt$$

$$\int \frac{dx}{x} = \int a \cdot dt$$

$$\log x = at + C$$

$$x = C_1 \cdot e^{at}$$

$$e^x = \sum_{n=0}^{\infty} \frac{x^n}{n!}$$

$$e^{\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} t} = \sum_{n=0}^{\infty} \frac{\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}^n}{n!} t^n$$

$$e^{it} = \cos t + i \cdot \sin t$$

insert $\sum_{n=0}^{\infty} \frac{(it)^n}{n!}$ and split \Re and \Im .

$$\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}^2 = \begin{bmatrix} -1 & \\ & -1 \end{bmatrix}$$

$$\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}^3 = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$$

$$\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}^4 = \begin{bmatrix} 1 & \\ & 1 \end{bmatrix}$$

$$i^2 = -1 \quad i^3 = -i \quad i^4 = 1$$

$$e^{\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} t} = \cos(t) \cdot \begin{bmatrix} 1 & \\ & 1 \end{bmatrix} + \sin(t) \cdot \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$$

$$U_{\alpha+\beta} = U_\alpha \cdot U_\beta$$

$$\begin{bmatrix} \cos(\alpha + \beta) & -\sin(\alpha + \beta) \\ \sin(\alpha + \beta) & \cos(\alpha + \beta) \end{bmatrix} = \begin{bmatrix} \cos \alpha & -\sin \alpha \\ \sin \alpha & \cos \alpha \end{bmatrix} \cdot \begin{bmatrix} \cos \beta & -\sin \beta \\ \sin \beta & \cos \beta \end{bmatrix}$$

$$= \begin{bmatrix} \cos \alpha \cos \beta - \sin \alpha \sin \beta & -\cos \alpha \sin \beta - \sin \alpha \cos \beta \\ \sin \alpha \cos \beta + \cos \alpha \sin \beta & \sin \alpha \sin \beta + \cos \alpha \cos \beta \end{bmatrix}$$

Example 3.23 (Reflection in \mathbb{R}^2).

$$S(e_1) = \begin{bmatrix} \cos(2\varphi) \\ \sin(2\varphi) \end{bmatrix}$$

$$S(e_2) = \begin{bmatrix} \cos(2\varphi - \frac{\pi}{2}) \\ \sin(2\varphi - \frac{\pi}{2}) \end{bmatrix} = \begin{bmatrix} \sin(2\varphi) \\ -\cos(2\varphi) \end{bmatrix}$$

$$\frac{\pi}{2} - 2\psi = \frac{\pi}{2} - 2(\frac{\pi}{2} - \varphi) = 2\varphi - \frac{\pi}{2}$$

$$S = \begin{bmatrix} \cos(2\varphi) & \sin(2\varphi) \\ \sin(2\varphi) & -\cos(2\varphi) \end{bmatrix}$$

This lecture took place on 2018/05/07.

Linear isometries:

Theorem 3.26.

$$\mathcal{O}(n) = \{ U \in \mathbb{R}^{n \times n} \mid U^T U = I \} \quad \text{orthogonal group}$$

$$\mathcal{U}(n) = \{ U \in \mathbb{C}^{n \times n} \mid U^* U = I \} \quad \text{unitary group}$$

$SO(n) = \{U \in \mathbb{O} \mid \det(U) = 1\} \subseteq O(n)$ subgroup, special orthogonal group

$SU(n) = \{U \in \mathbb{U} \mid \det(U) = 1\} \subseteq \mathcal{U}(n)$ subgroup, special unitary group

$\mathcal{GL}(n, \mathbb{K}) = \{A \in \mathbb{K}^{n \times n} \mid \text{invertible}\}$ general linear group

$S\mathcal{L}(n, \mathbb{K}) = \{A \in GL(n) \mid \det(A) = 1\}$ special linear group

Then, e.g. $O(2)$ is the group of rotations and reflections.

Remark 3.19. For $U \in \mathcal{U}(n)$ it holds that $|\det(U)| = 1$. Why?

We know: $U^*U = I \implies \det(U^*U) = I = \det(U^*)\det(U) = \det(\overline{U}^T)\det(U) = \overline{\det(U^T)}\det(U) = \overline{\det(U)}\det(U) = |\det(U)|^2 = 1$.

Example 3.24 (Rotation).

$$U = \begin{bmatrix} \cos \varphi & -\sin \varphi \\ \sin \varphi & \cos \varphi \end{bmatrix}$$

$$\det U_\varphi = \cos^2(\varphi) + \sin^2(\varphi) = 1 \implies U_\varphi \in SO(2)$$

$$S_\varphi = \begin{bmatrix} \cos(2\varphi) & \sin(2\varphi) \\ \sin(2\varphi) & -\cos(2\varphi) \end{bmatrix}$$

$$\det(S_\varphi) = -\cos^2(2\varphi) - \sin^2(2\varphi) = -1$$

General orthogonal matrix in $O(2)$.

$$U = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \text{ with } \overline{U}U = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

$$\begin{bmatrix} a & c \\ b & d \end{bmatrix} \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} a^2 + c^2 & ab + cd \\ ab + cd & b^2 + d^2 \end{bmatrix} \stackrel{!}{=} \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

Resulting constraints:

$$a^2 + c^2 = 1 \tag{1}$$

$$b^2 + d^2 = 1 \tag{2}$$

$$ab + cd = 0 \tag{3}$$

$$\tag{4}$$

$$a = \cos \varphi \quad c = \sin \varphi \quad b = \cos \psi \quad d = \sin \psi$$

$$\cos \varphi \cdot \cos \psi + \sin \varphi \cdot \sin \psi = 0$$

$$\begin{bmatrix} \cos \alpha & -\sin \alpha \\ \sin \alpha & \cos \alpha \end{bmatrix} \begin{bmatrix} \cos \beta & -\sin \beta \\ \sin \beta & \cos \beta \end{bmatrix} = \begin{bmatrix} \cos(\alpha + \beta) \\ \sin(\alpha + \beta) \end{bmatrix}$$

$$\cos \alpha \cos \beta - \sin \alpha \sin \beta = \cos(\alpha + \beta)$$

$$\cos \varphi \cdot \cos \psi = \cos(\varphi - \psi)$$

$$\cos \alpha = 0 \text{ for } \alpha = \frac{\pi}{2} + k \cdot \pi = (k + \frac{1}{2})\pi \quad (k \in \mathbb{Z})$$

$$\implies \varphi - \psi = (k + \frac{1}{2})\pi$$

$$\varphi = \psi + (k + \frac{1}{2})\pi$$

$$\begin{aligned} \cos \varphi &= \cos(\psi + (k + \frac{1}{2})\pi) = \cos \psi \cos(k + \frac{1}{2})\pi - \sin \psi \underbrace{\sin(k + \frac{1}{2})\pi}_{\varepsilon \in \{\pm 1\}} \\ &= -\varepsilon \cdot \sin \psi \implies \sin \psi = -\varepsilon \cos \varphi \end{aligned}$$

$$\sin \alpha \cos \beta + \cos \alpha \sin \beta = \sin(\alpha + \beta)$$

$$\begin{aligned} \sin(\varphi) &= \sin(\psi + (k + \frac{1}{2})\pi) = \underbrace{\sin \psi \cos(k + \frac{1}{2})\pi}_{=\varepsilon \cdot \cos(\psi)} + \underbrace{\cos \psi \sin(k + \frac{1}{2})\pi}_{=0} \\ \cos \psi &= \varepsilon \sin \varphi \end{aligned}$$

$$U = \begin{bmatrix} \cos \varphi & \varepsilon \cdot \sin(\psi) \\ \sin \varphi & -\varepsilon \cos \varphi \end{bmatrix} = \underbrace{\begin{bmatrix} \cos \varphi & -\sin \varphi \\ \sin \varphi & \cos \varphi \end{bmatrix}}_{\substack{\text{rotation} \\ \det=1}} \cdot \underbrace{\begin{bmatrix} 1 & \\ & -\varepsilon \end{bmatrix}}_{\substack{\varepsilon=1: \\ \text{reflection on } x\text{-axis} \\ \varepsilon=-1: \text{id}}}$$

$$U_\varphi = \cos \varphi \begin{bmatrix} 1 & \\ & 1 \end{bmatrix} + \sin \varphi \begin{bmatrix} & -1 \\ 1 & \end{bmatrix}$$

Hence, every orthogonal matrix is either a rotation ($\det = 1$) or a reflection ($\det = -1$).

$$SO(2) : \left\{ U_\varphi = \cos \varphi + i \cdot \sin \varphi \quad 1 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, i = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \right\}$$

$$SU(2) : \left\{ a_0 + ia_1 + ja_2 + ka_3 \mid \sum a_i^2 = 1 \right\}$$

3.8 Quaternions

William Rowan Hamilton (1805–1865).

Remark 3.20 (Quaternions). *Hamilton defined the complex numbers in the modern sense in 1833.*

$$C = \{(a, b) \mid a, b \in \mathbb{R}\}$$

$$(a, b) \cdot (c, d) = (ac - bd, ad + bc)$$

He tried to invent them over 10 years for the third dimension. He failed. On 1843/10/16, he invented the quaternions next to a bridge. It works on four dimensions, but it is non-commutative. It is a screw field (Schiefkörper).

$$ij = k \quad jk = i \quad ki = j \quad ji = -k \quad kj = -i \quad ik = -j$$

anti-commutative.

$$i^2 = j^2 = k^2 = -1$$

$$(a_0 + a_1i + a_2j + a_3k)(b_0 + b_1i + b_2j + b_3k) \quad \text{linear}$$

$$(a_0 + \vec{a})(b_0 + \vec{b}) = a_0b_0 + a_0\vec{b} + b_1\vec{a} + \vec{a} \times \vec{b}$$

$$SO(2) \approx \left\{ \cos \varphi + i \cdot \sin \varphi \mid \varphi \in [0, 2\pi] \right\} = \{z \in \mathbb{C} \mid |z| = 1\} = \mathcal{T} \text{ Torus}$$

$$SU(2) = \left\{ a_0 + ia_1 + ja_2 + ka_3 \mid \sum a_i^2 = 1 \right\}$$

$$SO(2) \approx \left\{ \cos \varphi + i \sin \varphi \mid \varphi \in [0, 2\pi] \right\}$$

4 Polynomials and algebras

Definition 4.1. Let \mathbb{K} be a field, a \mathbb{K} algebra, a vector space \mathcal{A} over \mathbb{K} with a multiplication operator $*$: $\mathcal{A} \times \mathcal{A} \rightarrow \mathcal{A}$ with $(a, b) \rightarrow a * b$ such that

1. $a * (b + c) = a * b + a * c$ (distributive law, $a, b, c \in \mathcal{A}$)
2. $(a + b) * c = a * c + b * c$
3. $\lambda \cdot (a * b) = (\lambda \cdot a) * b = a * (\lambda \cdot b)$ ($a, b \in \mathcal{A}, \lambda \in \mathbb{K}$, associativity)

Remark 4.1. **Associativity** is not generally required.

$$a * (b * c) = (a * b) * c$$

If satisfied, it is called associative algebra.

Commutativity is not generally required.

$$a * b = b * a$$

If satisfied, it is called commutative algebra.

Example 4.1. 1. $(\mathbb{K}, +, * = \cdot)$ is a one-dimensional \mathbb{K} algebra.

2. $(\mathbb{K}^{n \times n}, +, * = \text{matrix multiplication})$ is an associative non-commutative algebra where $\mathbb{K}^{n \times n} \simeq \text{Hom}(V, V)$ and $f * g = f \circ g$.

3. $\mathbb{K}^\times = \{f : X \rightarrow \mathbb{K}\}$. Let X be an arbitrary set.

$$(\lambda f + \mu g)(x) = \lambda \cdot f(x) + \mu \cdot g(x)$$

$$(f * g)(x) = f(x) \cdot g(x)$$

$(\mathbb{K}^\times, +, *)$ is an associative, commutative algebra.

4. \mathbb{R}^3 with $a \times b$ is an algebra.

$$a \times b = -b \times a$$

is non-commutative and also non-associative:

$$a \times (b \times c) \neq (a \times b) \times c$$

Jacobian identity:

$$a \times (b \times c) + b \times (c \times a) + c \times (a \times b) = 0$$

5. $\mathcal{A} = \mathbb{K}^{n \times n}$

$$A * B = [A, B] = A \cdot B - B \cdot A \quad \text{“commutator”}$$

is an algebra with Jacobian identity. Lie algebra:

$$[A, [B, C]] + [B, [C, A]] + [C, [A, B]] = 0$$

$$[A, B] = -[B, A]$$

The so-called Lie groups (like $O(n)$, $\mathcal{U}(n)$, $SO(n)$, $SU(n)$).

6. $\mathcal{A} = \mathbb{K}^{n \times n}$

$$A * B = A \cdot B + B \cdot A$$

is associative. It is an Jordan algebra. Pascual Jordan (1902–1980)¹⁰.

O. Perron (1880/05/07–1975)

Definition 4.2.

$$\mathbb{K}^\infty = \{(a_0, a_1, a_2, \dots) \mid a_i \in \mathbb{K}\}$$

$$P_{\mathbb{K}} = \{(a_0, a_1, \dots, a_n, 0, \dots) \mid n \in \mathbb{N}, a_i \in \mathbb{K}\}$$

Cauchy product:

$$(a_n)_{n \geq 0} * (b_n)_{n \geq 0} = (c_n)_{n \geq 0}$$

$$c_n = \sum_{k=0}^n a_k b_{n-k}$$

¹⁰Different Jordan than in Gauss-Jordan and different than C. Jordan (19th century) about to come

Lemma 4.1. 1. $(P_{\mathbb{K}}, *)$ is a commutative, associative algebra with one-element $(1, 0, \dots)$. The basis is given with $1, x, x^2, \dots$. The algebra is called polynomial algebra

$$\mathbb{K}[x] = \left\{ \sum_{k=0}^n a_k x^k \mid a_k \in \mathbb{K}, n \in \mathbb{N} \right\}$$

2. $(\mathbb{K}^{\infty}, *)$ is a commutative algebra with one-element $(1, 0, \dots)$ and is called algebra of formal power series¹¹

$$\mathbb{K}[[x]] = \left\{ \sum_{k=0}^{\infty} a_k x^k \mid a_k \in \mathbb{K} \right\}$$

Proof. Show that $\forall a, b \in P_{\mathbb{K}} : a * b \in P_{\mathbb{K}}$, hence only finitely many c_n are $\neq 0$.

Remark: $a_k = 0 \forall k > m$ and $b_k = 0 \forall k > n$.

Claim.

$$c_k = 0 \forall k > m + n$$

$$\begin{aligned} c_k &= \sum_{l=0}^k a_l b_{k-l} \\ &= \sum_{l=0}^{m-1} a_l b_{k-l} \quad \text{equality if } l > m \implies a_l = 0 \\ &= 0 \end{aligned}$$

$$k > m + n, l < m \implies -l > -m \implies k - l \underbrace{>}_{\implies b_{k-l}=0} m + n - m = n$$

About the Cauchy product:

$$c_n = \sum_{k=0}^n a_k b_{n-k} = \sum_{k'=0}^n a_{n-k'} b_{k'} = (b * a)_n \quad (k' = n - k)$$

Law of distributivity:

$$\begin{aligned} [(a + b) * c]_n &= \sum_{k=0}^n (a + b)_k \cdot c_{n-k} \\ &= \sum_{l=0}^n (a_l c_{n-l} + b_l c_{n-l}) \\ &= (a * c)_n + (b * c)_n \end{aligned}$$

□

¹¹We don't need to consider convergence. This is purely formal object.

Definition 4.3. Let $x^0 = (1, 0, \dots)$ and $x^k = (0, \dots, 1, 0, \dots)$ create a basis. The elements of $p(x) = \mathbb{K}[x]$ are called polynomials in the formal variable x

$\deg p(x) = \max \{k \mid a_k \neq 0\}$ is called degree of the polynomial

$$\deg(0) := -\infty$$

Lemma 4.2 (Will be done in the practicals). 1. $\deg(p(x) \cdot q(x)) = \deg(p(x)) + \deg(q(x))$

2. $\mathbb{K}[x]$ is zero-divisor-free, hence $p(x) \cdot q(x) = 0 \implies p(x) = 0 \vee q(x) = 0$

Definition 4.4. Every polynomial $p(x) \in \mathbb{K}[x]$ induces a polynomial function $p : \mathbb{K} \rightarrow \mathbb{K}$ with $\alpha \mapsto p(\alpha)$ with $p \in \mathbb{K}^{\mathbb{K}}$.

$$\implies (\lambda p + \mu q)(\alpha) = \lambda \cdot p(\alpha) + \mu \cdot q(\alpha)$$

$$(p \cdot q)(\alpha) = p(\alpha) \cdot q(\alpha)$$

The map $\mathbb{K}[x] \rightarrow \mathbb{K}^{\mathbb{K}}$ with $p(x) \mapsto$ polynomial function p is linear and multiplicative (called algebra homomorphism).

Remark 4.2. A polynomial and a polynomial function are not the same. If $|\mathbb{K}| < \infty$, for example consider \mathbb{Z}_5 .

$$|\mathbb{Z}_5^{\mathbb{Z}_5}| = 5^5$$

$$|\mathbb{K}[x]| = \infty$$

For example, $\prod_{\alpha \in \mathbb{K}} (x - \alpha)$ corresponds to the polynomial function 0. Hence the map $\mathbb{K}[x] \rightarrow \mathbb{K}^{\mathbb{K}}$ is surjective but not injective.

On finite fields, every function is a polynomial function.

$$\eta_i = f(\xi_i) \quad \{\xi_1, \dots, \xi_n\} = \mathbb{K}$$

From the practicals, it will follow that there exists a polynomial of degree n such that $p(\xi_i) = \eta_i$.

Definition 4.5. An algebra homomorphism is a linear map between ψ and two \mathbb{K} -algebras \mathcal{A} and \mathcal{B} such that $\forall a, b \in \mathcal{A} : \psi(a * b) = \psi(a) * \psi(b)$.

Example 4.2. 1. $\mathbb{K}[x] \rightarrow \mathbb{K}^{\mathbb{K}}$ with $p(x) \mapsto$ polynomial function

2. Let $\alpha \in \mathbb{K}$ be fixed. $\psi_\alpha : \mathbb{K}[x] \rightarrow \mathbb{K}$ with $p(x) \mapsto p(\alpha)$ is an algebra homomorphism of $\mathbb{K}[x] \rightarrow \mathbb{K}$.

$$\psi_\alpha(\lambda p + \mu q) = (\lambda p + \mu q)(\alpha) = \lambda p(\alpha) + \mu q(\alpha) = \lambda \psi_\alpha(p) + \mu \psi_\alpha(q)$$

3. Consider $\iota : \mathbb{K} \rightarrow \mathbb{K}[x]$ with $\iota : \alpha \mapsto \alpha \cdot x^0$.

$$(\alpha \cdot x^0) \cdot (\beta \cdot x^0) = (\alpha \cdot \beta) \cdot x^0$$

Theorem 4.1 (Insertion theorem, dt. Einsetzungssatz). *Let \mathcal{A} be an associative algebra with one-element $\mathbf{1}_A$ and $\iota : \mathbb{K} \rightarrow \mathcal{A}$ with $\alpha \mapsto \alpha \cdot \mathbf{1}_A$ is the insertion of \mathbb{K} .*

Then for every $a \in \mathcal{A}$ the map

$$\psi_a : \mathbb{K}[x] \rightarrow \mathcal{A}$$

$$\sum_{k=0}^n c_k x^k \mapsto \sum_{k=0}^n c_k a^k$$

of the unique algebra homomorphism of $\mathbb{K}[x] \rightarrow \mathcal{A}$ with the property $\psi_a(x) = a$. We say, $\mathbb{K}[x]$ is a free, associative algebra over \mathbb{K} . Every algebra homomorphism $\mathbb{K}[x] \rightarrow \mathcal{A}$ has the structure.

This lecture took place on 2018/05/09.

We consider algebras as vector spaces with associative multiplication. For example, matrices and polynomials. An algebra homomorphism is linear and multiplicative.

$$\Phi(a + b) = \Phi(a) * \Phi(b)$$

\mathcal{A} is an associative algebra with $\mathbf{1}_A$.

$$l : \mathbb{K} \rightarrow \mathcal{A}$$

$$\alpha \mapsto \alpha \cdot \mathbf{1}_{\mathcal{A}}$$

$a \in \mathcal{A} \implies \mathcal{L}(a^0, a^1, a^2, a^3, \dots) \subseteq \mathcal{A}$ subalgebra.

1.

$\exists! \Phi_a : \mathbb{K}[a] \rightarrow \mathcal{A}$ algebra homomorphism

such that $\Phi_a(x) = a$, namely $\Phi_a\left(\sum_{k=0}^n c_k x^k\right) = \sum_{k=0}^n c_k a^k$.

2. Every homomorphism $\Psi : \mathbb{K}[x] \rightarrow \mathcal{A}$ has this structure.

Proof. Let $a = \Psi(x) \implies \Psi(x^n) = \Psi(x)^n = a^n$ by homomorphism.

$$\Psi \text{ linear} \implies \Psi\left(\sum_{k=0}^n c_k x^k\right) = \sum_{k=0}^n c_k \Psi(x^k) = \sum_{k=0}^n c_k a^k$$

x^0, x^1, \dots give a basis of $\mathbb{K}[x]$. Hence $\Psi = \Phi_a$ with $a = \Psi(x)$. On the opposite (1.): Obviously Φ_a is linear. Multiplicative: Show that

$$\underbrace{\Psi_a(p(x) \cdot q(x))}_{=p(a) \cdot q(a)} \stackrel{!}{=} \underbrace{\Phi_a(p(x)) \cdot \mathcal{A}\Phi_a(q(x))}_{=p(a) \cdot q(a)}$$

□

Example 4.3. 1. $\mathcal{A} = \mathbb{K}$.

$$\Psi_\alpha : \mathbb{K}[x] \rightarrow \mathbb{K}$$

$$p(x) \mapsto p(\alpha)$$

2. $\mathcal{A} = \mathbb{K}^{n \times n} \approx \text{Hom}(V, V)$

$$A^0 = I \quad A^n = A \cdot A^{n-1}$$

$$I : \mathbb{K} \rightarrow \mathbb{K}^{n \times n}$$

$$\alpha \mapsto \alpha \cdot I$$

$$\Psi_\alpha : \mathbb{K}[x] \rightarrow \mathbb{K}^{n \times n}$$

$$p(x) \mapsto p(A)$$

$$\sum_{k=0}^n c_k x^k \mapsto \sum_{k=0}^n c_k \cdot A^k$$

Remark 4.3. Let $\mathbb{K}[x]$ be a free, associative algebra over \mathbb{K} with a generator. Hence, for all associative algebras \mathcal{A} , given some element $a \in \mathcal{A}$. There exists exactly one homomorphism $\varphi : \mathbb{K}[x] \rightarrow \mathcal{A}$ such that $\varphi(x) = a$.

Compare it with a free group with one generator. Is a group G generated by x such that \forall groups H , if $h \in H$ given, there exists exactly one group homomorphism $\varphi : G \rightarrow H$ such that $\varphi(x) = h$. Namely, $G = (\mathbb{Z}, +)$ is generated by **1**. Given $h \in H \rightarrow \varphi_h : \mathbb{Z} \rightarrow H_k$ and $k \mapsto h$.

Definition 4.6. A root of a polynomial $p(x) \in \mathbb{K}[x]$ is a $\xi \in \mathbb{K}$ such that $p(\xi) = \Psi_\xi(p) = 0$, hence $p(x) \in \ker \Psi_\xi$.

Remark 4.4. $p(x) = C_0$ is no root except $c_0 = 0$.

$p(x) = c_0 + c_1 x$ is the only root, $\xi = -\frac{c_0}{c_1}$.

$$p(x) = c_0 + c_1 x + c_2 x^2$$

has two roots over \mathbb{C} .

$$p(x) = c_0 + c_1 x + c_2 x^2 + c_3 x^3$$

has three roots.

To find roots, formulas up to fourth degree exist. For degree ≥ 5 , there is no equation.

Paolo Ruffini (1765–1822)

Niels Henrik Abel (1802–1829)

Gerolamo Cardano (1501–1576)

Remark 4.5. Cardano was a polymath.

1. founder of probability theory
2. Liber de ludo aleae: important book on probability
3. Cardan joint (dt. Kardanische Welle)
4. Gimbal (dt. Kardanische Aufhängung)

5. used $\sqrt{-1}$ as a valid expression for the first time
6. published a solution for roots of cubic polynomials (*Ars Magna*, 1545)

Scipione del Ferro (1465–1526)

1. used a solution for roots of cubic polynomials in competitions, kept it secret
2. came up with the same solution like Tartaglia
3. lost competitions on cubic polynomials to Antonio Fiore, because Ferro's solution was not generic enough

Niccolò Fontana Tartaglia (1500–1557)

1. Cardano cajoled Tartaglia into revealing his solution to the cubic equations by promising not to publish them.

Ludovico Ferrari (1522–1565)

Theorem 4.2 (Method by Cardano/del Ferro).

$$a_0 + a_1x + a_2x^2 + a_3x^3 = 0$$

$$x \rightarrow x + a \quad \text{such that } a_2 = 0$$

$$x^3 + px + q = 0$$

Cubus p.6 rebus aeq 20

$$x^3 + 6x = 20$$

$x = \text{res}$, $x^2 = \text{census}$, $x^3 = \text{cubus}$.

Approach: $x = u + v$.

$$u^3 + 3u^2v + 3uv^2 + v^3 + p(u + v) + q = 0$$

$$u^3 + v^3 + (3uv + p)(u + v) + q = 0$$

Requirement: u and v such that $3uv + p = 0$.

$$\begin{cases} u^3 + v^3 + q = 0 & \implies v^3 = -(q + u^3) \\ 3uv + p = 0 & \implies uv = -\frac{p}{3u} \end{cases}$$

$$u^3 \cdot v^3 = -\frac{p^3}{27}$$

$$-u^3(q + u^3) = -\frac{p^3}{27}$$

$$u^6 + qu^3 - \frac{p^3}{27} = 0$$

$$u^3 = ?$$

Equation for degree 2 by Viète, Francois (1540–1603):

$$(y - \alpha)(x - \beta) = x^2 - (\alpha + \beta)x + \alpha\beta$$

$$x^2 + px + q$$

$$p = -(\alpha + \beta)$$

$$q = \alpha \cdot \beta$$

$$\alpha = \frac{1}{2} \left[(\alpha + \beta) + \sqrt{(\alpha - \beta)^2} \right]$$

$$\beta = \frac{1}{2} \left[(\alpha + \beta) - \sqrt{(\alpha - \beta)^2} \right]$$

$$\frac{\alpha}{\beta} = \frac{1}{2} \left(\alpha + \beta \pm \sqrt{(\alpha - \beta)^2} \right) = \frac{1}{2} \left(\alpha + \beta \pm \sqrt{\underbrace{\alpha^2 + \beta^2 - 2\alpha\beta}_{(\alpha+\beta)^2 - 4\alpha\beta}} \right) = \frac{1}{2} \left(-p \pm \sqrt{p^2 - 4q} \right)$$

Hence,

$$u^3 = \frac{1}{2} \left(-q \mp \sqrt{q^2 + \frac{4p^3}{27}} \right)$$

$$u^3 = \frac{q}{2} \pm \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}$$

$$u = \sqrt[3]{-\frac{q}{2} \pm \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}$$

$$v^3 = -q - u^3 = -\frac{q}{2} \mp \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}$$

$$x = u + v = \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} + \sqrt[3]{-\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}$$

Theorem 4.3 (Division with remainder). $p(x), q(x) \in \mathbb{K}[x]$, $q(x) \neq 0$.

Then there exists exactly one polynomial $s(x), r(x) \in \mathbb{K}[x]$,

$$p(x) = s(x) \cdot q(x) + r(x)$$

with $\deg r(x) < \deg q(x)$.

Proof. Induction over $\deg p(x)$.

Induction base

$$\deg p(x) < \deg q(x) \leadsto p(x) = 0 \cdot q(x) + p(x)$$

If $\deg p(x) \geq \deg q(x)$,

$$p(x) = \sum_{k=0}^n a_k x^k \quad q(x) = \sum_{k=0}^m b_k x^k$$

$$a_n \neq 0 \quad m \leq n \quad b_m \neq 0$$

$$p_1(x) = p(x) - \frac{a_n}{b_m} \cdot q(x) \cdot x^{n-m}$$

cancels the largest term $a_n x^n$ in $p(x)$.

$$\begin{aligned} &= \sum_{k=0}^n a_k x^k - \frac{a_n}{b_m} \sum_{k=0}^m b_k x^{k+n-m} \\ &= a_n x^n + \sum_{k=0}^{n-1} a_k x^k - \frac{a_n}{b_m} b_m \cdot x^{m+n-m} - \frac{a_n}{b_m} \sum_{k=0}^{m-1} b_k x^{k+n-m} \end{aligned}$$

what remains is a polynomial of degree $\deg p_1(x) \leq n - 1$.

$$\implies p(x) = \frac{a_n}{b_m} x^{n-m} \cdot q(x) + p_1(x)$$

By induction hypothesis,

$$p_1(x) = s_1(x) \cdot q(x) + r_1(x)$$

Hence,

$$p(x) = \left(\frac{a_n}{b_m} x^{n-m} + s_1(x) \right) q(x) + r_1(x)$$

□

Example 4.4.

$$p(x) = 3x^5 - x^4 + 2x^3 + x^2 + 1$$

$$q(x) = x^2 - 3x + 1$$

$$\begin{array}{r|rrrrrrrrrr} 3x^5 & -x^4 & +2x^3 & +x^2 & +1 & : & x^2 & -3x & +1 & = & 3x^3 & +8x^2 & +23x & +62 \\ -3x^5 & +9x^4 & -3x^3 & & & & & & & & & & & \\ 0 & 8x^4 & -x^3 & +x^2 & +1 & & & & & & & & & \\ & 8x^4 & -24x^3 & +8x^2 & & & & & & & & & & \\ & 0 & 23x^3 & -7x^2 & +1 & & & & & & & & & \\ & & 23x^3 & -69x^2 & +23x & & & & & & & & & \\ & & 0 & 62x^2 & -23x & +1 & & & & & & & & \\ & & & 62x^2 & -186x & +62 & & & & & & & & \\ & & & & 163x & -61 & & & & & & & & \end{array}$$

Hence, $s(x) = 3x^3 + 8x^2 + 23x + 62$ and $r(x) = 163x - 61$.

Definition 4.7. $q(x)$ divides $p(x)$ if the remainder is zero.

There exists $s(x)$ such that $p(x) = s(x) \cdot q(x)$.

Theorem 4.4. 1. If $p(x) = s(x) \cdot (x - \xi) + r$

$$q(x) = x - \xi \implies p(\xi) = r$$

2. ξ is root of $p(x) \implies x - \xi$ divides $p(x)$

Theorem 4.5 (Ruffini-Horner's method). Given $p(x) \in \mathbb{K}[x]$, $\lambda \in \mathbb{K}$. Find $p(\lambda)$.

$$\begin{aligned} p(x) &= a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0 \\ &= a_n \lambda^n + a_{n-1} \lambda^{n-1} + \dots + a_1 \lambda + a_0 \\ &= (a_n \lambda^{n-1} + \dots + a_1) \lambda + a_0 \\ &= ((a_n \lambda^{n-2} + \dots + a_1) \lambda + a_1) \lambda + a_0 \\ &= \vdots \end{aligned}$$

Algorithm:

$$\xi_n = a_n \text{ for } k = n - 1, \dots, 0 \quad \xi_k = \lambda \xi_{k+1} + a_k$$

$$p(\lambda) = \xi_0$$

If $p(x) = s(x)(x - \lambda) + r$, $p(\lambda) = r$.

Example 4.5.

$$\begin{array}{r}
 3x^5 - x^4 + 2x^3 + x^2 + 1 \\
 p(5) = ? \quad \xi_5 = 3 \\
 \begin{array}{r}
 3x^5 - x^4 + 2x^3 + x^2 + 1 : (x - 5) = 3x^4 + 14x^3 + 72x^2 + 361x + 1805 \\
 3x^5 - 15x^4 \\
 0 \quad 14x^4 + 2x^3 + x^2 + 1 \\
 \quad 14x^4 - 70x^3 \\
 \quad \quad 0 \quad +72x^3 + x^2 + 1 \\
 \quad \quad \quad 72x^3 - 360x^2 \\
 \quad \quad \quad \quad 0 \quad +361x^2 + 1 \\
 \quad \quad \quad \quad \quad 361x^2 - 1805x \\
 \quad \quad \quad \quad \quad \quad 1805x + 1 \\
 \quad \quad \quad \quad \quad \quad 1805x - 5 \cdot 1805 \\
 \quad \quad \quad \quad \quad \quad \quad 5 \cdot 1805 + 1
 \end{array} \\
 \xi_5 = 3 \\
 \xi_4 = 5 \cdot \xi_5 + (-1) = 5 \cdot 3 - 1 = 14 \\
 \xi_3 = 5 \cdot 14 + 2 = 72 \\
 \xi_2 = 5 \cdot 72 + 1 = 361 \\
 \xi_1 = 5 \cdot 361 + 0 = 1805 \\
 \xi_0 = 5 \cdot 1805 + 1 = 9026
 \end{array}$$

Definition 4.8. A polynomial $p(x) \in \mathbb{K}[x]$ is called *reducible*, if $\exists p_1(x), p_2(x) : \deg p_1(x) < \deg p(x)$ and $p(x) = p_1(x) \cdot p_2(x)$ (is the factorization). $\deg p_2(x) < \deg p(x)$ (proper divisor). Otherwise the polynomial is called *irreducible*.

Remark 4.6. An irreducible polynomial of degree > 1 has no roots.

Example 4.6. • Consider $x^2 = -2$ irreducible over $\mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$. Its roots are $\pm \sqrt{2}$.

It is reducible over \mathbb{R} : $x^2 - 2 = (x - \sqrt{2})(x + \sqrt{2})$.

It is reducible over $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$.

• Consider $x^2 + 1$ irreducible over \mathbb{Q}, \mathbb{R} and reducible over \mathbb{C} . Its roots are $\pm i$.

$\mathbb{Q}(i) = \{a + bi \mid a, b \in \mathbb{Q}\}$. $x^2 + 1 = (x + i)(x - i)$.

• Consider $\mathbb{K} = \mathbb{Z}_2$ and $p(x) = x^2 + x + 1$. This polynomial has no roots and is irreducible.

• $x^5 + x + 1$ has no roots, is reducible.

$$x^5 + x + 1 = (x^2 + x + 1)(x^3 + x^2 + 1)$$

Is there some field $\mathbb{K} \supseteq \mathbb{Z}_2$ such that $x^3 + x^2 + 1$ has roots?

Yes. Let α be a number such that $\alpha^3 + \alpha^2 + 1 = 0 \implies \alpha^3 = -\alpha^2 - 1 = \alpha^2 + 1$.

$$\mathbb{K} = \mathbb{Z}_2(\alpha) = \{a + b\alpha + c\alpha^2 \mid a, b, c \in \mathbb{Z}_2\}$$

with $\alpha^3 = \alpha^2 + 1$ is a field.

Let i be a number such that $i^2 + 1 = 0$, thus $i^2 = -1$

$$\mathbb{C} = \mathbb{R}(i) = \{a + bi \mid a, b \in \mathbb{R}\}$$

Hence, irreducible is not equivalent to some root exists. The implication works only in one direction. There always exists some field such that roots exist.

Theorem 4.6 (Fundamental theorem of Algebra). \mathbb{C} is algebraically closed, hence every polynomial has a root over \mathbb{C} .

Corollary. Every polynomial over \mathbb{C} . . .

1. has a factorization $p(x) = (x - \xi_1)(x - \xi_2) \dots (x - \xi_n)$.
2. $p(x)$ is irreducible $\iff \deg p(x) \leq 1$.

Remark 4.7. No algebraic proof exists. It is more like a Fundamental Theorem of Calculus over complex numbers. The proof is given by the Lionville theorem (not done here).

Theorem 4.7. For arbitrary fields, it holds that every polynomial has exactly one factorization (except for its order) in irreducible factors.

Index

- Adjoint map, 88
- Adjugate matrix, 32
- Algebra, 101
- Algebra homomorphism, 104
- Alternating group, 14
- Associative algebra, 101

- Basis of a polynomial, 104
- Bilinearity, 4

- Cauchy product, 102
- Chebyshev polynomials, 86
- Cofactor, 32
- Commutative algebra, 101
- Commutator, 101
- Complementary matrix, 32
- Complex numbers, 100
- Congruence of matrices, 50
- Conjugate transpose, 48
- Cross product, 39

- Degree of a polynomial, 104
- Determinant, 15
- Determinant form, 7
- Determinant of a matrix, 3

- Euclidean norm, 45
- Euclidean space, 62

- Factorization of a polynomial, 111
- Formal power series algebra, 102

- Gram matrix of tuple v_1, v_2, \dots, v_m , 77
- Gram-Schmidt process, 82

- Hermitian form, 43
- Hermitian matrix, 48

- Indefinite inner product, 43
- Involution, 90
- Irreducible polynomial, 111
- Isometry, 94, 95

- Jacobian identity, 101

- Jordan algebra, 101

- Lie algebra, 101
- Lie groups, 101
- Linear dependence, 5
- Linear isometry, 92

- Malposition, 11
- Method by Cardano/del Ferro, 107
- Minor of a square matrix, 60
- Multilinearity, 7

- Negative definite inner product, 43
- Norm, 45

- Orthogonal complement, 67
- Orthogonal matrix, 94
- Orthonormal, 64
- Orthonormal basis, 64
- Outer product, 39

- Permanent of a square matrix, 24
- Polynomial algebra, 102
- Polynomial division, 108
- Polynomial function, 104
- Positive inner product, 43
- Positive semidefinite inner product, 43

- Quaternions, 100

- Reducible polynomial, 111
- Root of a polynomial, 106

- Self-adjoint map, 92
- Self-adjoint matrix, 48
- Signature of π , 11
- Special linear group, 33
- Symmetric group, 9

- Unitary matrix, 94
- Unitary product, 43
- Unitary space, 62
- Unitary transformation, 92