LINEARE ALGEBRA U. ANALYTISCHE GEOMETRIE

Von Thomas Pajor

[pic]

Mitschrieb der Vorlesung von Prof. Weil im Wintersemester 2004/2005 an der UNI Karlsruhe (TH).

Vorwort

Dies ist ein Mitschrieb der Vorlesung „Lineare Algebra und Analytische Geometrie für die Fachrichtung Informatik“ an der Universität Karlsruhe (TH) aus dem Jahre 2004/2005. Wenn mir noch was tolles einfällt schreibe ich es hier rein.

Wenn sich Fehler finden, so teilt mir diese doch bitte via e-Mail mit (thomas.pajor@logn.de). Die aktuellste Version des Skripts findet sich immer auf www.logn.de

Viel Spass beim Lernen und viel Erfolg in der Klausur!

Inhaltsverzeichnis

0 Vorbemerkungen, Mengen, Abbildungen, Relationen 4
§1 Mengen . . . 4
§2 Teilmengen . . . 4
§3 Mengenoperationen . . . 5
§4 Abbildungen . . . 5
§5 Umgang mit Abbildungen . . . 6
§6 Relationen . . . 8

1 Grundbegriffe der Algebra 11
§1 Lineare Gleichungssysteme . . . 11
§2 Gruppen . . . 11
§3 Körper und Ringe . . . 20
§4 Matrizen und Polynome . . . 29
§5 Der Gauß-Algorithmus . . . 38

2 Vektorräume 44
§1 Vektorräume und Untervektorräume . . . 44
§2 Lineare Abhängigkeit und Unabhängigkeit . . . 46
§3 Basis und Dimension . . . 50
§4 Summen und Faktorräume . . . 58
§5 Affine Unterräume eines Vektorraums . . . 63

3 Lineare Abbildungen 67
§1 Definition und Eigenschaften linearer Abbildungen . . . 67
§2 Vektorräume linearer Abbildungen . . . 70
§3 Darstellung linearer Abbildungen durch Matrizen . . . 75

4 Determinanten und Eigenwerte 81
§1 Determinate . . . 81
§2 Eigenwerte und Diagonalisierbarkeit . . . 89
§3 Der Satz von Cayley-Hamilton . . . 95
§4 Die Jordansche Normalform . . . 99

5 Euklidische und Unitäre Vektorräume 108
§1 Skalarprodukte . . . 108
§2 Orthonormalbasen und Orthogonalprojektionen . . . 117
§3 Adjungierte Abbildungen . . . 127
§4 Isometrien . . . 130

6 Anhang 137
§1 Klausurvorbereitung . . . 137

0 Vorbemerkungen, Mengen, Abbildungen, Relationen

Vorlesung: 2004-10-20

§1 Mengen

$A := \{2, 3, 4, 7, 9\}$
$A := \{\text{Primzahlen}\}$

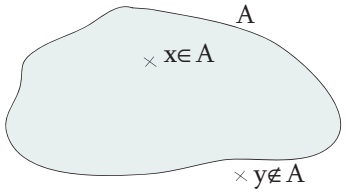

Abbildung 1: Menge

Beispiel:

- $\mathbb{N} := \{1, 2, 3, \ldots\}$ - natürliche Zahlen
- $\mathbb{Z} := \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\} = \{0, -1, 1, -2, 2, -3, 3, \ldots\}$ - ganze Zahlen
- $\{2, 3, 2, 4, 5\} = \{2, 3, 4, 5\}$
- $\mathbb{Q} = \left\{ \frac{p}{q} \mid p, q \in \mathbb{Z},\ q \neq 0 \right\}$ - rationale Zahlen
- $\mathbb{R}$ - reelle Zahlen
- $\emptyset$ - leere Menge

§2 Teilmengen

$A \subset B$ (A ist Teilmenge von B)
$A \subsetneq B$ (A ist *echte* Teilmenge von B)
$A \not\subset B$ (nicht Teilmenge): $\{1, 2, 4\} \not\subset \{1, 2, 5, 6\}$

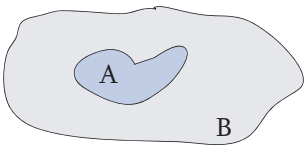

Abbildung 2: $A \subsetneq B$

Definition 0.1. A ist Teilmenge von B, wenn jedes Element von A auch Element von B ist.

$$A \subset B \ :\Leftrightarrow\ x \in A \Rightarrow x \in B$$

§3 Mengenoperationen

Definition 0.2. Es seien A, B Mengen, dann:

- Vereinigung: $A \cup B \ :\Leftrightarrow \ \{x \mid x \in A \vee x \in B\}$
- Durchschnitt: $A \cap B \ :\Leftrightarrow \ \{x \mid x \in A \wedge x \in B\}$
- Differenz: $A \backslash B \ :\Leftrightarrow \ \{x \mid x \in A, \ x \notin B\}$

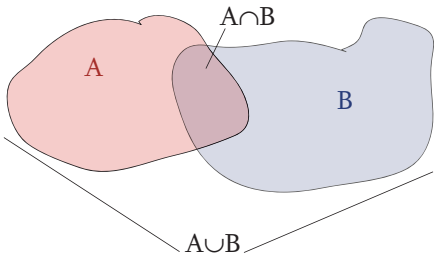

Abbildung 3: Durchschnitt und Vereinigung

Satz 0.1 (De Morgan). A, B, C Mengen, dann gilt:

(i) $A \backslash (B \cup C) \ = \ (A \backslash B) \cup (A \backslash C)$

(ii) $A \backslash (B \cap C) \ = \ (A \backslash B) \cap (A \backslash C)$

Beweis:

(i) $x \in A \backslash (B \cup C) \ \Leftrightarrow \ x \in A$ und $x \notin (B \cup C)$
$\Leftrightarrow \ x \in A$ und $x \notin B$ und $x \notin C$
$\Leftrightarrow \ (x \in A$ und $x \notin B)$ und $(x \in A$ und $x \notin C)$
$\Leftrightarrow \ x \in (A \backslash B) \cup (A \backslash C)$

(ii) analog.

□

§4 Abbildungen

Definition 0.3. A, B Mengen, Abb. $f : A \ \rightarrow \ B$

f ordnet jedem $x \in A$ ein (eindeutig bestimmtes) $y \in B$ zu.

$y = f(x)$

Definition 0.4 (Kreuzprodukt). Es seien A, B Mengen, dann ist das *Kreuzprodukt* $A \times B$ definiert als

$$A \times B = \{(x, y) \mid x \in A, \ y \in B\}$$

Beispiel:

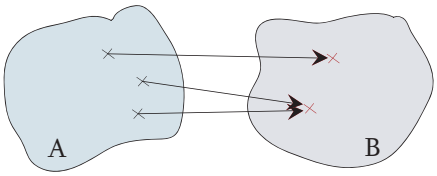

Abbildung 4: $f : A \to B$

- $f : \mathbb{R} \to \mathbb{R}$
  $x \mapsto (x-1)^2$
- $f : \mathbb{N} \to \mathbb{Z}$
  $n \mapsto \begin{cases} -\frac{n}{2} & n \text{ gerade} \\ \frac{n-1}{2} & n \text{ ungerade} \end{cases}$

Definition 0.5.

$$B^A := \{f : A \to B \mid f \text{ Abb}\}$$

Definition 0.6. Sei $f : A \to B$ Abb:

- A heißt *Definitionsbereich*
- B heißt *Wertebereich*
- $f(A) := \{f(x) \mid x \in A\}$ heißt *Bild* von A (unter f)
- $y = f(x)$ heißt Bild von x (unter f) und x heißt *Urbild* von y (unter f)
- Für $C \subset B$ sei $f^{-1}(C) := \{x \in A \mid f(x) \in C\}$ $\quad (\Rightarrow f^{-1}(B) = A)$ $\quad (\Rightarrow f^{-1}(A) = A)$

Definition 0.7. Sei $f : A \to B$ Abb:

(i) f heißt *surjektiv* $:\Leftrightarrow f(A) = B$

(ii) f heißt *injektiv* $:\Leftrightarrow x, y \in A(x \neq y) \Rightarrow f(x) \neq f(y)$

(iii) f heißt *bijektiv* $:\Leftrightarrow$ f injektiv und f surjektiv

Beispiel:

(i) $f : \mathbb{R} \to \mathbb{R}$
$x \mapsto (x-1)^2$ nicht injektiv und nicht surjektiv.

(ii) $f : \mathbb{R} \to \mathbb{R}$
$x \mapsto (x-1)x(x+1)$ nicht injektiv aber surjektiv.

Vorlesung: 2004-10-22

§5 Umgang mit Abbildungen

Definition 0.8. Seien A, B, C Mengen

(i) Die Abbildung $\mathrm{id}_A : A \to A,\ x \mapsto x$ heißt *identische* Abbildung (oder *Identität*) auf A.

(ii) Sei $f : A \to B,\ x \mapsto f(x)$ Abbildung und $C \subset A$. Dann heißt $f|_C : C \to B,\ x \mapsto f(x)$ *Einschränkung* oder Restriktion von f auf C.
Sei $g : C \to B$. Ist $g = f|_C$, so heißt f auch eine *Fortsetzung* von g auf die Menge A.

(iii) Sei $f : A \to B$ bijektiv. Dann heißt $f^{-1} : B \to A,\ y \mapsto x$ mit $f(x) = y$ *Umkehrabbildung* (oder auch inverse Abbildung) von f.

(iv) Seien $f : A \to B,\ g : B \to C$ Abbildungen. Dann heißt $g \circ f : A \to C,\ x \mapsto g(f(x))$ die zusammengesetzte Abbildung oder *Komposition* von f und g.

Bemerkung:

(i) Ist $f : A \to B$ bijektiv, so auch f^{-1} und $(f^{-1})^{-1} = f$.

Beweis:

f^{-1} surjektiv: Sei $x \in A$. Setze $y = f(x) \Rightarrow f^{-1}(y) = x \Rightarrow f$ surjektiv.

f^{-1} injektiv: Seien $y, \widetilde{y} \in B$ mit $f^{-1}(y) = f^{-1}(\widetilde{y})$. Nun ist $y = f(x),\ \widetilde{y} = f(\widetilde{x})$ für geeignete $x, \widetilde{x} \in A$.
$\Rightarrow x = f^{-1}(y) = f^{-1}(\widetilde{y}) = \widetilde{x}$.
$\Rightarrow x = f(x) = f(\widetilde{x}) = \widetilde{y}$
$\Rightarrow f$ injektiv. □

(ii) Ist f bijektiv, so gilt:

$$f^{-1} \circ f = \mathrm{id}_A$$

$$f \circ f^{-1} = \mathrm{id}_B$$

(iii) Komposition ist im Allgemeinen nicht kommutativ.

Beispiel:

- $f : \mathbb{R} \underset{x \mapsto x^2}{\to} \mathbb{R} \quad g : \mathbb{R} \underset{x \mapsto -x}{\to} \mathbb{R}$
  $g \circ f : x \mapsto -x^2$
  $f \circ f : x \mapsto x^2$
- $\left.\begin{array}{l} f : \mathbb{R} \underset{x \mapsto (x,2x)}{\to} \mathbb{R}^2 := \mathbb{R} \times \mathbb{R} \\ g : \mathbb{R} \underset{x \mapsto -x}{\to} \mathbb{R} \end{array}\right\} \begin{array}{l} f \circ g : \mathbb{R} \underset{x \mapsto (-x,-2x)}{\to} \mathbb{R}^2 \\ g \circ f \text{ ex nicht} \end{array}$

  Zitat Prof. Weil: „Pathologisches Beispiel“.

Einschub. $A_1, \ldots, A_n$ Mengen

$A_1 \times \ldots \times A_n := \{(x_1, \ldots, x_n) \mid x_1 \in A_1, \ldots, x_n \in A_n\}$

$A^n := \underbrace{A \times \ldots \times A}_{n\text{-mal}}$

$R^n := \{(x_1, \ldots, x_n) \mid x_i \in \mathbb{R}\}$

(iv) Ist $f : A \to B$ Abb, $C \subset B$, so ex. das Urbild $f^{-1}(C)$ immer! Falls aber f bijektiv ist, also f^{-1} ex, dann ist $f^{-1}(C)$ auch das Bild von C unter f^{-1}.

Beispiel:

$f : \mathbb{N} \to \mathbb{Z}$

$n \mapsto \begin{cases} \frac{n-1}{2} & \text{ungerade} \\ \frac{-n}{2} & \text{gerade} \end{cases}$

$f^{-1} : \mathbb{Z} \to \mathbb{N}$

$z \mapsto \begin{cases} 2z+1 & z \geq 0 \\ -2z & z < 0 \end{cases}$

$f \circ f^{-1} \begin{cases} f(2z+1) = \frac{2z+1-1}{2} = z & z \geq 0 \\ f(-2z) = \frac{-2z}{2} = z & z < 0 \end{cases}$

$\Rightarrow f \circ f^{-1} = \mathrm{id}_{\mathbb{Z}}$

Analog: $f^{-1} \circ f = \mathrm{id}_{\mathbb{N}}$

Satz 0.2. Seien A, B nichtleere Mengen, $f : A \to B$ Abb.

(i) f injektiv $:\Leftrightarrow \exists g : B \to A$ mit $g \circ f = \mathrm{id}_A$

(ii) f surjektiv $:\Leftrightarrow \exists g : B \to A$ mit $f \circ g = \mathrm{id}_B$

(iii) f bijektiv $:\Leftrightarrow \exists g : B \to A$ mit $f \circ g = \mathrm{id}_B$ und $g \circ f = \mathrm{id}_A$

Beweis:

(i) Sei f injektiv. Definiere $g : y \mapsto \begin{cases} x \text{ mit } f(x) = y & y \in f(A) \\ x_0 & y \notin f(A) \end{cases}$
$x_0 \in A$ festes Element

$\Rightarrow g \circ f : x \mapsto g(f(x)) = x$

Umgekehrt seien $x, x' \in A$ mit $f(x) = f(x')$
$\Rightarrow x = \mathrm{id}_A(x) = (g \circ f)(x) = g(f(x)) = (g \circ f)(x') = \mathrm{id}(x') = x'$
$\Rightarrow f$ injektiv

(ii) „⇒“: f ist surjektiv $\Rightarrow$ zu jedem $y \in B$ existiert mindestens ein $x \in A$ mit $f(x) = y$.
Definiere $g : B \to A$ durch $g : y \mapsto x$, wobei $x \in f^{-1}(\{y\})$ gewählt wird.

$\Rightarrow f \circ g : y \mapsto f(x) = y \Rightarrow f \circ g = \mathrm{id}_B$.

„⇐“: Sei $g : B \to A$ mit $f \circ g = \mathrm{id}_B$ und sei $y = B$.
Setze $x = g(y) \Rightarrow f(x) = f(g(y)) = f \circ g(y) = y$

$\Rightarrow f$ surjektiv.

(iii) „⇒“: Setze $g := f^{-1}$

„⇐“: Nach (i) ist f injektiv, nach (ii) ist f surjektiv, also bijektiv.

□

§6 Relationen

A Menge. Eine *Relation* R auf A ist formal eine Teilmenge von $A \times A = A^2$. Ist $(x, y) \in \mathbb{R}$ (wir schreiben dann xRy), so steht x und y in der Relation, andernfalls nicht.

Definition 0.9 (Äquivalenzrelation)**.** Relationen R (wir schreiben dann $\sim$), die die folgenden 3 Gesetze erfüllen:

(i) $\forall x \in A: \; x \sim x$ (Reflexivität)

(ii) $\forall x, y \in A: \; [x \sim y \;\Rightarrow\; y \sim x]$ (Symmetrie)

(iii) $\forall x, y, z \in A: \; [x \sim y, \; y \sim z \;\Rightarrow\; x \sim z]$ (Transitivität)

Beispiel: $A = \mathbb{Z}, \; x \sim y \;:\Leftrightarrow\; x - y$ durch 3 teilbar.

Vorlesung: 2004-10-27

Definition 0.10. Sei $\sim$ Äquivalenzrelation auf A. Dann heißt

$$[x]_\sim := \{y \in A \mid x \sim y\} \quad \text{für} \quad x \in A$$

Äquivalenzklasse zu x.

x heißt (ein) *Repräsentant* der Äquivalenzklasse.

Die Menge aller Äquivalenzklassen von $\sim$ wird mit $A/_\sim$ bezeichnet und heißt *Faktormenge*.

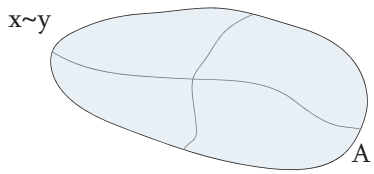

Abbildung 5: Äquivalenzklassen

Einschub. $\mathcal{M}$ Mengensystem

$$\bigcup_{B \in M} := \{x \mid \exists B \in M \text{ mit } x \in B\}$$

$$\bigcap_{B \in M} := \{x \mid x \in B, \; \forall B \in M\}$$

Satz 0.3. Die Faktormenge $A/_\sim$ ist eine *Partition* von A, das heißt:

(i) $[x]_\sim \neq 0, \forall x \in A$

(ii) $[x]_\sim \cap [y]_\sim \neq 0 \;\Rightarrow\; [x]_\sim = [y]_\sim$

(iii) $\bigcup_{[x]_\sim \in A/_\sim} = A$

Umgekehrt erzeugt *jede* Partition $\mathcal{M}$ von A eine Äquivalenzrelation $\sim$ mit $\mathcal{M} = \mathcal{A}/_\sim$.

Beweis:

(i) $x \in [x]_\sim$

(ii) Sei $z \in [x]_\sim \cap [y]_\sim \;\Rightarrow\; x \sim z, \; y \sim z \;\Rightarrow\; x \sim y$

Sei nun $x' \in [x]_\sim \Rightarrow x' \sim x \Rightarrow x' \sim y$
$\Rightarrow x' \in [y]_\sim$, d.h. $[x]_\sim \subset [y]_\sim$

Analog folgt $[y]_\sim \subset [x]_\sim$

(iii) Sei $x \in A \Rightarrow x \in [x]_\sim$

□

Definition 0.11. Umgekehrt sei $\mathcal{M}$ Partition von A. Wir definieren eine Abbildung $f : A \to \mathcal{M}$

$x \mapsto$ Menge $B_x \in M$, die x enthält

Jetzt $x \sim y :\Leftrightarrow f(x) = f(y) \Rightarrow \sim$ Äquivalenzrelation.

Allgemein gehört zu jeder Abb. $f : A \to B$ eine Äquivalenzrelation $\sim$:

$$x \sim y :\Leftrightarrow f(x) = f(y)$$

Jede Äquivalenzrelation entsteht auf diese Weise.

$$k : A \underset{x \mapsto [x]_\sim}{\to} A/_\sim$$

heißt *kanonische Abbildung*.

Satz 0.4 (Grundform des Homomorphiesatzes)**.** Sei $f : A \to B$ eine Abbildung und $k : A \to A/_f$ die kanonische Abbildung auf die Faktormenge. Dann existiert eine injektive Abbildung $\overline{f} : A/_f \to B$ mit $f = \overline{f} \circ k$.

Ist f surjektiv, so ist $\overline{f}$ bijektiv.

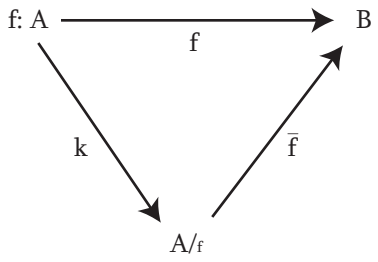

Abbildung 6: Skizze zum Homomorphiesatz

Beweis:

Def $\overline{f} : A/_f \to B$ durch $\overline{f}([x]_\sim) := f(x)$
$[x]_\sim = [y]_\sim$ (d.h. wenn $x \sim y$) $\overset{?}{\Rightarrow} \overline{f}([x]_\sim) = \overline{f}([y]_\sim)$.
Aber $x \sim y$ bedeutet $f(x) = f(y)$, also ist Def unabh. vom Repräsentanten $x \in [x]_\sim$.

Nun ist $\overline{f} \circ k = f$

Aus $\overline{f}([x]_\sim) = \overline{f}([y]_\sim)$ folgt $f(x) = f(y)$, also $x \sim y$, also $[x]_\sim = [y]_\sim$. □

1 Grundbegriffe der Algebra

§1 Lineare Gleichungssysteme

Lineares Gleichungssystem (LGS):

$$\begin{array}{ccccccc} a_{11}x_1 & + & \dots & + & a_{1n}x_n & = & b_1 \\ \vdots & & & & \vdots & & \vdots \\ a_{m1}x_1 & + & \dots & + & a_{mn}x_n & = & b_m \end{array} \tag{1}$$

$x_1 \dots x_n$ Unbekannte (Variable) des LGS.
$a_{11} \dots a_{mn}$ die Koeffizienten.
$b_1 \dots b_m$ Konstanten auf der rechten Seite.

Hierbei sind zunächst $a_{ij}, b_{ij} \in \mathbb{R}$, also handelt es sich um ein reelles LGS. Gesucht sind reelle Zahlen $x_1 \dots x_n$, die das LGS lösen.

Jedes $n-$Tupel $(x_1, \dots, x_n)$ solcher Zahlen heißt *Lösung* des LGS.

Für ein *reelles* LGS gibt es die folgenden Möglichkeiten

(i) (1) ist unlösbar

(ii) (1) hat genau eine Lösung

(iii) (1) hat unendlich viele Lösungen

Beispiel:

$$\left.\begin{array}{ccccc} x_1 & + & x_2 & = & 1 \\ 2x_1 & + & 2x_2 & = & 4 \end{array}\right\} \Rightarrow \text{ unlösbar}$$

$$\left.\begin{array}{ccccc} x_1 & + & x_2 & = & 0 \\ x_1 & - & x_2 & = & 2 \end{array}\right\} \Rightarrow \begin{array}{l} x_1 = 1 \\ x_2 = -1 \end{array} \text{ einzige Lsg}$$

$$\left.\begin{array}{ccccc} x_1 & + & x_2 & = & 1 \\ 3x_1 & + & 3x_2 & = & 3 \end{array}\right\} \Rightarrow \text{ Jedes Paar } (t, 1-t),\ t \in \mathbb{R} \text{ ist Lsg}$$

Ist in (1) $b_1 = \dots = b_n = 0$, so nennt man das LGS *homogen*, andernfalls *inhomogen*. Ein homogenes LGS hat immer die *triviale Lösung* $(0, \dots, 0)$, hier sucht man nach *nicht trivialen* Lösungen.

„Blockschreibweise“:

$$\begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & & \vdots \\ a_{m1} & \cdots & a_{mn} \end{pmatrix} \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} b_1 \\ \vdots \\ b_m \end{pmatrix}$$

§2 Gruppen

Betrachte Menge $A \neq \emptyset$ mit einer *Verknüpfung*.

Formal ist eine Verknüpfung eine Abbildung

$$\begin{array}{rccc} f : & A \times A & \to & A \\ & (x,y) & \mapsto & f(x,y) \end{array}$$

Statt $\left|\begin{array}{c} f \\ f(x,y) \end{array}\right|$ schreibt man hier: $\left|\begin{array}{c} +, \cdot, \circ, *, \dots \\ x+y, x \cdot y, x \circ y, \dots \end{array}\right|$

Beispiel:

(i) $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$ mit $+$ bzw $\cdot$

(ii) Komposition von Abb: $A := B^B = \{f : B \to B \text{ Abb}\}$

(iii) $\mathcal{P}(B)$, $\cup$, $\cap$, $\setminus$, Δ $\quad (A\Delta C = (A\setminus C) \cup (C\setminus A))$

Verknüpfungen können *kommutativ* sein

$$x \circ y = y \circ x \quad \forall x, y \in A \quad \text{(„Kommutativgesetz“)}$$

Verknüpfungen können *assoziativ* sein

$$(x \circ y) \circ z = x \circ (y \circ z) \quad \forall x, y, z \in A \quad \text{(„Assoziativgesetz“)}$$

Vorlesung: 2004-10-29

Definition 1.1. Eine Menge $A \neq \emptyset$ mit einer Verknüpfung $\circ$ heißt *Halbgruppe*, wenn das Assoziativgesetz erfüllt ist. Gilt auch das Kommutativgesetz, so heißt die Halbgruppe *kommutativ*.

Schreibweise: $(A, \circ)$

Klammern bei Ausdrücken $(x \circ y) \circ z$ werden weggelassen: $x \circ y \circ z$. Speziell: $x^n := \underbrace{x \circ \ldots \circ x}_{n-\text{mal}}$

Definition 1.2. Sei $(A, \circ)$ Halbgruppe. Existiert ein $e \in A$ mit

$$x \circ e = e \circ x = x \quad \forall x \in A$$

so heißt e *Neutralelement*.

Es gibt höchstens ein Neutralelement in einer Halbgruppe.

Beweis: Angenommen e, e' Neutralelemente $\Rightarrow$ $e = e \circ e' = e'$. □

Definition 1.3. Sei $(A, \circ)$ Halbgruppe mit Neutralelement e.

Existiert zu einem $x \in A$ ein Element $x^{-1} \in A$, das $x \circ x^{-1} = x^{-1} \circ x = e$ erfüllt, so heißt x^{-1} das *Inverse* zu x. Existiert x^{-1}, so ist das Inverse eindeutig.

Beweis: Seien x^{-1}, x' Inverse zu $x \in A$

$$\Rightarrow \; x \circ x^{-1} = x^{-1} \circ x = e$$
$$x \circ x' = x' \circ x = e$$

$$\Rightarrow \; x \circ x^{-1} = x \circ x' \;\Rightarrow\; x^{-1} \circ x \circ x^{-1} = x^{-1} \circ x \circ x' \;\Rightarrow\; x^{-1} = x'$$ □

Beispiel:

(i) $(\mathbb{N}, +)$, $(\mathbb{Z}, +)$ Halbgruppen. $(\mathbb{Z}, +)$ hat neutr. Element 0. $(\mathbb{Z}, +)$ hat Inverses.
$(\mathbb{R}, \cdot)$, $(\mathbb{Q}, \cdot)$ Halbgruppen mit Neutralelement 1. 0 hat kein Inverses.
$\Rightarrow$ $(\mathbb{Q}\setminus\{0\}, \cdot)$, $(\mathbb{R}\setminus\{0\}, \cdot)$ komm. Halbgruppe mit Neutralelement 1 und Inversen $x^{-1} = \frac{1}{x}$.

(ii) $(B^B, \circ)$ nicht komm. Halbgruppe mit Neutralelement id_B.
I.A. gibt es keine Inversen, nur für bijektive $f : B \to B$ ist das Inverse die Umkehrabbildung f^{-1}.

(iii) $(\mathcal{P}(A), \cup)$ komm. Halbgruppe mit Neutralelement $\emptyset$, keine Inversen.
$(\mathcal{P}(A), \Delta)$ komm. Halbgruppe mit Neutralelement $\emptyset$. Jedes $B \subset A$ ist zu sich selbst invers! $B\Delta B = \emptyset$.

Definition 1.4. Sei A eine Menge mit einer Verknüpfung $\circ$

$(A, \circ)$ heißt *Gruppe*, wenn

(i) $(A, \circ)$ ist Halbgruppe

(ii) $(A, \circ)$ besitzt Neutralelement e

(iii) Jedes $x \in A$ besitzt ein Inverses x^{-1}

Ist $(A, \circ)$ kommutativ, so spricht man von einer *abelschen Gruppe*.

Statt $x \circ y$ schreibt man häufig xy und redet von der Gruppe A.

Bei abelschen Gruppen wird häufig $+$ gewählt. Statt e benutzt man dann meist 0 und statt x^{-1} schreibt man $-x$ und $x - y := x + (-y)$.

Bemerkung: Axiome (ii), (iii) kann man abschwächen:

(i) Es existiert ein linksneutrales Element:

$$e \circ x = x \quad \forall x \in A$$

(ii) Es existiert zu jedem $x \in A$ ein linksinverses Element x^{-1}

$$x \circ x^{-1} = e$$

Beweis:

Vor.: ex e: $e \circ x = x \; \forall x$ und es ex. zu x ein x^{-1} mit $x^{-1} \circ x = e$.

Beh.: $x \circ e = x \; \forall x$ und $x \circ x^{-1} = e \; \forall x$.

Zu x^{-1} ex ein Linksinverses x' mit $x' \circ x^{-1} = e$

$$\begin{aligned}
&\Rightarrow x' \circ x^{-1} \circ x = e \circ x = x \\
&\quad x' \circ x^{-1} \circ x = x' \circ e \\
&\Rightarrow x' \circ e = x \\
&\Rightarrow x \circ e = x \circ x^{-1} \circ x = \underbrace{x' \circ \underbrace{e \circ x^{-1}}_{=x^{-1}}}_{=e} \circ x = x
\end{aligned}$$

$$\begin{aligned}
&x' = e \circ x' = x' \circ e = x \\
&\Rightarrow x \circ x^{-1} = e
\end{aligned}$$

□

Satz 1.1. Sei $(A, \circ)$ eine Halbgruppe. Dann ist $(A, \circ)$ genau dann eine Gruppe, wenn zu jedem $x, y \in A$ Elemente $z, \overline{z} \in A$ existieren, die $x \circ z = y$ und $\overline{z} \circ x = y$ erfüllen.

Diese Elemente $z, \overline{z}$ sind dann eindeutig bestimmt.

Beweis: Ist $(A, \circ)$ Gruppe, so gilt (*) mit $z = x^{-1} \circ y$ und $\overline{z} = y \circ x^{-1}$

Umgekehrt gelte (*)!

Neutralelement:

Sei $x_0 \in A$ (ex, weil $A \neq \emptyset$)
$\Rightarrow\ \exists e, e' \in A \quad$ mit $\quad x_0 \circ e = x_0,\ e' \circ x_0 = x_0$
$\overset{(*)}{\Rightarrow}\ x_0 \circ e = e' \circ x_0 = x_0$
$x \in A$ beliebig $\Rightarrow\ \exists z, \overline{z} \quad$ mit $\quad x_0 \circ z = x,\ \overline{z} \circ x_0 = x$
$$\Rightarrow \begin{array}{l} \underline{e' \circ x} = e' \circ x_0 \circ z = x_0 \circ z = \underline{x} \\ \underline{x \circ e} = \overline{z} \circ x_0 \circ e = \overline{z} \circ x_0 = \underline{x} \end{array} \Bigg\} \begin{array}{l} x = e \\ x = e' \end{array} \Rightarrow\ e' \circ e = e \ \Rightarrow\ e' = e$$

Vorlesung: 2004-11-03

Inverses:

Setze $y = e\ \Rightarrow\ \exists z, \overline{z} \in A : x \circ z = e,\ \overline{z} \circ x = e$
$\Rightarrow\ \underbrace{\overline{z} \circ x}_{=e} \circ z = \overline{z} \circ e\ \Rightarrow\ z = \overline{z}\ \Rightarrow\ z$ erfüllt $x \circ z = z \circ x = e\ \Rightarrow\ z$ ist Inverses zu x

Also $(A, \circ)$ Gruppe.

Eindeutigkeit:

Sei $x \circ z = y, \quad z \circ \overline{z} = y$
$\Rightarrow\ x \circ z = x \circ \overline{z}\ \Rightarrow\ \underbrace{x^{-1} \circ x}_{=e} \circ z = \underbrace{x^{-1} \circ x}_{=e} \circ \overline{z}$
$\Rightarrow\ z = \overline{z}$

□

Beispiel:

(i) $(\mathbb{Z}, +),\ (\mathbb{Q}, +),\ (\mathbb{R}, +)$, NE 0, abelsch

(ii) $(\mathbb{Q}\backslash\{0\}, \cdot),\ (\mathbb{R}\backslash\{0\}, \cdot)$, NE 1, abelsch

(iii) $\mathbb{Z}^n,\ \mathbb{Q}^n,\ \mathbb{R}^n$ sind abelsche Gruppen bzgl $+$:

$$(x_1, \ldots, x_n) + (y_1, \ldots, y_n) := (x_1 + y_1, \ldots, x_n + y_n)$$

NE: $(0, \ldots, 0)$, Inverse von $(x_1, \ldots, x_n)$ ist $(-x_1, \ldots, -x_n)$.

(iv) $A := \{a_1, \ldots, a_n\}$ endl. Menge. Verknüpfung erklärt durch *Verknüpfunstafel*

$\circ$	a_1	$\cdots$	a_n
a_1	a	$\cdots$	$*$
$\vdots$	$\vdots$		$\vdots$
a_n	$*$	$\cdots$	$*$

$\circ$	1	2	3
1	2	1	3
2	3	1	1
3	1	1	2

keine Gruppe

Falls Gruppe: *Gruppentafel*.

Ist Verknüpfungstafel Gruppentafel, dann tritt zu jeder Zeile (und in jeder Spalte) jedes Element von A genau einmal auf.

Beispiel:

$\circ$	0	1
0	0	1
1	1	0

Beispiel:

$\circ$	e	a	b
e	e	a	b
a	b	e	a
b	a	b	e

Nicht assoziativ:

$$(a \circ e) \circ b = b \circ b = e$$
$$a \circ (e \circ b) = a \circ b = a$$

(v) Die Menge $B^B := \{f : B \to B \text{ Abb}\}$ ist mit $\circ$ (Komposition) keine Gruppe (falls $|B| \geq 2$).
„Konstante“ Abbildungen haben hier kein Inverses (Inverses = Umkehrabbildung).

Die Teilmenge $S_B := \{f : B \to B, f\text{bijektiv }\}$ ist eine Gruppe bzgl. $\circ$ mit Neutralelement id_B und Inversen f^{-1} (Umkehrabb.). Sie heißt *Symmetrische Gruppe*.

Sei jetzt $B := \{1, \ldots, m\}$. Statt S_B schreiben wir S_m.
S_m heißt auch *Permutationsgruppe* und die Elemente $\pi \in S_m$ heißen *Permutationen*. Schreibweise:

$$\pi = \begin{pmatrix} 1 & \cdots & m \\ \pi(1) & \cdots & \pi(m) \end{pmatrix}, \quad \mathrm{id} = \begin{pmatrix} 1 & \cdots & m \\ 1 & \cdots & m \end{pmatrix}$$

Satz 1.2. $|S_m| = m! \quad (m! := 1 \cdot 2 \cdot \ldots \cdot (m-1) \cdot m)$

Beweis: Wir beweisen allgemeiner: Seien A, B Mengen mit m Elementen:

$$A = \{a_1, \ldots, a_m\}, \quad B = \{b_1, \ldots, b_m\}$$

Behaptung: $|\{f : A \to B \mid f \text{ bijektiv }\}| = m!$

Induktion nach m: $m = 1$ stimmt.

$m - 1 \to m \quad (m \geq 2)$:
Betrachte $\Phi : A \to B$ bijektiv.
Sei $\varphi(a_n) = b_j \in B$. Wieviele bijektive Abbildungen $\Phi : A \to B$ mit $\Phi(a_n) = b_j$ gibt es?

Zu jedem solchen Φ existiert ein $\overline{\Phi} : \overline{A} = \{a_1, \ldots, a_{m-1}\} \to B \backslash \{b_j\} = \{b_1, \ldots b_{j-1}, b_{j+1}, \ldots, b_m\}$, $\overline{\Phi}$ bijektiv.

Nach IV ex $(m-1)!$ derartige Abb.
Insgesamt gibt es also $m \cdot (m-1)! = m!$ bijektive Abbildungen von $A \to B$. □

Beispiel: S_3 hat $3! = 6$ Elemente:

$$\pi_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \quad \pi_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \quad \pi_3 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$
$$\pi_4 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \quad \pi_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \quad \pi_6 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

$\circ$	π_1	π_2	π_3	π_4	π_5	π_6
π_1	π_1	π_2	π_3	π_4	π_5	π_6
π_2	π_2	π_3	π_1	π_6	π_4	π_5
π_3	π_3	π_1	π_2	π_5	π_6	π_4
π_4	π_4	π_5	π_6	π_1	π_2	π_3
π_5	π_5	π_6	π_4	π_3	π_1	π_2
π_6	π_6	π_4	π_5	π_2	π_3	π_1

nicht kommutativ

$$\pi_5 \circ \pi_4 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \pi_3$$
$$\pi_4 \circ \pi_5 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \pi_2$$

Eine *Transposition* ist eine Permutation, die 2 Elemente vertauscht, und die anderen fest lässt.
Schreibweise: $(i < j)$

$$\tau^{(i,j)} = \begin{pmatrix} 1 & 2 & \dots & i-1 & i & i+1 & \dots & j-1 & j & j+1 & \dots & m \\ 1 & 2 & \dots & i-1 & j & i+1 & \dots & j-1 & i & j+1 & \dots & m \end{pmatrix}$$

Satz 1.3. Jedes $\pi \in S_m,\ m \geq 2$ ist Verkettung von Transpositionen

Beweis: Vollständige Induktion nach m

$m = 2$:

$$S_2 = \left(\begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} \right) \quad \text{stimmt}$$

Es gilt: $\tau^{(i,j)} \circ \tau^{(i,j)} = \mathrm{id}$, d.h. $\tau^{(i,j)} = (\tau^{(i,j)})^{-1}$.

Vorlesung: 2004-11-05

$m-1 \ \to \ m \quad (m \geq 3)$:

Sei $\pi \in S_m$.
Fall 1:

$\pi(m) = m$

$\Rightarrow \ \pi = \begin{pmatrix} 1 & \cdots & m-1 & m \\ \pi(1) & \cdots & \pi(m-1) & m \end{pmatrix}$

$\Rightarrow \ \exists$ Transpositionen $\widetilde{\tau}_1, \dots, \widetilde{\tau}_k \in S_{m-1}$ mit $\widetilde{\pi} = \widetilde{\pi}_1 \circ \dots \circ \widetilde{\pi}_k$

Setze $\tau_i := \begin{pmatrix} 1 & \cdots & m-1 & m \\ \tau_1(1) & \cdots & \tau_i(m-1) & m \end{pmatrix} \in S_m \quad i = 1..k$

$\Rightarrow \ \pi = \tau_1 \circ \dots \circ \tau_k$

Fall 2:

$\pi(m) = n \quad (n < m) \ \Rightarrow \ \pi' := \tau^{(n,m)} \circ \pi \ \Rightarrow \ \pi'(m) = m$

$\overset{\text{Fall 1}}{\Rightarrow} \pi' = \tau_1 \circ \dots \circ \tau_r \quad (\tau_i \text{ Transposition})$

$\Rightarrow \ \pi = \tau^{(n,m)} \circ \tau_1 \circ \dots \circ \tau_r$ □

Beispiel:

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

$$\left.\begin{array}{lllllll} \pi^{(1,5)} \circ \pi & 1 & 3 & 2 & 6 & 4 & 5 \\ \pi^{(2,3)} \circ & 1 & 2 & 3 & 6 & 4 & 5 \\ \pi^{(4,6)} \circ & 1 & 2 & 3 & 4 & 6 & 5 \\ \pi^{(5,6)} \circ & 1 & 2 & 3 & 4 & 5 & 6 \end{array}\right\} \Rightarrow \ \pi^{(5,6)} \circ \pi^{(4,6)} \circ \pi^{(2,3)} \circ \pi^{(1,5)} \circ \pi = \mathrm{id}$$

$\Rightarrow \ \pi = \pi^{(1,5)} \circ \pi^{(2,3)} \circ \pi^{(4,6)} \circ \pi^{(5,6)}$

Bemerkung: Die Darstellung als Produkt von Transpositionen ist nicht eindeutig. Gibt es eine Darstellung von π mit einer geraden Anzahl von Transpositionen, so besteht jede Darstellung von π aus einer geraden Anzahl von Transpositionen.

Definition 1.5. Eine Permutation $\pi \in S_m$ heißt *gerade*, wenn es eine Darstellung von π durch eine gerade Anzahl von Transpositionen gibt, andernfalls heißt π *ungerade*.

Bemerkung:

- id ist gerade.
- π, π' gerade $\Rightarrow$ $\pi \circ \pi'$ gerade
- π gerade $\Rightarrow$ π^{-1} gerade

Also bilden die geraden Permutationen mit $\circ$ eine Gruppe (Untergruppe von S_m).

Definition 1.6. Sei $(A, \circ)$ eine Gruppe und $B \subset A$. B heißt *Untergruppe* von A, wenn $\circ$ eingeschränkt auf B eine Verknüpfung ist, und $(B, \circ)$ eine Gruppe ist.

Bemerkung:

(i) Ist B Untergruppe von A, so ist das Neutralelement von B gleich dem Neutralelement von A.

Beweis: Neutralelemente $e_A, e_B \Rightarrow \underbrace{e_B}_{=e_B \circ e_B} = e_B \circ e_A \overset{\text{Satz 1.1}}{\Rightarrow} e_A = e_B$ □

(ii) Ist B Untergruppe von A, $x \in B$, so ist das Inverse von x in B gleich dem Inversen von x in A.

Beweis: $x_B^{-1} \circ x = e = x_A^{-1} \circ x \Rightarrow x_A^{-1} = x_B^{-1}$ □

Satz 1.4. Sei $(A, \circ)$ eine Gruppe und $B \subset A$. Dann gilt B ist Untergruppe von A $:\Leftrightarrow$

(i) $e \in B$

(ii) mit $x \in B$ gilt auch $x^{-1} \in B$

(iii) mit $x, y \in B$ gilt auch $x \circ y \in B$

Beweis:

„$\Rightarrow$“: stimmt
„$\Leftarrow$“: Wegen (iii) ist $\circ$ eine Verknüpfung auf B. Assoziativität gilt in B, weil sie in A gilt.
Die Existenz des Neutralelement folgt aus (i). Die Existenz des Inversen folgt aus (ii).

□

Variante von Satz 1.4: $(A, \circ)$ Gruppe, $B \subset A$. Dann gilt B Untergruppe $:\Leftrightarrow$ $B \neq \emptyset$ und aus $x, y \in B$ folgt $x \circ y^{-1} \in B$.

Beweis:

„$\Rightarrow$“: stimmt
„$\Leftarrow$“: Wegen $B \neq \emptyset$ ex. ein $x_0 \in B \Rightarrow \underbrace{x_0 \circ x_0^{-1}}_{=e} \in B \Rightarrow$ (i)

Sei $x \in B$. Wegen $e \in B$ gilt dann $e \circ x^{-1} \in B \Rightarrow$ (ii)
Seien $x, y \in B$. Wegen $y^{-1} \in B$ folgt $\underbrace{x \circ (y^{-1})^{-1}}_{=x \circ y} \in B \Rightarrow$ (iii)

□

Beispiel: Für jedes $m \in \mathbb{N}$ ist $mz := \{mx \mid x \in \mathbb{Z}\}$ eine Untergruppe von $(Z, +)$.

Definition 1.7. Seien $(A, \circ)$, $(B, *)$ Gruppen. Einne Abbildung $f : A \to B$ heißt (Gruppen-) *Homomorphismus*, wenn

$$f(a \circ b) = f(a) * f(b) \quad \forall a, b \in A$$

gilt. Ein bijektiver Homomorphismus heißt *Isomorphismus*. Gibt es einen Isomorphismus $f : A \to B$, so heißen die Gruppen A und B *isomorph*. Schreibweise $A \cong B$. Gilt $A = B$ und $\circ = *$, so heißt ein Isomorphismus f auch *Automorphismus*.

Bemerkung:

(i) Sind e, e' die Neutralelemente von A, B, $f : A \to B$ Homomorphismus, so gilt $f(e) = e'$.

Beweis:

$$\left.\begin{array}{rcl} f(e) = f(e \circ e) & = & f(e) * f(e) \\ & = & e' * f(e) \end{array}\right\} \overset{\text{Satz 1.1}}{\Rightarrow} f(e) = e'$$

□

Weiter ist $f(x^{-1}) = (f(x))^{-1}$

Beweis: $\underbrace{f(e)}_{=e'} = f(x \circ x^{-1} = f(x) * f(x^{-1}) \Rightarrow f(x^{-1}) = f(x)^{-1}$ □

(ii) Zu jedem Homomorphismus $f : A \to B$ gehören zwei Untergruppen:

- $f(a) = \{f(x) \mid x \in A\}$ Untergruppe von B.
- $\operatorname{Kern} f := \{x \in A \mid f(x) = e'\} = f^{-1}(\{e\})$ Untergruppe von A.

Denn $e \in \operatorname{Kern} f$. Seien $x, y \in \operatorname{Kern} f \Rightarrow f(x \circ y^{-1}) = f(x) * f(y^{-1}) = f(x) * (f(y))^{-1} = e' * (e')^{-1} = e' \Rightarrow x \circ y^{-1} \in \operatorname{Kern} f$.

(iii) f ist surjektiv $:\Leftrightarrow f(A) = B$
f ist injektiv $:\Leftrightarrow \operatorname{Kern} f = \{e\}$

Beweis:

$$\begin{aligned} f \text{ inj} &\Leftrightarrow [f(x) = f(y) \Rightarrow x = y] \\ &\Leftrightarrow [\underbrace{f(x) * f(y)^{-1}}_{=f(x \circ y^{-1})} = e' \Rightarrow x \circ y^{-1} = e] \\ &\Leftrightarrow \operatorname{Kern} f = \{e\} \end{aligned}$$

□

Vorlesung: 2004-11-10

$f : A \to A'$ Homomorphismus, $(A, \circ)$, $(A', *)$ Gruppen, das heißt $f(x \circ y) = f(x) * f(y)$

$$\begin{aligned} A/_f &= \{[x]_\sim \mid x \in A\} \\ x \sim y &:\Leftrightarrow f(x) = f(y) \\ &\Leftrightarrow f(x) * f(y)^{-1} = e' \\ &\Leftrightarrow f(x \circ y^{-1}) = e' \end{aligned}$$

$$\boxed{x \sim y \;\Leftrightarrow\; x \circ y^{-1} \in \operatorname{Kern} f}$$

Können wir $A/_f$ zu einer Gruppe machen? Verknüpfung $\cdot$?

Ansatz:

$$[x]_\sim \cdot [y]_\sim := [x \circ y]_\sim \tag{2}$$

$$\begin{aligned} &x' \sim x,\ y' \sim y \overset{?}{=} x' \sim y' \sim x \sim y \\ &\left.\begin{aligned} x' \sim x &\;\Leftrightarrow\; f(x) = f(x') \\ y' \sim y &\;\Leftrightarrow\; f(x) = f(y') \end{aligned}\right\} \text{ weil } f \text{ Homomorphismus} \\ &\Rightarrow\; x' \circ y' \sim x \circ y \;\Leftrightarrow\; f(x \circ y) = f(x' \circ y') \end{aligned}$$

also ist (2) eine sinnvolle Definition.

Wohldefiniertheit von (2) kann auch als Eigenschaft des Kerns angesehen werden:

$$\begin{aligned} &x' \circ x^{-1}, y' \circ y^{-1} \in \operatorname{Kern} f \\ &\Rightarrow\; x' \circ y' \circ y^{-1} \circ x^{-1} \in \operatorname{Kern} f \end{aligned}$$

Neue Schreibweise: $A/_{\operatorname{Kern} f}$ statt $A/_f$.

Satz 1.5 (Homomorphiesatz für Gruppen)**.** Seien $(A, \circ)$, $(A', *)$ Gruppen, $f : A \to A'$ Homomorphismus.

(i) $(A/_{\operatorname{Kern} f}, \cdot)$ ist eine Gruppe und die kannonische Abbildung $k : A \to A/_{\operatorname{Kern} f}$ ist Homomorphismus.

(ii) Es gibt einen injektiven Homomorphismus $\overline{f} : A/_{\operatorname{Kern} f} \to A'$ mit $\overline{f} \circ k = f$.

(iii) Ist f surjektiv, so ist $\overline{f}$ ein Isomorphismus, also gilt $A/_{\operatorname{Kern} f} \cong A'$.

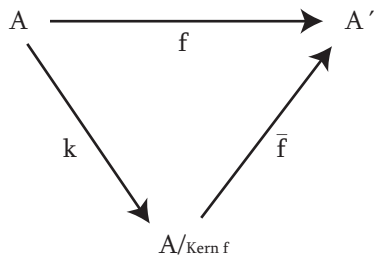

Abbildung 7: Skizze zum Homomorphiesatz für Gruppen

Beweis:

(i) Assoziativität:

$$\begin{aligned} [x]_\sim \cdot ([y]_\sim \cdot [z]_\sim) &= [x]_\sim \cdot [y \circ z]_\sim \\ &= [x \circ (y \circ z)]_\sim = [(x \circ y)] \circ z]_\sim \\ &= ([x]_\sim \cdot [y]_\sim) \cdot [z]_\sim \end{aligned}$$

Neutrales Element: $[e]_\sim$, denn

$$[x]_\sim \cdot [e]_\sim = [x \circ e]_\sim = [x]_\sim = [e]_\sim \cdot [x]_\sim$$

Inverse Elemente: $[x]_\sim^{-1} := [x^{-1}]_\sim$, denn

$$[x]_\sim \cdot [x^{-1}]_\sim = [x \circ x^{-1}]_\sim = [e]_\sim = [x^{-1}]_\sim \cdot [x]_\sim$$

$\Rightarrow A/_{\text{Kern } f}$ Gruppe.

$k : x \mapsto [x]_\sim$.

$$\underbrace{k(x \circ y)}_{[x\circ y]_\sim} = \underbrace{k(x)}_{[x]_\sim} \cdot \underbrace{k(y)}_{[y]_\sim}$$

folgt aus der Definition von „·“.

Für (ii), (iii) bleibt nurnoch zu zeigen, dass $\overline{f}$ Homomorphismus. Rest folgt aus Satz 0.4.

$$\begin{array}{c}\overline{f} : [x]_\sim \mapsto f(x) \\ A/_{\text{Kern } f} \to A'\end{array}$$

$$\begin{aligned}\overline{f}([x]_\sim \cdot [y]_\sim) &\stackrel{?}{=} \overline{f}([x]_\sim) * \overline{f}([y]_\sim) \\ \overline{f}([x \circ y]_\sim) &= f(x) * f(y) \\ \overline{f}(x \circ y) &= f(x) * f(y)\end{aligned}$$

klar, da f Homomorphismus.

□

Korollar 1.6. Es gilt: $A/_{\text{Kern } f} \cong f(A)$.

Definition 1.8. $A/_{\text{Kern } f}$ heißt *Faktorgruppe*.

Verfahren funktioniert auch allgemeiner:

Sei B Untergruppe von A, $x \sim y \ :\Leftrightarrow \ x \circ y^{-1} \in B$. Funktioniert dann (2) als Definition von $\cdot$ auf $A/_B$?

Im allgemeinen nicht! Nur, wenn B die Eigenschaft

$$x' \circ x^{-1},\ y' \circ y^{-1} \in B \ \Rightarrow \ x' \circ y' \circ y^{-1} \circ x^{-1} \in \text{Kern} \tag{3}$$

hat.

Untergruppen, die (3) erfüllen, heißen *Normalteiler*. Es gilt: Ist A abelsch, so ist jede Untergruppe Normalteiler.

$$x \circ B = B \circ x \quad \forall x \in A \qquad (x \circ B := \{x \circ b \mid b \in B\})$$

Beispiel: $(\mathbb{Z}, +)$, Untergruppe $n\mathbb{Z} \quad (n \in \mathbb{N})$: $\mathbb{Z}/m\mathbb{Z}$

$x \sim y \ :\Leftrightarrow \ x - y \in m\mathbb{Z}$

$[0]_\sim, [1]_\sim, \ldots, [m-1]_\sim$

§3 Körper und Ringe

Mengen A mit zwei Verknüpfungen $+$ und $\cdot$, Neutralelemente 0 und 1, Inverse $-x$ und $x^{-1} = \frac{1}{x}$.

Definition 1.9. $(A, +, \cdot)$ heißt *Körper*, wenn

(i) $(A, +)$ ist abelsche Gruppe

(ii) $(A\backslash\{0\}, \cdot)$ ist abelsche Gruppe

(iii) $\forall x, y, z \in A : x \cdot (y + z) = (x \cdot y) + (x \cdot y)$ und $(x + y) \cdot z = (x \cdot z) + (y \cdot z)$ (Distributivgesetz)

Konvention: Statt $\begin{vmatrix} x \cdot y \\ (xy) + z \end{vmatrix}$ schreibt man $\begin{vmatrix} xy \\ xy + z \end{vmatrix}$.

Bemerkung:

(i) Ein Körper besitzt ≥ 2 Elemente (weil 0 und 1 existieren).

Beispiel: $A := \{0, 1\}$

$+$	0	1
0	0	1
1	1	0

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

Dieser Körper heißt $\mathbb{F}_2$.

(ii) Es gilt $x \cdot 0 = 0 \cdot x \quad \forall x \in A$, denn

$$x \cdot x = x \cdot (x + 0) = x \cdot x + x \cdot 0$$
$$\Rightarrow\ x \cdot 0 = 0$$

(iii) $\forall x, y \in A : x \cdot (-y) = -x \cdot y$, denn

$$xy + x(-y) = x(y - y) = x \cdot 0 = 0$$

(iv) $x \cdot y = 0\ \Rightarrow\ [x = 0 \vee y = 0]$, denn

$$x \neq 0,\ x \cdot y = 0\ \Rightarrow\ \underbrace{x^{-1} \cdot x}_{1} \cdot y = 0$$
$$\Rightarrow\ y = 0$$

Vorlesung: 2004-11-12

Beispiel:

- $\mathbb{R}$, $\mathbb{Q}$
- $A := \{x + \sqrt{(2)}y \mid x, y \in Q\}$
- Restklassenkörper $\mathbb{F}_p$ (p Primzahl) ($\mathbb{F}_2$ kennen wir schon)

Betrachte $\mathbb{Z}_m = \mathbb{Z}/_{m\mathbb{Z}} = \{\underbrace{[0]_\sim, [1]_\sim, \ldots, [m-1]_\sim}_{\text{Restklassen}}\}$ ist abelsche Gruppe (bzgl $+$).

Definition einer Multiplikation auf $\mathbb{Z}_m$:

$$[x]_\sim \cdot [y]_\sim = [x \cdot y]_\sim$$

sinnvoll, da repräsentantenunabhängig.

$$x' \sim y,\ y' \sim y\ \Rightarrow\ x' \cdot y' \sim x \cdot y$$

Das heißt

$$x - x' = mr,\ y - y' = ms,\ r, s \in \mathbb{Z}$$

$$\Rightarrow xy - x'y' = (x' + mr)(y' + ms) - x'y'$$
$$= m \cdot (\underbrace{ry' + sx' + mrs}_{\in\mathbb{Z}})$$

□

Aus $\mathbb{Z}$ überträgt sich auf $(\mathbb{Z}_m, +, \cdot)$:

- Assoziativität bzgl $\cdot$
- Kommutativität bzgl $\cdot$
- Distributivgesetze
- Neutralelement bzgl $\cdot$ ist $[1]_\sim$

Inverse bzgl $\cdot$??

Sei m keine Primzahl $\Rightarrow\ m = p \cdot q \quad (p, q \in \mathbb{Z})$

$$\begin{array}{rcl} [m]_\sim & = & [0]_\sim \leftarrow \text{ NE bzgl } + \\ \shortparallel & & \\ [p \cdot q]_\sim & = & \underbrace{[p]_\sim}_{\neq [0]_\sim} \cdot \underbrace{[q]_\sim}_{\neq [0]_\sim} \end{array}$$

$\Rightarrow\ (\mathbb{Z}_m, +, \cdot)$ kein Körper!!

Satz 1.7. Sei $m \in N$, $m \geq 2$. Dann gilt:

$$\mathbb{Z}_m \text{ Körper } :\Leftrightarrow\ m \text{ Primzahl}$$

Beweis:

„$\Rightarrow$:“ schon gezeigt.

„$\Leftarrow$:“

Sei m Primzahl. Was fehlt noch von den Körperaxiomen?

(i) $\cdot$ ist Verknüpfung auf $\mathbb{Z}_m \backslash \{[0]_\sim]\}$

(ii) Existenz von Inversen (bzgl $\cdot$)

Dazu zeigen wir:

Seien $[x]_\sim, [y]_\sim, [z]_\sim \in \mathbb{Z}_m,\ [x]_\sim \neq [0]_\sim$
mit $[x]_\sim \cdot [y]_\sim = [x]_\sim \cdot [z]_\sim$
$\Rightarrow\ [y]_\sim = [z]_\sim$

Beweis:

Aus (3) folgt $[xy - xz]_\sim = [0]_\sim \ \Leftrightarrow\ [x(y-z)]_\sim = [0]_\sim$

$\Rightarrow\ x(y-z) = ms,\ s \in \mathbb{Z}$

$\overset{m \text{ prim}}{\Rightarrow}$ $\underbrace{m \text{ teilt } x}_{\text{nein, wegen } [x]_\sim \neq [0]_\sim}$ oder m teilt $(y-z)$

$\Rightarrow\ m$ teilt $(y-z)\ \Rightarrow\ [y]_\sim = [z]_\sim$

□

zu (i): $[x]_\sim, [y]_\sim \neq [0]_\sim\ \Rightarrow\ [x]_\sim \cdot [y]_\sim \neq [0]_\sim = [x]_\sim \cdot [0]_\sim$

zu (ii): Sei $[x]_\sim \neq [0]_\sim$

$\Rightarrow\ [x]_\sim \cdot [1]_\sim,\ [x]_\sim \cdot [2]_\sim, \ldots, [x]_\sim \cdot [m-1]_\sim$

paarweise verschieden! Das sind $m - 1 \neq [0]_\sim$ Elemente. Also ist eins davon $[1]_\sim$. □

Neue Schreibweise: Statt $x \sim y$ (d.h. $[x]_\sim = [y]_\sim$) schreibt man

$$x \equiv y \mod m \quad (x \text{ kongruent } y \text{ modulo } m)$$

Beispiel:

$n = 5$ ($\Rightarrow$ $\mathbb{Z}_m$ Körper)

$$\begin{aligned}[4^3]_\sim^{-1} &=? \quad \text{Gesucht } x : 4^3 x \equiv 1 \mod 5,\ x \in \{1,2,3,4\} \\ &= ([4]_\sim^{-1})^3 \qquad [4]_\sim^{-1} = [4]_\sim \\ &= [4^3]_\sim = [4]_\sim\end{aligned}$$

Lösung von $4x \equiv 3 \mod 5$?

$$\begin{aligned}&\Leftrightarrow \underbrace{4 \cdot 4}_{16 \equiv 1} \cdot x = 4 \cdot 3 \mod 5 \\ &\Leftrightarrow x \equiv 12 \mod 5\end{aligned}$$

$\Rightarrow$ $x = 2$ ist Lösung, alle Lösugen $x = 2 + 5r,\ r \in \mathbb{Z}$.

$m = 6$: Lsg von $4x = 3 \mod 6$?

$\cdot$	1	2	3	4	5
4	4	2	0	4	2

$\Rightarrow$ Gleichung unlösbar.

Definition 1.10. Seien $(A, +, \cdot)$ und $(A', +', \cdot')$ Körper. Eine Abbildung $f : A \to A'$ heißt *Homomorphismus*, wenn

$$\begin{aligned}f(x+y) &= f(x) +' f(y) \\ f(x \cdot y) &= f(x) \cdot' f(y)\end{aligned} \qquad \forall x, y \in A$$

gilt. Desweiteren muss gelten $f(0) = 0'$ und $f(1) = 1'$. Ein bijektiver Homomorphismus heißt *Isomorphismus*, A und A' heißen dann *isomorph* $A \cong A'$.

Bemerkung: Ist p Primzahl, so können wir $\mathbb{F}_p := \{0, 1, 2, \ldots, p-1\}$ mit der Abbildung

$$f : \underset{[x]_\sim \mapsto r}{\mathbb{Z}_p \to \mathbb{F}_p} \qquad x = r + ms,\ s \in \mathbb{Z},\ r \in \{0, \ldots, p-1\}$$

und den dadurch induzierten Verknüpfungen $+$ und $\cdot$ zu einem Körper machen, der zu $\mathbb{Z}_p$ isomorph ist.

Bemerkung: In $\mathbb{F}_p$ gilt

$$\underbrace{1 + \ldots + 1}_{p-\text{Mal}} = 0$$

Man nennt p die Charakteristik von $\mathbb{F}_p$.

Ist $\mathbb{K}$ ein beliebiger Körper (mit Nullelementen 0 und 1), so heißt die kleinste Zahl $p \in \mathbb{N}$ mit

$$\underbrace{1 + 1 + \ldots + 1}_{p-\text{Mal}} = 0$$

die *Chrakteristik* von $\mathbb{K}$.

Gibt es kein geeignetes p, so hat $\mathbb{K}$ die Charakteristik 0.

Der Körper der komplexen Zahlen

Wir betrachten $(\mathbb{R}^2, +)$ abelsche Gruppe mit

- $(a, b) + (c, d) = (a + c, b + d)$

- Neutralelement $(0,0)$
- Inversen $-(x,y) = (-x,-y)$

Multiplikation auf $\mathbb{R}^2$?

$$(a,b)\cdot(c,d) := (ac-bd, ad+bc)$$
$$(a+ib)(c+id) = ac+ibc+iad+\underbrace{i^2}_{=-1}bd$$

Vorlesung: 2004-11-17

$\Rightarrow \cdot$ kommutativ, assoziativ, distributiv.

$$\begin{aligned}[(a,b)+(c,d)] &= (a+c,b+d)\cdot(e,f)\\ &= (ae+ce-bf-df, af+cf+be+de)\\ &= (a,b)\cdot(e,f)+(c,d)\cdot(e,f)\end{aligned}$$

Neutralelement: $(1,0)$

$$(a,b)\cdot(1,0) = (1,0)\cdot(a,b) = (a,b)$$

Inverses zu $(a,b)\neq(0,0)$:

$$\left(\frac{a}{a^2+b^2}, \frac{-b}{a^2+b^2}\right)$$

Denn

$$\underbrace{(a,b)\cdot\left(\frac{a}{a^2+b^2}, \frac{-b}{a^2+b^2}\right)}_{\left(\frac{a^2+b^2}{a^2+b^2}, \frac{a(-b)+ab}{a^2+b^2}\right)=(1,0)} = (1,0)$$

Satz 1.8. $(\mathbb{R}^2,+,\cdot)$ ist ein Körper.

Definition 1.11. $(R^2,+,\cdot)$ heißt Körper der *komplexen Zahlen*. Schreibweise: $\mathbb{C}$.

$$z\in\mathbb{C} : z = (a,b)$$

a heißt *Realteil* und b heißt *Imaginärteil* von z.

Die Elemente $z=(a,0),\ a\in\mathbb{R}$ bilden einen Unterkörper von $\mathbb{C}$, der isomorph zu $\mathbb{R}$ ist.

$$(a,0)\cdot(b,0) = (a\cdot b,0) \qquad (a,0)+(b,0) = (a+b,0)$$
$$(1,0)$$
$$(a,0)^{-1} = \left(\frac{1}{a^2+0^2}, \frac{0}{a^2+0^2}\right) = \left(\frac{1}{a},0\right) \quad (a\neq 0)$$

Isomorphismus $f:\mathbb{R} \underset{a\mapsto(a,0)}{\to} \{(a,0)\mid a\in\mathbb{R}\}$.

Neue Darstellung von $z\in\mathbb{C}$.

$$(a,b) = (a,0)+\underbrace{(0,1)(b,0)}_{(0,b)}$$

Setze $i = (0,1)$.

Ersetze

$$(a,0) \leftrightarrow a$$
$$(b,0) \leftrightarrow b$$

$\Rightarrow (a,b) = a + ib \Rightarrow$ Rechnen wie in $\mathbb{R}$.

$i^2 = -1$

$$\underbrace{(0,1)}_{i} \cdot \underbrace{(0,1)}_{i} = (-1,0) = -1$$

$$(a+ib)\cdot(c+id) = (ac + \underbrace{i^2}_{-1} bd + i(ad+bc)) = (ac-bd, ad+bc)$$

Definition 1.12. Ist $z = a + ib \in \mathbb{C}$, so heißt $\overline{z} := a - ib$ die zu z *konjugiert komplexe Zahl*

Rechenregeln:

(i) $\overline{z+w} = \overline{z} + \overline{w}$; $\quad \overline{z \cdot w} = \overline{z} \cdot \overline{w}$.

(ii) $\overline{\overline{z}} = z$.

(iii) $z \in \mathbb{R} \Leftrightarrow z = \overline{z}$.

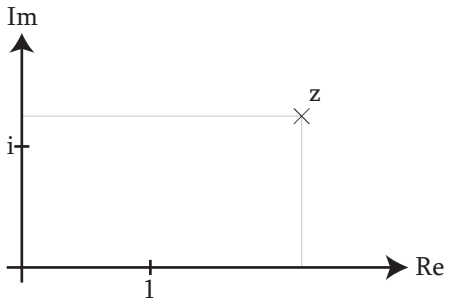

Abbildung 8: $\mathbb{C} \cong \mathbb{R}^2$

$f : \mathbb{C} \underset{z \mapsto \overline{z}}{\to} \mathbb{C}$ ist ein Automorphismus.

Betrag: $|z|$ von z:

$$|z| := \sqrt{z \cdot \overline{z}}$$

sinvoll, weil

$$\begin{aligned} z \cdot \overline{z} &= (a+ib)(a-ib) \\ &= a^2 - i^2 b^2 + aib - aib \\ &= a^2 + b^2 \geq 0 \end{aligned}$$

$a^2 + b^2 = 0 \leftrightarrow z = 0$.

Definition 1.13. Eine Menge A mit zwei Verknüpfungen $+$ und $\cdot$ heißt *Ring*, wenn

(i) $(A, +)$ ist abelsche Gruppe

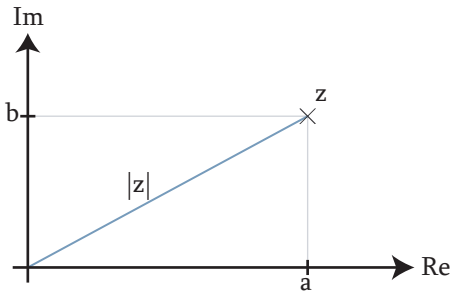

Abbildung 9: $|z|$

(ii) $(A, \cdot)$ ist Halbgruppe

(iii) Beide Distributivgesetze gelten

$$\left.\begin{array}{l} a(b+c) = ab + ac \\ (a+b)c = ac + bc \end{array}\right\} \quad \forall a, b, c \in A$$

Gelten in $(A, \cdot)$ die Kommutativgesetze, so heißt der Ring *kommutativ*. Existiet ein Neutralelement 1 in $(A, \cdot)$, so spricht man von einem *Ring mit Eins*.

Definition 1.14. Seien $(A, +, \cdot)$, $(A', +', \cdot')$ Ringe. Eine Abbildung $f : A \to A'$ heißt (Ring-)*Homomorphismus*, wenn

(i) $f(a + b) = f(a) +' f(b)$

(ii) $f(a \cdot b) = f(a) \cdot' f(b)$

für alle $a, b \in A$ gilt. Sind beides Ringemit Eins (1 bzw. $1'$), so verlangt man zusätzlich $f(1) = 1'$.

Beispiel:

(i) Jeder Körper $\mathbb{K}$ ist kommutativer Ring mit Eins.

(ii) $\mathbb{Z}$ ist kommutativer Ring mit Eins.

(iii) $(\mathcal{P}(A), \Delta, \cup)$ ist kommutativer Ring mit Eins.

(iv) $\mathbb{Z}_m$ ist kommutativer Ring mit Eins $(m \geq 2)$.

Ausflug in die Kryptographie

$$\sigma : \{1, \ldots, n\} \to \{1, \ldots, n\}$$

σ Permutation.

Verschlüsselung: Nachricht als Folge $m_1, m_2, \ldots$ mit $m_i \in \{1, \ldots, n\}$. Gesendet wird $\sigma(m_1), \sigma(m_2), \ldots$ Dechiffriert wird mit σ^{-1}.

Öffentlicher Schlüssel: σ, n

Geheimschlüssel: σ^{-1}.

Frage: Gibt es σ, so dass σ^{-1} nicht für jeden berechnbar ist?.

Jeder kann schicken, nur T kann mit σ^{-1} entschlüsseln. $\xrightarrow{\sigma(x)}$ $\underset{\sigma,n}{\mathrm{T}}$ $\xrightarrow{\sigma^{-1}(x)}$ Jeder kann entschlüsseln, aber nur T kann verschicken.

Einschub aus §1.6:

Sei $m \in \mathbb{N}$, $x_1, \ldots, x_{\varphi(m)}$ die zu m teilerfremden Zahlen aus $\{1, \ldots, m\}$, $\varphi(m)$ Anzahl dieser teilerfremden Zahlen. φ heißt *Eulersche φ-Funktion*.

Einschub. x, y heißen *teilerfremd*, wenn es kein $r \in \mathbb{N}$ gibt, mit

$$x = r \cdot u \qquad y = r \cdot v \qquad u, v \in \mathbb{Z}, r \neq 1$$

$\Rightarrow$ ggT$(x, y) = 1$.

Es gilt: Seien $x, m \in \mathbb{Z}$.

$$x, m \text{ teilerfremd } :\Leftrightarrow \text{ Es gibt eine Darstellung } rx + sm = 1, \quad r, s \in \mathbb{Z} \tag{4}$$

Man findet (4) mit dem euklidischen Algorithmus.

Beispiel: $\mathrm{ggT}(21, 8) = 1$

$$\begin{aligned} 21 &= 2 \cdot 8 + 5 \\ 8 &= 1 \cdot 5 + 3 \\ 5 &= 1 \cdot 3 + 2 \\ 3 &= 1 \cdot 2 + \underline{\underline{1}} \\ 2 &= 2 \cdot 1 + 0 \end{aligned}$$

$\Rightarrow \; 1 = -3 \cdot 21 + 8 \cdot 8.$

Vorlesung: 2004-11-19

Satz 1.9. $B := \{x_1, \ldots, x_{\varphi(m-1)}\}$ mit Multiplikation

$$(x, y) \mapsto x \cdot y \mod m$$

ist abelsche Gruppe.

Beweis:

(i) x, y teilerfremd zu $m \;\Rightarrow\; x \cdot y \mod m$ teilerfremd zu m. Denn x, y teilerfremd zu $m \;\Rightarrow\; \begin{matrix} xr + ms = 1 \\ y\overline{r} + m\overline{s} = 1 \end{matrix}$.

$\Rightarrow \; xyr\overline{r} + mu = 1$

$xy \mod m = xy + vm$

(ii) $1 \in B$

(iii) Inverse: Sei $x \in B \;\Rightarrow\; x, m$ teilfremd

$\Rightarrow \; \exists$ Darstellung $xr + ms = 1;\; r, s \in \mathbb{Z}$

$\Rightarrow \; r, m$ teilerfremd $\Rightarrow \; \overline{r} = r \mod m \in B$ und $x\overline{r} + m\overline{s} = 1 \;\Rightarrow\; x\overline{r} = 1$ in B.

$\Rightarrow \; \overline{r} = x^{-1}$.

□

Eigenschaften der Eulerschen φ-Funktion.

Hat m die Primteiler $p_1, \ldots, p_n$, so gilt

$$\varphi(m) = m\left(1 - \frac{1}{p_1}\right) \cdot \ldots \cdot \left(1 - \frac{1}{p_n}\right)$$

Speziell für $p_1, \ldots, p_n$; p_i paarweise verschiedene Primzahlen:

$$\varphi(m) = (p_1 - 1) \cdot \ldots \cdot (p_n - 1)$$

Noch spezieller $m = pq$:

$$\begin{aligned}\varphi(m) &= (p-1)(q-1)\\ &= m - p - q + 1\end{aligned}$$

Beispiel: $\varphi(15) = 8$:

$$\underbrace{1, 2, 4, 7, 8, 11, 13, 14}_{\text{8 Stück}}$$

Satz 1.10 (Euler-Fermat)**.** Seien $a, m \in \mathbb{N}$ teilerfremd, dann gilt:

$$a^{\varphi(m)} \equiv 1 \mod m$$

Beweis: a, m teilerfremd, $x_1, \ldots, x_{\varphi(m)} \in B$

$\Rightarrow$ $x_1(\underbrace{a \mod m}_{\in B}), \ldots, x_{\varphi(m)}(a \mod m)$ paarweise verschieden

$\Rightarrow$ $\underbrace{x_1 \cdot a \cdot x_2 \cdot a \cdot \ldots \cdot x_{\varphi(m)} \cdot a}_{\equiv x_1 \cdot \ldots \cdot x_{\varphi(m)} \cdot a^{\varphi(m)}} \equiv x_1 \cdot \ldots \cdot x_{\varphi(m)} \mod m$

$\Rightarrow$ $a^{\varphi(m)} \equiv 1 \mod m$

□

Beispiel: Welchen Rest lässt 4^{10259} bei Division durch 15?

$4, 15$ teilerfremd $\Rightarrow$ $4^{\overbrace{\varphi(m)}^{8}} \equiv 1 \mod 15$

$\Rightarrow$ $4^{10259} = (4^3)^{1282} \cdot 4^3 \overset{\text{E.F.}}{\Rightarrow} 4^{10259} \equiv \underbrace{4^3}_{16 \cdot 2} \mod 15 \equiv 4 \mod 15.$

Der RSA Algorithmus (Rivest-Shamir-Adleman)

Aufgabe: Gibt es ein $n \in \mathbb{N}$, $\sigma \in S_n$, so dass σ^{-1} kaum zu berechnen ist?

Wähle zwei große Primzahlen p, q und setze $n = pq$ $\Rightarrow$ $\varphi(m)$

$\Rightarrow$ $\exists$ Darstellung $e\overline{d} + \varphi(m)\overline{s} = 1, \quad \overline{d}, \overline{s} \in \mathbb{Z}$

Setze $d = \overline{d} + \varphi(m)s; s \in \mathbb{N}$, so dass $d \in \{1, \ldots, \varphi(m) - 1\}$.

$\Rightarrow$ $ed = 1 + \varphi(m)s' = 1 \quad s' \in Z$

$\Rightarrow$ $ed = 1 + \varphi(m)\underbrace{(-s')}_{>0}$

$\Rightarrow$ $ed \equiv 1 \mod \varphi(m)$

Setze

$$\sigma : \{0,\dots,n-1\} \to \{0,\dots,n-1\}$$
$$\boxed{x \mapsto x^e \mod n}$$

$$\tau : \{0,\dots,n-1\} \to \{0,\dots,n-1\}$$
$$\boxed{y \mapsto y^d \mod n}$$

Behauptung: $\sigma \circ \tau = \tau \circ \sigma = \mathrm{id}_{\{0,\dots,n-1\}}$ ($\Rightarrow$ σ, τ bijektiv und $\tau = \sigma^{-1}$)

Beweis: $\sigma(\tau(x)) = x^{ed} \mod m = \tau(\sigma(x))$

1. Fall $x = 0 \Rightarrow x^{ed} \mod n = 0$

2. Fall $x \neq 0$

$\Rightarrow$ $x \in \{1,\dots n-1\}, x$ teilerfremd zu p

$\Rightarrow$ $x^{p-1} \equiv 1 \mod p$

$\Rightarrow$ $x^{ed} = x^{1+(p-1)(q-1)\overline{s}} = x\left(x^{p-1}\right)^{(q-1)\overline{s}} \equiv x \mod p$

□

Einschub.

$$\left.\begin{aligned} x &\equiv y \mod p \\ x &\equiv y \mod q \end{aligned}\right\} \Rightarrow x = y \mod pq$$

Ist x nicht teilerfremd zu p, also $x = ps \Rightarrow x^{ed} = 0 \mod p$, also $x^{ed} \equiv x \mod p$. Also gilt $x^{ed} \equiv x \mod p \quad \forall x \in \{0,\dots,n-1\}$.

Analog folgt $x^{ed} \equiv x \mod q \quad \forall x \in \{0,\dots,n-1\}$.

$\Rightarrow x^{ed} \equiv x \mod \underbrace{pq}_{n} \Rightarrow \sigma(\tau(x)) = x^{ed} \mod n = x.$

Öffentlicher Schlüssel: n, e.

Geheimer Schlüssel: d. Sicher, weil zur Berechnung von d die Angabe von $\varphi(n)$ notwendig ist. Dazu benötigt man die Zerlegung $n = pq$.

Vorlesung: 2004-11-24

§4 Matrizen und Polynome

Ab jetzt wird (meist) immer ein abstrakter Körper $\mathbb{K}$ zugrunde gelegt.

Definition 1.15. Eine *Matrix* A (über $\mathbb{K}$) vom Format $m \times n$, $m, n \in \mathbb{N}$ (kurz (m,n)-Matrix) ist ein rechteckiges Schema von $m \cdot n$ Körperelementen mit m Zeilen und n Spalten:

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

Kurzschreibweise: $A = \boxed{((a_{ij}))}$ oder (a_{ij}) oder $((a_{ij}))_{m\times n}$.

$\mathbb{K}^{m\times n}$ ist die Menge aller (m,n)-Matrizen über $\mathbb{K}$.

Ist $m = n$, so heißt A *quadratische* Matrix.

Speziell ist

$$E_n := \begin{pmatrix} 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \vdots & & \ddots & & \vdots \\ 0 & 0 & & 1 & 0 \\ 0 & 0 & \cdots & 0 & 1 \end{pmatrix}$$

die (n-reihige) *Einheitsmatrix*. Manchmal kurz E statt E_n.

Ist $m = 1$, also

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

so heißt A auch *Zeile* (Zeilenmatrix). Ist $n = 1$, also

$$A = \begin{pmatrix} a_{11} \\ \vdots \\ a_{m1} \end{pmatrix}$$

so heißt A auch *Spalte* (Spaltenmatrix)

Bemerkung:

(i) Mit dem Kroneckersymbol

$$\delta_{i_k},\ i,j \in \mathbb{N}: \quad \delta_{ij} := \begin{cases} 0 & \text{für } i \neq j \\ 1 & i = j \end{cases}$$

erhält man $E_n = ((\delta_{ij}))$.

(ii) Matrizen $A \in \mathbb{K}^{m\times n}$ entsprechen $(m \cdot n)$-Tupel $\in \mathbb{K}^{m\times n}$ in anderer Anordnung.
Damit ergibt sich:

(i) $A = B \ :\Leftrightarrow\ a_{ij} = b_{ij} \quad \forall i,j$

(ii) $A + B$: $((a_{ij} + b_{ij}))$, wenn $A = ((a_{ij}))$, $B = ((b_{ij})) \in \mathbb{K}^{m\times n}$.

$\Rightarrow\ (\mathbb{K}^{m\times n}, +)$ abelsche Gruppe (isomorph zu $\mathbb{K}^{m\cdot n}$)

Neutrales Element: Nullmatrix

$$0 = \begin{pmatrix} 0 & \cdots & 0 \\ \vdots & & \vdots \\ 0 & \cdots & 0 \end{pmatrix}$$

Definition 1.16 (Matrizenmultiplikation)**.** Sei $A = ((a_{ij})) \in \mathbb{K}^{m\times n}$, $B = ((b_{ij})) \in \mathbb{K}^{n\times k}$, dann heißt $C \in \mathbb{K}^{m\times k}$ mit den Einträgen

$$c_{ij} := \sum_{r=1}^{n} a_{ir} \cdot b_{rj}, \quad i = 1,\ldots,m,\ j = 1,\ldots,k$$

das *Produkt* $C = A \cdot B$ von A und B.

Beispiel:

- $$\underbrace{\begin{pmatrix} 1 & 2 \\ 0 & 1 \\ 0 & 0 \end{pmatrix}}_{=A} \cdot \underbrace{\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}}_{=B} = \begin{pmatrix} 1 & 3 \\ 0 & 1 \\ 0 & 0 \end{pmatrix}$$

$B \cdot A$ existiert nicht!

- $\underbrace{\begin{pmatrix} 1 & 2 \\ 0 & 1 \\ 0 & 0 \end{pmatrix}}_{=A} \cdot \underbrace{\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}}_{=B} = \begin{pmatrix} 1 & 3 & 2 \\ 0 & 1 & 1 \\ 0 & 0 & 0 \end{pmatrix} \in \mathbb{R}^{3\times 3}$

  $B \cdot A = \begin{pmatrix} 1 & 3 \\ 0 & 1 \end{pmatrix} \in \mathbb{R}^{2\times 2}$

Satz 1.11. Die folgenden Matrizenprodukte seien jeweils erklärt. Dann gilt

(i) $(AB)C = A(BC)$ für $A \in \mathbb{K}^{m\times k},\ B \in \mathbb{K}^{k\times r},\ C \in \mathbb{K}^{r\times n}$ (Assoziativität)

(ii) $A(B+C) = AB + AC$ für $A \in \mathbb{K}^{m\times n},\ B, C \in \mathbb{K}^{n\times k}$ (Distributivität 1)

$(A+B)C = AC + BC$ für $A, B \in \mathbb{K}^{m\times n},\ C \in \mathbb{K}^{n\times k}$ (Distributivität 2)

(iii) $AE_n = A$ für $A \in \mathbb{K}^{m\times n}$

$E_n A = A$ für $A \in \mathbb{K}^{n\times k}$

Schreibweise für Beweis:

$(A)_{ij} \mathrel{\widehat{=}} (i,j)$-tes Element von A

Beweis:

(i) Assoziativität

$$\begin{aligned}((AB)C)_{ij} &= \sum_k (AB)_{ij} c_{kj} \\ &= \sum_k (\sum_r a_{ij} b_{rk}) c_{kj} \\ &= \sum_k \sum_r (a_{ir} b_{rk} c_{kj}) \\ &= \sum_r a_{ir} (\sum_k b_{rk} c_{kj}) \\ &= \sum_r a_{ir} (BC)_{rj} \\ &= (A \cdot (B \cdot C))_{ij}\end{aligned}$$

(ii) $A(B+C) = AB + AC$, denn

$$\begin{aligned}(A(B+C))_{ij} &= \sum_k a_i k \underbrace{(B+C)}_{b_{kj}+c_{kj}})_{kj} \\ &= \underbrace{\sum_k a_{ik} b_{kj}}_{(AB)_{ij}} + \underbrace{\sum_k a_{ik} c_{kj}}_{(AC)_{ij}} \\ &= (AB + AC)_{ij}\end{aligned}$$

$(A+B)C = AC + BC$ analog.

(iii) $(AE_n)_{ij} = \sum_k a_{ik} \delta_{kj} = a_i j$

□

Bemerkung: Auch für quadratische Matrizen $A, B \in \mathbb{K}^{n\times n}$ gilt im Allgemeinen keine Kommutativität:

$$AB \neq BA$$

Beispiel:

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

Satz 1.12. Die Menge $\mathbb{K}^{n\times n}$ der n-reihigen quadratischen Matrizen bildet einen Ring mit Eins.
(Für $n \geq 2$ nicht kommutativ!)

Vorlesung: 2004-11-26

Bemerkung und Definition:

(i) Für $n \geq 2$ ist $\mathbb{K}^{n\times n}$ kein Körper.

(ii) Besitzt eine Matrix $A \in \mathbb{K}^{n\times n}$ ein Inverses in $\mathbb{K}^{n\times n}$, also eine Matrix $A^{-1} \in \mathbb{K}^{n\times n}$ mit $A^{-1}\cdot A = E_n = A\cdot A^{-1}$, so heißt A *regulär* und A^{-1} heißt *Inverses* von A.

Ist A nicht regulär, so heißt A *singulär*.

Die Menge $\underbrace{\mathrm{GL}(n,\mathbb{K})}_{\subset \mathbb{K}^{n\times n}}$ der regulären (n,n)-Matrizen bildet eine Gruppe, die *allgemeine lineare Gruppe*.

Beispiel:

- $\underbrace{\begin{pmatrix} 0 & \cdots & 1 \\ \vdots & & \vdots \\ 0 & \cdots & 0 \end{pmatrix}}_{\text{singulär}} \cdot \underbrace{\begin{pmatrix} 1 & \cdots & 0 \\ \vdots & & \vdots \\ 0 & \cdots & 0 \end{pmatrix}}_{\text{singulär}} = 0$
- $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ regulär, da

$$\begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}\cdot\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \underbrace{\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}}_{E_n} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\cdot\begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}$$

$\mathrm{GL}(n,\mathbb{K})$ ist (für $n \geq 2$) kein Körper, weil $\mathrm{GL}(n,\mathbb{K})$ nicht abgeschlossen bezüglich der Addition.

Beispiel:

- $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ regulär
  $\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = E_2$ regulär, da $(-E_2)(-E_2) = E_2$
  Aber $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} + \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ singulär

(iii) Mit dem Gauß-Algorithmus (→ 1.5) kann man feststellen, ob eine Matrix A regulär ist, und die Inversen berechnen.

(iv) Sei $\mathbb{K}^{m\times n}$, $A = ((a_{ij}))$. Dann heißt $A^T = ((b_{ij}))$, $b_{ij} = a_{ji}$, $A^T \in \mathbb{K}^{n\times m}$ die zu A *transponierte* Matrix. $(A^T)_{ij} = (A)_{ji}$.

Beispiel:

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

Rechenregeln:

(i) $(A^T)^T = A$

(ii) $(A+B)^T = A^T + B^T$

(iii) $(AB)^T = B^T A^T$

Beweis:

$$\begin{aligned}((AB)^T)_{ij} &= (AB)_{ji} \\ &= \sum_k a_{jk} b_{ki} \\ &= \sum_k (A^T)_{kj} (B^T)_{ik} \\ &= \sum_k (B^T)_{ik} (A^T)_{kj} \\ &= (B^T A^T)_{ij}\end{aligned}$$

□

(iv) A regulär $\Rightarrow$ A^T regulär. Und $(A^T)^{-1} = (A^{-}1)^T$.

(v) $A \in \mathbb{K}^{n\times n}$ heißt *symmetrisch*, wenn $A = A^T$ gilt.

Die Summe von symmetrischen Matrizen ist symmetrisch. Das Produkt im Allgemeinen nicht.

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

Definition 1.17. Seien $A \in \mathbb{K}^{m\times n}$, $a \in \mathbb{K}$. Dann definieren wir

$$aA = ((aa_{ij}))$$

Bemerkung:

(i) $(a+b)A = aA + bA$
$a(A+B) = aA + aB$

(ii) $a(AB) = (aA)B = A(a)B$
$(ab)A = a(bA) = b(aA)$

(iii) $(aA)^T = aA^T$

Polynome

Polynomfunktion:

$$p : x \mapsto a_0 + a_1 x + \ldots + a_n x^n,\ x \in \mathbb{R},\ a_0, \ldots, a_n \in \mathbb{R}$$

Allgemeinere Situation

$$A \mapsto a_0 E + a_1 A + \ldots + a_n A^n,\ A \in \mathbb{K}^{n\times n}$$

Definition 1.18. Ein *Polynom* (über $\mathbb{K}$) ist eine Folge $p = (a_0, a_1, a_2, \ldots) \in \mathbb{K}^{\mathbb{N}_0}$, die nur endlich viele von 0 verschiedene Elemente enthält, d.h. für jedes Polynom p existiert $n \in \mathbb{N}_0$ derart, dass $p = (a_0, a_1, \ldots, a_n, 0, \ldots)$

Symbolische Schreibweise

$$\begin{aligned} p &= a_0 + a_1 X + a_2 X + \ldots + a_n X^n \\ &= \sum_{i=0}^{n} a_i X^i = \sum_{i=0}^{\infty} a_i X^i = \sum a_i X^i \end{aligned}$$

$\rightarrow$ Rechnen mit Polynomen wie im Körper $\mathbb{K}$.

Die Menger aller Polynome (über $\mathbb{K}$) wird mit $\mathbb{K}[X]$ bezeichnet.

Das Polynom $(0, 0, \ldots) = o$ heißt das *Nullpolynom*.

Polynome $p = (a_0, 0, \ldots)$ heißen auch *konstante Polynome*. Statt $p = a_0 X^0$ schreibt man hier $p = a_0$.

Statt $1X^i$ schreiben wir X^i.

Sei $p \in \mathbb{K}[X]$, $p \neq o$, dann heißt das kleinste $n \in \mathbb{N}_0$ mit $a_k = 0 \; \forall k \geq n+1$ der *Grad* von p ($\Rightarrow \; a_n \neq 0$).

Schreibweise: $\operatorname{Grad} p = n$.

Wir setzen $\operatorname{Grad} o = -1$.

Hat p den Grad n, so heißt p *normiert*, wenn $a_n = 1$ ist ($\Rightarrow \; p = a_0 + a_1 X + \ldots + a_{n-1} X^{n-1} + X^n$)

Addition und Multiplikation von Polynomen

$$p = (a_0, a_1, \ldots) \qquad q = (b_0, b_1, \ldots)$$

dann gilt

$$p + q := (a_0 + b_0, a_1 + b_1, \ldots)$$

$$p \cdot q := (c_0, c_1, \ldots) \text{ mit } c_i = \sum_{k=0}^{i} a_k b_{i-k}; \; i = 0, 1, 2, \ldots$$

Vorlesung: 2004-12-01

Satz 1.13. $(\mathbb{K}[X], +, \cdot)$ ist ein kommutativer Ring mit Eins.

Schreibweise für den Beweis:

$p \in \mathbb{K}[X]$, $p = (a_0, a_1, \ldots) \Rightarrow (p)_j = a_j$

zum Beweis: Assoziativgesetz bezüglich $\cdot$:

$$(p \cdot q) \cdot r = p \cdot (q \cdot r) \qquad p = \sum a_i X^i \quad q = \sum b_i X^i \quad r = \sum c_i X^i$$

$$
\begin{aligned}
((p\cdot q)\cdot r)_j &= \sum_{k=0}^{j}(p\cdot q)_j c_{j-k} \\
&= \sum_{k=0}^{j}(\sum_{l_0}^{k} a_l b_{k-l})c_{j-k} \\
&= \sum_{0\le l\le k\le j} a_l b_{k-l} c_{j-k} \\
&= \sum_{l=0}^{j} a_l \sum_{k=l}^{j} b_{k-l}c_{j-k} \\
&= \sum_{l=0}^{j} a_l \underbrace{\sum_{i=0}^{j-l} b_i c_{j-l-i}}_{(q\cdot r)_{j-l}} \quad (i=k-l) \\
&= (p\cdot(q\cdot r))_j
\end{aligned}
$$

□

Eigenschaften des Grads:

(i) $\mathrm{Grad}(p+q) \le \max(\mathrm{Grad}\, p,\ \mathrm{Grad}\, q)$

(ii) $\mathrm{Grad}(p\cdot q) = \mathrm{Grad}\, p + \mathrm{Grad}\, q$

Zusammenhang Polynom und Polynomfunktion

Jedes $p \in \mathbb{K}[X]$, $p = a_0 + a_1X + \ldots + a_nX^n$ definiert eine Funktion $\underset{t\mapsto a_o+a_1t+\ldots+a_nt^n}{f : \mathbb{K} \to \mathbb{K}}$.

Die Polynomfunktionen bilden mit der Addition

$$(f+g)(t) = f(t) + g(t)$$

und der Multiplikation

$$(f\cdot g)(t) = f(t)\cdot g(t)$$

mit $t \in \mathbb{K}$ einen kommutativen Ring mit Eins.

Die Abbildung, die jedem $p = \sum_{i=0}^{n} a_iX^i \in \mathbb{K}[X]$ die Polynomfunktion $p(t) = \sum_{i=0}^{n} q_it^i$ zuordnet, ist ein surjektiver Ringhomomorphismus, der im Allgemeinen nicht injektiv ist.

Beispiel: $F_2[X]$ und $p = X^2 + X$ dann gilt

$$p(t) = \begin{cases} 0 & \text{für } t=0 \\ 0 & \text{für } t=1 \end{cases}$$

$q = X^5 + X^3 + X^2 + X$

$$q(t) = \begin{cases} 0 & \text{für } t=0 \\ 0 & \text{für } t=1 \end{cases}$$

$\Rightarrow\ p(t) = q(t) = 0$

Teilbarkeit von Polynomen

Satz 1.14. Zu $p, q \in \mathbb{K}[X]$, $q \neq 0$ gibt es $r, s \in \mathbb{K}[X]$ mit $p = s \cdot q + r$, $\mathrm{Grad}(r) < \mathrm{Grad}(q)$.
Diese Darstellung ist eindeutig.

Beweis:

1. $\mathrm{Grad}\, p < \mathrm{Grad}\, q \overset{\text{trivial}}{\Rightarrow} p = \underbrace{0}_{s} \cdot q + \underbrace{p}_{r}$

2. $\mathrm{Grad}\, p \geq \mathrm{Grad}\, q$

   Induktion nach $\mathrm{Grad}\, p = n$

   $n = 0;\ p = a_0;\ q = b_0;\ a_0, b_0 \neq 0 \ \Rightarrow\ p = \underbrace{\frac{a_0}{b_0}}_{s} \cdot q$

   $n - 1 \ \rightarrow\ n \quad (n \geq 1)$

   $$p = a_0 + \ldots + a_n X^n; \quad q = b_0 + \ldots + b_m X^m; \quad a_n, b_m \neq 0$$
   $$p_1 := p - \frac{a_n}{b_m} X^{n-m} \cdot q \ \Rightarrow\ \mathrm{Grad}(p_1) \leq n - 1$$
   $$\Rightarrow\ p_1 = s_1 q + r_1,\ \mathrm{Grad}\, r < \mathrm{Grad}\, q$$
   $$\Rightarrow\ p = s_1 q + r_1 + \frac{a_n}{b_m} X^{n-m} q = \underbrace{\left(s_1 + \frac{a_n}{b_m} X^{n-m}\right)}_{s} q + \underbrace{r_1}_{r}$$

□

Eindeutigkeit:

$p = sq + r,\ p = s'q + r',\ \mathrm{Grad}\, r < \mathrm{Grad}\, q,\ \mathrm{Grad}\, r' < \mathrm{Grad}\, q$

$\Rightarrow\ 0 = (s - s')q + r - r'$, also $(s - s')q = r' - r$, $\mathrm{Grad}(r' - r) < \mathrm{Grad}\, q$

$\Rightarrow\ s - s' = 0\ \Rightarrow\ s = s'\ \Rightarrow\ r = r'$

Definition 1.19 (Nullstellen von Polynomen)**.** Sei $p \in \mathbb{K}[X]$, $p = \sum_{i=0}^{n} a_i X^i$.
Ein Element $c \in \mathbb{K}$ heißt *Nullstelle* von p, wenn

$$p(c) = \sum_{i_0}^{n} a_i c^i = 0$$

ist.

Korollar 1.15. $c \in \mathbb{K}$ ist Nullstelle von $p \in \mathbb{K}[X]\ :\Leftrightarrow\ p = (X - c) \cdot q$ mit einem $q \in \mathbb{K}[X]$.

Beweis:

„ $\Leftarrow$ “ trivial

„ $\Rightarrow$ “ folgt aus Satz 1.14. □

Bemerkung:

(i) Ein Polynom $p \neq 0$ vom Grad n hat höchstens n Nullstellen.

(ii) Nicht jedes Polynom p besitzt Nullstellen.

Beispiel: Sei $p = 1 + X^2$

$\mathbb{K} = \mathbb{R} \Rightarrow$ keine Nullstellen
$\mathbb{K} = \mathbb{C} \Rightarrow$ 2 Nullstellen
$\mathbb{K} = \mathbb{F}_2 \Rightarrow$ eine Nullstelle: 1

(iii) Ist $\mathbb{K}$ unendlich, so ist $p \mapsto p(t)$ injektiv. Denn $p(t) = q(t)\ \forall t \in \mathbb{K} \Rightarrow p - q$ unendlich viele Nullstellen. †

Satz 1.16 (Fundamentalsatz der Algebra)**.** Jedes $p \in \mathbb{C}[X]$ mit $\operatorname{Grad} p \geq 1$ hat eine Nullstelle.

Ohne Beweis.

$\Rightarrow$ Jedes Polynom $p \in \mathbb{C}[X]$ vom Grad $p \geq 1$ zerfällt in Linearfaktoren

$$p = d(X - c_1)(X - c_2)\cdots(X - c_n)$$

Definition 1.20 (Teiler von Polynomen)**.** Sei $p \in \mathbb{K}[X]$, $s \in \mathbb{K}[X]$, s heißt *Teiler* von p, wenn ein $r \in \mathbb{K}[X]$ existiert mit

$$p = r \cdot s$$

Definition 1.21. $p, q \in \mathbb{K}[X]$ heißen *teilerfremd*, wenn es keine gemeinsamen Teiler s vom Grad ≥ 1 gibt.

Satz 1.17. p, q teilerfremd $:\Leftrightarrow \exists$ Darstellung $pr + qs = 1$ mit $r, s \in \mathbb{K}[X]$.

Vorlesung: 2004-12-03

Beweis:

„$\Leftarrow$“

Sei $rp + sq = 1$ und $t \in \mathbb{K}[X]$ gemeinsame Teiler von p, q

$\Rightarrow \exists r's' \in \mathbb{K}[X]$ mit $p = r't,\ q = s't$
$\Rightarrow (r \cdot r' + s \cdot s') \cdot t = 1$
$\Rightarrow \operatorname{Grad} t = 0$
$\Rightarrow p, q$ teilerfremd

„$\Rightarrow$“

Sei $I := \{rp + sq \mid r, s \in \mathbb{K}[X]\} \Rightarrow I$ Untergruppe von $(\mathbb{K}[X], +)$.

Weiter gilt: $u \in I, t \in \mathbb{K}[X] \Rightarrow tu \in I$ (I ist ein *Ideal* im Ring $\mathbb{K}[X]$)

Sei $\widetilde{t} \in I$ normiert mit minimalem Grad. Sei $t \in I \Rightarrow t = s_1\widetilde{t} + r_1$ mit Grad $r_1 \leq$ Grad $\widetilde{t}$.

$\Rightarrow r_1 = t - s_1\widetilde{t} \in I \Rightarrow r_1 = 0$, weil sonst Widerspruch zur Minimalität von $\widetilde{t}$.

$\Rightarrow$ Jedes $t \in I$ ist von der Form $s\widetilde{t}$, $s \in \mathbb{K}[X]$, d.h. $I = \{s\widetilde{t} \mid s \in \mathbb{K}[X]\}$.

Wegen $p, q \in I$ folgt $p = s_1\widetilde{t}$, $q = s_2\widetilde{t}$, also $\widetilde{t} = 1$, weil p, q teilerfremd.

$\Rightarrow 1 \in I \Rightarrow$ Behauptung. □

Bemerkung:

(i) Sind p und q_1, p und q_2, …, p und q_k teilerfremd, dann sind auch p und $(q_1 \cdots q_k)$ teilerfremd.

Beweis: (nur $k = 2$, allgemein $\rightarrow$ Skript)
p und q_i teilerfremd, $i \in \{1, 2\}$.

$$\Rightarrow \left.\begin{array}{l} r_1 p + s_1 q_1 = 1 \\ r_2 p + s_2 q_2 = 1 \end{array}\right\} \Longrightarrow \underbrace{(r_1 r_2 p + r_1 s_2 q_2 + r_2 s_1 q_1)}_{\overline{r}}\, p + \underbrace{s_1 s_2}_{\overline{s}}\, q_1 q_2 = 1$$

$\Rightarrow$ $p, q_1 \cdot q_2$ teilerfremd. □

(ii) Die Darstellung $rp + sq = 1$ kann mit dem Euklid-Algorithmus gefunden werden (Übung)

Beispiel: Seien

$$p = X^5 + 2X^3 - 3X^2 + 4$$
$$q = X^2 + 1$$

$$\begin{array}{rl} X^5 + 2X^3 - 3X^2 + 4 = & \big(X^2+1\big)\big(X^3 + X - 3\big) - X + 7 \\ \underline{-X^5 - X^3} & \\ X^3 - 3X^2 & \\ \underline{-X^3 - X} & \\ -3X^2 - X + 4 & \\ \underline{3X^2 + 3} & \\ -X + 7 & \end{array}$$

$$\Rightarrow \boxed{\underbrace{(X^3 + X - 3)}_{s_1} q + \underbrace{(-X + 7)}_{r_1}}$$

Dividiere q durch r_1

$$\begin{array}{rl} X^2 + 1 = & \big(-X+7\big)\big(-X-7\big) + 50 \\ \underline{-X^2 + 7X} & \\ 7X + 1 & \\ \underline{-7X + 49} & \\ 50 & \end{array}$$

$$\Rightarrow \boxed{q = \underbrace{(-X+7)}_{s_2} r_1 + \underbrace{50}_{r_2}}$$

$$\Rightarrow 50 = q - s_2 r_1 = q - s_2(p - s_1 q) = (1 + s_1 s_2)q + (-s_2)p$$

$$\Rightarrow 1 = \underbrace{\frac{1}{50}(1 + s_1 s_2)}_{s}\, q + \underbrace{\frac{1}{50}(-s_2)}_{r}\, p$$

$$\Rightarrow \left(\frac{1}{50}X + \frac{7}{50}\right) p + \frac{1}{50}\big(-X^4 - 7X^3 - X^2 - 4X + 22\big)\, q = 1$$

§5 Der Gauß-Algorithmus

Betrachte LGS (über $\mathbb{K}$):

$$\begin{array}{ccccccc} a_{11}x_1 & + & \ldots & + & a_{1n}x_n & = & b_1 \\ \vdots & & \vdots & & \vdots & & \vdots \\ a_{m1}x_1 & + & \ldots & + & a_{mn}x_n & = & b_m \end{array} \qquad (*)$$

$\Rightarrow$ Matrixform:

$$\underbrace{\begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & & \vdots \\ a_{m1} & \cdots & a_{mn} \end{pmatrix}}_{A\in\mathbb{K}^{m\times n}} \cdot \underbrace{\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}}_{x\in\mathbb{K}^{n\times 1}} = \underbrace{\begin{pmatrix} b_1 \\ \vdots \\ b_m \end{pmatrix}}_{b\in\mathbb{K}^{m\times 1}} \Leftrightarrow Ax = b$$

Erweiterte Matrix des LGS:

$$\left(\begin{array}{c|c} A & b \end{array}\right) = \left(\begin{array}{ccc|c} a_{11} & \cdots & a_{1n} & b_1 \\ \vdots & & \vdots & \vdots \\ a_{m1} & \cdots & a_{mn} & b_m \end{array}\right)$$

Bemerkung: L_{inh}, L_{hom} seien die Lösungsmengen von $Ax = b$ bzw. $Ax = 0$.

Ist $x, y \in L_{\text{inh}} \Rightarrow x - x' \in L_{\text{hom}}$.

Ist $y \in L_{\text{hom}}$, und $x \in L_{\text{inh}} \Rightarrow x + y \in L_{\text{inh}}$.

$\Rightarrow L_{\text{inh}} = \{x_0 + y \mid y \in L_{\text{hom}}\}$, x_0 eine spezielle Lösung von $Ax = b$.

Der Gauß-Algorithmus verwendet *elementare Zeilenumformungen*

$$\begin{array}{lcccccccc} z_1 & \to & a_{11}x_1 & + & \ldots & + & a_{1n}x_n & = & b_1 \\ & & \vdots & & & & \vdots & & \vdots \\ z_m & \to & a_{m1}x_1 & + & \ldots & + & a_{mn}x_n & = & b_m \end{array}$$

(i) $z_i \leftrightarrow z_j$

(ii) $a \cdot z_i$, $a \neq 0$

(iii) $z_i \to z_i + a \cdot z_j$, $a \in \mathbb{K}$

Satz 1.18. Durch elementare Zeilenumformungen geht das LGS $Ax = b$ in ein LGS $\widetilde{A}x = \widetilde{b}$ über, wobei $Ax = b$ und $\widetilde{A}x = \widetilde{b}$ die gleiche Lösungsmenge besitzen.

Beweis: Klar. □

Beispiel:

LGS:

$$\begin{array}{rcrcrcrcrcr} x_1 & - & 2x_2 & + & x_3 & - & x_4 & + & x_5 & = & 0 \\ 4x_1 & - & 8x_2 & + & 3x_3 & - & 3x_4 & + & x_5 & = & 2 \\ -2x_1 & + & 4x_2 & - & 2x_3 & - & x_4 & + & 4x_5 & = & -3 \\ x_1 & - & 2x_2 & & & - & 3x_4 & + & 4x_5 & = & a \end{array}$$

$a \in \mathbb{K}$.

Es ergeben sich folgende Umformungen:

$$\left(\begin{array}{rrrrrr} 1 & -2 & 1 & -1 & 1 & 0 \\ 4 & 8 & 3 & -3 & 1 & 2 \\ -2 & 4 & -2 & -1 & 4 & -3 \\ 1 & -2 & 0 & -3 & 4 & a \end{array}\right) \begin{array}{l} \\ \leftarrow \\ \leftarrow \\ \leftarrow \end{array} \begin{array}{l} \left|\cdot(-4)\right. \\ +\\ \left|\cdot 2\right. \\ +\\ \left|\cdot(-1)\right. \\ + \end{array}$$

$$\rightsquigarrow \left(\begin{array}{rrrrrr} 1 & -2 & 1 & -1 & 1 & 0 \\ 0 & 0 & -1 & 1 & -3 & 2 \\ 0 & 0 & 0 & -3 & 6 & -3 \\ 0 & 0 & -1 & -2 & 3 & a \end{array}\right) \begin{array}{l} \left|\cdot(-1)\right. \\ \left|\cdot(-\frac{1}{3})\right. \\ \leftarrow \end{array} \begin{array}{l} \\ \\ + \end{array}$$

$$\rightsquigarrow \left(\begin{array}{rrrrrr} 1 & -2 & 1 & -1 & 1 & 0 \\ 0 & 0 & 1 & -1 & 3 & -2 \\ 0 & 0 & 0 & 1 & -2 & 1 \\ 0 & 0 & 0 & -3 & 6 & a-2 \end{array}\right) \begin{array}{l} \\ \\ \left|\cdot 3\right. \\ \leftarrow \end{array} \begin{array}{l} \\ \\ \\ + \end{array}$$

$$\rightsquigarrow \left(\begin{array}{rrrrr|r} 1 & -2 & 1 & -1 & 1 & 0 \\ 0 & 0 & 1 & -1 & 3 & -2 \\ 0 & 0 & 0 & 1 & -2 & 1 \\ 0 & 0 & 0 & 0 & 0 & a+1 \end{array}\right)$$

Treppennormalform (TNF) von $\left(\begin{array}{c|c} A & b \end{array}\right)$.

$\Rightarrow$ LGS ist lösbar nur für $a = -1$.

$$\left(\begin{array}{rrrrrr} 1 & -2 & 1 & -1 & 1 & 0 \\ 0 & 0 & 1 & -1 & 3 & -2 \\ 0 & 0 & 0 & 1 & -2 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{array}\right) \begin{array}{l} \\ \leftarrow \\ \leftarrow \\ \\ \end{array} \begin{array}{l} \\ + \\ + \\ \\ \end{array}$$

$$\rightsquigarrow \left(\begin{array}{rrrrrr} 1 & -2 & 1 & 0 & -1 & 1 \\ 0 & 0 & 1 & 0 & 1 & -1 \\ 0 & 0 & 0 & 1 & -2 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{array}\right) \begin{array}{l} \\ \left|\cdot(-1)\right. \\ \\ \\ \end{array} \begin{array}{l} \\ + \\ \\ \\ \end{array}$$

$$\rightsquigarrow \left(\begin{array}{rrrrr|r} 1 & -2 & 0 & 0 & 1 & 2 \\ 0 & 0 & 1 & 0 & 1 & -1 \\ 0 & 0 & 0 & 1 & -2 & 1 \end{array}\right)$$

Gaußsche Normalform (GNF)

Vorlesung: 2004-12-08

$\Rightarrow$ LGS

$$\begin{array}{rrrrcr} x_1 & -2x_2 & & -2x_5 & = & 2 \\ & & x_3 & +x_5 & = & -1 \\ & & x_4 & -2x_5 & = & 1 \end{array}$$

$x_5 = 5 \Rightarrow x_4 = 1 + 2s;\ x_3 = -1 - s;\ x_2 = t \Rightarrow x_1 = 2 + 2s + 2t$

$\Rightarrow$ Allgemeine Lösung

$$x = \begin{pmatrix} 2+2s+2t \\ t \\ -1-s \\ 1+2s \\ s \end{pmatrix} = \begin{pmatrix} 2 \\ 0 \\ -1 \\ 1 \\ 0 \end{pmatrix} + s \begin{pmatrix} 2 \\ 0 \\ -1 \\ 2 \\ 1 \end{pmatrix} + t \begin{pmatrix} 2 \\ 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} \quad s,t \in \mathbb{R}$$

Der Gauß Algorithmus

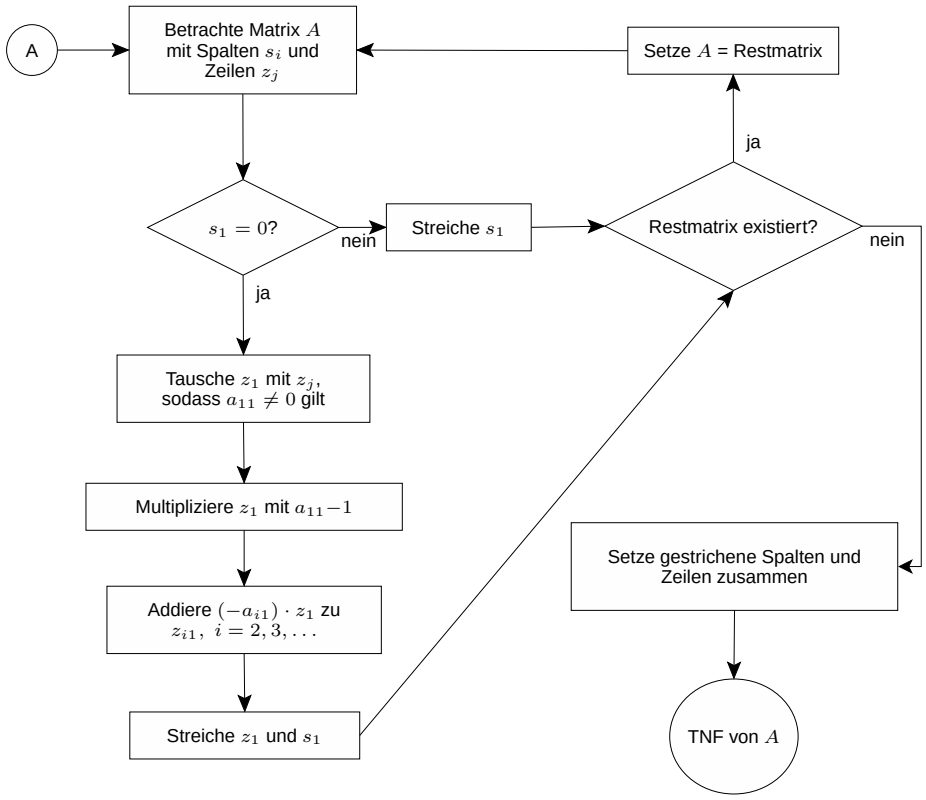

Abbildung 10: Der Gauß Algorithmus

Anwendungen des Gauß Algorithmus

- LGS $Ax = B$. Anwendung auf $\left(\begin{array}{c|c} A & b \end{array}\right)$.

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

$$\left(\begin{array}{c|c} A & b \end{array}\right) = \left(\begin{array}{ccc|c} a_{11} & \cdots & 1_{1n} & b_1 \\ \vdots & & \vdots & \vdots \\ a_{m1} & \cdots & a_{mn} & b_m \end{array}\right)$$

Treppennormalform der Matrix A

$$\left(\begin{array}{ccccccccccccccccccc}
0 & \cdots & 1 & * & \cdots & & & & & & & & & & & & & & \\
0 & \cdots & \cdots & \cdots & 0 & 1 & * & \cdots & & & & & & & & & & & \\
0 & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & 0 & 1 & * & \cdots & & & & * & & & & \\
\vdots & & & & & & & & & & & \ddots & & & & & & & \\
0 & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & 0 & 1 & * & \cdots & \cdots & \cdots & * \\
0 & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & 0 & 1 & * & \cdots & * \\
\hline
0 & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & 0 \\
\vdots & & & & & & & & & & & & & & & & & \vdots \\
0 & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & 0
\end{array}\right)$$

Gauß'sche Normalform von A

$$\left(\begin{array}{cccccccccccccc}
0 & \cdots & 0 & 1 & * & \cdots & & 0 & * & \cdots & * & 0 & * & \cdots & * \\
\vdots & & & & & & \ddots & \vdots & \vdots & & \vdots & \vdots & \vdots & & \vdots \\
0 & \cdots & \cdots & \cdots & \cdots & \cdots & 0 & 1 & * & \cdots & * & 0 & * & \ldots & * \\
0 & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & 0 & 1 & * & \cdots & * \\
\hline
0 & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & 0 \\
\vdots & & & & & & & & & & & & & & \vdots \\
0 & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & 0
\end{array}\right)$$

Gauß'sche Normalform von $\left(\begin{array}{c|c} A & b \end{array}\right)$

$$\left(\begin{array}{cccccccccccccc|c}
0 & \cdots & 0 & 1 & * & \cdots & & 0 & * & \cdots & * & 0 & * & \cdots & * & a_1 \\
\vdots & & & & & & \ddots & \vdots & \vdots & & \vdots & \vdots & \vdots & & \vdots & \vdots \\
0 & \cdots & \cdots & \cdots & \cdots & \cdots & 0 & 1 & * & \cdots & * & 0 & * & \ldots & * & a_{k-1} \\
0 & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & 0 & 1 & * & \cdots & * & a_k \\
\hline
0 & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & 0 & 0 \\
\vdots & & & & & & & & & & & & & & \vdots & \vdots \\
0 & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & 0 & 0
\end{array}\right)$$

$\Rightarrow$ LGS $Ax = b$ ist lösbar $:\Leftrightarrow$ $a_{k+1} \ldots a_m = 0$

Im Falle der Lösbarkeit gibt es $n-k$ frei wählbare Variablen, nämlich alle aus $\{x_1, \ldots, x_n\} \backslash \{x_{j1}, \ldots, x_{jk}\}$.
Daraus bestimmen sich dann die restlichen Variablen $x_{j1}, \ldots, x_{jk}$.

Satz 1.19. Ein homogenes LGS mit m Gleichungen und n Variablen, wobei $m < n$ ist immer nicht-trivial lösbar.

Beweis: Direkte Konsequenz des vorangegangenen Abschnitts □

- Bestimmung der Inversen

Satz 1.20. Sei $A \in \mathbb{K}^{n \times n}$. Hat $\left(\begin{array}{c|c} A & b \end{array}\right) \in \mathbb{K}^{n \times 2n}$ die Gaußnormalform $\left(\begin{array}{c|c} E_n & A' \end{array}\right)$, so ist A regulär, und $A^{-1} = A'$.

Beweis: $\left(\begin{array}{c|c} A & E_n \end{array}\right)$, GNF: $\left(\begin{array}{c|c} E_n & A' \end{array}\right)$ wobei

$$\begin{array}{l} A' = (a'_1 \mid \ldots \mid a'_n) \\ E_n = (e_1 \mid \ldots \mid e_n) \\ X = (x_1 \mid \ldots \mid x_n) \end{array} \in \mathbb{K}^{n \times n} \text{ mit } x_i = \begin{pmatrix} x_{1i} \\ \vdots \\ x_{mi} \end{pmatrix}$$

Die Matrizengleichung $AX = E_n$ entspricht n Gleichungssystemen $Ax_i = e_i$, $i = 1, \ldots, n$.
Nach Voraussetzung ist GNF von $\left(\begin{array}{c|c} A & e_i \end{array}\right)$ die Matrix $\left(\begin{array}{c|c} E_n & a'_i \end{array}\right)$

$\Rightarrow$ Das LGS $Ax_i = e_i$ ist lösbar und $x_i = a'_i$ ist die (eindeutige) Lösung.

$$\left(\begin{array}{ccc|c} 1 & & 0 & a'_{1i} \\ & \ddots & & \vdots \\ 0 & & 1 & a'_{mi} \end{array}\right)$$

$\Rightarrow$ $AX = E_n$ hat Lösung $X = A'$.

$\Rightarrow$ $\boxed{A \cdot A' = E_n}$.

Durch Zeilenumformungen geht $\left(\begin{array}{c|c} E_n & A' \end{array}\right)$ wieder in $\left(\begin{array}{c|c} A & E_n \end{array}\right)$ über.

$\Rightarrow$ Dabei geht $\left(\begin{array}{c|c} A' & E_n \end{array}\right)$ in $\left(\begin{array}{c|c} E_n & A' \end{array}\right)$ über.

$\overset{\text{s.o.}}{\Rightarrow}$ $A' \cdot A = E_n$

$\Rightarrow$ $A' = A^{-1}$ □

Beispiel:

$$\left(\begin{array}{cccc|cccc} 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 2 & 1 & 0 & 1 & 0 & 0 \\ 0 & -1 & 0 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 2 & 0 & 0 & 0 & 1 \end{array}\right) \rightarrow \cdots \rightarrow \left(\begin{array}{cccc|cccc} 1 & 0 & 0 & 0 & 2 & -1 & -1 & 0 \\ 0 & 1 & 0 & 0 & -1 & \frac{1}{2} & -\frac{1}{2} & \frac{1}{2} \\ 0 & 0 & 1 & 0 & 0 & \frac{1}{2} & \frac{1}{2} & -\frac{1}{2} \\ 0 & 0 & 0 & 1 & -1 & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} \end{array}\right)$$

- Sei $A \in \mathbb{K}^{n\times n}$. Die obere (untere) Dreiecksmatrix ist

  $A = ((a_{ij}))$ mit $a_{ij} = 0$ für $i > j$ $(i < j)$

  Hier gilt:

  A regulär $:\Leftrightarrow\ a_{ij} \neq 0;\ i = 1, \ldots, n$

  In diesem Fall ist auch A^{-1} obere (untere) Dreiecksmatrix.
  Die oberen (unteren) Dreiecksmatrizen bilden eine Untergruppe von $GL(n, \mathbb{K})$.

2 Vektorräume

§1 Vektorräume und Untervektorräume

Hier wieder allgemeiner Körper $\mathbb{K}$.

Definition 2.1. Ein *Vektorraum* V (über dem Körper $\mathbb{K}$), kurz $\mathbb{K}$-Vektorraum ($\mathbb{K}$-VR) ist eine Menge mit zwei Abbildungen $+ : V \times V \to V$, $\cdot : \mathbb{K} \times V \to V$, die die folgenden Gesetze erfüllen:

1. $(V, +)$ ist abelsche Gruppe (mit Neutralelement 0)
2. $a \cdot (x + y) = a \cdot x + a \cdot y \quad \forall a \in \mathbb{K},\ x, y \in V$
3. $(a + b) \cdot x = a \cdot x + b \cdot x \quad \forall a, b \in \mathbb{K},\ x \in V$
4. $a \cdot (b \cdot x) = (a \cdot b) \cdot x \quad \forall a, b \in \mathbb{K},\ x \in V$
5. $1 \cdot x = x \quad \forall x \in V$

Vorlesung: 2004-12-10

Definition 2.2. Sei V ein $\mathbb{K}$-Vektorraum und $U \subset V$. U heißt *Untervektorraum* von V (oder *Unterraum* oder auch *linearer Teilraum*), wenn U mit den auf $U \times U$ bzw. $\mathbb{K} \times U$ eingeschränkten Abbildungen $+$ und $\cdot$ ein Vektorraum ist.

Definition 2.3. Seien V, W $\mathbb{K}$-Vektorräume und $f : V \to W$ Abbildung. Dann heißt f *Homomorphismus* oder *lineare Abbildung*, wenn

$$f(a \cdot x + b \cdot y) = a \cdot f(x) + b \cdot f(y) \qquad \forall x, y \in V;\ a, b \in \mathbb{K}$$

Bezeichungen

- V Vektorraum: Elemente $x \in V$ heißen *Vektoren*.
- $\mathbb{K} = \mathbb{R}$: *reeller Vektorraum*. $\mathbb{K} = \mathbb{C}$: *komplexer Vektorraum*.

Satz 2.1. In einem $\mathbb{K}$-Vektorraum gilt:

(i) $a \cdot o = o \quad \forall a \in \mathbb{K}$

(ii) $0 \cdot x = o \quad \forall x \in V$

(iii) Aus $a \cdot x = o$ folgt $a = 0$ oder $x = o$

(iv) $(-1) \cdot x = -x \quad \forall x \in V$

Beweis:

(i) $a \cdot o = a \cdot (o + o) = a \cdot o + a \cdot o \overset{\text{Satz 1.1}}{\Longrightarrow} a \cdot o = o$

(ii) $0 \cdot x = (0 + 0) \cdot x = 0 \cdot x + 0 \cdot x \ \Rightarrow\ 0 \cdot x = o$

(iii) $a \cdot x = o$ und $a \neq 0 \ \Rightarrow\ a^{-1} \cdot (a \cdot x) = a^{-1} \cdot o \ \Rightarrow\ x = o$

(iv) $o = 0 \cdot x = (1 - 1) \cdot x = 1 \cdot x + (-1) \cdot x = x + (-1) \cdot x \overset{\text{Satz 1.1}}{\Longrightarrow} (-1) \cdot x = -x$

□

Satz 2.2. Sei V ein $\mathbb{K}$-Vektorraum und $U \subset V$. Dann gilt U Untervektorraum $:\Leftrightarrow$ $U \neq \emptyset$ und aus $x, y \in U$, $a \in \mathbb{K}$ folgt $x + y \in U$, $ax \in U$.

Beweis: trivial □

Beispiel:

(i) V $\mathbb{K}$-Vektorraum $\Rightarrow$ V, $\{o\}$ triviale Untervektorräume

(ii) $V = \mathbb{K}^n$ mit komponentenweiser Addition und Skalarmultiplikation

$$(x_1, \ldots, x_n) + (y_1, \ldots, y_n) := (x_1 + y_1, \ldots, x_n + y_n)$$
$$a(x_1, \ldots, x_n) := (ax_1, \ldots, ax_n)$$
$$o = (0, \ldots, 0)$$

(iii) $V = \mathbb{K}^{m \times n}$ mit komponentenweiser Addition und Skalarmultiplikation

Speziell sind also $\mathbb{K}^n$, $\mathbb{K}^{1\times n}$ und $\mathbb{K}^{n\times 1}$ Vektorräume von n-Tupeln

$$(x_1, \ldots, x_n) \qquad \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \qquad (x_1 \cdots x_n)$$

Wir werden in Zukunft $\mathbb{K}^n$ und $\mathbb{K}^{n\times 1}$ identifizieren, also n-Tupel auch als Spaltenvektoren auffassen, aber Spalten- und Zeilenmatrizen auseinander halten.

($\Rightarrow$ $x = (x_1, \ldots, x_n)$, $A \in \mathbb{K}^{m\times n}$, dann ist Ax erklärt)

Damit ist die Lösungsmenge $\mathcal{L}_{\text{hom}}$ eines homogenen LGS $Ax = 0$, $A \in \mathbb{K}^{m\times n}$, $x \in \mathbb{K}^n$ ein Untervektorraum von K^n.

(iv) $\mathbb{K}^{\mathbb{N}_0}$ (Menge der Folgen $(c_0, c_1, \ldots)$ mit $c \in \mathbb{K}$) ist $\mathbb{K}$-Vektorraum, wenn $+$ und $\cdot$ komponentenweise erklärt werden (siehe (b)).

$\mathbb{K}[X]$ ist Untervektorraum von $\mathbb{K}^{\mathbb{N}_0}$.

(v) $\mathbb{K}^A$, A beliebige Menge, ist $\mathbb{K}$-VR bezüglich $+$ und $\cdot$:

$$\{f : A \to \mathbb{K}\} \qquad \left.\begin{array}{c}(f+g)(x) := f(x) + g(x) \\ (a \cdot f)(x) := a \cdot f(x)\end{array}\right\} x \in A,\ a \in \mathbb{K}$$

Allgemeiner ist V^A $\mathbb{K}$-Vektorraum, wenn V $\mathbb{K}$-Vektorraum ist.

(vi) Speziell ist $\mathbb{R}^{[0,1]} := \{$ relle Funktion $f : [0, 1] \to \mathbb{R}\}$ reeller Vektorraum.

Die Menge $C(0, 1)$ der stetigen Funktionen auf $[0, 1]$ bildet einen Unterkvektorraum von $\mathbb{R}^{[0,1]}$.

(vii) Homomorphismus $f : V \to W$, V, W $\mathbb{K}$-Vektorräume.

$\Rightarrow$ $\operatorname{Kern} f$ Untervektorraum von V. Bild $f := f(V)$ Untervektorraum von W.

Vorlesung: 2004-12-15

Korollar 2.3. Sei V $\mathbb{K}$-Vektorraum. Dann ist der Durchschnitt beliebig vieler Untervektorräume von V wieder Untervektorraum.

Beweis: Folgt direkt aus Satz 2.2. □

Definition 2.4. Sei V $\mathbb{K}$-Vektorraum und $A \subset V$. Dann heißt

$$[A] := \bigcap_{U \text{ UVR von } V,\ A \subset U} U$$

der *von A erzeugte* Untervektorraum oder die *lineare Hülle* von A.

Ist $A := \{x_1, \ldots, x_k\}$, so schreiben wir

$$[A] = [x_1, \ldots, x_k]$$

und sagen, dass $x_1, \ldots, x_k$ den Unterraum $[x_1, \ldots, x_k]$ *aufspannen*.

Allgemein heißt die Menge A auch *Erzeugendensystem* von $[A]$.

Beispiel:

- $[V] = V$
- $[\emptyset] = \{\emptyset\}$
- $[x] = \{ax \mid a \in \mathbb{K}\} \quad x \in V$

Definition 2.5. Seien $x_1, \ldots, x_k \in V$. Jeder Vektor der Form

$$a_1x_1 + \ldots + a_kx_k$$

mit $a_1, ldots, a_k \in \mathbb{K}$ heißt *Linearkombination* der Vektoren $x_1, \ldots, x_k$.

Satz 2.4. Sei V $\mathbb{K}$-Vektorraum und $A \subset V$, $A \neq \emptyset$. Dann ist $[A]$ die Menge aller Linearkombinationen von Vektoren aus A.

(Speziell $[x_1, \ldots, x_k] = \{a_1x_1 + \ldots + a_kx_k \mid a_1, \ldots, a_k \in \mathbb{K}\}$)

Beweis:

Sei U die Menge aller Linearkombinationen von Vektoren aus $A \Rightarrow A \subset U$ und U ist Untervektorraum von V nach Satz 2.2.

$\Rightarrow [A] \subset U$.

Umgekehrt gilt $A \subset [A]$. Da $[A]$ Untervektorraum ist, enthält $[A]$ alle Linearkombinationen von Vektoren aus A

$\Rightarrow U \subset [A]$. □

Frage:

$$\left[\begin{pmatrix}1\\0\\1\\0\end{pmatrix}, \begin{pmatrix}1\\2\\3\\4\end{pmatrix}, \begin{pmatrix}-1\\-2\\1\\0\end{pmatrix}, \begin{pmatrix}4\\3\\1\\2\end{pmatrix}\right] \stackrel{?}{=} \mathbb{R}^4$$

§2 Lineare Abhängigkeit und Unabhängigkeit

Definition 2.6. Sei V $\mathbb{K}$-Vektorraum, $x_1, \ldots, x_k \in V$, $k \in \mathbb{N}$. Die Vektoren $x_1, \ldots, x_k$ heißen *lineare abhängig* (l.a.), wenn es Skalare $a_1, \ldots, a_k$ gibt, die nicht alle Null sind und

$$a_1x_1 + \ldots + a_kx_k = o$$

erfüllen.

$x_1, \ldots, x_k$ heien *lineare unabhängig* (l.u.), wenn aus $a_1x_1 + \ldots + a_kx_k = o$ immer folgt, dass $a_1 = \ldots = a_k = 0$.

Bemerkung:

(i) $x_1, \ldots, x_k$ sind entweder l.a. oder l.u.

(ii) $x_1, \ldots, x_k$ sind l.a. falls ein $x_i = o$ existiert, oder falls $x_i = x_j$ für ein paar $i \neq j$ gilt.

(iii) $x_1, \ldots, x_k$ l.a. $\Leftrightarrow$ Einer der Vektoren x_i ist Linearkombination der anderen.

(iv) Betrachte $x_1, \ldots, x_k \in V$ und

$$y_1 = \sum_{i=1}^{k} a_{i1} x_1, \ldots, y_m = \sum_{i=1}^{k} a_{im} x_i$$

Dann gilt

$$\sum_{j=1}^{m} t_j y_j = o \;\Leftrightarrow\; o = \sum_{j=1}^{m} t_j y_j = \sum_{j=1}^{m} t_j \left(\sum_{i=1}^{k} a_{ij} x_i \right) = \sum_{i=1}^{k} \left(\sum_{j=1}^{m} t_j a_{ij} \right) x_i \tag{5}$$

Nun setzen wir voraus, dass die Vektoren $x_1, \ldots, x_k$ l.a. sind.

Dann gilt

$$\begin{aligned} & \sum_{j=1}^{k} t_j y_j = o \\ \Leftrightarrow\; & \sum_{j=1}^{m} t_j a_{ij} = o \quad i = 1, \ldots, k \\ \Leftrightarrow\; & \sum_{j=1}^{m} t_j \widehat{y}_j = o \quad \text{wobei} \quad \widehat{y}_1 := \begin{pmatrix} a_{ij} \\ \vdots \\ a_{kj} \end{pmatrix} \in \mathbb{K}^k \end{aligned}$$

Dann gilt $y_1, \ldots, y_m$ l.a. $:\Leftrightarrow$ $\widehat{y}_1, \ldots, \widehat{y}_m$ l.a.

Satz 2.5. Sei V $\mathbb{K}$-Vektorraum, $x_1, \ldots, x_k \in V$, $y_1, \ldots, y_m$ Linearkombinationen der x_i, und $m \geq k+1$.
Dann sind $y_1, \ldots, y_m$ linear abhängig.

Beweis:

Sei $y_j = \sum_{i=1}^{k} a_{ij} x_i$, $j = 1, \ldots, m$.

Dann gilt

$$\sum_{j=1}^{m} t_j y_j = o \;\Leftrightarrow\; \sum_{i=1}^{k} \left(\sum_{j=1}^{m} t_j a_{ij} \right) x_i = o \quad \text{nach (5)}$$

Wegen $m \geq k+1$ hat das homogene LGS $\sum_{j=1}^{m} t_j a_{ij} = o$, $i = 1, \ldots, k$ eine nicht triviale Lösung $(t_1, \ldots, t_m) \neq (0, \ldots, 0)$. □

Beispiel:

(i) $V = \mathbb{R}^4$, $x_1 = \begin{pmatrix} 2 \\ -3 \\ 1 \\ 4 \end{pmatrix}$, $x_2 = \begin{pmatrix} 1 \\ 0 \\ 1 \\ 2 \end{pmatrix}$, $x_3 = \begin{pmatrix} -2 \\ 1 \\ -1 \\ 1 \end{pmatrix}$, $x_4 = \begin{pmatrix} 1 \\ -5 \\ 0 \\ 7 \end{pmatrix}$

Frage: x_1, x_2, x_3, x_4 linear abhängig oder linear unabhängig?

LGS:

$$\begin{array}{rcrcrcrcl} 2a_1 & + & a_2 & - & 2a_3 & + & a_4 & = & 0 \\ -3a_1 & & & + & a_3 & - & 5a_4 & = & 0 \\ a_1 & + & a_2 & - & a_3 & & & = & 0 \\ 4a_1 & + & 2a_2 & + & a_3 & + & 7a_4 & = & 0 \end{array}$$

$$\rightsquigarrow \begin{pmatrix} 1 & 1 & -1 & 0 \\ 2 & 1 & -2 & 1 \\ -3 & 0 & 1 & -5 \\ 4 & 2 & 1 & 7 \end{pmatrix}$$

$$\overset{\text{Gauss}}{\rightsquigarrow} \begin{pmatrix} 1 & 1 & -1 & 0 \\ 0 & 1 & 0 & -1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

$\Rightarrow$ LGS nicht-trivial lösbar.

$\Rightarrow$ x_1, x_2, x_3, x_4 l.a.

(ii) $x_1, \ldots, x_k \in V$ über $\mathbb{R}$ seien l.u. und

$$\begin{array}{rcrcrcrcl} y_1 & = & x_1 & - & 2x_2 & + & x_3 & - & x_4 \\ y_2 & = & -4x_1 & - & 2x_2 & & & + & 4x_4 \\ y_3 & = & 2x_1 & + & 3x_2 & - & x_3 & - & 3x_4 \\ y_4 & = & x_1 & + & x_2 & + & x_3 & + & x_4 \end{array}$$

Frage: $y_1, \ldots, y_k$ l.a. oder l.u. $\Leftrightarrow$ $\widehat{y}_1, \ldots, \widehat{y}_k$ l.a. oder l.u.?

$$\widehat{y}_1 = \begin{pmatrix} 1 \\ -2 \\ 1 \\ -1 \end{pmatrix} \quad \widehat{y}_2 = \begin{pmatrix} -4 \\ -2 \\ 0 \\ 4 \end{pmatrix} \quad \widehat{y}_3 = \begin{pmatrix} 2 \\ 3 \\ -1 \\ 3 \end{pmatrix} \quad \widehat{y}_4 = \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \end{pmatrix}$$

$$\Rightarrow \begin{pmatrix} 1 & -4 & 2 & 1 \\ -2 & -2 & 3 & 1 \\ 1 & 0 & -1 & 1 \\ -1 & 4 & -3 & 1 \end{pmatrix}$$

$$\overset{\text{Gauss}}{\rightsquigarrow} \begin{pmatrix} 1 & -4 & 2 & 1 \\ 0 & 1 & -\frac{7}{10} & \frac{3}{10} \\ 0 & 0 & 1 & -6 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

$\Rightarrow$ $y_1, \ldots, y_k$ l.a.

Vorlesung: 2004-12-17

Definition 2.7. Sei V $\mathbb{K}$-Vektorraum und $A \subset V$. Dann heißt A *linear abhängig*, wenn es (paarweise) verschiedene Vektoren $x_1, \ldots, x_k \in A$, $k \in \mathbb{N}$ gibt, die linear abhängig sind.

A heißt *linear unabhängig*, wenn A nicht linear abhängig ist.

Bemerkung:

(i) A l.u. $\Leftrightarrow$ $A = \emptyset$ oder je endlich viele verschiedene Vektoren $x_1, \ldots, x_k$ aus A sind l.u.

(ii) Ist $A = \{x_1, \ldots, x_m\}$ (mit $|A| = m$), dann gilt A l.a. $\Leftrightarrow$ $x_1, \ldots, x_m$ l.a.

(iii) $o \in A \Rightarrow A$ l.a.

(iv) Jede Obermenge einer l.a. Menge ist l.a.
Jede Teilmenge einer l.u. Menge ist l.u.

(v) A l.a. $\Leftrightarrow \exists x \in A$ mit $[A] = [A\backslash\{x\}]$

Beweis:
„$\Rightarrow$“:
Sei A l.a. $\Rightarrow \exists x_1, \ldots, x_k \in A$ und $a_1, \ldots, a_k$ mit $(a_1, \ldots, a_k) \neq (0, \ldots, 0)$ und $a_1x_1 + \ldots + a_kx_k = o$
$\Rightarrow$ (O.B.d.A. $a_k \neq 0$)

$$x_k = -\frac{a_1}{a_k}x_k - \ldots - \frac{a_{k-1}}{a_k}x_{k-1} \in [A\backslash\{x_k\}]$$

$\Rightarrow [A] = [A\backslash\{x_k\}]$
„$\Leftarrow$“:
Sei $x \in A$ mit $[A] = [A\backslash\{x\}]$.

- 1. Fall:

$$\begin{aligned} & A\backslash\{x\} = \emptyset \\ \Rightarrow\ & [A\backslash\{x\}] = \{o\} \\ \Rightarrow\ & A = \{o\} \\ \Rightarrow\ & x = o \\ \Rightarrow\ & A \text{ l.a.} \end{aligned}$$

- 2. Fall

$$\begin{aligned} & A\ \{x\} \neq \emptyset \\ \Rightarrow\ & x \in [A\backslash\{x\}] \\ & \text{d.h. } \exists x_1, \ldots, x_k \in A\backslash\{x\} \text{ und } a_1, \ldots, a_k \in \mathbb{K} \text{ mit } x = a_1x_1 + \ldots + a_kx_k \\ \Rightarrow\ & x - a_1x_1 - \ldots - a_kx_k = o \\ \Rightarrow\ & x, x_1, \ldots, x_k \text{ l.a.} \\ \Rightarrow\ & A \text{ l.a.} \end{aligned}$$

□

(vi) A l.u., $x \notin [A] \Rightarrow A \cup \{x\}$ l.u.

Beweis:
Aus $x \notin [A]$ folgt $x \neq o$. Angenommen $A \cup \{x\}$ l.a.
$\Rightarrow \exists x_1, \ldots, x_k \in A \cup \{x\}$ und $a_1, \ldots, a_k \in \mathbb{K}$ mit $(a_1, \ldots, a_k) \neq (0, \ldots, 0)$ und $a_1x_1 + \ldots + a_kx_k = o$
$\Rightarrow$ Ein $x_i = x$ (O.B.d.A. $x_k = x$) $\Rightarrow a_k \neq 0$.
$\Rightarrow x \in [x_1, \ldots, x_{k-1}] \subset [A]$ †. □

Beispiel:

- $V = \mathbb{K}^n$, $A = \{e_1, \ldots, e_n\}$, $e_i = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$, 1 an der i-ten Stelle.

$$\Rightarrow\ o = a_1e_1 + \ldots + a_ne_n = \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} \Rightarrow\ a_i = 0$$

$\Rightarrow$ A l.u.

- $V = \mathbb{K}^{\mathbb{N}}$, $A \subset \mathbb{K}[X]$ mit $A = \{p_1, p_2, \ldots\}$, $p_i = (0, \ldots, 0, 1, 0, \ldots)$, 1 an i-ter Stelle. ($\widehat{=}\ p_i = X^i$)
  $\Rightarrow$ A l.u., denn angenommen A l.a.
  $\Rightarrow$ $\exists p_{i_1}, \ldots, p_{i_k} \in A$ und $a_1, \ldots, a_k \in \mathbb{K}$, nicht alle 0, $\underbrace{a_1p_{i_1} + \ldots + a_kp_{i_k}}_{(0,\ldots,0,a_1,0,\ldots,0,a_k,0,\ldots)} = o = (0, \ldots)$
  $\Rightarrow$ $a_1 = a_2 = \ldots = a_k = 0$ †.

§3 Basis und Dimension

Definition 2.8. Sei V $\mathbb{K}$-Vektorraum

(i) Ein Erzeugendensystem A von V heißt *minimal*, wenn keine echte Teilmenge von A Erzeugendensystem ist.

(ii) Eine linear unabhängige Menge $A \subset V$ heißt *maximal*, wenn es keine echte Obermenge von A gibt, die linear unabhängig ist.

(iii) Ein linear unabhängiges Erzeugendensystem A heißt *Basis* von V.

Satz 2.6. Sei V $\mathbb{K}$-Vektorraum und $B \subset V$, $B \neq \emptyset$. Dann sind äquivalent:

(i) B ist Basis

(ii) B ist minmales Erzeugendensystem

(iii) B ist maximal linear unabhängige Menge

(iv) Jedes $x \in V$ besitzt eine Darstellung als Linearkombination von Vektoren aus B und diese Darstellung ist eindeutig. Das heißt aus

$$x = \sum_{i=1}^{k} a_ix_i = \sum_{i=1}^{k} b_ix_i \qquad x_i \in B,\ a_i, b_i \in \mathbb{K}$$

folgt

$$a_i = b_i \qquad i = 1, \ldots, k$$

Beweis: Ringschlussverfahren.

„(i) $\Rightarrow$ (ii)“:

Sei B Basis $\Rightarrow$ B Erzeugendensystem. Angenommen B nicht minimal

$\Rightarrow$ $\exists \hat{B} \subsetneq B$ mit $[\hat{B}] = V$ $\Rightarrow$ $\exists x \in B \backslash \hat{B}$ und $x \in [\hat{B}]$, d.h. $x = a_1x_1 + \ldots a_kx_k$, $B \neq \emptyset$ mit $a_i \in \mathbb{K}$ und $x_i \in \hat{B}$ paarweise verschieden.

$\Rightarrow$ $\underbrace{x, x_1, \ldots, x_k}_{\in B}$ l.a. $\Rightarrow$ B l.a. †.

„(ii) $\Rightarrow$ (iii)“:

Sei B minimales Erzeugendensystem. Angenommen B l.a.

$\Rightarrow$ $\exists x \in B$ mit $V = [B] = [B\backslash\{x\}]$ Widerspruch zur Minimalität.

$\Rightarrow$ B l.u.

Angenommen B nicht maximal $\Rightarrow$ $\exists \hat{B} \supsetneq B$, $\hat{B}$ l.u.

$\Rightarrow$ $\exists x \in \hat{B}, x \notin B$ und $x \notin [B]$ $\Rightarrow$ $[B] = V$ †.

„(iii) $\Rightarrow$ (iv)“:

B sei maximale l.u. Menge, $x \in V$.

$\Rightarrow$ $x \in [B]$, weil sonst $B \cup \{x\}$ l.u. wäre († zur Maximalität)

$\Rightarrow$ x hat Darstellung

$$\sum_{i=1}^{k} a_i x_i \qquad x_i \in B,\ a_i \in \mathbb{K}$$

Aus

$$\sum_{i=1}^{k} a_i x_i = \sum_{i=1}^{k} b_i x_i$$

folgt

$$\sum (a_i - b_i) x_i = o \overset{B \text{ l.u.}}{\Longrightarrow} a_i = b_i \qquad i = 1, \ldots, k$$

„(iv) $\Rightarrow$ (i)“:

Aus (iv) folgt $V = [B]$. Angenommen B l.a.

$\Rightarrow$ $\exists a_1 x_1 + \ldots + a_k x_k = o$ mit $x_i \in B$ paarweise verschieden und o.B.d.A. $a_1 \neq 0$.

$\Rightarrow$ $x_1 = -\frac{a_2}{a_1} x_2 - \ldots - \frac{a_k}{a_1} x_k$ $\Rightarrow$ $1 = 0$ †. □

Beispiel:

(i) $V = \{o\}$ $\Rightarrow$ $B = \emptyset$ ist Basis.

(ii) $V = \mathbb{K}^n$ $\Rightarrow$ $B = \{e_1, \ldots, e_n\}$ ist Basis.

(iii) $V = \mathbb{K}[X]$ $\Rightarrow$ $B = \{p_1, p_2, \ldots\}$, $p_i = X^i$ ist Basis.

(iv) $V = \mathbb{K}^{\mathbb{N}}$ $\Rightarrow$ B ist l.u., aber keine Basis.

(v) $V = \mathbb{R}^4$, $A = \left\{ \underbrace{\begin{pmatrix} 2 \\ -3 \\ 1 \\ 4 \end{pmatrix}}_{a_1}, \underbrace{\begin{pmatrix} 1 \\ 0 \\ 1 \\ 2 \end{pmatrix}}_{a_2}, \underbrace{\begin{pmatrix} -2 \\ 1 \\ -1 \\ 1 \end{pmatrix}}_{a_3} \right\}$ ist l.u.

A keine Basis, weil $e_4 = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} \notin [A]$

$\Rightarrow$ $\{a_1, a_2, a_3, e_4\}$ Basis.

Vorlesung: 2004-12-22

Satz 2.7. Sei V $\mathbb{K}$-Vektorraum und B, B' Basen von V. Dann gilt $|B| = |B'|$.

Beweis:

- 1. Fall
  $|B| = 0$ oder $|B'| = 0 \Leftrightarrow B = \emptyset$ oder $B' = \emptyset$
  $\Leftrightarrow V = \{o\} \Leftrightarrow B = B' = \emptyset \Leftrightarrow |B| = |B| = 0$
- 2. Fall
  $V \neq \{o\} \Leftrightarrow |B| \geq 1, |B'| \geq 1.$
  - Fall 2a
    $$|B| = |B'| = \infty \surd$$
  - Fall 2b
    $$|B| = k \in \mathbb{N} \overset{\text{Satz } 2.5}{\Rightarrow} |B'| \leq k \overset{\text{Satz } 2.5}{\Rightarrow} |B| \leq |B'| \leq k = |B| \Rightarrow |B| = |B'|$$
  - Fall 2c
    $$|B'| = m \in \mathbb{N} \overset{\text{analog}}{\Rightarrow} |B| = |B'|$$

□

Definition 2.9. Sei V $\mathbb{K}$-Vektorraum. Existiert in V ein endliches Erzeugendensystem A, so nennen wir V *endlich dimensional*. Schreibweise: $\dim V < \infty$.

Ist jedes Erzeugendensystem unendlich, so heißt V *unendlich dimensional*. Schreibweise $\dim V = \infty$.

Satz 2.8. Sei V $\mathbb{K}$-Vektorraum mit $\dim V < \infty$ und A Erzeugendensystem von V. Dann existiert eine Teilmenge $B \subset A$, die Basis ist.

Beweis:

Nach Definition existiert in V ein endliches Erzeugendensystem $A' \Rightarrow$ Jedes $x \in A'$ ist Linearkombination von Vektoren aus $A \Rightarrow \exists$ endliche Teilmenge $\widetilde{A} \subset A$, die alle Vektoren aus A' und damit auch V erzeugt.

Ist $\widetilde{A}$ minimal, so ist $\widetilde{A}$ Basis von V.

Ist $\widetilde{A}$ nicht minimal, so existiert Teilmenge $\overline{A} \subset \widetilde{A}$, die auch Erzeugendensystem ist. Nach endlich vielen Schritten endet man so bei einem Erzeugendensystem $B \subset A$, das minimal ist. Nach Satz 2.6 ist B Basis. □

Bemerkung und Definition: Sei V $\mathbb{K}$-Vektorraum mit $\dim V < \infty$. Nach Satz 2.8 existiert eine Basis B von V mit $|B| = n$, $n \in \mathbb{N}_0$. Nach Satz 2.7 enthält dann jede Basis von V n Elemente. V heißt dann n-*Dimensional*. Schreibweise: $\dim V = n$.

Korollar 2.9. Sei V $\mathbb{K}$-Vektorraum und B Basis mit $|B| = n \in \mathbb{N}_0$ (d.h. $\dim V = n$). Ist A Erzeugendensystem von V mit $|A| = n$, so ist A Basis.

Beweis:

Nach Satz 2.8 existiert Basis B' von V mit $B' \subset A$.

$\Rightarrow |B| \overset{\text{Satz } 2.7}{=} |B'| \leq |A| = n \Rightarrow |B'| = |A| \ (= n)$

$\Rightarrow B' = A \Rightarrow A$ Basis. □

Satz 2.10 (Basisergänzungssatz)**.** Sei V $\mathbb{K}$-Vektorraum mit $\dim V < \infty$ und sei $A \subset V$ linear unabhängig. Dann existiert eine Obermenge $B \supset A$, die Basis von V ist.

Beweis:

Sei $\dim V = n$, $n \in \mathbb{N}_0 \Rightarrow |A| \leq n$ (wegen Satz 2.6 und weil es in V eine Basis $\widetilde{B}$ mit $|\widetilde{B}| = n$ gibt)

Ist $[A] = V$, so ist A Basis. Andernfalls existiert $x \in V : x \notin [A] \Rightarrow \underbrace{A \cup \{x\}}_{=:A}$ linear unabhängig mit $|A'| = |A| + 1 \leq n$.

Nach endlich vielen Schritten landen wir so bei einer maximal linear unabhängigen Menge B, die $V = [B]$ erfüllt. B ist Basis. □

Korollar 2.11. Sei V $\mathbb{K}$-Vektorraum, $\dim V = n$, $n \in N_0$ und sei $A \subset V$ linear unabhängig mit $|A| = n$. Dann ist A Basis.

Beweis: Nach Satz 2.10 existiert Basis B mit $A \subset B$.

$\Rightarrow n = |A| \leq |B| = n$ (weil $\dim V = n$)

$\Rightarrow A = B$, d.h. A Basis. □

Satz 2.12. Sei V $\mathbb{K}$-Vektorraum mit $\dim V = n$ und $U \subset V$ Untervektorraum. Dann gilt:

(i) $\dim U \leq n$

(ii) $\dim U = n \Leftrightarrow U = V$

Beweis:

(i) Sei $A \subset U \subset V$ l.u. $\overset{\text{Satz 2.10}}{\Rightarrow}$ $\exists$ Basis B von V mit $A \subset B$.
$\Rightarrow |A| \leq |B| = n$
$\Rightarrow \exists$ maximale l.u. Menge $\widetilde{B}$ in U und $|\widetilde{B}| \leq n$
$\Rightarrow \widetilde{B}$ ist Basis von U, also ist $\dim U = |\widetilde{B}| \leq n$

(ii) „$\Leftarrow$“: trivial.
„$\Rightarrow$“: Aus Beweis von (i) folgt $|\widetilde{B}| = n \overset{\text{Korollar 2.11}}{\Rightarrow} \widetilde{B}$ Basis von V. $\Rightarrow U = [\widetilde{B}] = V \Rightarrow U = V$.

□

Bemerkung:

In unendlich dimensionalen Vektorräumen V gelten die Sätze 2.8 und 2.10 auch (entsprechend modifiziert). Beim Beweis wird Zorn'sches Lemma benutzt ($\Rightarrow$ nicht konstruktiv)

Damit hat jeder Vektorraum eine Basis.

Korollar 2.9 und 2.11 gelten nicht. Auch Satz 2.12 (b) gilt nicht.

Vorlesung: 2005-01-07

Beispiel:

$$\underbrace{\begin{pmatrix} 1 \\ 2 \\ -1 \\ -1 \\ -1 \end{pmatrix}}_{x_1}, \underbrace{\begin{pmatrix} 2 \\ -1 \\ 1 \\ 2 \\ -1 \end{pmatrix}}_{x_2}, \underbrace{\begin{pmatrix} 3 \\ -4 \\ 3 \\ 5 \\ -3 \end{pmatrix}}_{x_3}, \underbrace{\begin{pmatrix} -1 \\ 8 \\ -5 \\ -6 \\ 1 \end{pmatrix}}_{x_4}$$

$U := [x_1, x_2, x_3, x_4]$

Basis von U?

Allgemein: $x_1, \ldots, x_m \in \mathbb{K}^n$, $U := [x_1, \ldots, x_m]$, Basis von U?

1. Verfahren

$$A := \begin{pmatrix} x_1^\top \\ \vdots \\ x_m^\top \end{pmatrix} \in \mathbb{K}^{m\times n} \quad \overset{\text{Gauß}}{\rightsquigarrow} \quad \widetilde{A} = \begin{pmatrix} z_1^\top \\ \vdots \\ z_m^\top \end{pmatrix}$$

Satz 2.13. Seien $x_1, \ldots, x_m \in \mathbb{K}^n$, $U := [x_1, \ldots, x_m]$, $A := \begin{pmatrix} x_1^\top \\ \vdots \\ x_m^\top \end{pmatrix}$ und $\widetilde{A} = \begin{pmatrix} z_1^\top \\ \vdots \\ z_m^\top \end{pmatrix}$ die Gaußnormalform von A.

Dann bilden $z_1, \ldots z_k$ (k Anzahl der Treppenstufen) eine Basis von U. Speziell gilt $\dim U = k$.

Beweis: Es gilt offensichtlich $z_1, \ldots, z_m \in U = [x_1, \ldots, x_m]$. Umgekehrt folgt entsprechend $x_1, \ldots, x_m \in [z_1, \ldots, x_m]$.

$\Rightarrow [z_1, \ldots, x_m] = U$. Da $z_1, \ldots, z_k$ linear unabhängig $\Rightarrow$ Behauptung. □

zum Beispiel

$$\begin{pmatrix} 1 & 2 & -1 & -1 & -1 \\ 2 & -1 & 1 & 2 & -2 \\ 3 & -4 & 3 & 5 & -3 \\ -1 & 8 & -5 & -6 & 1 \end{pmatrix}$$

$$\rightsquigarrow \begin{pmatrix} 1 & 2 & -1 & -1 & -1 \\ 0 & 1 & -\frac{3}{5} & -\frac{4}{5} & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix} \quad \text{Treppennormalform}$$

$$\rightsquigarrow \begin{pmatrix} 1 & 0 & \frac{1}{5} & 0 & -1 \\ 0 & 1 & -\frac{3}{5} & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix} \quad \text{Gaußnormalform}$$

$$\Rightarrow \begin{pmatrix} 1 \\ 0 \\ \frac{1}{5} \\ 0 \\ -1 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ -\frac{3}{5} \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} \quad \text{Basis von } U$$

Alternatives Verfahren

$$\begin{pmatrix} 1 & 2 & 3 & -1 \\ 2 & -1 & -4 & 8 \\ -1 & 1 & 3 & 5 \\ -1 & 2 & 5 & -6 \\ -1 & -2 & -3 & 1 \end{pmatrix}$$

$$\rightsquigarrow \begin{pmatrix} 1 & 2 & 3 & -1 \\ 0 & 1 & 2 & -2 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$ Treppennormalform

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

2. Verfahren

$$A := \begin{pmatrix} x_1 & \cdots & x_m \end{pmatrix} \in \mathbb{K}^{n\times m} \quad \overset{\text{Gauß}}{\rightsquigarrow} \quad \widetilde{A} = \begin{pmatrix} v_1 & \cdots & v_m \end{pmatrix}$$

$U := [x_1, \ldots, x_m]$, $V = [v_1, \ldots, v_m]$

Zusammenhang U und V?

Satz 2.14. Seien $x_1, \ldots, x_m \in \mathbb{K}^n$, $U := [x_1, \ldots, x_m]$, $A := \begin{pmatrix} x_1 & \cdots & x_m \end{pmatrix}$, $\widetilde{A} = \begin{pmatrix} v_1 & \cdots & v_m \end{pmatrix}$ die Gaußnormalform von A, $V = [v_1, \ldots, v_m]$.

Dann gilt $\dim U = \dim V = k$ (k Anzahl der Treppenstufen). Seien $j_1, \ldots, j_k$ die Indizes der Treppenstufen, dann bilden $x_{j_1}, \ldots, x_{j_k}$ eine Basis von U.

Beweis:

Sei $t = (t_1, \ldots, t_m) \in \mathbb{K}^m$. Dann gilt

$$At = o \quad \Leftrightarrow \quad \widetilde{A}t = o \tag{6}$$

$$t_1x_1 + \ldots + t_mx_m = o \quad \Leftrightarrow \quad t_1v_1 + \ldots + t_mv_m = o \tag{7}$$

Hier gilt: Die Variablen t_j, $j \notin \{j_1, \ldots, j_k\}$ können frei gewählt werden. Z.B. $t_j = 1$, $t_i = 0\ \forall i \neq j$, $i \notin \{j_1, \ldots, j_k\}$.

$\Rightarrow\ v_j \in \{\underset{e_1}{v_{j_1}}, \ldots, \underset{e_k}{v_{j_k}}\}\ \Rightarrow\ V = [v_{j_1}, \ldots, v_{j_k}] = [e_1, \ldots, e_k]$

$\Rightarrow\ \dim V = k$

Wegen (6) folgt daraus, dass $x_j \in \{x_{j_1}, \ldots, x_{j_k}\}$, d.h. $U = [x_{j_1}, \ldots, x_{j_k}]$

Weiter sind $x_{j_1}, \ldots, x_{j_k}$ linear unabhängig weil $\underset{e_1}{v_{j_1}}, \ldots, \underset{e_k}{v_{j_k}}$ linear unabhängig sind.

$a_1x_{j_1} + \ldots + a_kx_{j_k} = o$

Setze $t = (0, \ldots, 0, a_1, 0, \ldots, 0, a_2, \ldots)$

$\Rightarrow\ At = o$

$\Leftrightarrow\ \widetilde{A}t = o$

$\Leftrightarrow\ a_1e_1 + \ldots + a_ke_k = o$

$\Leftrightarrow\ a_1 = \ldots = a_k = 0$

Also ist $x_{j_1}, \ldots, x_{j_k}$ Basis von U ($\Rightarrow \dim U = k$) □

Im Beispiel bilden damit x_1, x_2, x_4 eine Basis von U.

Bemerkung: Verfahren und Resultate gelten auch für die Treppennormalform (statt Gaußnormalform).

Vorlesung: 2005-01-12

Beispiel:

$$U := \left[\begin{pmatrix} 1 \\ -1 \\ -1 \\ -2 \end{pmatrix}, \begin{pmatrix} 0 \\ 3 \\ 3 \\ 3 \end{pmatrix}, \begin{pmatrix} 1 \\ -3 \\ 1 \\ -2 \end{pmatrix}, \begin{pmatrix} 1 \\ -2 \\ -6 \\ -5 \end{pmatrix} \right] \subset \mathbb{R}^4$$

Basis?

- 1. Verfahren

$$A = \begin{pmatrix} 1 & -1 & -1 & -2 \\ 0 & 3 & 3 & 3 \\ 1 & -3 & 1 & -2 \\ 1 & -2 & -6 & -5 \end{pmatrix} \overset{\text{Gauß}}{\rightsquigarrow} \begin{pmatrix} 1 & -1 & -1 & -2 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & \frac{1}{2} \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

$$\Rightarrow \text{ Basis } \begin{pmatrix} 1 \\ -1 \\ -1 \\ -2 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 1 \\ \frac{1}{2} \end{pmatrix}$$

- 2. Verfahren

$$A = \begin{pmatrix} 1 & 0 & 1 & 1 \\ -1 & 3 & -3 & -2 \\ -1 & 3 & 1 & -6 \\ -2 & 3 & -2 & -5 \end{pmatrix} \overset{\text{Gauß}}{\rightsquigarrow} \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & -\frac{2}{3} & -\frac{1}{3} \\ 0 & 0 & 1 & -1 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

$$\Rightarrow \text{ Basis } \begin{pmatrix} 1 \\ -1 \\ -1 \\ -2 \end{pmatrix}, \begin{pmatrix} 0 \\ 3 \\ 3 \\ 3 \end{pmatrix}, \begin{pmatrix} 1 \\ -3 \\ 1 \\ -2 \end{pmatrix}$$

Definition 2.10. Sei $A \in \mathbb{K}^{m \times n}$, $A = \begin{pmatrix} z_1^\top \\ \vdots \\ z_m^T \end{pmatrix} = \begin{pmatrix} s_1 & \cdots & s_n \end{pmatrix}$, $z_i \in \mathbb{K}^n$, $s_j \in \mathbb{K}^m$.

Wir nennen $\dim[z_1, \ldots, z_m]$ den *Zeilenrang* von A.
Wir nennen $\dim[s_1, \ldots, s_n]$ den *Spaltenrang* von A.

Satz 2.15. Für jede Matrix $A \in \mathbb{K}^{m \times n}$ gilt Zeilenrang = Spaltenrang = Anzahl k der Treppenstufen in der Treppennormalform von A.

Beweis: Folgt sofort aus Satz 2.13 und 2.14. □

Definition 2.11. Wir nennen k den *Rang* von A. Schreibweise: $\operatorname{Rang} A$, $\operatorname{Rg} A$.

Korollar 2.16.

(i) $\operatorname{Rang} A = \operatorname{Rang} A^\top$

(ii) $A \in \mathbb{K}^{n\times n}$ regulär $\Leftrightarrow$ $\operatorname{Rg} A = n$

(iii) $Ax = b$ lösbar $\Leftrightarrow$ $\operatorname{Rg} A = \operatorname{Rg}\left(\begin{array}{c|c} A & b \end{array}\right)$

Beweis: trivial. □

Korollar 2.17. Sei $A \in \mathbb{K}^{m\times n}$ und L der Lösungsraum des homogenen LGS $Ax = o$, $L \subset \mathbb{K}^n$.
Dann gilt $\dim L = n - \operatorname{Rg} A$.

Beweis:

$$Ax = o \quad \Leftrightarrow \quad \widetilde{A}x = o \qquad (\widetilde{A} \text{ GNF von } A)$$

Seien $i_1, \ldots, i_k$ die Indizes der Treppenstufen. Dann erhält man die allgemeine Lösung von $\widetilde{A}x = o$ wie folgt:
Jede Variable x_i, $i \notin \{i_1, \ldots, i_k\}$ kann frei gewählt werden. Die Werte von $x_{i_1}, \ldots, x_{i_k}$ ergeben sich dann aus $\widetilde{A}x = o$.
Für jedes $i \notin \{i_1, \ldots, i_k\}$ setzen wir $x_i = 1$, $x_j = 0$, $j \notin \{i_1, \ldots, i_k\}$, $i \neq j$.
$\Rightarrow$ $n - k$ Vektoren, die L aufspannen und linear unabhängig sind.
$\Rightarrow$ $\dim L = n - k$
Spezialfall: $i_1 = 1, \ldots, i_k = k$

$$\left(\begin{array}{cccc|ccc} 1 & & & & * & \cdots & * \\ & 1 & & & & & \\ & & 1 & & & & \\ 0 & & & & * & \cdots & * \end{array}\right)$$

$\Rightarrow$ Lösungen

$$\begin{array}{cccccccc} (* & \cdots & * & 1 & 0 & 0 & \ldots & 0) \\ (* & \cdots & * & 0 & 1 & 0 & \cdots & 0) \\ & & & \vdots & & & & \\ (* & \cdots & * & 0 & 0 & \cdots & 0 & 1) \end{array}$$

□

Bemerkung: Jeder Unterraum $U \subset \mathbb{K}^n$ ist Lösungsraum eines LGS $Bx = o$ mit $n - \dim U$ Gleichungen.

Beweis: Sei $U = [x_1, \ldots, x_m]$. Betrachte $A = \begin{pmatrix} x_1^\top \\ \vdots \\ x_n^\top \end{pmatrix}$ und das LGS $Ay = o$.

$\Rightarrow$ Lösungsraum ist $(n - \underbrace{\operatorname{Rg} A}_{=:r})$ dimensional, besitzt also Basis $y_1, \ldots, y_{n-r} \in \mathbb{K}^n$.

Sei $B = \begin{pmatrix} y_1^\top \\ \vdots \\ y_{n-r}^\top \end{pmatrix} \in \mathbb{K}^{n-r\times n}$.

U ist der Lösungsraum L von $Bx = o$, denn es gilt $\underbrace{AB^\top}_{=(Ay_1 \quad \cdots \quad Ay_{n-r})} = o \Rightarrow \underbrace{BA^\top}_{=(Bx_1 \quad \cdots \quad Bx_m)} = o$

$\Rightarrow$ x_i löst $Bx = o$

$\Rightarrow\ U \subset L$

Es gilt

$$\begin{aligned}\dim U &= r \\ &= n - \operatorname{Rg} B \\ &= n - (n-r) \\ &= r\end{aligned}$$

$\Rightarrow\ U = L$ □

Beispiel:

$$U = \left[\begin{pmatrix} 1 \\ -1 \\ -1 \\ -2 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 3 \\ 3 \\ 3 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ -3 \\ 1 \\ -2 \\ 4 \end{pmatrix} \right]$$

$$W = \left[\begin{pmatrix} -1 \\ 0 \\ -4 \\ -5 \\ 1 \end{pmatrix}, \begin{pmatrix} -5 \\ -1 \\ 2 \\ 2 \\ 6 \end{pmatrix}, \begin{pmatrix} 1 \\ 2 \\ -1 \\ 3 \\ 2 \end{pmatrix}, \begin{pmatrix} 3 \\ 1 \\ 0 \\ 3 \\ 3 \end{pmatrix} \right]$$

$U \cup W$?

$$\begin{pmatrix} 1 & -1 & -1 & -2 & 1 \\ 0 & 3 & 3 & 3 & 0 \\ 1 & -3 & 1 & -2 & 4 \end{pmatrix} \overset{\text{Gauß}}{\rightsquigarrow} \begin{pmatrix} 1 & 0 & 0 & -1 & 1 \\ 0 & 1 & 0 & \frac{1}{2} & -\frac{3}{4} \\ 0 & 0 & 1 & \frac{1}{2} & \frac{3}{4} \end{pmatrix}$$

$\Rightarrow$ Basis des Lösungsraums von $Ay = o$:

$$\begin{pmatrix} 2 \\ -1 \\ -1 \\ 2 \\ 0 \end{pmatrix}, \begin{pmatrix} -4 \\ 3 \\ -3 \\ 0 \\ 4 \end{pmatrix}$$

$\Rightarrow$ U Lösungsraum von

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

Analog folgt W Lösungsraum von

$$-12x_1 - 6x_2 + 5x_3 + x_4 + 13x_5 = 0$$

Basis dieses Lösungsraums ist

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

Basis von $U \cup W$.

Vorlesung: 2005-01-14

§4 Summen und Faktorräume

Definition 2.12. Seien $A_1, \ldots, A_n$ Teilmengen des $\mathbb{K}$-Vektorraums V.

Dann heißt

$$A_1 + \ldots + A_n := \{x_1 + \ldots + x_n \mid x_1 \in A_1, \ldots, x_n \in A_n\}$$

die *Summe* von $A_1, \ldots, A_n$. Kurzschreibweise: $\sum_{i=1}^{n} A_i$.

Definition 2.13. Seien $U_1, \ldots, U_n$ Untervektorräume von V und $U_1 + \ldots + U_k$ die Summe.

Die Summe heißt *direkt*, wenn gilt:

$$U_i \cap \sum_{\substack{j=1 \\ j \neq i}}^{k} U_j = \{o\} \quad \text{für } i = 1, \ldots, k$$

Schreibweise: $U_1 \oplus \ldots \oplus U_k$.

Bemerkung:

(i) Die Summe $U_1 + \ldots + U_k$ von Untervektorräumen ist wieder Untervektorraum.

(ii) Es gilt: $[A_1] + \ldots + [A_k] = [A_1 \cup \ldots \cup A_k]$

Beweis: $[A_1] + \ldots + [A_k] \subset [A_1 \cup \ldots \cup A_k]$ folgt aus Satz 2.4.

$A_1 \cup \ldots \cup A_k \subset [A_1] + \ldots + [A_k] \overset{\text{(i)}}{\Rightarrow} [A_1 \cup \ldots \cup A_k] \subset [A_1] + \ldots + [A_k]$ □

Satz 2.18. Seien $U_1, \ldots, U_k$ Untervektorräume des $\mathbb{K}$-Vektorraums V.

Dann gilt: Die Summe $U_1 + \ldots + U_k$ ist direkt $:\Leftrightarrow$ Jedes $x \in U_1 + \ldots + U_k$ hat eine eindeutige Darstellung $x = x_1 + \ldots + x_k$, $x_i \in U_i$

Beweis:

„$\Rightarrow$“:

Seien $x = x_1 + \ldots + x_k$, $x = x_1' + \ldots + x_k'$ zwei Darstellungen von x. $x_i, x_i' \in U_i$

$$\Rightarrow (x_1 - x_1') + \ldots + (x_k - x_k') = o$$

$$\Rightarrow x_1 - x_1' = \sum_{i=2}^{k} (x_i' - x_i)$$

$$\Rightarrow x_1 - x_1' \in U_1 \cap \sum_{i=2}^{k} U_i$$

$$\Rightarrow x_1 - x_1' = o \quad \text{weil Summe direkt}$$

$$\Rightarrow x_1 = x_1'$$

Analog folgt $x_2 = x_2', \ldots, x_k = x_k'$.

„$\Leftarrow$“:

Sei $x \in U_i \cap \sum_{\substack{j=1 \\ j \neq i}}^{k} x_j$, $x \neq o$

$$\Rightarrow \subset \in U_j x = \sum_{\substack{j=1 \\ j \neq i}}^{k} x_j \quad x_j \in U_j$$

$\Rightarrow$ Widerspruch, also $x = o$ $\Rightarrow$ Summe ist direkt. □

Satz 2.19 (Dimensionssatz für Unterräume)**.** Sei V $\mathbb{K}$-Vektorraum und $U, W \subset V$ Untervektorräume. Dann gilt

$$\dim(U+W) + dim(U \cap W) = \dim U + \dim W$$

Beweis:

Sei $\dim U = \infty$ oder $\dim W = \infty \Rightarrow \dim(U+W) = \infty$. $\Rightarrow$ Behauptung.

Sei jetzt $\dim U = m < \infty$, $\dim W = n < \infty$. $\Rightarrow \dim(U \cap W) < \infty$, etwa $\dim(U \cap W) = k$ $(k \leq m \wedge k \leq n)$

Sei $x_1, \ldots, x_k$ eine Basis von $U \cap W$. Wir ergänzen dies zu einer Basis von U und einer Basis von W:

$$x_1, \ldots, x_k, x_{k+1}, \ldots, x_m \quad x_1, \ldots, x_k, x'_{k+1}, \ldots, x'_n$$

Im Fall $U \cap W = \{o\}$ ist die Basis von $U \cap W$ leer. Dies ist mit $k = 0$ in der obigen Überlegung enthalten.

Behauptung: $x_1, \ldots, x_k, x_{k+1}, \ldots, x_m, x'_{k+1}, \ldots, x'_n$ Basis von $U + W$.

Beweis der Behauptung:

$$[x_1, \ldots, x_k, x_{k+1}, \ldots, x_m, x'_{k+1}, \ldots, x'_n] = U + W$$

Lineare Unabhängigkeit:

$$\begin{aligned} & a_1x_1 + \ldots + a_mx_m + a'_{k+1}x'_{k+1} + \ldots + a'_nx'_n = o \\ \Rightarrow\ & a'_{k+1}x'_{k+1} + \ldots + a'_nx'_n \in U \cap W \\ \Rightarrow\ & a'_{k+1} = \ldots = a'_n = 0 \\ \Rightarrow\ & a_1x_1 + \ldots + a_mx_m = o \\ \Rightarrow\ & a_1 = \ldots = a_m = 0 \end{aligned}$$

Also folgt $\dim(U+W) = m + (n-k) = \dim U + \dim W - \dim(U \cap W)$. □

Korollar 2.20. Für direkte Summen gilt $\dim(U+W) = \dim U + \dim W$.

Bemerkung:

(i) Im Fall $\dim V < \infty$ folgt aus $\dim(U+W) = \dim U + \dim W$, dass die Summe direkt ist.

(ii) U, W, Z seien Untervektorräume von V. Dann können die Summen $U \oplus W$, $U \oplus Z$, $W \oplus Z$ alle direkt sein, ohne dass die Summe $U + W + Z$ direkt ist.

Definition 2.14. Sei V $\mathbb{K}$-Vektorraum und U, W Untervektorräume mit $V = U \oplus W$.

Dann heißt W *Komplementärraum* zu U, und U Komplementärraum zu W.

Satz 2.21. Sei V $\mathbb{K}$-Vektorraum mit $\dim V = n < \infty$, und sei $U \subset V$ Untervektorraum. Dann existiert ein Komplementärraum W von U, d.h. ein Untervektorraum W mit $V = U \oplus W$.

Beweis: Betrachte Basis $x_1, \ldots, x_k$ von U und ergänze diese zu Basis $x_1, \ldots, x_k, x_{k+1}, \ldots, x_n$ von V. Dann setze $W = [x_{k+1}, \ldots, x_n]$. □

Beispiel:

$$U = \left[\begin{pmatrix} 1 \\ 2 \\ -1 \\ 1 \\ -1 \end{pmatrix}, \begin{pmatrix} 2 \\ -2 \\ 1 \\ -2 \\ -1 \end{pmatrix}, \begin{pmatrix} 1 \\ 2 \\ -1 \\ -1 \\ -2 \end{pmatrix} \right]$$

$$\begin{pmatrix} 1 & 2 & -1 & 1 & -1 \\ 2 & -2 & 1 & -2 & -1 \\ 1 & 2 & -1 & -1 & -2 \end{pmatrix} \overset{\text{Gauß}}{\rightsquigarrow} \begin{pmatrix} 1 & 2 & -1 & 1 & -1 \\ 0 & -6 & 3 & -4 & 1 \\ 0 & 0 & 0 & -2 & -1 \end{pmatrix}$$

$$\Rightarrow \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} \text{ Basis eines Komplementärraums } W \text{ von } U$$

Andere Möglichkeit

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

Vorlesung: 2005-01-19

Faktorraum

$$\left.\begin{array}{rcl} V\ \mathbb{K}\text{-VR} & \rightarrow & (V,+) \text{ ablesche Gruppe} \\ U \subset V \text{ UVR} & \rightarrow & U \text{ Untergruppe} \end{array}\right\} \Rightarrow V/_U \text{ Faktorgruppe ex.}$$

$x \sim y \Leftrightarrow x - y \in U$
$x \sim y,\ x' \sim y' \Rightarrow x + x' \sim y + y'$
Daher $[x]_\sim + [y]_\sim = [x+y]_\sim$

Skalarmultiplikation auf $V/_U$

$$a \cdot [x]_\sim = [a \cdot x]_\sim$$

Sinnvoll, weil nicht von der Wahl des Repräsentanten abhängig. $x \sim y$, $a \in \mathbb{K} \Rightarrow ax \sim ay$

Satz 2.22. Sei V $\mathbb{K}$-Vektorraum und $U \subset V$ Untervektorraum.

Dann ist $V/_U$ mit

$$[x]_\sim + [y]_\sim = [x+y]_\sim$$
$$a[x]_\sim = [ax]_\sim$$

ein $\mathbb{K}$-Vektorraum. Er heißt *Faktorraum* (oder *Quotientenraum*).

Beweis: selbst. □

Bemerkung:

- $U = \{o\} \Rightarrow V/_U = \{\{x\} \mid x \in V\}$ isomorph zu V
- $U = V \Rightarrow V/_U = \{V\} = \{[o]_\sim\}$ isomorph zu $\{o\}$

Satz 2.23. Sei V $\mathbb{K}$-Vektorraum und $U \subset V$ Untervektorraum.

Dann gilt

$$\dim V = \dim U + \dim V/_U$$

Beweis: Nur für $\dim V < \infty$.

Sei $B := \{x_1, \ldots, x_k\}$ Basis von U ($\dim U = k$). Wir ergänzen B zu einer Basis von V.

$$x_1, \ldots, x_k, \underbrace{y_1, \ldots, y_m}_{B'} \quad (\dim V = k + m)$$

$\Rightarrow\ V = U \oplus [B']$

Betrachte $V/_U$

Behauptung: $[y_1]_\sim, \ldots, [y_m]_\sim$ bilden Basis von $V/_U$.

- Erzeugendensystem:

$$\begin{aligned} &\text{Sei } [x]_\sim \in V/_U \quad x \in V \\ &\Rightarrow x = a_1x_1 + \ldots + a_kx_k + b_1y_1 + \ldots + b_my_m \quad a_i, b_i \in \mathbb{K} \\ &\Rightarrow [x]_\sim = \underbrace{[a_1x_1 + \ldots + a_kx_k]_\sim}_{=[o]_\sim} + b_1[y_1]_\sim + \ldots + b_m[y_m]_\sim \end{aligned}$$

- Lineare Unabhängigkeit:

$$\begin{aligned} &\text{Seien } b_1, \ldots, b_m \in \mathbb{K} \text{ mit } b_1[y_1]_\sim + \ldots + b_m[y_m]_\sim = [o]_\sim \\ &\Rightarrow \underbrace{b_1y_1 + \ldots + b_my_m}_{[B']} \in U \\ &\Rightarrow b_1y_1 + \ldots + b_my_m = o \\ &\Rightarrow b_1 = \ldots = b_m = 0 \end{aligned}$$

□

Korollar 2.24. Sei V $\mathbb{K}$-Vektorraum und $U \subset V$ Untervektorraum.

(i) Ist B Basis von U und $B \cup B'$ Basis von V mit $B \cap B' = \emptyset$, dann ist $\{[y]_\sim \mid y \in B'\}$ Basis von $V/_U$.

(ii) Ist W Komplementärraum von U (in V), so sind W und $V/_U$ isomorph.

Beweis:

(i) Siehe Beweis von Satz 2.23

(ii) Es gilt: $V = U \oplus W$.

Setze

$$f : W \underset{x \mapsto [x]_\sim}{\to} V/_U$$

Dann ist

- f injektiv: $f(x) = [o]_\sim \ \Rightarrow\ x \in U$ (und $x \in W$) $\Rightarrow\ x \in U \cup W \ \Rightarrow\ x = o$

- f surjektiv: Sei $[x]_\sim \in V/_U, x \in V$

$$\Rightarrow\ x = u + w \qquad u \in U,\ w\ in W$$
$$\Rightarrow\ [x]_\sim = [w]_\sim\ \Rightarrow\ f(w) = [x]_\sim$$

□

Beispiel:

$$\mathbb{R}^5 \supset U = \left[\begin{pmatrix} 1 \\ 2 \\ -1 \\ 1 \\ -1 \end{pmatrix}, \begin{pmatrix} 2 \\ -2 \\ 1 \\ -2 \\ -1 \end{pmatrix}, \begin{pmatrix} 1 \\ 2 \\ -1 \\ -1 \\ -2 \end{pmatrix} \right]$$

Gesucht: Basis von $V/_U$?

Basis von U

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

Basisergänzung:

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

$\Rightarrow$ Basis von $V/_U$.

Elemente von $V/_U$: $[x]_\sim = x + U$, also

$$\begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} + U, \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} + U$$

§5 Affine Unterräume eines Vektorraums

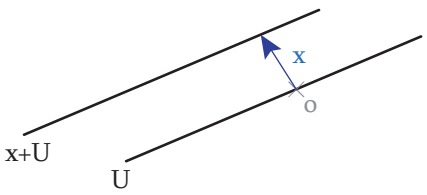

Abbildung 11: Um x verschobener Untervektorraum $U \subset \mathbb{R}^2$

Definition 2.15. Sei V $\mathbb{K}$-Vektorraum und $U \subset V$ Untervektorraum, $x \in V$.

Dann heißt $L := x + U$ *affiner Unterraum* von V. U heißt *Richtungsraum* von L.

Bemerkung: Sind $L = x + U$, $\widetilde{L} = \widetilde{x} + \widetilde{U}$ affine Unterräume. Dann gilt:

$$L \subset \widetilde{L} \quad \Leftrightarrow \quad U \subset \widetilde{U} \text{ und } x - \widetilde{x} \in \widetilde{U}$$

Speziell gilt $L = \widetilde{L} \Leftrightarrow U = \widetilde{U}$ und $x - \widetilde{x} \in U$)

Beweis:

„$\Rightarrow$“: Sei $x + U \subset \widetilde{x} + \widetilde{U}$

$\Rightarrow$ $x \in \widetilde{x} + \widetilde{U}$, also $x - \widetilde{x} \in U$

Sei $y \in U$ $\Rightarrow$ $x + y \in \widetilde{x} + \widetilde{U}$, d.h. $x + y = \widetilde{x} + \widetilde{y}$, $\widetilde{y} \in \widetilde{U}$

$\Rightarrow$ $y = (\widetilde{x} - x) + \widetilde{y} \in \widetilde{U}$

„$\Leftarrow$“: Sei $U \subset \widetilde{U}$, $x - \widetilde{x} \in \widetilde{U}$

Sei $x + y \in L$, $y \in U \subset \widetilde{U}$

$\Rightarrow$ $x + y = \widetilde{x} + (x - \widetilde{x}) + y \in \widetilde{x} + \widetilde{U} = \widetilde{L}$

□

Bemerkung und Bezeichnung: Ist $L = x + U$, so setzen wir $\dim L := \dim U$. Weiter heißt $\dim V/_U$ die *Kodimension* von L.

- $\dim L = 0$, $L = x + \{o\} = \{x\} \leftrightarrow x$

  Punkte (Vektoren $\leftrightarrow$ Punkte)

- $\dim L = 1$, $L = x + [y]$, $y \neq o$

  Gerade mit Aufpunkt x und Richtung y

- $\dim L = 2$, $L = x + [u, v]$, u, v linear unabhängig

  Ebene

- Kodimension $L = 1$: *Hyperebene*

Vorlesung: 2005-01-21

Bemerkung:

(i) Die Lösungsmenge eines lösbaren (inhomogenen) LGS $Ax = b$ ist ein affiner Unterraum der Dimension $n - \operatorname{Rg} A$ in $\mathbb{K}^n$ (falls $A \in \mathbb{K}^n$).

(ii) Jeder affine Unterraum $L \subset \mathbb{K}^n$ lässt sich als Lösungsmenge eines LGS $Ax = b$ schreiben, wobei $A \in \mathbb{K}^{k \times n}$, $b \in \mathbb{K}^k$, $k = n - \dim L$, $\operatorname{Rg} A = k$.

Insbesondere lässt sich eine Hyperebene durch eine lineare Gleichung

$$a_1 x_1 + \ldots + a_n x_n = b$$

beschreiben, weobei $(a_1, \ldots, a_n) \neq (0, \ldots, 0)$

Denn $L = x + U$, $U =$ Lösungsraum eines LGS $Ax = o$, $A \in \mathbb{K}^{n \times m}$, $m = n - \dim U$, $\operatorname{Rg} A = m$.

Sei $y \in L \Leftrightarrow y = x + u \Leftrightarrow y - x \in U \Leftrightarrow Ay = Ax =: b$.

Geometrische Interpretation:

Jeder affine Unterraum $L \subset \mathbb{K}^n$ ist Durchschnitt von m Hyperebenen, $m = n - \dim L$.

(iii) $L = x + U$, $U = [x_1, \ldots, x_4]$, $x_1, \ldots, x_4$ Basis von U

$\Rightarrow$ Jedes $y \in L$ hat Darstellung

$$y = x + a_1 x_1 + \ldots + a_k x_k \quad a_i \in \mathbb{K}$$

(*Parameter-Darstellung* von L)

Beispiel:

- Gerade: $L = \{x + a_1 x_1 \mid a_1 \in \mathbb{K}\}$, $x \neq o$
- Ebene: $L = \{x + a_1 x_1 + a_2 x_2 \mid a_1, a_2 \in \mathbb{K}\}$, x_1, x_2 linear unabhängig

Beispiel:

$$L = \begin{pmatrix}2\\0\\0\\1\end{pmatrix} + \left[\begin{pmatrix}1\\1\\0\\0\end{pmatrix}, \begin{pmatrix}0\\1\\1\\0\end{pmatrix}, \begin{pmatrix}0\\0\\1\\1\end{pmatrix}\right] \quad L' = \begin{pmatrix}3\\1\\0\\0\end{pmatrix} + \left[\begin{pmatrix}1\\1\\2\\0\end{pmatrix}, \begin{pmatrix}0\\1\\0\\0\end{pmatrix}\right] \subset \mathbb{R}^4$$

$L \cap L'$? Jedes $x \in L \cap L'$ erfüllt

$$x = \begin{pmatrix}2\\0\\0\\1\end{pmatrix} + a_1 \begin{pmatrix}1\\1\\0\\0\end{pmatrix} + a_2 \begin{pmatrix}0\\1\\1\\0\end{pmatrix} + a_3 \begin{pmatrix}0\\0\\1\\1\end{pmatrix} = \begin{pmatrix}3\\1\\0\\0\end{pmatrix} + b_1 \begin{pmatrix}1\\1\\2\\0\end{pmatrix} + b_2 \begin{pmatrix}0\\1\\0\\0\end{pmatrix}$$

$$\Leftrightarrow \begin{pmatrix}1&0&0&1&0\\1&1&0&-1&-1\\0&1&1&-2&0\\0&0&1&0&0\end{pmatrix} \begin{pmatrix}a_1\\a_2\\a_3\\b_1\\b_2\end{pmatrix} = \begin{pmatrix}1\\1\\0\\-1\end{pmatrix}$$

$$\overset{\text{Gauß}}{\rightsquigarrow} \left(\begin{array}{ccccc|c}1&0&0&1&0&1\\0&1&0&-2&-1&0\\0&0&1&0&1&0\\0&0&0&0&1&1\end{array}\right)$$

$\Rightarrow$ $b_2 = 1$, $b_1 = a \in \mathbb{K}$ beliebig.

$$L \cap L' = \{x = \begin{pmatrix}3\\1\\0\\0\end{pmatrix} + a \begin{pmatrix}-1\\1\\0\\0\end{pmatrix} + \begin{pmatrix}0\\1\\0\\0\end{pmatrix} \mid a \in \mathbb{R}\}$$

$$= \{x = \begin{pmatrix}3\\2\\0\\0\end{pmatrix} + a \begin{pmatrix}-1\\1\\0\\0\end{pmatrix} \mid a \in \mathbb{R}\}$$

$\Rightarrow$ $L \cap L'$ Gerade.

Satz 2.25. Sei $\mathcal{M}$ ein System von affinen Unterräumen. $L = x_L + U_L$ (U_L Richtungsraum von L) in einem $\mathbb{K}$-Vektorraum V. Dann ist

$$\bigcap_{L \in \mathcal{M}} L$$

entweder $\emptyset$ oder acuh ein affiner Unterraum M mit Richtungsraum

$$U_M = \bigcap_{L \in \mathcal{M}} U_L$$

Beweis: Sei $\bigcap_{L\in\mathcal{M}} L \neq \emptyset$, d.h. $x_0 \in \bigcap_{L\in\mathcal{M}} L$.

$$\Rightarrow\ L = x_0 + U_L \quad L \in \mathcal{M}$$

$$\Rightarrow \bigcup_{L\in\mathcal{M}} L = \bigcup_{L\in\mathcal{M}} (x_0 + U_L) = x_0 + \underbrace{\bigcup_{L\in\mathcal{M}} U_L}_{U_M}$$

□

Bemerkung:

(i) Zwei affine Unterräume $L := x + U$, $L' := x' + U'$ heißen *parallel*, wenn $U \subset U'$ oder $U' \subset U$. Schreibweise $L \parallel L'$.

(ii) Zwei Geraden in V, die disjunkt, aber nicht parallel sind, heißen *windschief*.

3 Lineare Abbildungen

§1 Definition und Eigenschaften linearer Abbildungen

Definition 3.1. Seien V, W $\mathbb{K}$-Vektorräume. Eine Abbildung $\Phi : V \to W$ heißt *linear* (oder Vektorraum-*Homomorphismus*), wenn

$$\Phi(ax + by) = a\Phi(x) + b\Phi(y) \qquad \forall x, y \in V,\ a, b \in \mathbb{K}$$

Ist Φ bijektiv, so heißt Φ *Isomorphismus* (und U, W dann *isomorph*, $V \cong W$)

Ist $W = V$, d.h. $\Phi : V \to V$, so heißt Φ *Endomorphismus*.

Ein Isomorphismus $\Phi : V \to V$ heißt *Automorphismus*.

Ist $\Phi : V \to W$ linear, so ist $\operatorname{Bild}\Phi := \Phi(V)$ Untervektorraum von W und $\operatorname{Kern}\Phi := \{x \in V \mid \Phi(x) = o\}$ Untervektorraum von V.

Beispiel:

(i) $\Phi : V \underset{x \mapsto w_0}{\to} W$ mit w_0 fest linear $\Leftrightarrow\ w_0 = o$
$\Phi = o$ Nullabbildung.

(ii) $A \in \mathbb{K}^{m \times n}$, $A = \begin{pmatrix} a_1 & \vdots & a_n \end{pmatrix}$, $\Phi :\subset x \mapsto Ax\mathbb{K}^n \to \mathbb{K}^m$ linear

$$\begin{aligned} \operatorname{Bild}\Phi &= \{Ax \mid x \in \mathbb{K}^n\} \\ &= \{x_1a_1 + \ldots + x_na_n \mid x_1 \ldots, x_n \in \mathbb{K}\} \\ &= [a_1, \ldots, a_n] \end{aligned}$$

$\Rightarrow \dim \operatorname{Bild}\Phi = \operatorname{Rg} A$
$\operatorname{Kern}\Phi =$ Lösungsraum von $Ax = o \Rightarrow \dim \operatorname{Kern} = n - \operatorname{Rg} A$.

(iii) $D : \underset{\sum_{i=0}^n a_i X^i \mapsto \sum_{i=1}^n a_i i X^{i-1}}{\mathbb{R}[X] \to \mathbb{R}[X]}$ linear.

Vorlesung: 2005-01-26

$U := [X, X^2, X^3, \ldots] \subsetneq \mathbb{R}[X]$.
$D : U \to \mathbb{R}[X]$ bijektiv, also sind U und $\mathbb{R}[X]$ isomorph.

(iv) $V = C[0,1]$ Vektorraum der stetigen Funktionen auf $[0,1]$
$I : C[0,1] \to \mathbb{R}$, $f \mapsto \int_0^1 f(x)\,dx$

(v) $V \subset \mathbb{R}^{\mathbb{N}}$ Unterraum der konvergenten Folgen.

$$\Phi : (a_i)_{i \in \mathbb{N}} \mapsto \lim_{i \to \infty} a_i$$

ist linear.

Satz 3.1 (Homomorphiesatz für Vektorräume)**.** Sei $\Phi : V \to W$ linear, V, W $\mathbb{K}$-Vektorräume. Dann gilt

(i) Die kanonische Abbildung $k : V \to V/_{\operatorname{Kern}\Phi}$ ist linear

(ii) Es existiert eine injektive lineare Abbildung $\overline{\Phi} : V/_{\operatorname{Kern}\Phi} \to W$ mit $\Phi = \overline{\Phi} \circ k$

(iii) Ist Φ surjektiv, so ist $\overline{\Phi}$ bijektiv

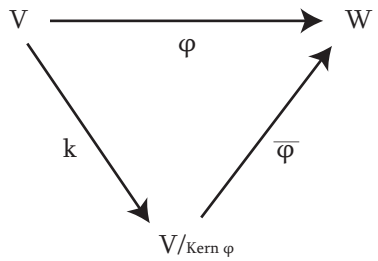

Abbildung 12: Homomorphiesatz für Vektorräume

Beweis: Der Großteil wurde schon beim Homomorphiesatz für Gruppen bewiesen. Rest:

(i) $k(a \cdot x) = [a \cdot x]_\sim = a \cdot [x]_\sim = a \cdot k(x)$

(ii) $\overline{\Phi}(a \cdot [x]_\sim) = \overline{\Phi}([ax]_\sim) = \Phi(ax) = a \cdot \Phi(x) = a \cdot \overline{\Phi}(x)$

□

Korollar 3.2. $V/_{\text{Kern}\,\Phi} \cong \text{Bild}\,\Phi$

Korollar 3.3. Ist $V = U \oplus W$, so ist $V/_U \cong W$, $V/_W \cong U$.

Beweis: Sei $\Phi : V \underset{x \mapsto u}{\to} W$. Jedes $x \in V$ hat eine eundeutige Zerlegung $x = u + w$, $u \in U$, $w \in W$.

$\Rightarrow$ Φ linear. $\text{Kern}\,\Phi = W$, $\text{Bild}\,\Phi = U$.

$\Rightarrow$ $V/_W \cong U$. Analog folgt $V/_U \cong W$. □

Bemerkung:

(i) Die Abbildung Φ aus dem Beweis heißt *Projektion* (auf den Unterraum U). Φ erfüllt $\underbrace{\Phi^2}_{\Phi \circ \Phi} = \Phi$.

(ii) Allgemein heißt eine Abbildung $\Phi : V \to V$ *Projektion*, wenn $\Phi^2 = \Phi$ gilt. Es gilt dann $V = \text{Kern}\,\Phi \oplus \text{Bild}\,\Phi$. Die Umkehrung ist im Allgemeinen falsch.

Beweis: Sei $x \in V$, $w := \underset{\in \text{Bild}\,\Phi}{\Phi(x)}$, $v := x - \Phi(x) \in \text{Kern}\,\Phi$, da

$$\Phi(v) = \Phi(x) - \Phi^(x) = \Phi(x) - \Phi(x) = o$$

Die Summe ist direkt.

$x \in (\text{Kern}\,\Phi \cap \text{Bild}\,\Phi) \Rightarrow \Phi(x) = o,\ x = \Phi(x) \qquad y \in V$ geeignet

$o = \Phi(x) = \Phi(\Phi(x) = \Phi(x) = x \Rightarrow x = o$

□

Satz 3.4. Seien V, W $\mathbb{K}$-Vektorräume und B eine Basis von V.

Zu jeder Abbildung $\Phi' : B \to W$ existiert genau eine lineare Abbildung $\Phi : V\ raW$ mit $\Phi|_B = \Phi'$, also $\Phi(x) = \Phi'(x)\ \forall x \in B$.

Insbesondere ist eine lineare Abbildung $\Phi : V \to W$ durch ihre Werte auf B eindeutig festgelegt.

Beweis: Wir betrachten nur $\dim V = n < \infty$.

Also $B = \{x_1, \ldots, x_n\}$

Jedes $x \in V$ hat (eindeutige) Darstellung

$$x = a_1 x_1, \ldots, a_n x_n \quad a_1, \ldots, a_n \in \mathbb{K}$$

Setze $\Phi(x) := a_1\Phi(x_1) + \ldots + a_n\Phi(x_n) \Rightarrow \Phi : V \to W$ linear und $\Phi|_B = \Phi'$. □

Satz 3.5. Seien V, W $\mathbb{K}$-Vektorräume, $\dim V = n$, $B = \{x_1, \ldots, x_n\}$ Basis von V. Sei $\Phi : V \to W$ linear. Dann gilt

(i) Φ injektiv $\Leftrightarrow$ $\Phi(x_1), \ldots, \Phi(x_n)$ linear unabhängig

(ii) Φ surjektiv $\Leftrightarrow$ $[\Phi(x_1), \ldots, \Phi(x_n)] = W$

(iii) Φ bijektiv $\Leftrightarrow$ $\Phi(x_1), \ldots, \Phi(x_n)$ Basis von W

Beweis:

(i) „$\Rightarrow$“: Sei $a_1\Phi(x_1) + \ldots + a_n\Phi(x_n) = o$

$$\begin{aligned} &\Rightarrow \Phi(a_1x_1 + \ldots + a_nx_n) = o \\ &\Rightarrow a_1x_1 + \ldots + a_nx_n = o \\ &\overset{B \text{ Basis}}{\Rightarrow} a_1 = \ldots = a_n = o \end{aligned}$$

„$\Leftarrow$“: Sei $\Phi(x) = o \Rightarrow x$ hat Darstellung

$$\begin{aligned} & x = a_1x_1 + \ldots + a_nx_n \\ &\Rightarrow \Phi(a_1x_1 + \ldots + a_nx_n) = o \\ &\Rightarrow a_1\Phi(x_1) + \ldots + a_n\Phi(x_n) = o \\ &\Rightarrow a_1 = \ldots = a_n = o \\ \Rightarrow\ & x = o \end{aligned}$$

(ii) „$\Rightarrow$“: Zu jedem $y \in W$ existiert $x \in V$ mit $y = \Phi(x)$

$$\begin{aligned} x &= a_1x_1 + \ldots + a_nx_n \\ &= \Phi(a_1x_1 + \ldots + a_nx_n) \\ &= a_1\Phi(x_1) + \ldots + a_n\Phi(x_n) \end{aligned}$$

„$\Leftarrow$“: Sei $y \in W$

$$\begin{aligned} y &= a_1\Phi(x_1) + \ldots + a_n\Phi(x_n) \\ &= \Phi(\underbrace{a_1x_1 + \ldots + a_nx_n}_{=:x}) \end{aligned}$$

(iii) Folgt aus (i) und (ii).

□

Korollar 3.6. Sei $\dim V = \dim W = n < \infty$ und $\Phi : V \to W$ linear. Dann gilt

Φ injektiv $\Leftrightarrow$ Φ surjektiv $\Leftrightarrow$ Φ bijektiv

Vorlesung: 2005-01-28

Satz 3.7. Seien V, W $\mathbb{K}$-Vektorräume mit $\dim V < \infty$. Dann gilt

$$V \cong W \quad \Leftrightarrow \quad \dim V = \dim W$$

Beweis:

„$\Rightarrow$“: $V \cong W$, d.h. es existiert ein Isomorphismus $\Phi : V \to W$.
Seien $x_1, \ldots, x_n$ eine Basis von V, d.h. $\dim V = n$.
$\Rightarrow$ $\Phi(x_1), \ldots, \Phi(x_n)$ Basis von W $\Rightarrow$ $\dim W = n = \dim V$

„$\Leftarrow$“: Sei $\dim V = \dim W = n$ und seien $x_1, \ldots, x_n$ Basis von V und $y_1, \ldots, y_n$ Basis von W.
Setze $\Phi(x_i) = y_i$, $i = 1, \ldots, n$
$\overset{\text{Satz 3.4}}{\Rightarrow}$ Φ lässt sich zu einer linearen Abbildung von V nach W fortsetzen.
$\overset{\text{Satz 3.5}}{\Rightarrow}$ Φ Isomorphismus.

□

Bemerkung:

(i) Jeder n-dimensionale $\mathbb{K}$ Vektorraum ist isomorph zu $\mathbb{K}^n$

(ii) Satz 3.7 gilt nicht für Vektorräume V, W mit $\dim V = \dim W = \infty$.

Satz 3.8 (Dimensionssatz für lineare Abbildungen)**.** Seien V, W $\mathbb{K}$-Vektorräume und $\Phi : V \to W$ linear. Dann gilt

$$\dim \operatorname{Kern} \Phi + \dim \operatorname{Bild} \Phi = \dim V$$

Beweis: Es gilt $\operatorname{Bild} \Phi \cong V/_{\operatorname{Kern} \Phi}$ $\Rightarrow$ $\dim \operatorname{Bild} \Phi = \dim V/_{\operatorname{Kern} \Phi}$ und $\dim V/_{\operatorname{Kern} \Phi} = \dim V - \dim \operatorname{Kern} \Phi$.
□

§2 Vektorräume linearer Abbildungen

Satz 3.9. Seien V, W, X $\mathbb{K}$-Vektorräume

(i) Sind $\Phi : V \to W$, $\Psi : W \to X$ linear, so auch $\Psi \circ \Phi : V \to X$

(ii) Ist $\Phi : V \to W$ Isomorphismus, so auch $\Phi^{-1} : W \to V$

(iii) Sind $\Phi, \Psi : V \to W$ linear, und $a \in \mathbb{K}$, so sind auch $\Phi + \Psi$ und $a\Phi$ linear.

Beweis:

(i) trivial.

(ii) Linearität von Φ^{-1}

$$\begin{aligned} \Phi(\Phi^{-1}(ax + by)) &= ax + by \qquad x, y \in W;\ a, b \in \mathbb{K} \\ &= a\Phi(\Phi^{-1}(x)) + b\Phi(\Phi^{-1}(y)) \\ &= \Phi(a\Phi^{-1}(x) + b\Phi^{-1}(y)) \end{aligned}$$

$\Rightarrow$ $\Phi^{-1}(ax + by) = a\Phi^{-1}(x) + b\Phi^{-1}(y)$

(iii) trivial.

□

Bemerkung und Definition:

(i) Die Menge $\mathrm{Hom}(V,W)$ aller linearen Abbildungen $\Phi : V \to W$ ist ein $\mathbb{K}$-Vektorraum.

(ii) Für $\mathrm{Hom}(V,V)$ schreibt man auch $\mathrm{End}(V)$.
$\mathrm{End}(V)$ ist $\mathbb{K}$-Vektorraum und Ring mit Eins (bzgl. $+, \circ$). Eine solche Struktur heißt *Algebra*, weil noch

$$a \cdot (\Phi \circ \Psi) = (a \cdot \Phi) \circ \Psi = \Phi \circ (a \cdot \Psi)$$

für alle $a \in \mathbb{K}$, $\Phi, \Psi \in \mathrm{End}(V)$ gilt.

(iii) Die Menge $\mathrm{Aut}(V)$ der Automorphismen $\Phi : V \to V$ bildet bzgl. $\circ$ eine Gruppe.

Satz 3.10. Seien V, W $\mathbb{K}$-Vektorräume, $\dim V < \infty$, $\dim W < \infty$. Dann gilt

$$\dim Hom(V,W) = \dim V \cdot \dim W$$

Beweis: Seien $v_1, \ldots, v_n$ Basis von V und $w_1, \ldots, w_m$ Basis von W.

$$\Phi_{ij} : V \underset{\substack{v_j \mapsto i \\ v_k \mapsto o;\ k \neq i}}{\to} W \qquad i \in \{1, \ldots, m\},\ j \in \{1, \ldots, n\}$$

$$\Rightarrow \boxed{\Phi_{ij}(v_k) = \delta_{kj} w_i} \qquad k = 1, \ldots, n$$

$\Rightarrow$ $m \cdot n$ lineare Abbildungen $\Phi_{ij} \in \mathrm{Hom}\, V, W$

1. Behauptung:

$\Phi_{ij},\ i = 1, \ldots, m,\ j = 1, \ldots, n$ sind linear unabhängig

Sei $\sum_i \sum_j a_{ij} \Phi_{ij} = o$

$$\begin{aligned} \Rightarrow\ o &= \left(\sum_j \sum_j a_{ij} \Phi_{ij} \right) (v_k) \\ &= \sum_i \sum_j a_{ij} \Phi_{ij}(k) \\ &= \sum_i \sum_j a_{ij} \delta_{kj} w_i \\ &= \sum_i a_{ik} w_i \end{aligned}$$

$\Rightarrow$ $a_{ik} = o$, $i = 1, \ldots, m$

Weil k beliebig war, sind alle $a_{ij} = o$

2. Behauptung:

$\Phi_{ij},\ i = 1, \ldots, m,\ j = 1, \ldots, n$ ist Erzeugendensystem von $\mathrm{Hom}(V,W)$

Sei $\Phi \in \mathrm{Hom}(V,W)$ $\Rightarrow$ $\Phi(v_k)$ hat Darstellung bezüglich der Basis $w_1, \ldots, w_m$:

$$\Phi(v_k) = \sum_{i=1}^{m} a_{ik} w_i \qquad k = 1, \ldots, n$$

Damit gilt

$$\begin{aligned}\left(\sum_i \sum_j a_{ij}\Phi_{ij}\right)(v_k) &= \sum_i \sum_j a_{ij}\delta_{kj}w_i \\ &= \sum_i \sum_j a_{ij}\delta_{kj}w_i \\ &= \sum_i a_{ik}w_i \\ &= \Phi(v_k) \quad k = 1, \ldots, n\end{aligned}$$

$\overset{\text{Satz 3.4}}{\Rightarrow} \sum_i \sum_j a_{ij}\Phi_{ij} = \Phi$ □

Jetzt: $W = \mathbb{K}$, d.h. $\Phi : V \to \mathbb{K}$.

Statt $\mathrm{Hom}(V, \mathbb{K})$ schreibt man hier V^* und nennt dies den *Dualraum* von V. Die Elemente $\Phi \in V^*$ schreiben wir auch als $x^*, y^*, \ldots$. Sie heißen *lineare Funktionale* oder *Linearformen*.

Beispiel:

(i) Integral (siehe früheres Beispiel) und Grenzwert sind Linearformen.

(ii) $V = \mathbb{K}^A$, A bel. Menge.

$$\Phi_{x_0} : \mathbb{K}^A \underset{f \mapsto f(x_0)}{\to} \mathbb{K} \quad x_0 \in A \text{ fest}$$

$\Rightarrow$ $\Phi \in V^*$ Auswertungsfunktional.

(iii) $V = \mathbb{K}^{n\times n}$, $\Phi = A = ((a_{ij})) \mapsto \sum_{i=1}^n a_{ii}$ lineares Funktional (*Spur* von A).

Vorlesung: 2005-02-02

Anm. des Autors. *Diese Vorlesung wurde von Prof. Drumm gehalten. Leider waren recht viele Fehler im Tafelanschrieb. Falls ihr welche findet, mailt mir bitte.*

$V^* = \mathrm{Hom}(V, \mathbb{K})$. $\dim V = n = \dim V^* \Rightarrow V \cong V^*$

$B = \{v_1, \ldots, v_n\}$ Basis in V. Durch

$$v_j^*(v_i) := \delta_{ji} \quad j, i = 1, \ldots, n$$

werden n linear unabhängige Vektoren $v_1^*, \ldots, v_n^*$ definiert. $\{v_1^*, \ldots, v_n^*\}$ ist Basis in V^*, bzw *Dualbasis* zu B.

Speziell: $V = \mathbb{K}^n$, $B := \{e_1, \ldots, e_n\}$ Standardbasis.

$\Rightarrow$ $B^* = \{e_1^*, \ldots, e_n^*\}$ Dualbasis mit $e_j^*(e_i) = \delta_{ji}$.

$e_j^* : \mathbb{K}^n \to \mathbb{K}$ festgelegt durch

$$\left(e_j^*(e_1), \ldots, e_j^*(e_j), \ldots, e_j^*(e_n)\right) = e_j$$

Allgemein: $x^* : \mathbb{K}^n \to \mathbb{K}$ festgelegt durch

$$\underset{x_1}{\left(x^*(e_1)\right.}, \ldots, \underset{x_n}{\left.x^*(e_n)\right)} \quad x = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$$

$\Rightarrow$ $x^* = x_1 e_1^* + \ldots + x_1 e_1^*$

$y \in \mathbb{K}^n$, $y = \sum_{j=1}^n y_i e_i = \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}$

$$\begin{aligned} x^*(y) &= \left(\sum_{j=1}^n x_j e_j^*\right)\left(\sum_{j=1}^n y_i e_i\right) \\ &= \sum_j \sum_i x_j y_i \underbrace{e_j^*(e_i))}_{\delta_{ji}} \\ &= \sum_{i=1}^n x_j y_i \\ &= x^\top y \end{aligned}$$

Standardskalarprodukt in $\mathbb{K}^n$.

Identifiziere $\mathbb{K}^n$ mit $(\mathbb{K}^n)^*$, damit $B = B^*$ (identifiziert).

Bemerkung: $V = \mathbb{R}[X]$, $V^* =?$ $B = \{1, X, X^2, X^3, \ldots\}$ kanonische Basis in V.

Sei $x^* \in V^*$. x^* festgelegt durch $\big(x^*(1), x^*(X), x^*(X^2), \ldots\big) \in \mathbb{R}^{\mathbb{N}_0}$.

Definiere $\Phi : (\mathbb{R}[X])^* \to \mathbb{R}^{\mathbb{N}_0}$, $x^* \mapsto \big(x^*(1), x^*(X), x^*(X^2), \ldots\big)$.

Φ ist linear, injektiv und surjektiv.

$\Rightarrow$ $V^* \cong \mathbb{R}^{\mathbb{N}_0}$, aber $V \ncong \mathbb{R}^{\mathbb{N}_0}$ $\Rightarrow$ $V \ncong V^*$.

V, V^*, $(V^*)^* =: V^{**}$ Bidualraum.

Bemerkung:

$x^*(x) = 0$ für alle $x \in V \to x^* = 0 \in V^*$
$x^*(x) = 0$ für alle $x^* \in V^* \to x = 0 \in V$

denn:

Annahme: $x \neq 0 \in V$. Ergänze x zu einer Basis B von V.

Definiere $x^* \in V^*$ durch $x^*(x) := 1$, $x^*(x') = 0$ für alle $x' \in B \setminus \{x\}$. Widerspruch.

Satz 3.11. Die Abbildung $\Psi : V \underset{x \mapsto \Psi(x)}{\to} V^{**}$ mit $\Psi(x)(x^*) := x^*(x)$ ist linear und injektiv.

Ist $\dim V < \infty$, so ist Ψ auch surjektiv, also $V \cong V^{**}$.

Beweis: Sei $x, y \in V$. Für alle $x^* \in V^*$ gilt

$$\begin{aligned} \Psi(x+y)(x^*) &= x^*(x+y) \\ &= x^(x) + x^*(y) \\ &= \Psi(x)(x^+) + \Psi(y)(x^*) \\ &= (\Psi(x) + \Psi(y))\,(x^*) \end{aligned}$$

Analog: $\Psi(ax) = a\Psi(x)$ für alle $a \in \mathbb{K}$ und $x \in V$.

Injektivität: Sei $\Psi(x) = 0 \in V^{**}$. Zu Zeigen: $x = 0 \in V$.

Sei $x^* \in V^*$ beliebig $\Rightarrow$ $0 = 0(x^*) = \Psi(x) = x^*(x)$

$\Rightarrow$ $x = 0 \in V$. □

Ergebnis: Für $\dim V < \infty$ identifizieren wir V^{**} mit V. Für $\dim V = \infty$ fassen wir V als Untervektorraum von V^{**} auf.

Definition 3.2. $\Phi : V \to W$ linear, V^*, W^* Dualräume zu V, W.

$$\Phi^\top : W^* \to V^*,\ y^* \mapsto y^* \circ \Phi$$

heißt die *transponierte* oder *duale Abbildung* von Φ.

Bemerkung:

(i) $\Phi^\top$ surjektiv $\Rightarrow$ Φ injektiv

(ii) $\Phi^\top$ injektiv $\Rightarrow$ Φ surjektiv

Beweis:

(i) Sei $\Phi(x) = 0 \in W$, zu zeigen: $x = 0 \in V$
$\Leftrightarrow\ x^*(x) = 0 \in \mathbb{K}$ für alle $x^* \in V^*$
Sei $x^* \in V^*$ beliebig $\overset{\text{Vor.}}{\Rightarrow}\ \exists y^* \in W^* : \Phi^\top(y^*) = x^*$
$\Rightarrow\ x^*(x) = \Phi^\top(y^*)(x^*) = (x^* \circ \Phi)(x) = y^*(\underbrace{\Phi(x)}_{0}) = 0$

(ii) Φ surjektiv $\Rightarrow\ \Phi(V) = W$.
Ann.: $\Phi(V) \subsetneq W$

$$\begin{aligned}\Phi^\top \text{ injektiv} &\Leftrightarrow \Phi^\top(y^*) = 0 \in V^* \Rightarrow y^* = 0 \in W^* \\ &\Leftrightarrow y^* \circ \Phi = 0 \in V^* \Rightarrow y^* = 0 \in W^* \\ &\Leftrightarrow \forall x \in V : y^* \circ \Phi(x) = 0 \in \mathbb{K} \Rightarrow y^* = 0 \in W^* \\ &\Leftrightarrow y^*|_{\operatorname{Bild}\Phi} = 0 \Rightarrow y^* = 0\end{aligned}$$

Also: Ergänze Basis B von $\Phi(V)$ zu einer Basis B' von W.
Definiere $y^* \in W^*$ wie folgt

$$y^*(y) := \begin{cases} 0 & \text{für alle } y \in B \\ 1 & \text{für alle } y \in B' \setminus B \end{cases}$$

Widerspruch!

□

Satz 3.12.

(i) $(\mathrm{id}_V)^\top = \mathrm{id}_{V^*}$

(ii) $(\Phi + \Psi)^\top = \Phi^\top + \Psi^\top \quad \Phi, \Psi \in \operatorname{Hom}(V, W)$

(iii) $(a\Phi)^\top = a(\Phi)^\top \quad a \in \mathbb{K}$

(iv) $(\Psi \circ \Phi)^\top = \Phi^\top \circ \Psi^\top \quad \Phi : V \to W$ linear und $\Psi : W \to X$ linear

(v) Ist $\Phi : V \to W$ Isomorphismus, so ist $\Phi^\top : W^* \to V^*$ Isormorphismus und $(\Phi^{-1})^\top = (\Phi^\top)^{-1}$ und umgekehrt

Vorlesung: 2005-02-04

Anm. des Autors. *Diese Vorlesung wurde von Herr Hoffmann gehalten.*

§3 Darstellung linearer Abbildungen durch Matrizen

Im Folgenden sei $\mathbb{K}$ ein Körper, V, W $\mathbb{K}$-Vektorräume, $\dim V = n$ und $\dim W = m$.

Da es auf die Reihenfolge der Basisvektoren ankommt, bezeichne

$$B = (v_1, \ldots, v_n) \neq (v_2, v_1, v_2, \ldots, v_n) \quad \text{und} \quad C = (w_1, \ldots, w_m)$$

eine *geordnete Basis* von V bzw. W.

Nach Satz 2.6 existieren für jedes $x \in V$ eindeutig bestimmte Skalare $x_1, \ldots, x_n \in \mathbb{K}$ mit

$$x = x_1 v_1 + \ldots + x_n v_n$$

Die Zahlen $x_1, \ldots, x_n \in \mathbb{K}$ nennen wir *Koordinaten* von x bzgl. B (geordnet).

Der Vektor

$$\hat{x} = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \in \mathbb{K}^n$$

heißt *Koordinatenvektor* x bzgl. B (geordnet).

Die Abbildung $x \mapsto \hat{x}$ ist ein Isomorphismus zwischen V und $\mathbb{K}^n$.

Sei $\Phi : V \to W$ eine lineare Abbildung. Für $j = 1, \ldots, n$ existieren nun $a_{ij}, \ldots, a_{nj}$ (eindeutig bestimmt) mit

$$\Phi(v_j) = a_{1j} \cdot w_1 + \ldots + a_{mj} \cdot w_m$$

Die Matrix

$$A_\Phi := \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & & \vdots \\ a_{m1} & \cdots & a_{mn} \end{pmatrix} \in \mathbb{K}^{m \times n}$$

heißt *Abbildungsmatrix* von Φ bzgl. B und C.

Beispiel: Sei $n = 3$, $m = 4$ und $\Phi \in \mathrm{Hom}(V, W)$ mit

$$\begin{aligned} \Phi(v_1) &= w_1 - w_2 + 3w_3 - w_4 \\ \Phi(v_2) &= 2w_1 + w_2 + 7w_3 + 2w_4 \\ \Phi(v_3) &= 3w_2 + w_3 + 4w_4 \end{aligned}$$

Also ist

$$A_\Phi = \begin{pmatrix} 1 & 2 & 0 \\ -1 & 1 & 3 \\ 3 & 7 & 1 \\ -1 & 2 & 3 \end{pmatrix}$$

In der j-ten Spalte von A_Φ steht der Koordinatenvektor von $\Phi(v_j)$ bzgl. C.

Außerdem gilt $\dim \mathrm{Bild}\, \Phi = \mathrm{Rg}\, A_\Phi$ (vgl. Übungsbaufgabe). Die Dimension von $\mathrm{Bild}\, \Phi$ bezeichnet man deshalb auch als Rang von Φ, kurz $\mathrm{Rg}\, \Phi$.

Satz 3.13. Die Abbildung $\Phi \mapsto A_\Phi$ ist ein Isomorphismus von $\mathrm{Hom}(V, W)$ nach $\mathbb{K}^{m \times n}$.

Beweis: Sei $A_\Phi = ((a_{ij}))$ und $A_{\Phi'} = ((a'_{ij}))$. Für $a, a' \in \mathbb{K}$ und $j = 1, \ldots, n$ gilt

$$\begin{aligned}(a\Phi + a'\Phi')(v_j) = a\Phi(v_j) + a'\Phi'(v_j) & \\ &= a \cdot \sum_{i=1}^{m} a_{ij} w_i + a' \cdot \sum_{i=1}^{m} a'_{ij} w_i \\ &= \sum_{i=1}^{m} (a \cdot a_{ij} + a' \cdot a'_{ij}) \cdot w_i\end{aligned}$$

Damit gilt $A_{a\Phi + a'\Phi'} = a \cdot A_\Phi + a' \cdot A_{\Phi'}$.

Gilt $A_\Phi = A_{\Phi'}$ für $\Phi, \Phi' \in \mathrm{Hom}(V, W)$

$$\Rightarrow \widehat{\Phi(v_1)} = \widehat{\Phi'(v_1)}, \ldots, \widehat{\Phi(v_n)} = \widehat{\Phi'(v_n)}$$

Also Spalten aus Matrizen gleich.

$$\Leftrightarrow \Phi(v_1) = \Phi'(v_1), \ldots, \Phi(v_n) = \Phi'(v_n)$$
$$\overset{\text{Satz 3.4}}{\Leftrightarrow} \Phi = \Phi'$$

Also ist die Abbildung injektiv.

Sei $A \in \mathbb{K}^{m \times n}$. Wir definieren $\Phi_A : \mathbb{K}^n \to \mathbb{K}^m$ als $x \mapsto Ax$. Das ist eine lineare Abbildung mit Abbildungsmatrix A.

Definieren wir weiter

$$\begin{aligned}\Phi(v_1) &= a_{11} w_1 + \ldots + a_{1m} w_m \\ &\vdots \\ \Phi(v_n) &= a_{n1} w_1 + \ldots + a_{nm} w_m\end{aligned}$$

Dann ist dies eine lineare Abbildung mit Abbildungsmatrix $A = ((a_{ij}))$.

Damit ist die Abbildung auch surjektiv. □

Beispiel: (Fortsetzung des vorhergehenden Beispiels.)

$$\widehat{v_1} = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \quad v_n = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix}$$

Es gilt:

$$\begin{pmatrix} a_1 1 & \cdots & a_{1n} \\ \vdots & & \vdots \\ a_{m1} & \cdots & a_{mn} \end{pmatrix} \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} = \begin{pmatrix} a_{1i} \\ \vdots \\ a_{mi} \end{pmatrix}$$

Sei $\hat{x} = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \in \mathbb{K}^n$.

$$\begin{aligned}
\begin{pmatrix} a_1 1 & \cdots & a_{1n} \\ \vdots & & \vdots \\ a_{m1} & \cdots & a_{mn} \end{pmatrix} \cdot \hat{x} = A \cdot \left(x_1 \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} + \ldots + x_n \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix} \right) \\
&= x_1 A\widehat{v_1} + x_1 A\widehat{v_2} + \ldots + x_n A\widehat{v_n} \\
&= x_1 \widehat{\Phi(v_1)} + \ldots + x_n \widehat{\Phi(v_n)} \\
&= \Phi(x_1 v_1 \widehat{+ \ldots +} x_n v_n) \\
&= \widehat{\Phi(x)}
\end{aligned}$$

Also gilt Satz 3.14.

Satz 3.14. Ist A_Φ die Abbildungsmatrix von $\Phi \in \mathrm{Hom}(V, W)$, so gilt für alle $x \in V$

$$\widehat{\Phi(x)} = A\hat{x}$$

Beispiel: (Fortsetzung des vorhergehenden Beispiels.) Wie sieht $\mathrm{Kern}\,\Phi$ aus? $\mathrm{Kern}\,\Phi = \{x \in V \mid \Phi(x) = 0\}$

Wir bestimmen alle $\hat{x} \in \mathbb{R}^3$ mit

$$A\hat{x} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

Dies ist die Lösungsmenge des LGS

$$\begin{pmatrix} 1 & 2 & 0 \\ -1 & 1 & 3 \\ 3 & 7 & 1 \\ -1 & 2 & 4 \end{pmatrix}$$

$\Rightarrow \hat{x} \in [\begin{pmatrix} 2 \\ -1 \\ 1 \end{pmatrix}] \Rightarrow \mathrm{Kern}\,\Phi = [2v_1 - v_2 + v_3]$.

Satz 3.15. Sei X ein $\mathbb{K}$-Vektorraum mit $\dim X = k$ und geordneter Basis D. Weiter sei $\Phi' : W \to X$ linear. Dann gilt

$$A_{\Phi' \circ \Phi} = A_{\Phi'} \cdot A_\Phi$$

Beweis: $B = (v_1, \ldots, v_n)$. $\Phi(v_i) = y_i$ für $i = 1, \ldots, n$. $\Phi'(y_i) = z_i$ für $i = 1, \ldots, n$. Also $\Phi' \circ \Phi(v_i) = z_i$.

Nach Satz 3.14 gilt dann

$$\begin{aligned}
\widehat{z_i} &= A_\Phi \cdot \widehat{y_i} \\
&= A_{\Phi'} \cdot (A_\Phi \cdot \widehat{v_i}) \\
&= (A_{\Phi'} \cdot A_\Phi)\widehat{v_i}
\end{aligned}$$

$\Rightarrow A_{\Phi' \circ \Phi} = A_{\Phi'} \cdot A_\Phi$. □

Satz 3.16. $\Phi : V \to W$ ist genau dann Isomorphismus wenn A_Φ regulär ist. Dann gilt

$$(A_\Phi)^{-1} = A_{\Phi^{-1}}$$

Man beachte in diesem Fall muss $\dim V = \dim W = n$ sein.

Beweis:

$$\begin{aligned}\Phi \text{ Isomorphismus } &\Rightarrow \Phi^{-1} \circ \Phi = \mathrm{id}_V,\ \Phi \circ \Phi^{-1} = \mathrm{id}_V \\ &\overset{\text{Satz 3.15}}{\Rightarrow} A_{\Phi^{-1}} \cdot A_\Phi = E_n \quad \text{und} \quad A_\Phi \cdot A_{\Phi^{-1}} = E_n \\ &\Rightarrow A_{\Phi^{-1}} = (A_\Phi)^{-1}\end{aligned}$$

Sei nun A_Φ regulär, das heißt $(A_\Phi)^{-1}$ existiert. Nach Satz 3.13 existiert eine lineare Abbildung $\Phi' : W \to V$ mit $A_{\Phi'} = (A_\Phi)^{-1}$. Es gilt:

$$A_\Phi \cdot A_{\Phi'} = E_n \qquad A_{\Phi'} \cdot A_\Phi = E_n$$

Nach Satz 3.15: $\Phi \circ \Phi' = \mathrm{id}_V$, $\Phi' \circ \Phi = \mathrm{id}_V$.

$\Rightarrow\ \Phi' = \Phi^{-1}$. □

Vorlesung: 2005-02-09

Anm. des Autors. *Diese Vorlesung wurde von Herr Hoffmann gehalten.*

Sei $\mathbb{K}$ ein Körper, V, W endlich dimensionale $\mathbb{K}$-Vektorräume mit $\dim V = n$ und $\dim W = m$ und geordenete Basen $B = (v_1, \ldots, v_n)$ von V und $C = (w_1, \ldots, w_m)$ geordnete Basen und $\Phi : V \to W$ linear.

Satz 3.17. Seien V, W, B, C, Φ wie oben und A_Φ von Φ bzgl. B und C. Ist $A_{\Phi^\top}$ die Abbildungsmatrix von $\Phi^\top$ bzgl. der dualen Basis C^* und B^*, so gilt

$$A_{\Phi^\top} = A_\Phi^\top$$

Beweis: Sei $A_{\Phi^\top} = ((c_{kl}))$. Dann gilt (nach Aufbau von $A_{\Phi^\top}$):

$$\Phi^\top(w_l^*) = \sum_{j=1}^{n} c_{jl} v_j^*$$

Damit

$$(\Phi^\top(w_l^*))(v_k) = \sum_{j=1}^{n} c_{jl} \underbrace{v_j^*(v_k)}_{\delta_{jk}} = c_{kl}$$

Nach Definition von $\Phi^\top$ gilt

$$\begin{aligned}(\Phi^\top(w_l^*))(v_k) &= w_l^*(\Phi(v_k)) \\ &= w_l^*\Big(\sum_{i=1}^{m} a_{ik} w_i\Big) \\ &= \sum_{i=1}^{m} a_{ik} \underbrace{w_l^*(w_i)}_{\delta_{li}} \\ &= a_{lk}\end{aligned}$$

wobei $A_\Phi = ((a_{ij}))$.

$\Rightarrow\ c_{kl} = a_{lk}$ für alle $k = 1, \ldots, n$, $l = 1, \ldots, m$. □

Seien $\widetilde{B} = (\widetilde{v_1}, \ldots, \widetilde{v_n})$ eine weitere geordnete basis von V und $\widetilde{C} = (\widetilde{w_1}, \ldots, \widetilde{w_m})$ eine weitere geordnete Basis von W. $A_\Phi := ((a_{ij}))$ die Abbildungsmatrix bzgl. B und C und $\widetilde{A}_\Phi$ die Abbildungsmatrix bzgl. $\widetilde{B}$ und $\widetilde{C}$.

Sei S die Abbildungsmatrix von id_V bzgl. der Basen $\widetilde{B}$ und $\widetilde{B}$. Dann gilt: Ist $S := ((s_{ij}))$, so gilt

$$\widetilde{v}_j = s_{1j}v_1 + \ldots + s_{nj}v_n \qquad \forall j = 1, \ldots, n$$

und umgekehrt.

Aus Satz 3.16 folgt: S ist regulär, und S^{-1} ist die Abbildungsmatrix von id_V bzgl. B und $\widetilde{B}$.

Ist $\widetilde{w}_k = t_{1k}w_1 + \ldots + t_{mk}w_m$ für $k = 1, \ldots, m$ so ist $T := ((t_{ij}))$ die Abbildungsmatrix von id_W bzgl. $\widetilde{C}$ und C und T^{-1} die Abbildungsmatrix von id_W bzgl. C und $\widetilde{C}$.

Sei nun $x \in V$ beliebig.

(i) $\hat{x}_B = S\hat{x}_{\widetilde{B}}$

(ii) $\Phi(\hat{x})_C = A_\Phi \hat{x}_B$

(iii) $\Phi(\hat{x})_{\widetilde{C}} = T^{-1}\Phi(\hat{x})_C$

$\Leftrightarrow$

$$\begin{aligned}\widetilde{A}_\Phi \hat{x}_B = \Phi(\hat{x})_C \\ &= T^{-1}\Phi(\hat{x})_C \\ &= T^{-1}A_\Phi \hat{x}_B \\ &= T^{-1}A_\Phi S\hat{x}_B\end{aligned}$$

$\Rightarrow\ \widetilde{A} = T^{-1}A_\Phi S$

Definition 3.3. Zwei Matrizen $A, \widetilde{A}$ aus $\mathbb{K}^{m\times n}$ heißen *äquivalent*, wenn es reguläre Matrizen $S \in \mathbb{K}^{m\times n}$ und $T \in \mathbb{K}^{n\times m}$ gilt mit

$$\widetilde{A} = T^{-1}AS$$

Beispiel:

$$\Phi : \mathbb{R}^3 \ \to\ \mathbb{R}^4$$

habe bzgl. der Standardbasis die Abbildungsmatrix

$$A_\Phi := \begin{pmatrix} 1 & 2 & 0 \\ -1 & 1 & 3 \\ 3 & 7 & 1 \\ -1 & 2 & 4 \end{pmatrix}$$

$$\widetilde{B} = (\begin{pmatrix}1\\1\\0\end{pmatrix}, \begin{pmatrix}0\\1\\1\end{pmatrix}, \begin{pmatrix}1\\0\\1\end{pmatrix}),\ \widetilde{C} = (\begin{pmatrix}1\\1\\0\\0\end{pmatrix}, \begin{pmatrix}1\\0\\1\\0\end{pmatrix}, \begin{pmatrix}0\\1\\1\\0\end{pmatrix}, \begin{pmatrix}1\\0\\0\\1\end{pmatrix})$$

geordnete Basen von $\mathbb{R}^3$ bzw. $\mathbb{R}^4$.

$$\Rightarrow\ S = \begin{pmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix} \quad T = \begin{pmatrix} 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

$\Rightarrow\ T^{-1}$.

$\widetilde{A}_\Phi$ die Abbildungsmatrix bzgl. $\widetilde{B}$ und $\widetilde{C}$, ist

$$\widetilde{A}_\Phi = T^{-1} A_\Phi S = \begin{pmatrix} -4 & -4 & -2 \\ 6 & 0 & 0 \\ 4 & 8 & 4 \\ 1 & 6 & 3 \end{pmatrix}$$

Die Äquivalenz von Matrizen ist eine Äquivalenzrelation auf $\mathbb{K}^{m\times n}$.

Durch elementare Zeilen oder Spaltenumformungen geht eine Matrix A in eine äquivalente Matrix $\widetilde{A}$ über.

Jede Matrix ist zu ihrer Gaußschen Normalform äquivalent.

Zwei Matrizen sind genau dann äquivalent wenn sie den selben Rang haben.

Sei $\Phi : V \to V$ ein Endomorphismus und A_Φ die Abbildungsmatrix bzgl. B und B. Wie sieht die Abbildungsmatrix $\widetilde{A}_\Phi$ von Φ bzgl. $\widetilde{B}$ und $\widetilde{B}$ aus? Es gilt

$$\widetilde{A}_\Phi = S^{-1} A_\Phi S$$

Definition 3.4. Zwei Matrizen $A, \widetilde{A} \in \mathbb{K}^{n\times n}$ heißen *ähnlich*, falls es eine reguläre Matrix $S \in \mathbb{K}^{n\times n}$ gibt mit

$$\widetilde{A} = S^{-1} A S$$

Auch das ist eine Äquivalenzrelation auf $\mathbb{K}^{n\times n}$.

Ähnliche Matrizen sind auch äquivalent, aber die Umkehrung gilt im Allgemeinen nicht.

4 Determinanten und Eigenwerte

§1 Determinate

Sei

$$\pi = \begin{pmatrix} 1 & \cdots & i & \cdots & j & \cdots & m \\ \pi(1) & \cdots & \pi(i) & \cdots & \pi(j) & \cdots & \pi(m) \end{pmatrix} \in S_m$$

Ein Paar $(i,j) \in \{1,\dots,m\} \times \{1,\dots,m\}$ heißt *Fehlstand*, falls

$$i < j \quad \text{aber} \quad \pi(i) > \pi(j)$$

$\mathrm{F}(\pi)$ ist die Anzahl der Fehlstände von π.

Beispiel:

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

$(1,2)$, $(1,3)$, $(1,4)$, $(2,3)$ sind Fehlstände, also ist $\mathrm{F}(\pi) = 4$.

Bemerkung:

(i) Für $\pi \in S_m$ gilt

$$\prod_{1 \le i < j \le m} \frac{\pi(j) - \pi(i)}{j - 1} = (-1)^{\mathrm{F}(\pi)}$$

(ii) Für alle $\sigma, \pi \in S_m$ gilt

$$(-1)^{\mathrm{F}(\sigma \circ \pi)} = (-1)^{\mathrm{F}(\sigma)} \cdot (-1)^{F(\pi)}$$

(iii) $(-1)^{\mathrm{F}(\pi)} = (-1)^{\mathrm{F}(\pi^{-1})}$
$\mathrm{F}(\tau^{i,j}) = 2(j-1) - 1$

Aus diesen Eigenschaften folgt: Eine Permutation ist genau dann gerade, wenn ihre Fehlstandszahl gerade ist.

Definition 4.1. Sei $A \in \mathbb{K}^{n \times m}$. Dann heißt

$$\det A := \sum_{\pi \in S_n} (-1)^{\mathrm{F}(\pi)} \cdot a_{\pi(1),1} \cdots a_{\pi(n),n}$$

die *Determinante* von A.

Wir schreiben $|A|$. Ist $A = ((a_{ij}))$, dann

$$\det A = \begin{vmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & & \vdots \\ a_{n1} & \cdots & a_{nn} \end{vmatrix}$$

Vorlesung: 2005-02-11

Bemerkung:

(i) $n = 1$: $\det A = a_{11}$

$$A = \begin{pmatrix} a_{11} \end{pmatrix}$$

$n = 2$: $\det A = a_{11}a_{22} - a_{21}a_{12}$

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

$n = 3$: $\det A = a_{11}a_{22}a_{33} + a_{21}a_{32}a_{13} + a_{31}a_{12}a_{23} - a_{11}a_{32}a_{23} - a_{31}a_{22}a_{13} - a_{21}a_{12}a_{33}$

$$A = \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix}$$

$n \geq 4$: Keine entsprechende Regel.

(ii) A obere oder untere Dreiecksmatrix, dann ist

$$\det A = a_{11} \cdots a_{nn}$$

(iii) $\det E_n = 1$

Satz 4.1. Es gilt

$$\det A = \det A^\top$$

Beweis: $A = ((a_{ij}))$, $A^\top = ((\widetilde{a}_{ij}))$ mit $\widetilde{a}_{ij} = a_{ji}$. Dann gilt

$$\begin{aligned}
\det A^\top &= \sum_{\pi \in S_n} (-1)^{\mathrm{F}(\pi)} \cdot \widetilde{a}_{\pi(1),1} \cdots \widetilde{a}_{\pi(n),n} \\
&= \sum_{\pi \in S_n} (-1)^{\mathrm{F}(\pi)} \cdot a_{1,\pi(1)} \cdots a_{n,\pi(n)} \\
&= \sum_{\pi \in S_n} (-1)^{\mathrm{F}(\pi)} \cdot a_{\pi^{-1}(\pi(1)),\pi(1)} \cdots a_{\pi^{-1}(\pi(n)),\pi(n)} \\
&= \sum_{\pi \in S_n} (-1)^{\mathrm{F}(\pi)} \cdot a_{\pi^{-1}(1),1} \cdots a_{\pi^{-1}(n),n} \\
&= \sum_{\underbrace{\pi^{-1}}_{\tau} \in S_n} (-1)^{\mathrm{F}(\underbrace{\pi^{-1}}_{\tau})} a_{\underbrace{\pi^{-1}}_{\tau}(1),1} \cdots a_{\underbrace{\pi^{-1}}_{\tau}(n),n} \\
&= \det A
\end{aligned}$$

□

Bemerkung:

$$\det A = \sum_{\pi \in S_n} (-1)^{\mathrm{F}(\pi)} \cdot a_{1,\pi(1)} \cdots a_{n,\pi(n)}$$

Sei $\Delta : (\mathbb{K}^n)^n \to \mathbb{K}$, $(x_1, \ldots, x_n) \mapsto \det \begin{pmatrix} x_1 & \cdots & x_n \end{pmatrix}$ und $\widetilde{\Delta} : (\mathbb{K}^n)^n \to \mathbb{K}$, $(y_1, \ldots, y_n) \mapsto \det \begin{pmatrix} y_1 & \cdots & y_n \end{pmatrix}^\top$.

Nach Satz 4.1 gilt

$$\Delta = \widetilde{\Delta}$$

Satz 4.2. Die Funktion Δ hat folgende Eigenschaften

(i) Δ ist *multilinear*, d.h.

$$\Delta(a_1 x1 + a_1' x_1', x_2, \ldots, x_n) = a_1 \Delta(x_1, x_2, \ldots, x_n) + a_1' \Delta(x_1', x_2, \ldots, x_n)$$

usw...

(ii) $\Delta(x_{\pi(1)}, \ldots, x_{\pi(n)}) = (-1)^{\mathrm{F}(\pi)} \Delta(x_1, \ldots, x_n)$, insbesondere ist Δ *alternierend*, d.h.

$$\Delta(x_1, \ldots, x_j, \ldots, x_i, \ldots, x_n) = -\Delta(x_1, \ldots, x_i, \ldots, x_j, \ldots, x_n)$$

(iii) Δ ist *normiert*, d.h. $\Delta(e_1, \ldots, e_n) = 1$

(iv) $\Delta(x_1, \ldots, x_n) = 0 \Leftrightarrow x_1, \ldots, x_n$ linear abhängig.

Beweis:

(i) Folgt direkt aus der Definition von Δ.

(ii) Sei $\begin{pmatrix} x_1 & \cdots & x_n \end{pmatrix} = ((a_{ij}))$

$$\begin{aligned}
\Delta(x_{\pi(1)}, \ldots, x_{\pi(n)}) &= \det(x_{\pi(1)}, \ldots, x_{\pi(n)}) \\
&= \sum_{\tau \in S_n} (-1)^{\mathrm{F}(\tau)} a_{\tau(1),\pi(1)} \cdots a_{\tau(n),\pi(n)} \qquad \tau = \sigma \circ \pi \\
&= \sum_{\sigma \in S_n} (-1)^{\mathrm{F}(\sigma \circ \pi)} a_{\sigma(\pi(a)),\pi(1)} \cdots a_{\sigma(\pi(n)),\pi(n)} \\
&= \sum_{\sigma \in S_n} (-1)^{\mathrm{F}(\sigma)} (-1)^{\mathrm{F}(\pi)} a_{\sigma(1),1} \cdots a_{\sigma(n),n} \\
&= (-1)^{\mathrm{F}(\pi)} \cdot \det A \\
&= (-1)^{\mathrm{F}(\pi)} \cdot \Delta(x_1, \ldots, x_n)
\end{aligned}$$

(iii) $\Delta(e_1, \ldots, e_n) = \det E_n = 1$

(iv) Zunächst Spezialfall: Gilt $x_i = x_j$ für ein Paar (i, j) mit $i \neq j$, so ist

$$\Delta(x_1, \ldots, x_n) = 0$$

$A = \begin{pmatrix} x_1 & \cdots & x_n \end{pmatrix}$. In $\det A = \Delta(x_1, \ldots, x_n)$ tritt mit

$$(-1)^{\mathrm{F}(\pi)} a_{\pi(1),1} \cdots a_{\pi(n),n}$$

auch der Summand

$$(-1)^{\mathrm{F}(\pi \circ \tau^{(i,j)})} a_{\pi(\tau^{(i,j)}(1)),1} \cdots a_{\pi(\tau^{(i,j)}(n)),n}$$

auf.

$$\Rightarrow \; -(-1)^{\mathrm{F}(\pi)} a_{\pi(1),1} \cdots \underbrace{a_{\pi(j),i}}_{a_{\pi(j),j}} \cdots \underbrace{a_{\pi(i),j}}_{a_{\pi(i),i}} \cdots a_{\pi(n),n}$$

$\Rightarrow$ Summe ist 0.

$\Rightarrow \; \Delta(x_1, \ldots, x_n) = 0.$

Einschub. Wäre hier auch ein kürzerer Schluss möglich gewesen? Also so:

$$\begin{aligned}
&\Delta(x_1,\ldots,x_i,\ldots,\underset{=x_i}{x_j},\ldots,x_n) \overset{\text{(ii)}}{=} -\Delta(x_1,\ldots,x_j,\ldots,x_i,\ldots,x_n)\\
\Rightarrow\ &\Delta(x_1,\ldots,x_n) = -\Delta(x_1,\ldots,x_n)\\
\Leftrightarrow\ &\Delta(x_1,\ldots,x_n) + \Delta(x_1,\ldots,x_n) = 0\\
\Rightarrow\ &\Delta(x_1,\ldots,x_n) = 0
\end{aligned}$$

Dies gilt jedoch z.b. nicht in $\mathbb{F}_2$, daher wäre dieser Beweis nicht allgemeingültig!

Allgemeiner Fall: $x_1,\ldots,x_n$ linear abhängig $\Rightarrow$ $\Delta(x_1,\ldots,x_n)=0$.

$x_1,\ldots,x_n$ linear abhängig $\Rightarrow$ $\exists$ Darstellung

$$\begin{aligned}
&x_1 = b_2x_2 + \ldots + b_nx_n\\
\Rightarrow\ &\Delta(x_1,\ldots,x_n) \overset{\text{(i)}}{=} \sum_{i=2}^{n} b_i \underbrace{\Delta(x_i,x_1,\ldots,x_n)}_{=0} = 0
\end{aligned}$$

Sei nun $\Delta(x_1,\ldots,x_n)=0$.

Annahme: $x_1,\ldots,x_n$ linear unabhängig $\Rightarrow$ $x_1,\ldots,x_n$ Basis von $\mathbb{K}^n$.

$$\Rightarrow\ e_j = \sum_{k=1}^{n} a_{kj}x_k \qquad j=1,\ldots,n$$

Also

$$\begin{aligned}
1 &= \Delta(e_1,\ldots,e_n)\\
&= \sum_{k_1=1}^{n}\sum_{k_n=1}^{n} a_{k_1,1}\cdots a_{k_n,n}\Delta(x_{k_1},\ldots,x_{k_n})\\
&= \sum_{\pi\in S_n} a_{\pi(1),1}\cdots a_{\pi(n),n}\underbrace{\Delta(x_{\pi(1)},\ldots,x_{\pi(n)})}_{=0}\\
&= 0
\end{aligned}$$

Widerspruch.

□

Satz 4.3 (Rechenregeln für Determinanten)**.**

(i) Addition eines Vielfachen einer Spalte (Zeile) zu einer anderen ändert $\det A$ nicht.

(ii) Multiplikation einer Spalte (Zeile) mit $a\in\mathbb{K}$ ändert $\det A$ um den Faktor a.

(iii) Vertauschen zweier Spalten (Zeilen) ändert das Vorzeichen von $\det A$.

(iv) A regulär $\Leftrightarrow$ $\det A \neq 0$.

Beweis: klar. □

Vorlesung: 2005-02-16

Beispiel:

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

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

$$= \begin{vmatrix} 1 & 0 & 2 & 1 & 2 \\ 0 & 2 & 2 & 2 & 3 \\ 0 & 0 & -1 & 0 & -3 \\ 0 & 0 & 4 & 1 & 5 \\ 0 & 0 & -2 & -1 & -2 \end{vmatrix}$$

$$= \begin{vmatrix} 1 & 0 & 2 & 1 & 2 \\ 0 & 2 & 2 & 2 & 3 \\ 0 & 0 & -1 & 0 & -3 \\ 0 & 0 & 0 & 1 & -7 \\ 0 & 0 & 0 & -1 & 4 \end{vmatrix} = \begin{vmatrix} 1 & 0 & 2 & 1 & 2 \\ 0 & 2 & 2 & 2 & 3 \\ 0 & 0 & -1 & 0 & -3 \\ 0 & 0 & 0 & 1 & -7 \\ 0 & 0 & 0 & 0 & -3 \end{vmatrix}$$

$$= 1 \cdot 2 \cdot (-1) \cdot 1 \cdot (-3)$$
$$= 6$$

Satz 4.4. Sei $A \in \mathbb{K}^{n \times n}$ und $j \in \{1, \ldots, n\}$. Dann gilt

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

(ii) $\det A = \sum_{k=1}^{n} (-1)^{k+j} a_{jk} \cdot \det A_{jk}$

Hierbei ist $A_{ij} \in \mathbb{K}^{n-1 \times n-1}$ die Matrix A nach Streichen der i-ten Zeile und j-ten Spalte.

Beweis:

(i) Spezialfall:

$$\begin{vmatrix} a_{1,1} & \cdots & a_{1,n-1} & 0 \\ \vdots & & \vdots & \vdots \\ a_{n-1,1} & \cdots & a_{n-1,n-1} & 0 \\ a_{n,1} & \cdots & a_{n,n-1} & 1 \end{vmatrix}_B = \begin{vmatrix} a_{1,n} & \cdots & a_{1,n-1} \\ \vdots & & \vdots \\ a_{n-1,1} & \cdots & a_{n-1,n-1} \end{vmatrix}$$

$$\begin{aligned}\det B &= \sum_{\pi\in S_n} (-1)^{F(\pi)} b_{\pi(1),1}\cdots b_{\pi(n-1),n-1}\cdot b_{\pi(n),n}\\ &= \sum_{\substack{\pi\in S_n\\ \pi(n)=n}} (-1)^{F(\pi)} a_{\pi(1),1}\cdots a_{\pi(n-1),n-1}\cdot 1\\ &= \sum_{\tau\in S_{n-1}} (-1)^{F(\tau)} a_{\tau(1),1}\cdots a_{\tau(n-1),n-1}\\ &= \det A_{n,n}\end{aligned}$$

Allgemeiner Fall:

Nach Satz 4.3 gilt:

$$\begin{aligned}\det A &= a_{1j}\begin{vmatrix} a_{11} & \cdots & 1 & \cdots & a_{1n}\\ \vdots & & 0 & & \vdots\\ \vdots & & \vdots & & \vdots\\ a_{n1} & \cdots & 0 & \cdots & a_{1n}\end{vmatrix} + \ldots + a_{nj}\begin{vmatrix} a_{11} & \cdots & 0 & \cdots & a_{1n}\\ \vdots & & \vdots & & \vdots\\ \vdots & & 0 & & \vdots\\ a_{n1} & \cdots & 1 & \cdots & a_{1n}\end{vmatrix}\\ &= \sum_{k=1}^{n} a_{kj}\cdot \underbrace{(-1)^{n-j}\cdot(-1)^{n-k}}_{(-1)^{k+j}}\cdot \det A_{kj}\end{aligned}$$

(ii) Folgt aus a) (mit Satz 4.1)

□

Beispiel:

$$\begin{vmatrix} 2 & 0 & 1 & 2 & 0\\ 2 & -1 & 0 & 1 & 1\\ 0 & 1 & 2 & 1 & 2\\ -2 & 0 & 2 & -1 & 2\\ 2 & 0 & 0 & 1 & 1\end{vmatrix} \overset{\hookleftarrow^{+}}{=} \begin{vmatrix} 2 & 0 & 1 & 2 & 0\\ 2 & 0 & 2 & 2 & 3\\ 0 & 1 & 2 & 1 & 2\\ -2 & 0 & 2 & -1 & 2\\ 2 & 0 & 0 & 1 & 1\end{vmatrix} = -\begin{vmatrix} 2 & 1 & 2 & 0\\ 2 & 2 & 2 & 3\\ -2 & 2 & -1 & 2\\ 2 & 0 & 1 & 1\end{vmatrix} \overset{\hookleftarrow^{+}}{=}$$

$$= -\begin{vmatrix} 2 & 1 & 2 & 0\\ 2 & 2 & 2 & 3\\ 0 & 2 & 0 & 3\\ 2 & 0 & 1 & 1\end{vmatrix} = 2\cdot \underbrace{\begin{vmatrix} 2 & 2 & 0\\ 2 & 2 & 3\\ 2 & 1 & 2\end{vmatrix}}_{=6} + 3\cdot \underbrace{\begin{vmatrix} 2 & 1 & 2\\ 2 & 2 & 2\\ 2 & 0 & 2\end{vmatrix}}_{=-2}$$

$$= 12 + 3\cdot(-2)$$

$$= 6$$

Vandermonde-Determinante $x_1, \ldots, x_n \in \mathbb{K}$

$$\begin{vmatrix} 1 & \cdots & 1 \\ x_1 & \cdots & x_n \\ x_1^2 & \cdots & x_n^2 \\ \vdots & & \vdots \\ x_1^{n-1} & \cdots & x_n^{n-1} \end{vmatrix} \begin{array}{l} | -x_1 \\ | -x_1 \\ | \ddots \\ | -x_1 \\ \end{array}$$

$$= \begin{vmatrix} 1 & 1 & \cdots & 1 \\ 0 & (x_2 - x_1) & \cdots & (x_n - x_1) \\ \vdots & \vdots & & \vdots \\ 0 & (x_2 - x_1)x_2^{n-3} & \cdots & (x_n - x_1)x_n^{n-3} \\ 0 & (x_2 - x_1)x_2^{n-2} & \cdots & (x_n - x_1)x_n^{n-2} \end{vmatrix}$$

$$= (x_2 - x_1) \cdots (x_n - x_1) \cdot \begin{vmatrix} 1 & \cdots & 1 \\ x_2 & \cdots & x_n \\ \vdots & & \vdots \\ x_2^{n-2} & \cdots & x_n^{n-2} \end{vmatrix}$$

$$= \ldots$$

$$= (x_2 - x_1) \cdots (x_n - x_1) \cdot (x_3 - x_2) \cdots (x_n - x_2) \cdot \cdots \cdot (x_n - x_{n-1})$$

$$= \prod_{1 \le i < j \le n} (x_j - x_i)$$

Satz 4.5. Für zwei Matrizen $A, B \in \mathbb{K}^{n \times n}$ gilt:

$$\det(A \cdot B) = \det A \cdot \det B$$

Beweis:

$$AB = \begin{pmatrix} Ab_1 & \cdots & Ab_n \end{pmatrix}$$
$$= \begin{pmatrix} b_{11}a_1 + \ldots + b_{n1}a_n & \cdots & b_{1n}a_1 + \ldots + b_{nn}a_n \end{pmatrix}$$

$$\Rightarrow \det(AB) = \sum_{i_1, \ldots, i_n = 1}^{n} b_{i_1 1} b_{i_2 2} \cdots b_{i_n n} \cdot \Delta(a_{i_1}, a_{i_2}, \ldots, a_{i_n})$$
$$= \sum_{\pi \in S_n} b_{\pi(1),1} \cdots b_{\pi(n),n} \cdot \Delta(a_{\pi(1)}, \ldots, a_{\pi(n)})$$
$$= \sum_{\pi \in S_n} b_{\pi(1),1} \cdots b_{\pi(n),n} \cdot (-1)^{\mathrm{F}(\pi)} \cdot \Delta(a_1, \ldots, a_n)$$
$$= \det A \cdot \sum_{\pi \in S_n} (-1)^{\mathrm{F}(\pi)} b_{\pi(1),1} \cdots b_{\pi(n),n}$$
$$= \det A \cdot \det B$$

□

Korollar 4.6 (Kästchenmultiplikationssatz)**.**

(i) Es gitl für $A = \left(\begin{smallmatrix} B & 0 \\ C & D \end{smallmatrix}\right)$, dass
$$\det A = \det B \cdot \det D$$

(ii) Es gitl für $A = \left(\begin{smallmatrix} B & C \\ 0 & D \end{smallmatrix}\right)$, dass
$$\det A = \det B \cdot \det D$$

Beweis:

(i) $A = \left(\begin{smallmatrix} B & 0 \\ C & D \end{smallmatrix}\right) = \left(\begin{smallmatrix} B & 0 \\ C & E_{n-m} \end{smallmatrix}\right) \cdot \left(\begin{smallmatrix} E_m & 0 \\ 0 & D \end{smallmatrix}\right)$

$$\Rightarrow \det A = \begin{vmatrix} B & 0 \\ C & E_{n-m} \end{vmatrix} \cdot \begin{vmatrix} E_m & 0 \\ 0 & D \end{vmatrix}$$
$$= \det B \cdot \det D$$

(ii) Folgt aus a)

□

Vorlesung: 2005-02-18

Bemerkung und Definition:

(i) Ist A regulär, so ist

$$\det A^{-1} = \frac{1}{\det A} = (\det A)^{-1} \qquad (A \cdot A^{-1} = E_n)$$

(ii) Ist $A' = S^{-1}AS$ (ähnlich zu A), so ist

$$\det A' = \det A$$

(iii) Ist $\Phi \in \mathrm{End}(V)$ und A_Φ Abbildungsmatrix von Φ bzgl. Basis B, so hängt $\det \Phi := \det A_\Phi$ nicht von der Basis B ab.

$\det \Phi$ heißt *Determinante* von Φ.

Satz 4.7 (Cramersche Regel)**.** Sei $Ax = b$ ein LGS mit regulärer Matrix A

$$A := \begin{pmatrix} a_1 & \cdots & a_n \end{pmatrix}$$

und $b \in \mathbb{K}^n$, dann hat die eindeutige Lösung $x = (x_1, \ldots, x_n) = A^{-1}b$ die Form

$$x_i = \frac{1}{\det A} \cdot \begin{vmatrix} a_1 & \cdots & a_{i-1} & b & a_{i+1} & \cdots & a_n \end{vmatrix} \qquad i = 1, \ldots, n$$

Beweis:

$$x_i \cdot \det A = \begin{vmatrix} a_1 & \cdots & a_{i-1} & x_i a_i & a_{i+1} & \cdots & a_n \end{vmatrix}$$
$$= \begin{vmatrix} a_1 & \cdots & a_{i-1} & \underbrace{\sum_{j=1}^{n} x_j a_j}_{Ax=b} & a_{i+1} & \cdots & a_n \end{vmatrix}$$

□

Satz 4.8. Sei A regulär mit inverser Matrix $A^{-1} = ((b_{ij}))$. Dann gilt:

$$b_{ij} = (-1)^{i+j} \cdot (\det A)^{-1} \cdot \det A_{ji} \qquad i, j = 1, \ldots, n$$

Beweis:

$$AA^{-1} = E_n \Leftrightarrow A \cdot b_j = e_j \qquad j = 1, \ldots, n$$

Also folgt

$$\begin{aligned} b_{ij} &\overset{\text{Satz 4.7}}{=} (\det A)^{-1} \cdot \left|a_1 \quad \cdots \quad e_j \quad \cdots \quad a_n\right| \\ &= (-1)^{i+j} \cdot (\det A)^{-1} \cdot \det A_{j,i} \end{aligned}$$

□

Bemerkung: Man kann auch Matrizen betrachten, deren Einträge a_{ij} Polynome sind, dann ist speziell $\det A$ erklärt und ein Polynom.

Sei nun $\Phi : V \to V$, $\dim V = n$, A_Φ bzgl. Basis $B = (x_1, \ldots, x_n)$

Die einfachste Form der Abbildungsmatrix ist

$$A_\Phi = \begin{pmatrix} a_{11} & & 0 \\ & \ddots & \\ 0 & & a_{11} \end{pmatrix}$$

Wann existiert diese?

$$\begin{aligned} \widehat{\Phi(x_i)} &= A_\Phi \cdot \hat{x}_i = a_{ii} \cdot e_i = a_{ii} \cdot \hat{x}_i \\ \Rightarrow \Phi(x_i) &= a_{ii} x_i \end{aligned}$$

§2 Eigenwerte und Diagonalisierbarkeit

Im folgenden sei Φ immer ein Endomorphismus $\Phi \in \mathrm{End}(V)$.

Definition 4.2. Ein Skalar $c \in \mathbb{K}$ heißt *Eigenwert* von Φ, wenn es einen Vektor $x \in V$ gibt mit $x \neq 0$, der

$$\Phi(x) = c \cdot x$$

erfüllt. Jedes solche x heißt *Eigenvektor* zum Eigenwert c.

Bemerkung und Definition:

(i) Die Menge der Eigenvektoren zu einem Eigenwert c bildet zusammen mit O einen Untervektorraum E_c von V, den *Eigenraum* (zu c).

(ii) Sei $A \in \mathbb{K}^{n \times n}$ und $\Phi : \mathbb{K}^n \to \mathbb{K}^n$, $x \mapsto Ax$.

Jeder Eigenwert (bzw. Eigenvektor) von Φ heißt dann auch *Eigenwert* (*Eigenvektor*) von A.

(c heißt Eigenwert von $A \Leftrightarrow \exists x \in \mathbb{K}^n$, $x \neq 0$ mit $Ax = cx$)

(iii) Ähnliche Matrizen A, A' haben die gleichen Eigenwerte.

Denn: $A' = S^{-1}AS$. Sei c Eigenwert von A, das heißt $Ax = cx$ mit geeignetem $x \neq 0$, $x \in \mathbb{K}^n$. Setze $x' = S^{-1}x \Rightarrow x' \neq 0$. $\Rightarrow A'x' = S^{-1}ASS^{-1}x = S^{-1}Ax = S^{-1}cx = cx'$

Satz 4.9. Sei $\Phi \in \mathrm{End}(V)$ und $c_1, \ldots, x_k$ paarweise verschieden Eigenwerte mit Eigenvektoren $x_1, \ldots, x_k$. Dann sind $x_1, \ldots, x_k$ linear unabhängig.

Beweis: Sei $a_1x_1 + \ldots + a_kx_k = o$

$$\begin{aligned} \Rightarrow\ a_1x_1 + \ldots + a_kx_k &= 0 \\ &= a_1\Phi(x_1) + \ldots + a_k\Phi(x_k) \\ &= a_1c_1x_1 + \ldots + a_kcx_k \end{aligned}$$

Andererseits ist

$$c_1(a_1x_1 + \ldots + a_kx_k) = 0 = a_1c_1x_1 + \ldots + a_kc_1x_k$$

$$\Rightarrow\ a_2(c_2 - c_1)x_2 + \ldots + a_k(c_k - c_1)x_k = 0$$

Jetzt beweisen wir die Aussage mit vollständiger Induktion nach k.

$k = 1$: trivial.

$k - k\ \rightarrow\ k$:

Nach IV sind $x_2, \ldots, x_k$ linear unabhängig

$$\Rightarrow\ a_2(\underbrace{c_2 - c_1}_{\neq 0}) = \ldots = a_k(\underbrace{c_k - c_1}_{\neq 0}) = 0$$

$$\Rightarrow\ a_1 = \ldots = a_k = 0$$

$$\Rightarrow\ a_1x_1 = 0$$

$$\Rightarrow\ a_1 = 0$$

$$\Rightarrow\ x_1, \ldots, x_k \text{ linear unabhängig}$$

□

Korollar 4.10. Ist $\Phi \in \mathrm{End}(V)$, $\dim V = n$, so hat Φ maximal n verschiedene Eigenwerte. Entsprechend hat eine Matrix $A \in \mathbb{K}^{n\times n}$ höchstens n verschiedene Eigenwerte.

Beweis: klar. □

Sei nun $\dim V < \infty$, $\Phi \in \mathrm{End}(V)$ und B Basis von V.

$$\Rightarrow\ \Phi(v) = c \cdot v\ \Leftrightarrow\ \hat{\Phi}(v) = c \cdot \hat{v}\ \Leftrightarrow\ A_\Phi\hat{v} = c\hat{v}$$

Deshalb betrachten wir jetzt Eigenwerte und Eigenvektoren von Matrizen A.

$$Av \overset{*}{=} cv \qquad v \in \mathbb{K}^n,\ v \neq 0$$

c Eigenwert von $A\ \Leftrightarrow$ * hat Lösung $v \neq 0\ \Leftrightarrow\ (A - cE_n)v = 0$ hat Lösung $v \neq 0\ \Leftrightarrow\ \det(A - cE_n) = 0 = \sum_{\pi\in S_n}(-1)^{\mathrm{F}(\pi)} \cdot (a_{\pi(1),1} - c \cdot \delta_{\pi(1),1}) \cdots (a_{\pi(n),n} - c \cdot \delta_{\pi(n),n})$

Definition 4.3. Das Polynom

$$\begin{aligned} p :&= \sum_{\pi\in S_n}(-1)^{\mathrm{F}(\pi)}(a_{\pi(1),1} - X \cdot \delta_{\pi(1),1}) \cdots (a_{\pi(n),n} - X \cdot \delta_{\pi(n),n}) \\ &= \det(A - XE_n) \end{aligned}$$

heißt *charakteristisches Polynom* von A.

Satz 4.11. c ist Eigenwert von $A\ \Leftrightarrow\ c$ ist Nullstelle von p.

Vorlesung: 2005-04-13

Beweis: selbst. □

Bemerkung: Ähnliche Matrizen besitzen das gleiche charakteristische Polynom p

Beweis: A, A' ähnlich, das heißt $A' = S^{-1}AS$

$$\begin{aligned} p_{A'} &= \det(A' - XE_n) \\ &= \det(S^{-1}AS - S^{-1}XE_nS) \\ &= \det S^{-1}(A - XE_n)S \\ &= \det S^{-1} \det(A - XE_n) \det S \\ &= \det(A - XE_n) \\ &= p_A \end{aligned}$$

□

Damit kann das charakteristische Polynom von Φ über A_Φ gebaut werden.

Beispiel:

(i) Sei $A = \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right) \in \mathbb{K}^{2\times 2}$ mit $\mathbb{K} = \mathbb{F}_2, \mathbb{R}, \mathbb{C}$.
Eigenwerte: Charakteristisches Polynom

$$p = \begin{vmatrix} -X & 1 \\ -1 & -X \end{vmatrix} = X^2 + 1$$

Also

- $\mathbb{K} = \mathbb{F}_2$: Eigenwert $c = 1$ mit $E_c = [\left(\begin{smallmatrix} 1 \\ 1 \end{smallmatrix}\right)]$
- $\mathbb{K} = \mathbb{R}$: Keine Eigenwerte!
- $\mathbb{K} = \mathbb{C}$: Zwei Eigenwerte $c_1 = i$ mit $E_{c_1} = [\left(\begin{smallmatrix} 1 \\ i \end{smallmatrix}\right)]$ und $c_2 = -i$ mit $E_{c_2} = [\left(\begin{smallmatrix} 1 \\ -i \end{smallmatrix}\right)]$

(ii) Sei

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

Dann gilt

$$\begin{aligned} p &= \begin{vmatrix} -X & -1 & 1 & 1 \\ -1 & 1-X & -2 & 3 \\ 2 & -1 & -X & 0 \\ 1 & -1 & 1 & -X \end{vmatrix} = \begin{vmatrix} -X & -1 & 1 & 1 \\ 0 & -X & -1 & 3-X \\ 0 & 1 & -2-X & 2X \\ 1 & -1 & 1 & -X \end{vmatrix} \\ &= -\begin{vmatrix} 3X-1 & 4-X & -5 \\ 2 & -1 & -X \\ 1 & -1 & 1 \end{vmatrix} - X \cdot \begin{vmatrix} -X & -1 & 1 \\ 3X-1 & 4-X & -5 \\ 2 & -1 & -X \end{vmatrix} \\ &= -(-3X + 1 + 10 + X^2 - 4X - 5 - 8 + 2X - 3X^3 + X) \\ &\quad - X(4X^2 - X^3 + 10 - 3X + 1 - 8 + 2X + 5X + 3X^2 + X) \\ &= 2X^2 + 4X + 2 + X(X^3 - X^2 - 5X - 3) \\ &= 2(X+1)^2 + (X+1)X(X^2 - 2X - 3) \\ &= (X+1)^2(X-1)(X-2) \end{aligned}$$

$\Rightarrow$ $c_1 = -1, c_2 = 1, c_3 = 2$.

$$E_{c_1} : \begin{pmatrix} 1 & -1 & 1 & 1 \\ -1 & 2 & -2 & 3 \\ -2 & -1 & 1 & 0 \\ 1 & -1 & 1 & 1 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 1 & -1 & 1 & 1 \\ 0 & 1 & -1 & 4 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix} \Rightarrow E_{c_1} = [\begin{pmatrix} 0 \\ 1 \\ 1 \\ 0 \end{pmatrix}]$$

Definition 4.4. Eine Matrix $A \in \mathbb{K}^{n\times n}$ heißt *diagonalisierbar* wenn sie zu einer Diagonalmatrix

$$\begin{pmatrix} c_1 & & 0 \\ & \ddots & \\ 0 & & c_n \end{pmatrix}$$

ähnlich ist. Das heißt wenn es reguläres S mit $S^{-1}AS = A'$ gibt.

Ein $\Phi \in \mathrm{End}(V)$ heißt *diagonalisierbar* wenn es eine Basis gibt, bzgl. der A_Φ Diagonalmatrix ist.

Satz 4.12. Für $\Phi \in \mathrm{End}(V)$ sind äquivalent:

(i) Φ ist diagonalisierbar

(ii) V besitzt eine Basis aus Eigenvektoren von Φ

(iii) V ist die direkte Summe der Eigenräume E_{c_i}

(iv) $\sum_{\text{Eigenwerte } c_i} \dim E_{c_i} = n$

Vorlesung: 2005-04-20

Beweis: Sei $\Phi \in \mathrm{End}(V)$, $\dim V = n$.

(i) $\Rightarrow$ (ii): Φ sei diagonalisierbar, d.h. es existiert eine Basis $B = (x_1, \ldots, x_n)$ von V bzgl. der A_Φ Diagonalgestalt hat.

$$A_\Phi = \begin{pmatrix} c_1 & & 0 \\ & \ddots & \\ 0 & & c_n \end{pmatrix} \qquad c_i \in \mathbb{K}$$

$\Rightarrow$ $\Phi(x_i) = c_i x_i$ mit $i = 1, \ldots, n$

$\Rightarrow$ $x_1, \ldots, x_n$ Eigenvektoren von V.

(ii) $\Rightarrow$ (iii): Sei $x_1, \ldots, x_n$ Basis von V aus Eigenvektoren von Φ. Seien $c_1, \ldots, c_k$ die (verschiedenen) Eigenwerte von Φ und $E_{c_1}, \ldots, E_{c_k}$ die zugehörigen Eigenräume.

$\overset{\text{Satz 4.9}}{\Longrightarrow}$ Summe der Eigenräume ist direkt:

$$E_{c_1} \oplus \ldots \oplus E_{c_k} \subset V$$

Sei $x \in V \Rightarrow x = a_1 x_1 + \ldots + a_n x_n$, $a_i \in \mathbb{K}$ geeignet.

$\Rightarrow$ $x = v_1 + \ldots + v_k$, $v_i \in E_{c_i}$

$\Rightarrow$ $E_{c_1} \oplus \ldots \oplus E_{c_n} = V$

(iii) $\Rightarrow$ (iv): Aus $V = E_{c_1} \oplus \ldots \oplus E_{c_k}$ folgt

$$n = \dim V = \dim E_{c_1} + \ldots + E_{c_k}$$

(iv) $\Rightarrow$ (i): Sei $\sum_{i=1}^{k} \dim E_{c_i} = n$. Wähle Basis B_i in E_{c_i}.

$\overset{\text{Satz 4.9}}{\Longrightarrow}$ $B = B_1 \cup \ldots \cup B_k$ ist linear unabhängig.

Nun gilt

$$|B| = \sum_{i=1}^{k} \underbrace{|B_i|}_{\dim E_{c_i}} = n$$

$\Rightarrow$ B Basis von V.

Die Abbildungsmatrix A_Φ bzgl. B ist von der Form

$$A_\Phi = \begin{pmatrix} c_1 & & & & & & 0 \\ & \ddots & & & & & \\ & & c_1 & & & & \\ & & & \ddots & & & \\ & & & & c_k & & \\ & & & & & \ddots & \\ 0 & & & & & & c_k \end{pmatrix}$$

$\Rightarrow$ Φ ist diagonalisierbar.

□

Bemerkung:

(i) Satz 4.12 gilt analog auch für Matrizen $A \in \mathbb{K}^{n\times n}$

(ii) Ist $A \in \mathbb{K}^{n\times n}$ diagonalisierbar und $(v_1, \ldots, v_n)$, $v_i \in \mathbb{K}^n$ Basis aus Eigenvektoren von A, so gilt mit $S := (v_1 \cdots v_n) \in \mathbb{K}^{n\times n}$, dass

$$S^{-1}AS = \text{ Diagonalmatrix}$$

Korollar 4.13. Hat der Endomorphismus Φ (bzw. die Matrix A) n verschiedene Eigenwerte ($n = \dim V$, bzw. $A \in \mathbb{K}^{n\times n}$), dann ist Φ (bzw. A) diagonalisierbar.

Satz 4.14. Sei V ein n-dimensionaler $\mathbb{K}$-Vektorraum und $\Phi \in \mathrm{End}(V)$. Dann gilt:

Φ ist genau dann diagonalisierbar wenn das charakteristische Polyon p die Form

$$p = (-1)^n (X - c_1)^{r_1} \cdots (X - c_k)^{r_k} \tag{8}$$

mit $c_i \in \mathbb{K}$, $r_i \in \mathbb{N}$, c_i paarweise verschieden hat, und es gilt

$$\dim \mathrm{Bild}(\Phi - c_i \cdot \mathrm{id}_V) = n - r_i \qquad i = 1, \ldots, k \tag{9}$$

Bemerkung:

(i) Für (8) sagt man auch, dass p in *Linearfaktoren* zerfällt und nennt r_i die *Vielfachheit* (des Linearfaktors bzw. des Eigenwerts c_i)

(ii) (9) bedeutet, dass $\dim E_{c_i} = r_i$

(iii) Satz 4.14 gilt analog für Matrizen $A \in \mathbb{K}^{n\times n}$. Dann bedeutet (9)

$$\mathrm{Rang}(A - c_i \cdot E_n) = n - r_i$$

Beweis:

„ $\Rightarrow$ “: Φ diagonalisierbar, d.h. es existiert Basis so dass

$$A_\Phi = \begin{pmatrix} c_1 & & & & & & 0 \\ & \ddots & & & & & \\ & & c_1 & & & & \\ & & & \ddots & & & \\ & & & & c_k & & \\ & & & & & \ddots & \\ 0 & & & & & & c_k \end{pmatrix}$$

$$\Rightarrow\ p = \det \begin{pmatrix} c_1 - X & & & & & & 0 \\ & \ddots & & & & & \\ & & c_1 - X & & & & \\ & & & \ddots & & & \\ & & & & c_k - X & & \\ & & & & & \ddots & \\ 0 & & & & & & c_k - X \end{pmatrix} = (c_1 - X)^{r_1} \cdots (c_k - X)^{r_k}$$

„ $\Leftarrow$ “: Gelte (8) und (9). Aus (9) und (8) folgt, dass $\dim E_{c_i} = r_i$ mit $i = 1, \ldots, k$.
Wegen $\sum_{i=1}^k r_i = n$ folgt $\sum_{i=1}^k \dim E_{c_i} = n$.
Die Diagonalisierbarkeit folgt damit aus Satz 4.12.

□

Beispiel:

(i) $A = \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$, $\mathbb{K} = \mathbb{R}, \mathbb{C}, \mathbb{F}_2$.

- $\mathbb{K} = \mathbb{R}$ $\Rightarrow$ Keine Eigenwerte $\Rightarrow$ A nicht diagonalisierbar!
- $\mathbb{K} = \mathbb{F}_2$ $\Rightarrow$ Ein Eigenwert $c = 1$ mit $\dim E_c = 1$ $\Rightarrow$ A nicht diagonalisierbat!
- $\mathbb{K} = \mathbb{C}$ $\Rightarrow$ Zwei Eigenwerte $c_1 = i$ und $c_2 = -i$ $\Rightarrow$ A diagonalisierbar.

(ii) $A = \left(\begin{smallmatrix} 0 & -1 & 1 & 1 \\ -1 & 1 & -2 & 3 \\ 2 & -1 & 0 & 0 \\ 1 & -1 & 1 & 0 \end{smallmatrix}\right)$ $\Rightarrow$ $p = (1 + X)^2(1 - X)(2 - X)$

$E_{c_1} = [\begin{pmatrix} 0 \\ 1 \\ 1 \\ 0 \end{pmatrix}]$ $\Rightarrow$ A nicht diagonalisierbar.

(iii) Sei

$$A = \begin{pmatrix} 3 & 2 & -1 \\ 2 & 6 & -2 \\ 0 & 0 & 2 \end{pmatrix}$$

Das heißt

$$\begin{aligned} p &= \begin{vmatrix} 3 - X & 2 & -1 \\ 2 & 6 - X & -2 \\ 0 & 0 & 2 - X \end{vmatrix} \\ &= (2 - X) \begin{vmatrix} 3 - X & 2 \\ 2 & 6 - X \end{vmatrix} \\ &= (2 - X)(18 - 9X + X^2 - 4) \\ &= (2 - X)(2 - X)(7 - X) \\ &= (2 - X)^2(7 - X) \end{aligned}$$

$\Rightarrow$ $c_1 = 2$ mit $r_1 = 2$ und $c_2 = 7$ mit $r_2 = 1$

Rangbedingung:

$$\operatorname{Rang}\begin{pmatrix} 1 & 2 & -1 \\ 2 & 4 & -2 \\ 0 & 0 & 0 \end{pmatrix} = 1$$

$\Rightarrow$ A diagonalisierbar.

Transformationsmatrix S?

$$\left.\begin{array}{l} E_{c_1} = [\begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}, \begin{pmatrix} -2 \\ 1 \\ 0 \end{pmatrix}] \\ E_{c_2} = [\begin{pmatrix} 1 \\ 2 \\ 0 \end{pmatrix}] \end{array}\right\} S := \begin{pmatrix} 1 & -2 & 1 \\ 0 & 1 & 2 \\ 1 & 0 & 0 \end{pmatrix}$$

ergibt

$$S^{-1}AS = \begin{pmatrix} 2 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 7 \end{pmatrix}$$

§3 Der Satz von Cayley-Hamilton

Betrachte $\Phi \in \operatorname{End}(V)$ mit $\dim V = n$ und charakteristischem Polynom

$$p = a_0 + a_1 X + \ldots + a_{n-1}X^{n-1} + (-1)^n X^n$$

Wir setzen Φ in p ein:

$$p(\Phi) = a_0 \operatorname{id}_V + a_1\Phi + \ldots + a_{n-1}\Phi^{n-1} + (-1)^n\Phi^n \in \operatorname{End}(V)$$

Ziel: $p(\Phi) = 0$ (Nullabbildung)!

Vorlesung: 2005-04-27

Motivation: $\Phi \in \operatorname{End}(V)$ ($\dim V = n$) diagonalisierbar $\Leftrightarrow$ $V = \operatorname{Kern}(\Phi - c_1 \operatorname{id}_V) \oplus \ldots \oplus \operatorname{Kern}(\Phi - c_k \operatorname{id}_V)$.

Setze

$$m := (X - c_1) \cdots (X - c_k)$$

Wir „setzen Φ ein“:

$$m(\Phi) = (\Phi - c_1 \operatorname{id}_V) \circ \cdots \circ (\Phi - c_k \operatorname{id}_V) \in \operatorname{End}(V)$$

Behauptung: $m(\Phi) = 0$.

Beweis:

Einschub. Es gilt für $c, \widetilde{c} \in \mathbb{K}$

$$\begin{aligned}(\Phi - c\operatorname{id}_V) \circ (\Phi - \widetilde{c}\operatorname{id}_V) &= \Phi^2 - (c + \widetilde{c})\Phi + c\widetilde{c}\operatorname{id}_V \\ &= (\Phi - \widetilde{c}\operatorname{id}_V) \circ (\Phi - c\operatorname{id}_V)\end{aligned}$$

Sei $x \in V$ $\Rightarrow$ $x = x_1 + \ldots + x_k$ für $x_i \in E_{c_i}$, $i = 1, \ldots, k$.

$$\Rightarrow\ m(\Phi)(x) = (\Phi - c_1 \operatorname{id}_V) \circ \ldots \circ (\Phi - c_k \operatorname{id}_V)(x_1 + \ldots + x_k)$$

$$\Rightarrow\ \sum_{i=1}^{k} (\Phi - c_1 \operatorname{id}_V) \circ \ldots \circ (\underbrace{\Phi - c_i \operatorname{id}_V}_{=0})(x_i) = 0$$

□

Frage: Gibt es immer ein solches Polynom m ($\neq 0$) mit $m(\Phi) = 0$? (Minimalpolynom)

Einsetzungshomomorphismus: Sei

$$q := a_0 + a_1 X + \ldots + a_m X^m \in \mathbb{K}[X]$$

und $\Phi \in \mathrm{End}(V)$ (bzw. $A^{n\times n}$). Dann ist

$$q(\Phi) = a_0 \,\mathrm{id}_V + a_1\Phi + \ldots + a_m\Phi^m \in \mathrm{End}(V)$$

bzw.

$$q(A) = a_0 E_n + a_1 A + \ldots + a_m A^m \in \mathbb{K}^{n\times n}$$

Für festes Φ ist die Abbildung

$$f_\Phi : \mathbb{K}[X] \underset{q\mapsto q(\Phi)}{\to} \mathrm{End}(V)$$

ein Homomorphismus bezüglich der Ring– und der Vektorraum-Strukturen von $\mathbb{K}[X]$ bzw. $\mathrm{End}(V)$:

$$(q + \widetilde{q})(\Phi) = q(\Phi) + \widetilde{q}(\Phi) \tag{10}$$
$$(q \cdot \widetilde{q})(\Phi) = q(\Phi) \cdot \widetilde{q}(\Phi) \tag{11}$$
$$(a \cdot q)(\Phi) = a \cdot q(\Phi) \tag{12}$$

mit $q, \widetilde{q} \in \mathbb{K}[X]$, $a \in \mathbb{K}$.

Beweis: (10) und (12): klar.

$\Rightarrow$ f_Φ linear $\Rightarrow$ Es genügt (11) auf Basis $(1, X, X^2, \ldots)$ zu überprüfen, d.h.

$$\begin{aligned}(\underbrace{X^i}_{=X^{i+k}} \cdot X^k)(\Phi) &= \Phi^{i+k} \\ &= \Phi^i \circ \Phi^k \\ &= X^i(\Phi) \circ X^k(\Phi)\end{aligned}$$

□

Bemerkung: $f_\Phi(\mathbb{K}[X])$ ist ein Unterring (UR) von $\underbrace{\mathrm{End}(V)}_{\text{nicht kommutativ}}$ der kommutativ ist.

Satz 4.15 (Cayley-Hamilton)**.** Sei $\Phi \in \mathrm{End}(V)$, $\dim V = n$ und p das charakteristische Polynom von Φ, dann gilt

$$p(\Phi) = 0 \quad \text{(Nullpolynom)}$$

Beweis: Zu zeigen ist $p(\Phi)(v) = 0$ für alle $v \in V$.

Für $v = 0$ ist dies trivial.

Sei $v \neq 0$: Betrachte

$$\underbrace{v}_{\Phi^0(v)}, \Phi(v), \Phi^2(v), \ldots, \Phi^m(v)$$

$\Rightarrow$ Es existiert ein m so, dass gilt

$v, \Phi(v), \ldots, \Phi^m(v)$ linear abhängig

$v, \Phi(v), \ldots, \Phi^{m-1}(v)$ linear unabhängig

Daraus folgt

$$\Rightarrow \Phi^m(v) = a_0 v + a_1\Phi(v) + \ldots + a_{m-1}\Phi^{m-1}(v) \qquad \text{mit } a_i \in \mathbb{K}$$

Setze

$$q := a_0 + a_1 X + \ldots + a_{m-1}X^{m-1} + (-1)X^m \in \mathbb{K}[X]$$

Betrachte

$$\begin{aligned} & U := [v, \Phi(v), \ldots, \Phi^{m-1}(v)] \\ \Rightarrow\ & \Phi^m(v) \in U \\ \Rightarrow\ & \widetilde{\Phi} := \Phi|_U \text{ ist in } \operatorname{End}(U) \end{aligned}$$

Abbildungsmatrix von $\widetilde{\Phi}$ bezüglich Basis $(v, \Phi(v), \ldots, \Phi^{m-1}(v))$:

$$\widetilde{A} = A_{\widetilde{\Phi}} = \begin{pmatrix} 0 & 0 & \cdots & 0 & a_0 \\ 1 & 0 & \cdots & 0 & a_1 \\ 0 & 1 & \ddots & 0 & a_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & a_{m-1} \end{pmatrix}$$

Charakteristisches Polynom $\widetilde{p}$ von $\widetilde{\Phi}$:

$$\begin{aligned} \widetilde{p} &= \begin{vmatrix} -X & 0 & \cdots & \cdots & 0 & a_0 \\ 1 & -X & \cdots & \cdots & 0 & a_1 \\ 0 & 1 & \ddots & & 0 & a_2 \\ \vdots & \vdots & \ddots & \ddots & \vdots & \vdots \\ 0 & 0 & & \ddots & -X & a_{m-2} \\ 0 & 0 & \cdots & \cdots & 1 & a_{m-1} - X \end{vmatrix} \begin{matrix} \\ \\ \\ \\ \longleftarrow + \\ \longleftarrow + \ |X \\ |X \end{matrix} \\ &= \begin{vmatrix} 0 & \cdots & 0 & 0 & 0 & a_0 + a_1X + \ldots + a_{m-1}X^{m-1} - X^m \\ 1 & \cdots & 0 & 0 & 0 & a_1 + a_2X + \ldots + a_{m-2}X^{m-2} - X^{m-1} \\ \vdots & \ddots & \vdots & \vdots & \vdots & \vdots \\ 0 & \cdots & 1 & 0 & 0 & a_{m-3} + a_{m-2}X + a_{m-1}X^2 - X^3 \\ 0 & \cdots & 0 & 1 & 0 & a_{m-2} + a_{m-1}X - X^2 \\ 0 & \cdots & 0 & 0 & 1 & a_{m-1} - X \end{vmatrix} \\ &= (-1)^{m+1} q \end{aligned}$$

Ergänze $v, \Phi(v), \ldots, \Phi^m(v)$ zu Basis von V und betrachte zugehörige Abbildungsmatrix:

$$\begin{aligned} & A_\Phi = \begin{pmatrix} \widetilde{A} & C \\ 0 & D \end{pmatrix} \\ \Rightarrow\ & p = \widetilde{p} \cdot \overline{p} \text{ (wobei } \overline{p} \text{ char. Polynom von } D) \\ \Rightarrow\ & p(\Phi) = \widetilde{p}(\Phi) \circ \overline{p}(\Phi) = \overline{p}(\Phi) \circ \widetilde{p}(\Phi) \\ \Rightarrow\ & p(\Phi)(v) = \overline{p}(\Phi)(\widetilde{p}(\Phi)(v)) = (-1)^{m+1} \cdot \overline{p}(\Phi)(q(\Phi)(v)) = (-1)^{m+1}\overline{p}(\Phi)(0) = 0 \\ \Rightarrow\ & p(\Phi) = 0 \end{aligned}$$

□

Bemerkung und Definition:

(i) Satz 4.15 gilt analog für Matrizen $A \in \mathbb{K}^{n\times n}$

(ii) Man kann einfacher zeigen, dass immer ein $q \in \mathbb{K}[X]$ existiert mit $q(\Phi) = 0$, nämlich:
$id_V, \Phi, \Phi^2, \ldots, \Phi^{n^2}$ ($n^2 + 1$ Endomorphismen), $\dim V = n^2$.
$\Rightarrow$ lineare Abhängigkeit, d.h.

$$a_0 \,\mathrm{id}_V + \ldots + a_{n^2} \Phi^{n^2} = 0$$

Setze

$$q = a_0 + a_1 X + \ldots + a_{n^2} X^{n^2}$$
$$\Rightarrow\ q(\Phi) = 0$$

(iii) Es existiert genau ein normiertes Polynom m vom kleinsten Grad, das $m(\Phi) = 0$ erfüllt. m heißt *Minimalpolynom* von Φ ($\Rightarrow\ \mathrm{Grad}\, m \geq 1$).
Eindeutigkeit:

$$m, \widetilde{m} \text{ Minimalpolynome von } \Phi$$
$$\Rightarrow\ m(\Phi) = \widetilde{m}(\Phi) = 0$$
$$\Rightarrow\ (\underbrace{m - \widetilde{m}}_{\mathrm{Grad} < k})(\Phi) = 0$$
$$\Rightarrow\ \mathrm{Grad}\, m - \mathrm{Grad}\, \widetilde{m} = k$$
$$\Rightarrow\ m - \widetilde{m} = 0$$

Vorlesung: 2005-05-04

Satz 4.16. Das Minimalpolynom m teilt jedes annullierende Polynom von Φ, d.h. jedes $q \in \mathbb{K}[X]$, das $q(\Phi) = 0$ erfüllt.

Beweis: Division mit Rest ergibt

$$q = s \cdot m + r \qquad s, r \in \mathbb{K}[X]$$

mit $\mathrm{Grad}\, r < \mathrm{Grad}\, m$

$$\Rightarrow\ r(\Phi) = \underbrace{q(\Phi)}_{0} - \underbrace{s(\Phi) \cdot m(\Phi)}_{0} = 0$$

$\Rightarrow\ r = 0\ \Rightarrow$ Behauptung. □

Korollar 4.17.

(i) m teilt p

(ii) Die Nullstellen von m sind gerade die Nullstellen von p, also die Eigenwerte von Φ.

Beweis:

(i) klar.

(ii) Ist $m(c) = 0 \overset{\text{(i)}}{\Rightarrow} p(c) = 0$, also c Eigenwert.
Ist umgekehrt c Eigenwert, also $p(c) = 0$, so existiert $x \neq 0$ mit $\Phi(x) = cx$

$$\Rightarrow\ \Phi^i(x) = c^i x\ \Rightarrow\ \underbrace{m(\underbrace{\Phi}_{0})x}_{0} = m(c)x$$

□

Bemerkung:

(i) Gilt $p = (-1)^n (X - c_1)^{r_1} \cdots (X - c_k)^{r_k}$, c paarweise verschieden, dann folgt

$$m = (X - c_1)^{s_1} \cdots (X - c_k)^{s_k} \qquad 1 \leq s_i \leq r_i$$

(ii) Ist Φ diagonalisierbar, so gilt sogar

$$m = (X - c_1) \cdots (X - c_k)$$

(Umkehrung wird später bewiesen)

Beispiel:

(i) E_n. Wie sieht m aus?

$$p = \det \begin{pmatrix} 1 - X & & 0 \\ & \ddots & \\ 0 & & 1 - X \end{pmatrix} = (1 - X)^n$$

$\Rightarrow \; m = X - 1$

(ii) $A = 0 \; \Rightarrow \; p = (-X)^n$ und $m = X$.

(iii) Sei

$$A = \begin{pmatrix} 7 & -6 & 11 \\ 0 & 1 & -1 \\ -4 & 4 & -7 \end{pmatrix}$$

$\Rightarrow \; p = -(X - 1)^2 (X + 1)$

$\Rightarrow \; m = (X - 1)^s (X + 1)$ mit $s \in \{1, 2\}$

Test: Für $s = 1$ gilt

$$(A - E_n)(A + E_n) = \begin{pmatrix} 6 & -6 & 11 \\ 0 & 0 & -1 \\ -4 & 4 & -8 \end{pmatrix} \cdot \begin{pmatrix} 8 & -6 & 11 \\ 0 & 2 & -1 \\ -4 & 4 & -6 \end{pmatrix} \neq 0$$

$\Rightarrow \; s = 2$, d.h. $m = -p$.

§4 Die Jordansche Normalform

Generelle Voraussetzungen: $\Phi \in \mathrm{End}(V)$, $\dim V = n$

$$p = (-1)^n (X - c_1)^{r_1} \cdots (X - c_k)^{r_k}$$

Definition 4.5.

$$H_{c_i} := \mathrm{Kern}(\Phi - c_i \, \mathrm{id}_V)^{r_i}$$

heißt *Hauptraum* zum Eigenwert c_i, $i = 1, \ldots, k$.

Bemerkung: H_{c_i} ist Φ-invariant. Das heißt

$$\Phi(H_{c_i}) \subset H_{c_i}$$

$x \in H_{c_i}$, $\Phi(x) \in H_{c_i}$

$$(\Phi - c_i \operatorname{id}_V)^{r_i}(\Phi(x)) = \Phi((\Phi - c_i \operatorname{id}_V)^{r_i}(x)) = 0$$

Es ist

$$m = (X - c_1)^{s_1} \cdots (X - c_k)^{s_k} \qquad 1 \le s_i \le r_i$$

Definition 4.6. Die Potenz s_i im Minimalpolynom heißt *Index* des Hauptraums zum Eigenwert c_i.

Satz 4.18 (Ersetzt Sätze 18 und 20 des Skripts)**.** Es gilt

$$V = H_{c_1} \oplus \ldots \oplus H_{c_k}$$

Weiter ist

$$H_{c_i} = \operatorname{Kern}(\Phi - c_i \operatorname{id}_V)^{s_i} \qquad i = 1, \ldots, k$$

Schließlich ist s_i die kleinste Zahl $s \in \{1, 2, \ldots\}$, für die gilt

$$\operatorname{Kern}(\Phi - c_i \operatorname{id}_V)^{s} = \operatorname{Kern}(\Phi - c_i \operatorname{id}_V)^{s+1}$$

Beweis: Wir beweisen nur den Fall $k = 2$. Also

$$p = (-1)^n (X - c_1)^{r_1} (X - c_2)^{r_2} \qquad c_1 \neq c_2$$

$(X - c_1)^{r_1}$, $(X - c_2)^{r_2}$ teilerfremd

$\overset{1.17}{\Rightarrow}$ $\exists q, s \in \mathbb{K}[X]$ mit

$$q \cdot (X - c_1)^{r_1} + s \cdot (X - c_2)^{r_2} = 1$$

$\Rightarrow$ Für jedes $x \in V$ gilt

$$x = \underbrace{q(\Phi) \circ (\Phi - c_1 \operatorname{id}_V)^{r_1}(x)}_{y} + \underbrace{q(\Phi) \circ (\Phi - c_2 \operatorname{id}_V)^{r_2}(x)}_{z}$$

Behauptung: $y \in H_{c_2}$

$$(\Phi - c_2 \operatorname{id}_V)^{r_2}(y) = (-1)^n q(\Phi) \cdot \underbrace{p(\Phi)}_{0}(x)$$
$$= 0$$

Analog folgt $z \in H_{c_1}$

$$\Rightarrow V = H_{c_1} + H_{c_2}$$

Sei $x \in H_{c_1} \cap H_{c_2} \Rightarrow y = z = 0 \Rightarrow x = 0$

$$\Rightarrow V = H_{c_1} \oplus H_{c_2}$$

Weil $(X-c_1)^{s_1}$, $(X-c_2)^{s_2}$ teilerfremd sind und

$$m(\Phi) = (\Phi - c_1 \operatorname{id}_V)^{s_1} \circ (\Phi - c_2 \operatorname{id}_V)^{s_2} = 0$$

folgt analog

$$V = \operatorname{Kern}(\Phi - c_1 \operatorname{id}_V)^{s_1} \oplus \operatorname{Kern}(\Phi - c_2 \operatorname{id}_V)^{s_2}$$

Nun gilt

$$\operatorname{Kern}(\Phi - c_i \operatorname{id}_V)^{s_i} \subset \operatorname{Kern}(\Phi - c_2 \operatorname{id}_V)^{r_i}$$

Sei $x \in \operatorname{Kern}(\Phi - c_i \operatorname{id}_V)^{s_i}$. Betrachte

$$\begin{aligned}(\Phi - c_i \operatorname{id}_V)^{r_i}(x) &= (\Phi - c_i \operatorname{id}_V)^{r_i - s_i} \circ \underbrace{(\Phi - c_i \operatorname{id}_V)^{s_i}}_{=0}(x) \\ &= 0\end{aligned}$$

$$\Rightarrow \operatorname{Kern}(\Phi - c_i \operatorname{id}_V)^{s_i} = \operatorname{Kern}(\Phi - c_i \operatorname{id}_V)^{r_i}$$

Schließlich ist

$$\begin{aligned}H_{c_i} &= \operatorname{Kern}(\Phi - c_i \operatorname{id}_V)^{s_i} \\ &= \operatorname{Kern}(\Phi - c_i \operatorname{id}_V)^{s_i+1}\end{aligned}$$

denn analog wie oben gilt

$$V = \operatorname{Kern}(\Phi - c_i \operatorname{id}_V)^{s_i+1} \oplus H_{c_2}$$

mit $\operatorname{Kern}(\Phi - c_1 \operatorname{id}_V)^{s} = \operatorname{Kern}(\Phi - c_1 \operatorname{id}_V)^{s+1}$.

Sei s die kleinste derartige Zahl. Angenommen $1 \leq s < 1$. Dann folgt

$$\operatorname{Kern}(\Phi - c_1 \operatorname{id}_V)^{s} = \operatorname{Kern}(\Phi - c_1 \operatorname{id}_V)^{s_1} = H_{c_1}$$

$\widetilde{m} = (X-c_1)^s \cdot (X-c_2)^{s_2}$ ist annulierend, also $\widetilde{m(\Phi)} = 0$

Widerspruch zu Minimalpolynom! □

Vorlesung: 2005-05-11

Ergänzung zum Beweis von Satz 4.18:

Angenommen es existiert s mit $1 \leq s \leq s_1$, das

$$\begin{aligned}\operatorname{Kern}(\Phi - c_1 \operatorname{id}_V)^{s} &= \operatorname{Kern}(\Phi - c_1 \operatorname{id}_V)^{s+1} \\ &= \operatorname{Kern}(\Phi - c_1 \operatorname{id}_V)^{s+2} \\ &= \dots \\ &= \operatorname{Kern}(\Phi - c_1 \operatorname{id}_V)^{s_1}\end{aligned}$$

erfüllt.

$$\Rightarrow V = \operatorname{Kern}(\Phi - c_1 \operatorname{id}_V)^{s} \oplus H_{c_2}$$

D.h. jedes $x \in V$ hat Zerlegung $x = x_1 + x_2$ mit $x_1 \in \operatorname{Kern}(\Phi - c_1 \operatorname{id}_V)^s$ und $x_2 \in H_{c_2}$.

Jetzt $\widetilde{m} := (X-c_1)^s (X-c_2)^{s_2}$

$$\Rightarrow \widetilde{m}(\Phi)(x) = (\Phi - c_1 \operatorname{id}_V)^s = (\Phi - c_2 \operatorname{id}_V)^{s_2}(x_1 + x_2) = 0$$

$\Rightarrow \widetilde{m}(\Phi) = 0$ (Nullabbildung). Wegen $\operatorname{Grad}(\widetilde{m}) = s + s_2 < s_1 + s_2 = \operatorname{Grad}(m)$ ist dies ein Widerspruch.

Satz 4.19. Sei $\Phi \in \mathrm{End}(V)$ mit Minimalpolynom m und p zerfalle in Linearfaktoren

$$p = (-1)^k (X - c_1)^{r_1} \cdots (X - c_k)^{r_k}$$

Dann gilt:

$$\Phi \text{ diagonalisierbar} \quad \Leftrightarrow \quad m = (X - c_1) \cdots (X - c_k)$$

Das heißt: $s_1 = \ldots = s_k = 1$.

Beweis:

$\Rightarrow$: klar

$\Leftarrow$: Nach Satz 4.18 gilt: $V = H_{c_1} \oplus \ldots \oplus H_{c_k}$ mit $H_{c_i} = \underbrace{\mathrm{Kern}(\Phi - c_i \,\mathrm{id}_V)^{s_i}}_{E_{c_i}}$.

Nach Satz 4.12 ist Φ diagonalisierbar.

□

Bemerkung:

(i) Die Sätze 4.18 und 4.19 gelten analog für Matrizen $A \in \mathbb{K}^{n \times n}$

(ii) Der Index s des Hauptraums H_c erfüllt auch die folgenden Bedingungen:

- s ist die kleinste Zahl mit
$$\dim \mathrm{Kern}(\Phi - c\,\mathrm{id}_V)^s = \dim \mathrm{Kern}(\Phi - c\,\mathrm{id}_V)^{s+1}$$
- s ist die kleinste Zahl mit
$$\dim \mathrm{Bild}(\Phi - c\,\mathrm{id}_V)^s = \dim \mathrm{Bild}(\Phi - c\,\mathrm{id}_V)^{s+1}$$
- s ist die kleinste Zahl mit
$$\mathrm{Rang}(A_\Phi - cE_n)^s = \mathrm{Rang}(A_\Phi - cE_n)^{s+1}$$

(iii) Falls es nur einen Eigenwert c gibt, also
$$p = (-1)^n (X - c)^n$$
gilt, ist der Index s die kleinste Zahl s mit
$$(A_\Phi - cE_n)^s = 0$$
Aber nur dann!

Beispiel: Sei

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

Dann folgt

$$\begin{aligned} p &= (X-1)(X+3) \begin{vmatrix} -4-X & 1 \\ -1 & -2-X \end{vmatrix} \\ &= (X-1)(X+3)(X+3)^2 \\ &= (X-1)(X+3)^3 \end{aligned}$$

$\Rightarrow\ m = (X+3)^s(X-1)$ mit $1 \le s \le 3$.

$$A + 3E_4 : \begin{pmatrix} -1 & 1 & 0 & 1 \\ -1 & 1 & 0 & 1 \\ 0 & 0 & 4 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \Rightarrow \text{Rang } 2 \quad (\Rightarrow \dim E_c = 2)$$

$$(A + 3_E 4)^2 : \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 16 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \Rightarrow \text{Rang } 1$$

$$(A + 3_E 4)^3 : \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 64 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \Rightarrow \text{Rang } 1$$

$\Rightarrow\ s = 2\ \Rightarrow\ H_{c_1} = [\begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}]$

$\Rightarrow\ H_{c_2} = E_{c_2} = [\begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}]$ und $E_{c_1} = [\begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \end{pmatrix}]$

Sei

$$p = (-1)(X - c_1)^{r_1} \cdots (X - c_k)^{r_k}$$

$\Rightarrow\ V = H_{c_1} \oplus \ldots \oplus H_{c_k}$. Wähle Basis B_i in jedem H_{c_i}

$$\Rightarrow\ A_\Phi = \begin{pmatrix} \boxed{A_{c_1}} & & 0 \\ & \ddots & \\ 0 & & \boxed{A_{c_k}} \end{pmatrix}$$

Ziel: Finde B_i so, dass A_{c_i} besonders einfach wird.

Wir betrachten nun H_c mit c Eigenwert.

Setze

$$U_0 := \{o\},\ U_i := \text{Kern}(\Phi - c\,\text{id}_V)^i \quad i = 1, \ldots, s$$

$\Rightarrow\ U_0 = \{o\} \subsetneqq U_1 \subsetneqq \ldots \subsetneqq U_s = H_c\ (s \ge q)$

Zerlegung:

$$\begin{aligned} H_c = U_s &= U_{s-1} \oplus W_1 && \dim W_1 = q_1 \ge 1 \\ U_{s-1} &= U_{s-2} \oplus W_2 && \dim W_2 = q_2 \ge 1 \\ &\vdots \\ U_2 &= E_c \oplus W_{s-1} && \dim W_{s-1} = q_{s-1} \ge 1 \\ &E_c && \dim E_c = q_s = q \ge 1 \end{aligned}$$

$\Rightarrow\ H_c = W_1 \oplus \ldots \oplus W_{s-1} \oplus E_c$.

Wahl der Ergänzungsräume W_i:

W_1 belibig, Basis $B_1 = (x_1^{(1)}, \ldots, x_{q_1}^{(1)})$

Setze $x_i^{(2)} := (\Phi - c\,\text{id}_V)(x_i^{(1)})$ mit $i = 1, \ldots, q_1$.

Behauptung:

(i) $[x_1^{(2)}, \ldots, x_{q_1}^{(2)}] \subset U_{s-1}$

(ii) $[x_1^{(2)}, \ldots, x_{q_1}^{(2)}] \cap U_{s-1} = \{o\}$

(iii) $x_1^{(2)}, \ldots, x_{q_1}^{(2)}$ linear unabhängig

Beweis:

(i) $(\Phi - c\,\mathrm{id}_V)^{s-1}(x_i^{(2)}) = (\Phi - c\,\mathrm{id}_V)^s(\underbrace{x_i^{(1)}}_{\in H_c}) = 0$

(ii) Sei $a_1x_1^{(2)} + \ldots + a_{q_1}x_{q_1}^{(2)} \in U_{s-2}$

$$\begin{aligned}
&\Rightarrow\ (\Phi - c\,\mathrm{id}_V)^{s-1}(\sum_{i=1}^{q_1} a_i x_i^{(1)}) = 0\\
&\Rightarrow\ \sum a_i x_i^{(1)} \in U_{s-1} \cap W_1 = \{o\}\\
&\Rightarrow\ \sum a_i x_i^{(1)} = 0\\
&\Rightarrow\ \sum a_i x_i^{(2)} = 0
\end{aligned}$$

(iii) Sei $a_1x_1^{(2)} + \ldots + a_{q_1}x_{q_1}^{(2)} = 0$

$$\begin{aligned}
&\Rightarrow\ \underbrace{a_1x_1^{(1)} + \ldots + a_{q_1}x_{q_1}^{(1)}}_{\in W_1} \in E_c \subset U_{s-1}\\
&\Rightarrow\ a_1x_1^{(1)} + \ldots + a_{q_1}x_{q_1}^{(1)} = 0\\
&\Rightarrow\ a_1 = \ldots = a_{q_1} = 0 \quad \text{(Weil } x_i^{(1)} \text{ Basisvektoren)}
\end{aligned}$$

□

Wir wählen nun den Raum W_2 so, dass er $x_1^{(1)}, \ldots, x_{q_1}^{(1)}$ enthält und ergänzen diese zu einer Basis von W_2:

$$x_1^{(2)}, \ldots, x_{q_1}^{(2)}, x_{q_1+1}^{(2)}, \ldots, x_{q_2}^{(2)} \quad q_2 \geq q_1$$

Analog setzen wir nun $x_i^{(3)} := (\Phi - c\,\mathrm{id}_V)(x_i^{(2)})$ mit $i = 1, \ldots, q_2$ und erhalten die entsprechende Behauptung wie oben.

Allgemein: $x_i^{(j)} := (\Phi - c\,\mathrm{id}_V)(x_i^{(j-1)})$ mit $i = 1, \ldots, q_1$ und $j = 2, \ldots, s$.

Damit gilt

$$\begin{array}{lll}
(W_1) & B_1: & x_1^{(1)}, \ldots, x_{q_1}^{(1)}\\
(W_2) & B_2: & x_1^{(2)}, \ldots, x_{q_1}^{(2)}, x_{q_1+1}^{(2)}, \ldots, x_{q_2}^{(2)}\\
\vdots & \vdots & \\
(W_{s_1}) & B_{s-1}: & x_1^{(s-1)}, \ldots, x_{q_1}^{(s-1)}, x_{q_1+1}^{(s-1)}, \ldots, x_{q_2}^{(s-1)}, \ldots, x_{q_{s-2}}^{(s-1)}, x_{q_{s-2}+1}^{(s-1)}, \ldots, x_{q_{s-1}}^{(s-1)}\\
(E_c) & B_s: & x_1^{(s)}, \ldots, x_{q_1}^{(s)}, x_{q_1+1}^{(s)}, \ldots, x_{q_2}^{(s)}, \ldots, x_{q_{s-1}}^{(s)}, x_{q_{s-1}+1}^{(s)}, \ldots, x_{q_s}^{(s)}
\end{array}$$

$B = \bigcup_{i=1}^{s} B_i$.

Vorlesung: 2005-05-18

Anm. des Autors. *Diese Vorlesung wurde von Herr Hoffmann gehalten.*

Sei nun B die geordnete Basis von H_c gegebn durch

$$B = (x_1^{(1)}, \ldots, x_1^{(s)}, x_2^{(1)}, \ldots, x_2^{(s)}, \ldots, x_{q_1}^{(1)}, \ldots, x_{q_1}^{(s)}, x_{q_1+1}^{(2)}, \ldots, x_{q_1+1}^{(s)}, \ldots, x_{q_2}^{(2)}, \ldots, x_{q_2}^{(s)}, x_{q_2+1}^{(3)}, \ldots)$$

Dann gilt für $j = 1, \ldots, s-1$ und entsprechende i

$$(\Phi - c\,\mathrm{id}_V)(x_i^{(j)}) = x_i^{(j+1)}$$

also

$$\Phi(x_i^{(j)}) = cx_i^{(j)} + x_i^{(j+1)}$$

und für $j = s$, $i = 1, \ldots, q$ gilt

$$\Phi(x_i^{(s)}) = cx_i^{(s)}$$

Insgesamt hat A_c die Form

$$A_c = \begin{pmatrix} \boxed{A_1} & & 0 \\ & \ddots & \\ 0 & & \boxed{A_q} \end{pmatrix}$$

mit

$$A_i = \begin{pmatrix} c & & & 0 \\ 1 & \ddots & & \\ & \ddots & \ddots & \\ 0 & & 1 & c \end{pmatrix} \qquad \text{für } i = 1, \ldots, q$$

Wir nennen diese A_i in der Regel *Jordankästchen* (zum Eigenwert c) und A_c heißt *Jordanblock* (zum Eigenwert c).

Die Jordankästchen A_i haben eine Zeilenzahl (Länge) zwischen 1 und s. Dabei treten

- q_1 Kästchen der Länge s
- $q_2 - q_1$ Kästchen der Länge $s - 1$
- $\ldots$
- $q - q_{s-q}$ Kästchen der Länge 1

auf.

Insgesamt gibt es im Jordanblock A_c genau $q = \dim E_c$ Jordankästchen.

Nutzt man den obigen Zusammenhang aus, so erkennt man, dass die Anzahl der Kästchen der Länge l auch gegeben ist durch

$$\begin{aligned} & q_{s-l+1} - q_{s-l} \\ &= \dim W_{s-l+1} - \dim W_{s-l} \\ &= \dim U_l - \dim U_{l-1} - \dim U_{l+1} + \dim U_l \\ &= 2\dim \operatorname{Kern}(\Phi - c\,\mathrm{id}_V)^l - \dim \operatorname{Kern}(\Phi - c\,\mathrm{id}_V)^{l+1} - \dim \operatorname{Kern}(\Phi - c\,\mathrm{id}_V)^{l-1} \\ &= \underbrace{\left(\dim \operatorname{Kern}(\Phi - c\,\mathrm{id}_V)^l - \dim \operatorname{Kern}(\Phi - c\,\mathrm{id}_V)^{l-1}\right)}_{\text{Anzahl der Kästchen der Länge} \geq l} \\ &\quad - \underbrace{\left(\dim \operatorname{Kern}(\Phi - c\,\mathrm{id}_V)^{l+1} - \dim \operatorname{Kern}(\Phi - c\,\mathrm{id}_V)^l\right)}_{\text{Anzahl der Kästchen der Länge} \geq l+1} \end{aligned}$$

Wir haben für den Hauptraum H_c eine Basis gefunden, so dass die zugehörige Abbildungsmatrix A_c eine einfache Form hat.

Außerdem gilt

$$V = H_{c_1} \oplus \ldots \oplus H_{c_k}$$

Also können wir die Jordanblöcke $A_{c_1}, \ldots, A_{c_k}$ zur Jordanschen Normalform A_Φ von Φ zusammensetzen.

Der Jordanblock A_{c_i} besteht aus genau $t_i = \dim H_{c_i}$ Spalten. Das charakteristische Polynom der Matrix A_{c_i} ist $(c_i - \lambda)^{t_i}$.

Für das charakteristische Polynom p von Φ gilt dass

$$\begin{aligned} p &= (-1)^n \cdot (X - c_1)^{r_1} \cdots (X - c_k)^{r_k} \\ &= (-1) \cdot (X - c_1)^{r_1} \cdots (X - c_k)^{r_k} \end{aligned}$$

Also gilt $r_i = \dim H_{c_i}$ für $i = 1, \ldots, k$.

Satz 4.21 (Jordansche Normalform)**.** Sei V ein n-dimensionaler $\mathbb{K}$-Vektorraum, $\Phi : V \to V$ ein Endomorphismus mit dem charakteristischen Polynom

$$p := (-1)^n \cdot (X - c_1)^{r_1} \cdots (X - c_k)^{r_k}$$

wobei $c_1, \ldots, c_k \in \mathbb{K}$ paarweise verschieden und dem Minimalpolynom

$$m = (X - c_1)^{s_1} \cdots (X - c_k)^{s_k}$$

Dann gibt es eine geordnete Basis B von V bezüglich der die Abbildungsmatrix A_Φ von Φ die Form

$$A_\Phi = \begin{pmatrix} \boxed{A_{c_1}} & & 0 \\ & \ddots & \\ 0 & & \boxed{A_{c_k}} \end{pmatrix}$$

mit Jordanblöcken A_{c_i} zu den Eigenwerten c_i,

$$A_{c_i} = \begin{pmatrix} \boxed{\begin{matrix} c_i & & & \\ 1 & \ddots & & \\ & \ddots & \ddots & \\ & & 1 & c_i \end{matrix}} & & & \\ & \ddots & & \\ & & \ddots & \\ & & & \boxed{c_i} \end{pmatrix}$$

Der Jordanblock A_{c_i} hat die Länge r_i, $i = 1, \ldots, k$. Innerhalb des Jordanblocks A_{c_i} gibt es

$$2 \dim \operatorname{Kern}(\Phi - c_i \operatorname{id}_V)^l - \dim \operatorname{Kern}(\Phi - c_i \operatorname{id}_V)^{l+1} - \dim \operatorname{Kern}(\Phi - c_i \operatorname{id}_V)^{l-1}$$

Jordankästchen der Länge l, $l = 1, \ldots, s_i$.

Im Jordanblock A_{c_i} treten insgesamt $\dim E_{c_i}$ Jordankästchen auf. Es gibt mindestens ein Kästchen der Maximallänge s_i.

Ist $A \in \mathbb{K}^{n \times n}$ eine Matrix, dessen charakteristisches Polynom von der Form

$$p = (-1)^n \cdot (X - c_1)^{r_1} \cdots (X - c_k)^{r_k}$$

ist, so gilt für die lineare Abbildung

$$\begin{aligned} \Phi : \mathbb{K}^n &\to \mathbb{K}^n \\ v &\mapsto Av \end{aligned}$$

der Satz 4.21. $U_j^{(i)}$ ist dann der Lösungsraum des homogenen LGS $A - c_i E_n)$ und $H_c = U_j$ mit $E_c = U_1$.

Existiert die Jordansche Normalform von $B \in \mathbb{K}^{n \times n}$, so gilt

A, B ähnlich $\quad \Leftrightarrow \quad$ A, B haben dieselbe Jordansche Normalform

Beispiel: Sei

$$A = \begin{pmatrix} -4 & 1 & 0 & 1 \\ -1 & -2 & 9 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -3 \end{pmatrix} \in \mathbb{R}^{4\times 4}$$

$\Rightarrow\ p = (X-1)(X+3)^3$.

$$\widetilde{A} = \left(\begin{array}{|ccc|c} \hline -3 & 0 & 0 & 0 \\ ? & -3 & 0 & 0 \\ 0 & ? & -3 & 0 \\ \hline 0 & 0 & 0 & 1 \end{array}\right)$$

$H_{c_1} = E_{c_1} = [\begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}]$, $E_{c_2} = [\begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix}]$

$$\Rightarrow\ \widetilde{A} = \left(\begin{array}{|cc|c|c} \hline -3 & 0 & 0 & 0 \\ 1 & -3 & 0 & 0 \\ \hline 0 & 0 & -3 & 0 \\ \hline 0 & 0 & 0 & 1 \end{array}\right)$$

$$(A+3E_n)^2 = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 16 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

$\Rightarrow\ H_{c_2} = [\begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}]$

Gesucht $x_1 \in H_{c_2} \setminus E_{c_2}$, z.B. $x = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}$.

Nach Konstruktion:

$$x_2 = (A+3E_n)x_1 = \begin{pmatrix} -1 \\ -1 \\ 0 \\ 0 \end{pmatrix}$$

Nun suchen wir noch $x_3 \in E_{c_2}$ der linear unabhängig von x_1, x_2 ist. Z.B.

$$x_3 = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

Es fehlt noch $x_4 \in E_{c_1}$, z.B. $x_4 = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}$.

Also ist $B = (x_1, \ldots, x_4)$ Jordanbasis. Setzen wir

$$S = \begin{pmatrix} 1 & -1 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

so gilt

$$\widetilde{A} = S^{-1}AS$$

Vorlesung: 2005-05-25

5 Euklidische und Unitäre Vektorräume

Ab jetzt (meistens) relle Vektorräume V. Aber $\dim V$ beliebig!

§1 Skalarprodukte

Sei $\beta : V \times V \to \mathbb{R}$ eine *Bilinearform*, das heißt β ist in jeder der beiden Variablen linear.

- β heißt *symmetrisch*, wenn $\beta(x, y) = \beta(y, x)$ für alle $x, y \in V$ gilt.
- β heißt *positiv definit*, wenn $\beta(x, x) > 0$ für alle $x \neq 0$. ($\beta(0, 0) = 0$ gilt immer)

Definition 5.1. Eine symmetrische positiv definite Bilinearform β auf einem reellen Vektorraum V (also $\beta : V \times V \to \mathbb{R}$) heißt *Skalarprodukt* (auch *inneres Produkt*).

Schreibweise: $\langle x, y\rangle$ (statt $\beta(x, y)$; $x \cdot y$ bzw. xy manchmal in Büchern)

Das Paar $(V, \langle\cdot,\cdot\rangle)$ (bzw. V) heißt *euklidischer Vektorraum*.

Beispiel:

(i) $V = \mathbb{R}^n$ mit

$$\langle x, y\rangle := \sum_{i=0}^{n} x_i y_i = x^\top \cdot y \qquad x = (x_1, \ldots, x_n),\ y = (y_1, \ldots, y_n)$$

heißt *Standardskalarprodukt*.

(ii) $V = \mathbb{R}^2$, $\beta(x, y) = x_1y_1 - (x_1y_2 + x_2y_2) + 2x_2y_2$
Positiv definit weil $\beta(x, x) = x_1^2 - 2x_1x_2 + 2x_2^2 = (x_1 - x_2)^2 + x^2 > 0$ für $x \neq 0$.

(iii) $V = C([a, b])$, $f, g \in C([a, b])$

$$\langle f, g\rangle := \int_a^b f(t)g(t)s)t\ dt$$

ist Skalarprodukt (Wobei $s > 0$ eine feste Funktion ist).

Sei jetzt $(V, \langle\cdot,\cdot\rangle)$ ein Euklidischer Vektorraum

Definition 5.2.

(a) Sei $\|x\| := \sqrt{\langle\cdot,\cdot\rangle}$, $x \in V$.
$\|x\|$ heißt *Norm* von x (oder *Länge* von x)
Eigenschaften:

(i) $\|x\| \geq 0$ für alle $x \neq 0$ und $\|x\| = 0$ genau dann wenn $x = 0$.
(ii) $\|c \cdot x\| = |c| \cdot \|x\|$ für alle $c \in \mathbb{R}$, $x \in V$.
(iii) Minkowski-Ungleichung (siehe Satz 5.1).

(b) Sei $d(x, y) := \|x - y\|$, $x, y \in V$ (*Distanz*, *Länge*). Die Abbildung

$$\begin{array}{rccc} d: & V \times V & \to & \mathbb{R} \\ & (x, y) & \mapsto & d(x, y) \end{array}$$

heißt *Metrik*.
Eigenschaften:

(i) $d(x,y) \geq 0$ für alle $x \neq 0$ und $d(x,y) = 0$ für $x = y$.

(ii) $d(x,y) = d(y,x)$ für alle x, y.

(iii) Dreiecksungleichung (siehe Satz 5.1)

(c) $x, y \in V$ heißen *orthogonal* (zueinander) wenn $\langle x, y\rangle = 0$ gilt.
Schreibweise: $x \perp y$.

Für $A, B \subset V$ sei $A \perp B \Leftrightarrow x \perp y$ für alle $x \in A$, $y \in B$

Für $A \subset V$ sei

$$\begin{aligned} A^\perp :&= \{x \in V \mid \{x\} \perp A\} \\ &= \{x \in V \mid \{x\} \perp A\} \\ &= \{x \in V \mid \langle x, y\rangle = 0 \ \forall y \in A\} \end{aligned}$$

$A^\perp$ heißt *orthogonales Komplement* von A.

Eigenschaften:

(i) $A^\perp$ ist Untervektorraum von V

(ii) $A^\perp = [A]^\perp$

(iii) $A^\perp \cap [A] = \{o\}$

(iv) $(A^\perp)^\perp \supset [A]$ („=“ muss nicht gelten, wenn $\dim V = \infty$)

Satz 5.1. Sei V ein euklidischer Vektorraum und $x, y, z \in V$. Dann gilt

(i) $|\langle x, y\rangle| \leq \|x\| + \|y\|$ mit „=“ $\Leftrightarrow$ x, y linear unabhängig (Cauchy-Schwarzsche Ungleichung)

(ii) $\|x + y\| \leq \|x\| + \|y\|$ (Minkowski Ungleichung)

(iii) $d(x,y) \leq d(x,z) + d(z,y)$ (Dreiecksungleichung)

(iv) $\|x + y\|^2 + \|x - y\|^2 = 2\|x\|^2 + 2\|y\|^2$ (Parallelogramm-Identität)

(v) $4\langle x, y\rangle = \|x + y\|^2 - \|x - y\|^2$

(vi) $x \perp y \Leftrightarrow \|x + y\|^2 = \|x\|^2 + \|y\|^2$ (Satz von Pythagoras)

Beweis:

(i) Fall $y = 0$: „$\leq$“ und $=$ gilt
Fall $y \neq 0$:
Für alle $t \in \mathbb{R}$ gilt

$$0 \leq \langle x + ty, x + ty\rangle = \langle x, x\rangle + 2t\langle x, y\rangle + t^2\langle y, y\rangle \tag{13}$$

Setze $t = \frac{-\langle x,y\rangle}{\langle y,y\rangle}$ dann folgt

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

$\Rightarrow$ Cauchy-Schwarzsche Ungleichung.

„=“ in C.S.U. $\Leftrightarrow$ „=“ in (13) für dieses t

$$\overset{\text{pos.def.}}{\Rightarrow} x + ty = 0 \;\Rightarrow\; x, y \text{ linear abhängig}$$

Die Umkehrung ist trivial.

(ii) Es gilt

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

$\Rightarrow$ Wurzel ziehen, fertig.

(iii) Es gilt

$$\begin{aligned}d(x,y) &= \|x-y\| \\ &= \|x-z+z-y\| \\ &\overset{\text{(ii)}}{\leq} \|x-z\| + \|z-y\| \\ &= d(x,z) + d(z,y)\end{aligned}$$

(iv) Es gilt

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

(v) Es gilt

$$\begin{aligned}\|x+y\|^2 - \|x-y\|^2 &= \|x\|^2 + 2\langle x,y\rangle + \|y\|^2 - \|x\|^2 + 2\langle x,y\rangle - \|y\|^2 \\ &= 4\langle x,y\rangle\end{aligned}$$

(vi) Siehe (ii):

$$\|x+y\|^2 = \|x^2\| + \|y\|^2 + 2\underbrace{\langle x,y\rangle}_{\overset{!}{=}0 \;\Leftrightarrow\; \perp}$$

□

Vorlesung: 2005-06-01

Bemerkung:

(a) Jede Abbildung $\|\cdot\| : V \to \mathbb{R}$ mit

(i) $\|x\| \geq 0$, $\|x\| = 0 \;\Leftrightarrow\; x = 0$

(ii) $\|cx\| = |c|\|x\|$ $(c \in \mathbb{R})$

(iii) $\|x+y\| \leq \|x\| + \|y\|$

heißt *Norm* auf V.

Es gibt Normen, die nicht von einem Skalarprodukt $\langle\cdot,\cdot\rangle$ herrühren, zum Beispiel

$$\|\cdot\| : V \to \mathbb{R},\; \|x\| := \sum_{i=1}^{n} |x_i|$$

oder

$$\|x\| := \max_{i=1,\dots,n} |x_i|$$

Es gilt: Es existiert ein Skalarprodukt $\langle\cdot,\cdot\rangle$ mit $\|x\| = \sqrt{\langle x,y\rangle}$ genau dann wenn $\|\cdot\|$ die Parallelogrammidentität erfüllt.

(b) Sei $V \neq \emptyset$ eine beliebige Menge. Jede Abbildung $d : V \times V \to \mathbb{R}$ mit

(i) $d(x,y) \geq 0$, $d(x,y) = 0 \Leftrightarrow x = 0$
(ii) $d(x,y) \leq d(x,z) + d(z,y)$

heißt *Metrik* auf V.

Metriken existieren auch ohne Vektorraum-Struktur, aber auch im Vektorraum muss d nicht von einer Norm (also auch nicht von einem Skalarprodukt) herrühren.

Einfaches Beispiel:

$$d(x,y) = \begin{cases} 1 & \text{falls} \quad x \neq y \\ 0 & \text{sonst} \end{cases}$$

(c) Winkel: Für $x, y \in V$, $x, y \neq 0$ gilt

$$-1 \leq \frac{\langle x,y\rangle}{\|x\|\|y\|} \leq 1$$

$\Rightarrow$ Es existiert (genau) ein $\omega \in [0,\pi]$ mit

$$\cos\omega = \frac{\langle x,y\rangle}{\|x\|\|y\|}$$

ω heißt *Winkel* zwischen x und y.
($\Rightarrow \langle x,y\rangle = \|x\|\|y\|\cos\omega$)

Beispiel:

Beispiel für einen ∞-dimensionalen euklidischen Vektorraum: Der Standard-Hilbertraum ℓ^2.

$$\ell^2 := \{(x_0, x_1, \dots) \in \mathbb{R}^{\mathbb{N}_0} \mid \sum_{i=0}^{\infty} x_i^2 < \infty\}$$

ℓ^2 ist Untervektorraum:

$x = (x_0, x_1, \dots) \in \ell^2,\ x \in \mathbb{R} \overset{?}{\Rightarrow} cx \in \ell^2$

$$\sum_{i=0}^{\infty} (cx_i)^2 = c^2 \sum_{i=0}^{\infty} x_i^2 < \infty \quad \surd$$

$x \in \ell^2, y \in \ell^2 \overset{?}{\Rightarrow} x + y \in \ell^2$. Es sind

$$\sum_{i=0}^{\infty} x_i^2, \sum_{i=0}^{\infty} y_i^2 < \infty$$

Damit folgt

$$\underbrace{\Big(\sum_{i=0}^{n} (x_i + y_i)^2\Big)^{\frac{1}{2}}}_{\|(x_0,\dots,x_n)\| \in \mathbb{R}^{n+1}} \overset{\text{Minkowski}}{\leq} \Big(\sum_{i=0}^{n} x_i^2\Big)^{\frac{1}{2}} + \Big(\sum_{i=0}^{n} y_i^2\Big)^{\frac{1}{2}}$$

$$\leq \Big(\underbrace{\sum_{i=0}^{\infty} x_i^2}_{<\infty}\Big)^{\frac{1}{2}} + \Big(\underbrace{\sum_{i=0}^{\infty} y_i^2}_{<\infty}\Big)^{\frac{1}{2}}$$

$$= c < \infty$$

$\overset{n}{\Rightarrow}^{\infty} \sum_{i=0}^{\infty}(x_i+y_i)^2 \le c^2 < \infty$

Skalarprodukt auf ℓ^2?

$$\langle x, y\rangle := \sum_{i=0}^{\infty} x_i y_i \overset{?}{\in} \mathbb{R}$$

$\sum$ konvergiert absolut!

$$\begin{aligned}\sum_{i=0}^{n} |x_i||y_i| &= \langle \underbrace{(|x_0|,|x_1|,\ldots,|x_n|)}_{\in\mathbb{R}^{n+1}}, (|y_0|,|y_1|,\ldots,|y_n|)\rangle \\ &\overset{\text{CSU}}{\le} \Big(\sum_{i=0}^{n} x_i^2\Big)^{\frac{1}{2}} \cdot \Big(\sum_{i=0}^{n} y_i^2\Big)^{\frac{1}{2}} \\ &\le \Big(\sum_{i=0}^{\infty} x_i^2\Big)^{\frac{1}{2}} \cdot \Big(\sum_{i=0}^{\infty} y_i^2\Big)^{\frac{1}{2}} \\ &= c' < \infty\end{aligned}$$

$\overset{n}{\Rightarrow}^{\infty}$ Behauptung.

Sei nun $\dim V = n$, Basis $B = (v_1, \ldots, v_n)$, $x \in V \;\Rightarrow\; \hat{x} \in \mathbb{R}^n$.

Sei $\beta : V \to V$ Skalarprodukt auf V

$$\Rightarrow\; \beta(x,y) \overset{\text{Bilinearität}}{=} \sum_{i=1}^{n}\sum_{j=1}^{n} x_i y_j \beta(v_i, v_j) = \hat{x}^\top A \hat{y}$$

wobei

$$x := \sum x_i v_i \qquad A := ((\beta(v_i, v_j))) \in \mathbb{R}^{n\times n} \qquad y := \sum y_j v_j$$

Eigenschaften der Matrix A:

(i) A ist symmetrisch

(ii) $\hat{x}^\top A \hat{x} > 0$ für alle $\hat{x} \in \mathbb{R}^n$, $\hat{x} \neq 0$

Definition 5.3. Eine symmetrische Matrix $A \in \mathbb{R}^{n\times n}$ heißt *positiv definit*, wenn

$$z^\top A z > 0 \qquad \forall z \in \mathbb{R}^n, z \neq 0$$

Satz 5.2. Sei V ein n-dimensionaler Vektorraum mit Basis $B = (v_1, \ldots, v_n)$.

Jedes Skalarprodukt β auf V ist von der Form

$$\beta(x,y) = \hat{x}^\top A \hat{y}$$

mit einer positiv definiten symmetrischen Matrix $A \in \mathbb{R}^{n\times n}$. Jede derartige Matrix A erzeugt auch ein Skalarprodukt.

Satz 5.3. Sei $A \in \mathbb{R}^{n\times n}$ symmetrische Matrix.

Dann gilt

(i) A ist diagonalisierbar

(ii) Eigenvektoren zu verschiedenen Eigenwerten von A sind orthogonal

Beweis:

(i) Das charakteristische Polynom p von A zerfällt in Linearfaktoren. Zu zeigen ist, dass p nur reelle Nullstellen hat (als komplexes Polynom).

Sei $c = a + ib$ komplexer Eigenwert von A und $0 \neq z = u + iv$ komplexer Eigenvektor.

$$\begin{aligned} & A(u+iv) = (a+ib)(u+iv) = (au - bv) + i(bu + av) \\ \Rightarrow\ & Au = au - bv,\ Av = bu + av \\ \Rightarrow\ & \left.\begin{aligned} (Au)^\top v &= au^\top v - bv^\top v \\ (Au)^\top &= u^\top A^\top v = bu^\top u + au^\top v \end{aligned}\right\} \underbrace{bu^\top u}_{\|u\|^2} = \underbrace{-bv^\top v}_{\|v\|^2} \end{aligned}$$

$\Rightarrow\ b = 0$ weil $\|u\|^2 + \|v\|^2 > 0$

$\Rightarrow$ alle komplexen Eigenwerte von A sind reell.

$\Rightarrow\ p$ zerfällt (im Rellen) in Linearfaktoren

$$p = (-1)^n (X - c_1)^{r_1} \cdots (X - c_k)^{r_k}$$

$\Rightarrow\ \mathbb{R}^n = H_{c_1} \oplus \ldots \oplus H_{c_k}$

Index von H_{c_i}? Wir zeigen

$$(A - c_i E_n)^2 x = 0\ \Rightarrow\ (A - c_i E_n)x = 0$$

($\Rightarrow$ Index ist 1)

Denn

$$\begin{aligned} (A - c_i E_n)^2 x = 0\ &\Rightarrow\ x^\top (A - c_i E_n) x = 0 \\ &\Rightarrow\ \underbrace{[(A - c_i E_n)x]^\top (A - c_i E_n)}_{\|(A - c_i E_n)x\|^2} x = 0 \\ &\Rightarrow\ (A - c_i E_n)x = 0 \\ &\Rightarrow\ A \text{ diagonalisierbar} \end{aligned}$$

(ii) Seien $Ax = cx$, $Ay = dy$, $d \neq c$, $x, y \in \mathbb{R}^n \setminus \{o\}$.

$$\left.\begin{aligned} x^\top Ay = x^\top dy = d\langle x, y\rangle \\ x^\top Ay = (Ax)^\top y = cx^\top y = c\langle x, y\rangle \end{aligned}\right\} \overset{c \neq d}{\Rightarrow}\ \langle x, y\rangle = 0$$

□

Satz 5.4. Eine symmetrische Matrix $A \in \mathbb{R}^{n \times n}$ ist positiv definit $\Leftrightarrow$ Alle Eigenwerte von A sind > 0.

Beweis:

$\Rightarrow$: Sei $Ax = \underset{x \neq 0}{cx}$

$$\Rightarrow\ \underbrace{x^\top Ax}_{>0} = cx^\top x = c\|x\|^2\ \Rightarrow\ c > 0$$

$\Leftarrow$: Nach Satz 5.3 gilt $\mathbb{R}^n = E_{c_1} \oplus \ldots \oplus E_{c_k}$.

$\Rightarrow$ Jedes $x \in \mathbb{R}^n$ hat Darstellung

$$x = \sum_{i=1}^{n} x_i \qquad x_i \in E_{c_i}$$

Damit folgt

$$\begin{aligned}\sum_{i=1}^{n}\sum_{j=1}^{n} x_i^\top A x_j &= \sum_{i=1}^{n}\sum_{j=1}^{n} c_i\langle x_i, x_j\rangle \\ &= \sum_{i=1}^{n} c_i\|x_i\|^2 \\ &> 0 \text{ für } x \neq 0\end{aligned}$$

□

Vorlesung: 2005-06-08

Beispiel:

(i) Sei

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

Dann

$$\begin{aligned}&\Rightarrow\ p = -(X-3)(X-\frac{1}{2}(3+\sqrt{5}))(X-\frac{1}{2}(3-\sqrt{5})) \\ &\Rightarrow\ \text{Eigenwerte: } 3, \frac{1}{2}(3+\sqrt{5}), \frac{1}{2}(3-\sqrt{5}) \quad > 0 \\ &\Rightarrow\ A \text{ positiv definit}\end{aligned}$$

(ii) Sei

$$\beta(x,y) = x_1y_1 + x_2y_2 + x_3y_3 + x_1y_2 + x_2y_1 \qquad x, y \in \mathbb{R}^3$$

Ist β ein Skalarprodukt?

$$\beta(x,y) = \underset{x^\top}{\begin{pmatrix} x_1 & x_2 & x_3 \end{pmatrix}} \cdot \underset{A}{\begin{pmatrix} 1 & 1 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}} \cdot \underset{y}{\begin{pmatrix} y_1 \\ y_2 \\ y_3 \end{pmatrix}}$$

Damit gilt

$$p = \begin{vmatrix} 1-X & 1 & 0 \\ 1 & 1-X & 0 \\ 0 & 0 & 1-X \end{vmatrix} = (1-X)(-X)(2-X)$$

$\Rightarrow$ Eigenwerte: $1, 2, 0$ damit ist A nicht positiv definit und β kein Skalarprodukt.

Andere Methode zur Bestimmung der positiven Definitheit von Matrizen: *Hauptminoren*:

$$\left|A_k\right| = \begin{vmatrix} a_1 1 & \cdots & a_{1k} \\ \vdots & & \vdots \\ a_{k1} & \cdots & a_{kk} \end{vmatrix} \quad \text{mit} \quad A = \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & & \vdots \\ a_{n1} & \cdots & a_{nn} \end{pmatrix}$$

Satz 5.5. Sei $A \in \mathbb{R}^{n\times n}$ symmetrisch. Dann sind äquivalent:

(i) A ist positiv definit

(ii) Es existiert eine reguläre $(n \times n)$-Matrix B mit $A = B^\top B$

(iii) Alle Hauptminoren

$$\begin{vmatrix} a_{11} & \cdots & a_{1k} \\ \vdots & & \vdots \\ a_{k1} & \cdots & a_{kk} \end{vmatrix}$$

sind > 0 für $k = 1, \ldots, n$

Beweis:

(ii) $\Rightarrow$ (i): Sei $x \neq 0$

$$\overset{B \text{ reg.}}{\Rightarrow} Bx \neq 0 \;\Rightarrow\; x^\top \underbrace{A}_{B^\top B} x = \|Bx\|^2 > 0$$

(i) $\Rightarrow$ (iii): Ist A positiv definit, so ist $\det A > 0$ (folgt wegen Satz 5.3, (i) aus Satz 5.4)

$$\det A = \det S^{-1}DS \qquad \text{mit } D = \begin{pmatrix} c_1 & & 0 \\ & \ddots & \\ 0 & & c_n \end{pmatrix}$$

$$= \det D$$
$$= c_1 \cdots c_n > 0$$

Mit A ist auch

$$A_k = \begin{pmatrix} a_{11} & \cdots & a_{1k} \\ \vdots & & \vdots \\ a_{k1} & \cdots & a_{kk} \end{pmatrix}$$

positiv definit.

Sei $(x_1, \ldots, x_k) \in \mathbb{R}^4, \neq 0$

$$\Rightarrow\; x = (x_1, \ldots, x_k, 0, \ldots, 0) \in \mathbb{R}^n,\; \neq 0$$

$$\overset{\text{(i)}}{\Rightarrow}\; 0 < x^\top Ax = \begin{pmatrix} x_1 & \cdots & x_k \end{pmatrix} A_k \begin{pmatrix} x_1 \\ \vdots \\ x_k \end{pmatrix}$$

$$\Rightarrow\; A_k \text{ positiv definit}$$
$$\Rightarrow\; \det A_k > 0$$

(iii) $\Rightarrow$ (ii): Für $k = 2, \ldots, n$ sei

$$A_k := \begin{pmatrix} A_{k-1} & y_k \\ y_k^\top & a_{kk} \end{pmatrix} \qquad y_k = \begin{pmatrix} a_{1,k} \\ \vdots \\ a_{k-1,k} \end{pmatrix} \in \mathbb{R}^{k-1}$$

und

$$T_k := \begin{pmatrix} E_{k-1} & -A_{k-1}^{-1} y_k \\ 0^\top & 1 \end{pmatrix}$$

Dann folgt

$$\begin{aligned} T_k^\top A_k T_k &= \begin{pmatrix} E_{k-1} & 0 \\ -y_k^\top A_{k-1}^{-1} & 1 \end{pmatrix} \begin{pmatrix} A_{k-1} & y_k \\ y_k^\top a_{kk} & \end{pmatrix} \begin{pmatrix} E_{k-1} & -A_{k-1}^{-1} y_k \\ 0^\top & 1 \end{pmatrix} \\ &= \begin{pmatrix} E_{k-1} & 0 \\ -y_k^\top A_{k-1}^{-1} & 1 \end{pmatrix} \begin{pmatrix} A_{k-1} & 0 \\ y_k^\top & a_{kk} - y_k^\top A_{k-1}^{-1} y_k \end{pmatrix} \\ &= \begin{pmatrix} A_{k-1} & 0 \\ 0^\top & a_k k - y_k^\top A_{k-1}^{-1} y_k =: b_k \end{pmatrix} \end{aligned}$$

Also

$$\begin{aligned} \Rightarrow \det T_k^\top A_k T_k &= \det A_{k-1} b_k \\ &= \det \underset{=1}{T_k^\top} \det A_k \det \underset{=1}{T_k} \\ &= \det A_k \end{aligned}$$

$\Rightarrow b_k \frac{\det A_k}{\det A_{k-1}} > 0$ (nach Vor. (iii)) $k = 2, \ldots, n$. Setze

$$T := T_n \cdot \begin{pmatrix} T_{n-1} & 0 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} T_{n-2} & 0 \\ 0 & E_2 \end{pmatrix} \cdots \begin{pmatrix} T_2 & 0 \\ 0 & E_{n-2} \end{pmatrix}$$

$\Rightarrow T$ regulär

$$\begin{aligned} T^\top A T = &\begin{pmatrix} T_2^\top & 0 \\ 0 & E_{n-2} \end{pmatrix} \cdots \begin{pmatrix} T_{n-2}^\top & 0 \\ 0 & E_2 \end{pmatrix} \begin{pmatrix} T_{n-1}^\top & 0 \\ 0 & 1 \end{pmatrix} T_n^\top A T_n \\ &\begin{pmatrix} T_{n-1} & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} T_{n-1} & 0 \\ 0 & E_2 \end{pmatrix} \cdots \begin{pmatrix} T_2 & 0 \\ 0 & E_{n-2} \end{pmatrix} \\ = &\begin{pmatrix} T_2^\top & 0 \\ 0 & E_{n-2} \end{pmatrix} \cdots \begin{pmatrix} T_{n-2}^\top & 0 \\ 0 & E_2 \end{pmatrix} \begin{pmatrix} T_{n-1}^\top & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} A_{n-1} & 0 \\ 0 & b_n \end{pmatrix} \\ &\begin{pmatrix} T_{n-1} & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} T_{n-1} & 0 \\ 0 & E_2 \end{pmatrix} \cdots \begin{pmatrix} T_2 & 0 \\ 0 & E_{n-2} \end{pmatrix} \\ = &\begin{pmatrix} T_2^\top & 0 \\ 0 & E_{n-2} \end{pmatrix} \cdots \begin{pmatrix} T_{n-2}^\top & 0 \\ 0 & E_2 \end{pmatrix} \begin{pmatrix} T_{n-1}^\top A_{n-1} T_{n-1} & 0 \\ 0 & b_n \end{pmatrix} \\ &\begin{pmatrix} T_{n-1} & 0 \\ 0 & E_2 \end{pmatrix} \cdots \begin{pmatrix} T_2 & 0 \\ 0 & E_{n-2} \end{pmatrix} \\ = &\begin{pmatrix} T_2^\top & 0 \\ 0 & E_{n-2} \end{pmatrix} \cdots \begin{pmatrix} T_{n-2}^\top & 0 \\ 0 & E_2 \end{pmatrix} \begin{pmatrix} A_{n-2} & & 0 \\ & b_{n-1} & \\ 0 & & b_n \end{pmatrix} \begin{pmatrix} T_{n-1} & 0 \\ 0 & E_2 \end{pmatrix} \cdots \begin{pmatrix} T_2 & 0 \\ 0 & E_{n-2} \end{pmatrix} \\ = &\ldots \\ = &\begin{pmatrix} a_{11} & & & 0 \\ & b_2 & & \\ & & \ddots & \\ 0 & & & b_n \end{pmatrix} \end{aligned}$$

Setze

$$D := \begin{pmatrix} \sqrt{a_{11}} & & & 0 \\ & \sqrt{b_1} & & \\ & & \ddots & \\ 0 & & & \sqrt{b_n} \end{pmatrix}$$

und

$$B := DT^{-1}$$

$\Rightarrow B^\top B = (T^{-1})^\top D D T^{-1} = (T^{-1})^\top T^\top A T T^{-1} = A$

□

Die Zerlegung $A = B^\top B$ heißt in der numerischen Mathematik *Cholesky-Zerlegung*[1].

Beispiel: Sei

$$A = \begin{pmatrix} 1 & a & -1 \\ a & 9 & 0 \\ -1 & 0 & 4 \end{pmatrix} \qquad a \in \mathbb{R}$$

Wann ist A positiv definit?

$$\begin{aligned} \Rightarrow \det A_1 &= \left|1\right| = 1 > 0 \\ \det A_2 &= \begin{vmatrix} 1 & a \\ a & 9 \end{vmatrix} = 9 - a^2 > 0 \;\Leftrightarrow\; |a| < 3 \\ \det A_3 &= \begin{vmatrix} 1 & a & -1 \\ a & 9 & 0 \\ -1 & 0 & 4 \end{vmatrix} = 27 - 4a^2 \;\Leftrightarrow\; |a| < \frac{3}{2}\sqrt{3} \end{aligned}$$

$\Rightarrow$ A positiv definit $\Leftrightarrow$ $|a| < \frac{3}{2}\sqrt{3}$

§2 Orthonormalbasen und Orthogonalprojektionen

Definition 5.4. Sei V ein Euklidischer Vektorraum, $A \subset V$ eine nichtleere Teilmente. A heißt *Orthogonalsystem*, wenn gilt

(i) $0 \notin A$

(ii) $x, y \in A, x \neq y \;\Rightarrow\; x \perp y$

Gilt weiter

(iii) $\|x\| = 1$ für alle $x \in A$

so heißt A *Orthonormalsystem*.

Ist A sogar Basis von V, so heißt A *Orthogonalbasis* bzw *Orthonormalbasis* (kurz ONB).

Bemerkung: Hat V endliche oder abzählbare Basis $B = (x_1, \ldots, x_n)$ bzw. $B = (x_1, \cdot_2, \ldots)$, so ist B ONB $\Leftrightarrow$ $\langle x_i, x_j \rangle = \delta_{ij}$

Satz 5.6. Orthogonalsysteme $A \in V$ sind linear unabhängig.

Beweis: Sei $a_1x_1 + \ldots + a_kx_k = 0$ mit $a_i \in \mathbb{R}$, $x_i \in A$, $k \in \mathbb{N}$.

$$\begin{aligned} \Rightarrow\; 0 &= \langle a_1x_1 + \ldots + a_kx_k, x_j \rangle \\ &= \sum_{i=1}^{k} a_i \underbrace{\langle x_i, x_j \rangle}_{=0 \text{ für } i \neq j} \\ &= a_j \|x_j\|^2 \end{aligned}$$

$\Rightarrow$ $a_j = 0$, $j = 1, \ldots, k$ □

[1] Siehe *Numerik Verfahren für Informatiker* auf www.logn.de

Satz 5.7. Ist V endlich dimensionaler Euklidischer Vektorraum, so existiert eine Orthonormalbasis.

Beweis: Sei $B = (x_1, \ldots, x_n)$ Basis von V. Gram-Schidt-sches Orthogonalisierungsverfahren:

$$\begin{aligned} y_1 &:= x_1 \\ y_2 &:= x_2 - \frac{\langle x_2, y_1\rangle}{\|y_1\|^2} y_1 \\ &\vdots \\ y_{k+1} &:= x_{k+1} - \sum_{i=1}^{k} \frac{\langle x_{k+1}, y_i\rangle}{\|y_i\|^2} y_i \qquad k = 1, \ldots, n \end{aligned}$$

Vorlesung: 2005-06-15

Behauptung: $y_1, \ldots, y_{k+1}$ sind Orthogonalsystem $\forall k = 0, \ldots, n-1$

$k = 0$: $y_1 = v_1 \neq 0 \Rightarrow y_1$ Orthogonalsystem

$k = 1$: $y_1, y_2 \neq 0$

$$\begin{aligned} \langle y_1, y_2\rangle &= \langle v_1, v_2\rangle - \frac{\langle v_2, y_1\rangle}{\|y_1\|^2}\langle v_1, y_1\rangle \\ &= \langle v_1, v_2\rangle - \frac{\langle v_2, v_1\rangle}{\|v_1\|^2}\langle v_1, v_1\rangle \\ &= 0 \end{aligned}$$

$k \to k+1$: $y \neq 0$ und $\langle y_i, y_j\rangle = 0$ für alle $i, j \in \{1, \ldots, k\}$ nach IV.

$$\begin{aligned} \langle y_{k+1}, y_j\rangle &= \langle y_{k+1}, v_j\rangle - \sum_{i=1}^{k} \frac{\langle v_{k+1}, y_i\rangle}{\|y_i\|^2}\langle y_i, y_j\rangle \\ &= \langle v_{k+1}, v_j\rangle - \frac{\langle v_{k+1}, y_j\rangle}{\|y_j\|^2}\langle y_j, y_j\rangle \\ &= 0 \end{aligned}$$

$\Rightarrow$ $(y_1, \ldots, y_n)$ Orthogonalsystem $\overset{\text{Satz } 5.6}{\Rightarrow}$ $(y_1, \ldots, y_n)$ linear unabhängig

$\Rightarrow$ Orthogonalbasis $\Rightarrow$ $(\frac{y_1}{\|y_i\|}, \ldots, \frac{y_n}{\|y_n\|})$ ONB. □

Bemerkung:

(i) Der Beweis funktioniert analog wenn $B = (v_1, v_2, \ldots)$ eine abzählbare Basis ist, und liefert dann eine ONB in V ($\dim V = \infty$). Beispiel: $\mathbb{R}[X]$.

(ii) Satz 5.7 folgt auch aus Satz 5.5 (O.b.d.A. $V = \mathbb{R}^n$). Nämlich:

$\mathbb{R}^n$ mit Skalaprodukt β. Basis $(e_1, \ldots, e_n)$.

ONB in $(\mathbb{R}^n, \beta)$? Wir wissen

$$\beta(x, y) = y^\top A x$$

Damit folgt nach Satz 5.5

$$A = B^\top B \qquad (B \text{ regulär})$$

Behauptung: $B^{-1}e_1, \ldots, B^{-1}e_n$ ONB bezüglich β. Denn

$$\begin{aligned} \beta(B^{-1}e_i, B^{-1}e_j) &= e_i^\top (B^{-1})^\top \underbrace{A}_{B^\top B} B^{-1} e_j \\ &= \delta_{ij} \end{aligned}$$

Beispiel:

(i) Im $\mathbb{R}^n$ mit Standardskalarprodukt ist die Standardbasis eine ONB.

(ii) $\mathbb{R}[X] \subset \ell^2$ mit induziertem Skalarprodukt

$$B = (\underbrace{1}_{e_0}, \underbrace{X}_{e_1}, \underbrace{X^2}_{e_2}, \ldots) \text{ ONB}$$

In ℓ^2 ist B ein Orthogonalsystem, aber keine Basis, denn $[B] = \mathbb{R}[X] \neq \ell^2$.

(iii) $\mathbb{R}^3$ mit Basis $B = (\underbrace{\begin{pmatrix}1\\1\\0\end{pmatrix}}_{v_1}, \underbrace{\begin{pmatrix}1\\1\\1\end{pmatrix}}_{v_2}, \underbrace{\begin{pmatrix}1\\0\\1\end{pmatrix}}_{v_3})$. Wie sieht ONB bzgl. Standardskalaprodukt aus?

$$y_1 = \begin{pmatrix}1\\1\\0\end{pmatrix} \Rightarrow \|y_1\|^2 = 2 \Rightarrow \|y_1\| = \sqrt{2}$$

$$y_2 = \begin{pmatrix}1\\1\\1\end{pmatrix} - \frac{2}{2}\begin{pmatrix}1\\1\\0\end{pmatrix} = \begin{pmatrix}0\\0\\1\end{pmatrix} \Rightarrow \|y_2\| = 1$$

$$y_3 = \begin{pmatrix}1\\0\\1\end{pmatrix} - \frac{1}{2}\begin{pmatrix}1\\1\\0\end{pmatrix} - \frac{1}{1}\begin{pmatrix}0\\0\\1\end{pmatrix} = \begin{pmatrix}\frac{1}{2}\\-\frac{1}{2}\\0\end{pmatrix} \Rightarrow \|y_3\|^2 = \frac{1}{2} \Rightarrow \|y_3\| = \frac{1}{\sqrt{2}}$$

$\Rightarrow$ ONB $(\frac{1}{\sqrt{2}}\begin{pmatrix}1\\1\\0\end{pmatrix}, \begin{pmatrix}0\\0\\1\end{pmatrix}, \frac{1}{\sqrt{2}}\begin{pmatrix}1\\-1\\0\end{pmatrix})$

(iv) $\mathbb{R}^3$ mit Basis wie in (iii), aber

$$\langle x, y\rangle = x^\top A y$$

mit

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

ONB?

Gram-Schmidt:

$$y_1 = \begin{pmatrix}1\\1\\0\end{pmatrix}$$

$$\Rightarrow \|y_1\|^2 = \begin{pmatrix}1 & 1 & 0\end{pmatrix}\begin{pmatrix}1 & 0 & -1\\0 & 3 & 0\\-1 & 0 & 2\end{pmatrix}\begin{pmatrix}1\\1\\0\end{pmatrix} = \begin{pmatrix}1 & 1 & 0\end{pmatrix}\begin{pmatrix}1\\3\\-1\end{pmatrix} = 4 \Rightarrow \|y_1\| = 2$$

$$y_2 = \begin{pmatrix}1\\1\\0\end{pmatrix} - \frac{\begin{pmatrix}1&1&1\end{pmatrix}\begin{pmatrix}1&0&-1\\0&3&0\\-1&0&2\end{pmatrix}\begin{pmatrix}1\\1\\0\end{pmatrix}}{4}\begin{pmatrix}1\\1\\0\end{pmatrix} = \begin{pmatrix}\frac{1}{4}\\\frac{1}{4}\\1\end{pmatrix}$$

$$\Rightarrow \|y_2\|^2 = \frac{1}{16}\begin{pmatrix}1\\1\\4\end{pmatrix}\begin{pmatrix}1 & 0 & -1\\0 & 3 & 0\\-1 & 0 & 2\end{pmatrix}\begin{pmatrix}1\\1\\4\end{pmatrix} = \frac{1}{16}\begin{pmatrix}1 & 1 & 4\end{pmatrix}\begin{pmatrix}-3\\3\\7\end{pmatrix} = \frac{28}{16} = \frac{7}{4} \Rightarrow \|y_2\| = \frac{\sqrt{7}}{2}$$

$$y_3 = \begin{pmatrix}1\\0\\1\end{pmatrix} - \frac{\begin{pmatrix}1&0&1\end{pmatrix}\begin{pmatrix}1\\3\\-1\end{pmatrix}}{4}\begin{pmatrix}1\\1\\0\end{pmatrix} - \frac{\begin{pmatrix}1&0&1\end{pmatrix}\begin{pmatrix}-\frac{3}{4}\\\frac{3}{4}\\\frac{7}{4}\end{pmatrix}}{\frac{7}{4}}\begin{pmatrix}\frac{1}{4}\\\frac{1}{4}\\1\end{pmatrix}$$

$$= \frac{1}{7}\begin{pmatrix}6\\-1\\3\end{pmatrix} \Rightarrow \|y_3\|^2 = \frac{3}{7}$$

$\Rightarrow$ ONB ist $(\frac{1}{2}\begin{pmatrix}1\\1\\0\end{pmatrix}, \frac{1}{2\sqrt{7}}\begin{pmatrix}1\\1\\4\end{pmatrix}, \frac{1}{\sqrt{21}}\begin{pmatrix}6\\-1\\3\end{pmatrix})$

Bemerkung:

(i) Sei $(v_1, \ldots, v_n)$ ONB von V und $x \in V$

$$\Rightarrow\ x = \sum_{i=1}^{n} \langle x, v_i\rangle v_i \qquad (\text{d.h. } \hat{x} = \begin{pmatrix}\langle x, v_1\rangle\\ \vdots \\ \langle x, v_n\rangle\end{pmatrix})$$

Beweis:

$$x = \sum_{j=1}^{n} a_j v_j$$

$$\Rightarrow\ \langle x, v_j\rangle = \sum_{j=1}^{n} a_j \underbrace{\langle v_j, v_i\rangle}_{\delta_{ij}} = a_i$$

Damit folgt auch

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

und

$$\langle x, y\rangle = \sum_{i=1}^{n} \langle x, v_i\rangle\langle y, v_i\rangle$$

(ii) Besselsche Ungleichung ($\rightarrow$ Übungsblatt)

Vorlesung: 2005-06-22

Orthogonalprojektionen

Wiederholung. $\pi : V \to V$ (V euklidischer Vektorraum) ist *Projektion*, wenn $\pi^2 = \pi$ (Projektion auf $U := \operatorname{Bild}\pi$)

$\Rightarrow\ V = \operatorname{Bild}\pi \oplus \operatorname{Kern}\pi$

Definition 5.5. Eine Abbildung $\pi : V \to V$ (V euklidischer Vektorraum) heißt *Orthogonalprojektion* (auf $U := \operatorname{Bild}\pi$), wenn π Projektion ist und

$$\pi(x) - x \perp \pi(x)$$

für alle $x \in V$ erfüllt.

Bemerkung: Ist $\pi : V \to V$ Orthogonalprojektion auf U, so gilt $\pi(x) - x \perp U$, also auch $\operatorname{Kern}\pi \perp \pi$.

Umgekehrt ist jede Projektion π, die $\operatorname{Kern}\pi \perp \operatorname{Bild}\pi$ erfüllt eine Orthogonalprojektion.

Beweis: Sei $u \in U\ \Rightarrow\ \pi(u - \pi(x) + x) = \pi(u) = u$

$$\Rightarrow\ \underbrace{\pi(u - \pi(x) + x) - (u - \pi(x) + x)}_{x - \pi(x)} \perp u$$

$$\Rightarrow\ \pi(x) - x \perp U$$

$$\Rightarrow\ \operatorname{Kern}\pi \perp U$$

Umgekehrt gelte $\operatorname{Kern}\pi \perp \operatorname{Bild}\pi$, $\pi^2 = \pi$

$$\Rightarrow \underbrace{\pi(x) - x}_{\in \operatorname{Kern}\pi} \perp \underbrace{\pi(x)}_{\in \operatorname{Bild}\pi}$$

□

Satz 5.8. Vermöge V euklidischer Vektorraum, $U \subset V$ Untervektorraum.
Dann gilt: Es existiert eine Orthogonalprojektion $\pi = \pi_U$ auf $U \Leftrightarrow V = U \oplus U^\perp$.
Die Orthogonalprojektion π_U ist eindeutig (wenn sie existiert) und es gilt dann auch

$$(U^\perp)^\perp = U$$

Beweis:

„$\Rightarrow$“: Sei π Orthogonalprojektion auf $U \Rightarrow$ Jedes $x \in V$ hat eine Zerlegung

$$x = (\pi(x) + x) + (x - \pi(x)) \in U + U^\perp$$
$$\Rightarrow V = U + U^\perp$$

Wegen $U \cap U^\perp = \{o\}$ ist die Summe direkt.

„$\Leftarrow$“: Sei $V = U \oplus U^\perp \Rightarrow$ Jedes $x \in V$ hat Darstellung $x = u + v$ mit $u \in U$ und $v \in U^\perp$.
Definiere $\pi(x) := u \Rightarrow x \in \operatorname{End}(V)$ mit $\pi(V) = U$ und $\pi^2 = \pi$
Weiter gilt $\pi(x) - x \in \operatorname{Kern}\pi = U^\perp$
$\Rightarrow \pi(x) - x \perp \pi(x) \in U \Rightarrow \pi$ ist Orthogonalprojektion.

Eindeutigkeit:
Seien π_U, π'_U beides Orthogonalprojektionen auf U Damit gilt

$$u := \pi_U(x), \quad u' := \pi'_U(x)$$

erfüllen

$$\underbrace{\langle u - u', u - u'\rangle}_{=\|u-u'\|^2} = \underbrace{\langle u - x, u - u'\rangle}_{=0} - \underbrace{\langle u' - x, u - u'\rangle}_{=0} = 0$$

$\Rightarrow u - u' = 0 \Rightarrow u = u'$
Wir wissen $(U^\perp)^\perp \supset U$. Sei also $x \in (U^\perp)^\perp$

$$\Rightarrow x = u + v \qquad u \in U,\ v \in V = U^\perp$$

$$\begin{aligned}\Rightarrow \langle u, v\rangle &= \langle x - u, v\rangle \\ &= \langle x, v\rangle - \langle u, v\rangle \\ &= 0 - 0 \\ &= 0\end{aligned}$$

$$\Rightarrow v = 0 \Rightarrow x \in U$$

□

Beispiel: $V = \ell^2, U = \mathbb{R}[X] \subset V$

$U^\perp = \{o\}$, Sei $x = (x_0, x_1, x_2, \ldots) \in (\mathbb{R}[X])^\perp$

$$\Rightarrow \underbrace{\langle x, e_i\rangle}_{x_i} = 0, \quad e_i = (0, \ldots, 0, \underset{i\text{-te Stelle}}{1}, 0, \ldots) = X^i \qquad i = 0, 1, 2, \ldots$$

$\Rightarrow x = 0.$

Hier gilt also $\ell^2 \neq \underset{U}{\mathbb{R}[X]} \oplus \underset{U^\perp}{\{o\}}$

$\Rightarrow$ keine Orthogonalprojektion auf $\mathbb{R}[X]$!

Satz 5.9. Sei V euklidischer Vektorraum (beliebiger Dimension) und U endlich dimensionaler Untervektorraum. Dann existiert die Orthogonalprojektion $\pi = \pi_U$ auf U.

Beweis: Nach Satz 5.7 existiert eine ONB $(v_1, \ldots, v_k)$ von U. Setze für $x \in V$

$$\pi(x) := \sum_{i=1}^{k} \langle x, v_i\rangle v_i \in U$$

$\Rightarrow \pi^2 = \pi$ wegen

$$\begin{aligned}
\pi^2 &= \sum \langle \pi(x), v_i\rangle v_i \\
&= \sum_{i=1}^{k}\sum_{j=1}^{k} \langle x, v_j\rangle \underbrace{\langle v_j, v_i\rangle}_{\delta_{ij}} \cdot v_i \\
&= \sum_{i=1}^{k} \langle x, v_i\rangle \cdot v_i \\
&= \pi(x)
\end{aligned}$$

Orthogonalität: $\langle \pi(x) - x, \pi(x)\rangle = 0$?

$$\begin{aligned}
\langle \pi(x) - x, v_i\rangle &= \langle \sum_{j=1}^{k} \langle x, v_j\rangle v_j, v_i\rangle \\
&= \sum_{j=1}^{k} \langle x, v_j\rangle \underbrace{\langle v_j, v_i\rangle}_{\delta_{ij}} - \langle x, v_i\rangle \\
&= 0
\end{aligned}$$

$\Rightarrow \pi(x) - x \perp U \Rightarrow \pi$ Orthogonalprojektion. □

Bemerkung: Insbesondere im Fall $\dim V = n < \infty$, U Untervektorraum, gilt $V = U \oplus U^\perp$ und $x = \pi_U(x) + \pi_{U^\perp}(x)$

Beispiel: Sei

$$U = [\underbrace{\begin{pmatrix}1\\1\\0\\1\\0\end{pmatrix}}_{x_1}, \underbrace{\begin{pmatrix}2\\0\\1\\1\\0\end{pmatrix}}_{x_2}, \underbrace{\begin{pmatrix}1\\-1\\1\\-1\\1\end{pmatrix}}_{x_3}, \underbrace{\begin{pmatrix}0\\0\\1\\1\\0\end{pmatrix}}_{x_4}] \subset \mathbb{R}^5$$

$\pi_U(x) =$?

1. Methode:

1. Bestimme ONB in U
2. Berechne $\pi(x) = \sum_{i=1}^{k} \langle x, u_i \rangle u_i$

2. Methode:

1. Bestimme $U^\perp$
2. Bestimme ONB in $U^\perp$
3. Bestimme $\pi_{U^\perp}(x)$
4. Berechne $\pi_U(x) = x - \pi_{u^\perp}(x)$

ONB in U: Gram-Schmidt:

$$y_1 = x_1 = \begin{pmatrix} 1 \\ 1 \\ 0 \\ 1 \\ 0 \end{pmatrix}, \ \|y_1\| = \sqrt{3}$$

$$y_2 = \begin{pmatrix} 1 \\ -1 \\ 1 \\ 0 \\ 0 \end{pmatrix}, \ \|y_2\| = \sqrt{3}$$

$$y_3 = x_3 - \frac{\langle x_3, y_1 \rangle}{\|y_1\|^2} y_1 - \frac{\langle x_3, y_2 \rangle}{\|y_2\|^2} = \begin{pmatrix} 1 \\ -1 \\ 1 \\ 0 \\ 0 \end{pmatrix} + \begin{pmatrix} 1 \\ -1 \\ 1 \\ 0 \\ 0 \end{pmatrix} = 0$$

$$y_4 = \frac{2}{3} \begin{pmatrix} -1 \\ 0 \\ 1 \\ 1 \\ 0 \end{pmatrix} \Rightarrow \ \|y_4\| = \frac{2}{\sqrt{3}}$$

$\Rightarrow$ ONB in U: $(\frac{1}{\sqrt{3}} \begin{pmatrix} 1 \\ 1 \\ 0 \\ 1 \\ 0 \end{pmatrix}, \frac{1}{\sqrt{3}} \begin{pmatrix} 1 \\ -1 \\ 1 \\ 0 \\ 0 \end{pmatrix}, \frac{1}{\sqrt{3}} \begin{pmatrix} -1 \\ 0 \\ 1 \\ 1 \\ 0 \end{pmatrix})$

$\Rightarrow \ \pi_U(x) = \frac{1}{3}(7 \begin{pmatrix} 1 \\ 1 \\ 0 \\ 1 \\ 0 \end{pmatrix} + 2 \begin{pmatrix} 1 \\ -1 \\ 1 \\ 0 \\ 0 \end{pmatrix} + 6 \begin{pmatrix} -1 \\ 0 \\ 1 \\ 1 \\ 0 \end{pmatrix}) = \frac{1}{3} \begin{pmatrix} 3 \\ 5 \\ 8 \\ 13 \\ 0 \end{pmatrix}$

Satz 5.10. Sei V euklidischer Vektorraum, U Untervektorraum, $\pi \in \mathrm{Hom}(V, V)$ und $\mathrm{Bild}\,\pi \subset U$.

Dann gilt: π ist Orthogonalprojektion auf U genau dann wenn

$$\begin{aligned} \|x - \pi(x)\| &= \inf_{u \in U} \|x - u\| \qquad \forall x \in V \\ &= \min_{u \in U} \|x - u\| \end{aligned}$$

Vorlesung: 2005-06-29

Beweis:

„$\Rightarrow$“: π sei Orthogonalprojektion auf U $\Rightarrow$ Sei $x \in V$, $u \in U$

$$\Rightarrow \|x-u\|^2 = \| \underbrace{x-\pi(x)}_{\in U^\perp} + \underbrace{\pi(x)-u}_{\in U} \|^2$$
$$= \|x-\pi(x)\|^2 + \|\pi(x)-u\|^2$$
$$\geq \|x-\pi(x)\|^2$$

Setze $u = \pi(x)$ $\Rightarrow$ Behauptung.

„$\Leftarrow$“: Ersetze x durch $\pi(x)$

$$\Rightarrow \|\pi(x)-\pi^2(x)\| = \inf_{u\in U} \|\pi(x)-u\|$$

Wegen $\pi(x) \in \pi(V) \subset U$ folgt

$$\|\pi(x)-\pi^2(x)\| = 0$$

also $\pi = \pi^2$. Analog folgt für $x \in U$

$$\|x-\pi(x)\| = 0$$

$\Rightarrow$ $x = \pi(x)$, das heißt Bild $\pi = U$.

Orthogonalität:

$$\pi(x) - x \perp \pi(x)$$

Betrachte $(1+a)\pi(x) \in U$ für alle $a \in \mathbb{R}$.

$$\Rightarrow \|x-\pi(x)\|^2 \leq \|x-(1+a)\pi(x)\|^2$$
$$\Rightarrow \|x-\pi(x)\|^2 \leq \|x-\pi(x)\|^2 + a^2\|\pi(x)\|^2 - 2a\langle x-\pi(x), \pi(x)\rangle$$
$$\Rightarrow 2a\langle x-\pi(x), \pi(x)\rangle \leq a^2\|\pi(x)\|^2$$
$$\Rightarrow 2|\langle x-\pi(x), \pi(x)\rangle| \leq |a|\|\pi(x)\|^2 \qquad \forall a \neq 0$$
$$\overset{a\to 0}{\Rightarrow} \langle x-\pi(x), \pi(x)\rangle = 0$$

□

Bemerkung: Eine ähnliche Aussage ist die Folgende:

Sei $\pi : V \to V$ Projektion. Dann sind die folgenden Aussagen äquivalent:

(i) π ist Orthogonalprojektion

(ii) $\|\pi(x)\| \leq \|x\| \qquad \forall x \in V$

(iii) $\|\pi(x)-\pi(y)\| \leq \|x-y\| \qquad \forall x, y \in V$

Beweis: Übung □

Definition 5.6. Seien $A, B \subset V$, V euklidischer Vektorraum ($\dim V < \infty$).

$$d(A,B) := \inf_{\substack{x\in A \\ y\in B}} \|x-y\|$$

heißt *Abstand* zwischen A und B

Hier: Affine Vektorräume $L, M \in V$ mit $L = x_0 + U$ und $M = y_0 + W$. $x_0 \in L$, $y_0 \in M$ Aufpunkte U, W Untervektorräume von V.

Schreibweise: $d(x, B) = d(\{x\}, B)$, Analog $d(x, y)$.

$\Rightarrow$ $d(x, U) = \|x - \pi_U(x)\|$ (nach Satz 5.10)

Satz 5.11. Für affine Unterräume $L = x_0 + U$ und $M = y_0 + W$ gilt:

$$\begin{aligned} d(L,M) &= d(y_0 - x_o, U + W) \\ &= \|(y_0 - x_0) - \pi_{U+W}(y_0 - x_0)\| \end{aligned}$$

Gilt $\pi_{U+W}(y_0 - x_0) = u - w$, $u \in U$, $w \in W$, so sind $x_1 = x_0 + u \in L$ und $y_1 = y_0 + W \in M$ und $d(L,M) = d(x_1, y_1)$

x_0, y_0 sind genau dann eindeutig bestimmt, wenn die Summe $U + W$ direkt ist.

Definition 5.7. x_1, y_1 heißen *Lotfußpunkte*

Beweis:

$$\begin{aligned} d(L,M) &= \inf_{\substack{y\in M \\ x\in L}} \|y - x\| \\ &= \inf_{\substack{u\in U \\ w\in W}} \|y_0 + w - x_0 - u\| \\ &= \inf_{z\in U+W} \|(y_0 - x_0) - z\| \\ &\overset{\text{Satz 5.10}}{=} \|(y_0 - x_0) - \pi_{U+W}(y_0 - x_0)\| \\ &= d(y_0 - x_0, U + W) \end{aligned}$$

Sei $\pi_{U+W}(y_0 - x_0) = u - w$, $u \in U$, $w \in W$

$$\begin{aligned} \Rightarrow\ d(y_0 - x_0, U + W) &= \|y_0 - x_0 - (u - w)\| \\ &= \| \underbrace{y_0 + w}_{=y_1} - \underbrace{x_0 + u}_{=x_1} \| \\ &= \|y_1 - x_1\| \end{aligned}$$

x_1, y_1 eindeutig bestimmt $\Leftrightarrow$ Darstellung von

$$\underbrace{\pi_{U+W}(y_0 - x_0)}_{\in U+W} = u - w$$

eindeutig $\Leftrightarrow$ $U + W = U \oplus W$. □

Beispiel: $V = \mathbb{R}^3$, 2 (windschiefe) Geraden

$$g = \underbrace{\begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}}_{x_0} + \underbrace{[\begin{pmatrix} -1 \\ 2 \\ 1 \end{pmatrix}]}_{U} \qquad h = \underbrace{\begin{pmatrix} 2 \\ 1 \\ -1 \end{pmatrix}}_{y_0} + \underbrace{[\begin{pmatrix} 2 \\ 0 \\ 3 \end{pmatrix}]}_{W}$$

Gesucht: $d(g,h)$ und Lotfußpunkte. Dazu:

$$y_0 - x_0 = \underbrace{\begin{pmatrix} 2 \\ 0 \\ -1 \end{pmatrix}}_{z} \qquad U + W = [\underbrace{\begin{pmatrix} -1 \\ 2 \\ 1 \end{pmatrix}}_{u}, \underbrace{\begin{pmatrix} 2 \\ 0 \\ 3 \end{pmatrix}}_{w}]$$

und

$$d(y_0 - x_0, U + W) \leftrightarrow \underbrace{\pi_{U+W}(y_0 - x_0)}_{\pi(z)}$$

und

$$\pi_{U+W}(y_0 - x_0) = u - w$$

1. Methode:

$$\pi_{[\begin{pmatrix}-1\\2\\1\end{pmatrix},\begin{pmatrix}2\\0\\3\end{pmatrix}]}\begin{pmatrix}2\\0\\-1\end{pmatrix} =?$$

Bestimme ONB in $U+W$.

$$\underbrace{\frac{1}{\sqrt{6}}\begin{pmatrix}-1\\2\\1\end{pmatrix}}_{z_1},\ \underbrace{\frac{1}{\sqrt{462}}\begin{pmatrix}13\\-2\\17\end{pmatrix}}_{z_2}$$

Damit

$$\pi_{[\ldots]}\begin{pmatrix}2\\0\\-1\end{pmatrix} = \langle\begin{pmatrix}2\\0\\-1\end{pmatrix}, z_1\rangle z_1 + \langle\begin{pmatrix}2\\0\\-1\end{pmatrix}, z_2\rangle z_w = \frac{1}{77}\begin{pmatrix}58\\-80\\-13\end{pmatrix}$$

Daraus folgt

$$d(g,h) = \|\begin{pmatrix}2\\0\\-1\end{pmatrix} - \frac{1}{77}\begin{pmatrix}58\\-80\\-13\end{pmatrix}\| = \frac{16}{\sqrt{77}}$$

Weiter ist

$$\begin{aligned}\frac{1}{77} &= \alpha u + \beta w\\ &= \underbrace{-\frac{44}{77}\begin{pmatrix}1\\-2\\-1\end{pmatrix}}_{\tilde{u}} \underbrace{-\frac{-9}{77}\begin{pmatrix}2\\0\\3\end{pmatrix}}_{\tilde{w}}\end{aligned}$$

$\Rightarrow$ Lotfußpunkte

$$\begin{pmatrix}0\\1\\0\end{pmatrix} + \frac{40}{77}\begin{pmatrix}1\\-2\\-1\end{pmatrix} = \frac{1}{77}\begin{pmatrix}40\\-3\\-40\end{pmatrix} \in g$$

$$\begin{pmatrix}2\\1\\-1\end{pmatrix} + \frac{9}{77}\begin{pmatrix}-2\\0\\-3\end{pmatrix} = \frac{1}{77}\begin{pmatrix}136\\77\\-104\end{pmatrix} \in h$$

2. Methode:

$$(U+W)^\perp = [\begin{pmatrix}6\\5\\-4\end{pmatrix}], \qquad \text{ONB: } \frac{1}{77}\begin{pmatrix}6\\5\\-4\end{pmatrix}$$

Damit folgt

$$\begin{aligned}d(g,h) &= \|z - \pi_{U+W}(z)\|\\ &= \|\pi_{(U+W)^\perp}(z)\|\\ &= \|\frac{16}{77}\begin{pmatrix}6\\5\\-4\end{pmatrix}\|\\ &= \frac{16}{\sqrt{77}}\end{aligned}$$

Also

$$\pi_{U+W}(z) = \begin{pmatrix} 2 \\ 0 \\ -1 \end{pmatrix} - \frac{16}{77} \begin{pmatrix} 6 \\ 5 \\ -4 \end{pmatrix}$$
$$= \frac{1}{77} \begin{pmatrix} 58 \\ -80 \\ -13 \end{pmatrix}$$

Weiter wie in Methode 1.

Methode 3 Setze $x \in L$, $y \in M$ so, dass

$$y - x = (y_0 - x_0) + (w - u) \perp U + W = [\begin{pmatrix} -1 \\ 2 \\ 1 \end{pmatrix}, \begin{pmatrix} 2 \\ 0 \\ 3 \end{pmatrix}]$$

$\Rightarrow$ x, y Lotfußpunkte und $d(g,h) = \|y - x\|$

$$\Rightarrow \quad \begin{matrix} 6\alpha - \beta = -3 \\ \alpha - 13\beta = 1 \end{matrix} \qquad u = \alpha \begin{pmatrix} -1 \\ 2 \\ 1 \end{pmatrix}, \quad w = \beta \begin{pmatrix} 2 \\ 0 \\ 3 \end{pmatrix}$$

Vorlesung: 2005-06-04

§3 Adjungierte Abbildungen

Definition 5.8. Seien V, W euklidische Vektorräume. $\Phi \in \mathrm{Hom}(V, W)$.
Ein $\Psi \in \mathrm{Hom}(W, V)$ heißt *adjungierte Abbildung* zu Φ wenn gilt:

$$\langle \Phi(x), w \rangle = \langle x, \Psi(w) \rangle \qquad \forall x \in V, w \in W$$

Statt Ψ schreiben wir später Φ^*.

Bemerkung:

(i) Links und rechts stehen verschiedene Skalarprodukte!

(ii) Existiert die adjungierte Abbildung Φ, so ist sie eindeutig. **Beweis:** Seien

$$\langle x, \Psi_1(w) \rangle = \langle \Phi(x), w \rangle = \langle x, \Psi_2(w) \rangle \qquad \forall x \in V, w \in W$$

Dann

$$\Rightarrow \ \langle x, (\Psi_1 - \Psi_2)(w) \rangle = 0 \qquad \forall x \in V, w \in W$$
$$\Rightarrow \ (\Psi_1 - \Psi_2)(w) = 0 \qquad \forall w \in W$$
$$\Rightarrow \ \Psi_1 = \Psi_2$$

□

(iii) Existiert Φ^*, so existiert auch $(\Phi^*)^*$, nämlich $(\Phi^*)^* = \Phi$.

(iv) Φ^* existiert nicht immer! Zum Beispiel

$$\Phi : \mathbb{R}[X] \to \ell^2, \ p \mapsto p$$

Angenommen $\Phi^* : \ell^2 \to \mathbb{R}[X]$ würde existieren

$$\Rightarrow \langle x, \Phi^*(y)\rangle = \langle x, y\rangle \qquad \forall x \in \mathbb{R}[X],\ y \in \ell^2$$
$$\Rightarrow \langle x, \Phi^*(y) - y\rangle = 0 \qquad \forall x \in \mathbb{R}[X]$$
$$\Rightarrow \underbrace{\Phi^*(y)}_{\in \mathbb{R}[X] \subset \ell^2} - \underbrace{y}_{\in \ell^2} \in (\mathbb{R}[X])^\perp = \{o\} \qquad \forall y \in \ell^2$$
$$\Rightarrow \underbrace{\Phi^*(y)}_{\in \mathbb{R}[X]} = y \qquad \forall y \in \ell^2 \quad \text{Widerpsruch!}$$

Ab jetzt seien V, W endlich dimensional.

Satz 5.12 (Darstellungssatz von Riesz)**.** Sei V ein n-dimensionaler euklidischer Vektorraum und $x^* \in V^*$.
Dann existiert genau ein $v \in V$ mit

$$x^*(x) = \langle x, v\rangle \qquad \forall x \in V$$

Beweis: Es existiert eine ONB in V: $(x_1, \ldots, x_n)$. Setze

$$v := \sum_{i=1}^{n} x^*(x_i) x_i$$

Dann

$$\begin{aligned}\langle x, v\rangle &= \sum_{i=1}^{n} x^*(x_i)\langle x, x_i\rangle \\ &= x^*\Big(\underbrace{\sum_{i=1}^{n}\langle x, x_i\rangle x_i}_{x}\Big) \\ &= x^*(x) \qquad \forall x \in V\end{aligned}$$

□

Satz 5.13. Seien V, W endlich dimensionale euklidische Vektorräume und $\Phi \in \mathrm{Hom}(V, W)$.
Dann existiert die adjungierte Abbildung $\Phi^* \in \mathrm{Hom}(W, V)$.

Beweis: Sei $w \in W$ fest. Gesucht $\Psi(w)$.

$\Rightarrow$ Die Abbildung $x^* : x \mapsto \langle \Phi(x), w\rangle$ ist in V^*

$\overset{\text{Satz 5.12}}{\Rightarrow}$ $\exists v \in V$ mit $\langle \Phi(x), w\rangle = x^*(x) = \langle x, v\rangle$, für alle $x \in V$.

Setze $\Phi(W) = V$

$$\Rightarrow \langle \Phi(x), w\rangle = \langle x, \Psi(w)\rangle \tag{14}$$

gilt für dieses w und alle $x \in V$. Da $w \in W$ beliebig war, gilt (14) allgemein für alle $x \in V$ und $w \in W$.

Noch zu zeigen ist dass $\Psi \in \mathrm{Hom}(W, V)$.

$$\begin{aligned}\langle x, \Psi(aw + a'w')\rangle &= \langle \Phi(x), aw + a'w'\rangle \\ &= a\langle \Phi(x), w\rangle + a'\langle \Phi(x), w'\rangle \\ &= a\langle x, \Psi(w)\rangle + a'\langle x, \Psi(w')\rangle \\ &= \langle x, a\Psi(w) + a'\Psi(w')\rangle \qquad \forall x, a, a', w, w'\end{aligned}$$

$$\Rightarrow \Psi(aw + a'w') = a\Psi(w) + a'\Psi(w')$$

□

Bemerkung:

(i) Sei $\dim V = n < \infty$. Wir hatten im ersten Semester V und V^{**} indetifiziert.

Satz 5.12 gibt nun auch einen natürlichen Isomorphismus $V \to V^*$, $v \mapsto \langle \cdot, v \rangle$. Also werden wir für euklidische Vektorräume V, $\dim V = n$ $V = V^*$ setzen. Die Basis B fällt dann mit der Dualbasis B^* zusammen genau dann wenn B eine ONB ist.

(ii) Seien nun V, W euklidische Vektorräume mit ONBs $(x_1, \ldots, x_n)$ bzw. $(y_1, \ldots, y_n)$, $\Phi : V \to W$ linear, Φ^* adjungierte Abbildung.

Zusammenhang $A_\Phi \leftrightarrow A_{\Phi^*}$?

Behauptung: $A_{\Phi^*} = A_\Phi^\top$

Beweis:

$$\begin{aligned}
\langle \Phi(x), w \rangle &= \widehat{\Phi(x)}^\top \hat{w} \\
&= (A_\Phi \hat{x})^\top \hat{w} \\
&= \hat{x}^\top A_\Phi^\top \hat{w} \\
&= \hat{x}^\top A_{\Phi^*} \hat{w} \\
&= \hat{x}^\top \Phi^*(w) \\
&= \langle x, \Phi^*(w) \rangle \\
&= \langle \Phi(x), w \rangle
\end{aligned}$$

□

(iii) Falls $\dim V = \dim W = n$ folgt

$$\det \Phi = \det \Phi^*$$

(iv) Rechenregeln für adjungierte Abbildungen

- $(\Phi^*)^* = \Phi$
- $(a\Phi)^* = a\Phi^*$
- $(\Phi + \Psi)^* = \Phi^* + \Psi^*$
- $(\Phi \circ \Psi)^* = \Psi^* \circ \Phi^*$

Selbstadjungierte Abbildungen

Definition 5.9. Sei $\Phi \in \mathrm{End}(V)$. Φ heißt *selbstadjungiert* wenn Φ^* existiert und $\Phi = \Phi^*$ gilt, das heißt wenn

$$\langle \Phi(x), y \rangle = \langle x, \Phi(y) \rangle \qquad \forall x, y \in V$$

gilt.

Bemerkung: Gilt $\dim V = n$ und ist B ONB, so gilt

$$\begin{aligned}
\Phi \text{ selbstadjungiert} &\Leftrightarrow A_\Phi = A_\Phi^\top \\
&\Leftrightarrow A_\Phi \text{ symmetrisch}
\end{aligned}$$

Satz 5.14. Sei V n-dimensionaler euklidischer Vektorraum und $\Phi \in \mathrm{End}(V)$. Dann gilt

$$\Phi \text{ selbstadjungiert} \Leftrightarrow \text{Es existiert eine ONB aus Eigenvektoren von } \Phi$$

Beweis:

„$\Rightarrow$“: Φ selbstadjungiert $\Rightarrow$ A_Φ symmetrisch

$$\overset{\text{Satz 5.3}}{\Rightarrow} V = E_{\lambda_1} \oplus \ldots \oplus E_{\lambda_k}$$

und die E_{λ_i} sind paarweise orthogonal. Wähle in jedem E_{λ_i} eine ONB.

$\Rightarrow$ ONB aus V aus Eigenvektoren.

„$\Leftarrow$“: Sei $B = (x_1, \ldots, x_n)$ ONB aus Eigenvektoren: $\Phi(x_i) = c_i x_i$, c_i Eigenwerte

$$\begin{aligned}\langle x_i, \Phi(x_j)\rangle &= \langle x_i, c_j x_j\rangle \\ &= c_j \delta_{ij} \\ &= c_i \delta_{ij} \\ &= \langle c_i x_i, x_j\rangle \\ &= \langle \Phi(x_i), x_j\rangle\end{aligned}$$

$$\Rightarrow \langle \Phi(x), y\rangle = \langle x, \Phi(y)\rangle$$

□

Bemerkung: Ist A symmetrisch, so existiert eine ONB $(x_1, \ldots, x_n)$, $x_i \in \mathbb{R}^n$ aus Eigenvektoren von A

$\Rightarrow$ Für $S = \begin{pmatrix} x_1 & \cdots & x_n \end{pmatrix}$ gilt: $S^{-1}AS$ ist Diagonalmatrix. Hier gilt

$$S^\top S = E_n \Leftrightarrow S^{-1} = S^\top$$

Solche Matrizen heißen *orthogonal*.

Die Matrizen A und $A' = S^\top AS$ heißen dann auch *orthogonal-äquivalent*.

Beispiel:

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

$\Rightarrow$ Eigenwerte 0 und -2. Eigenräume $E_0 = [\begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}]$ und $E_{-2} = [\begin{pmatrix} 1 \\ 0 \\ -1 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}]$

ONB: $(\frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}, \frac{1}{\sqrt{12}} \begin{pmatrix} 1 \\ 0 \\ -1 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix})$

$$\Rightarrow S = \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{12}} & 0 \\ 0 & 0 & 1 \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{12}} & 0 \end{pmatrix}$$

$$\Rightarrow S^\top AS = \begin{pmatrix} 0 & 0 & 0 \\ 0 & -2 & 0 \\ 0 & 0 & -2 \end{pmatrix}$$

Vorlesung: 2005-06-07

§4 Isometrien

Definition 5.10. Seien U, W euklidische Vektorräume und $\Phi \in \mathrm{Hom}(V, W)$.

Φ heißt *Isometrie*, wenn

$$\langle \Phi(x), \Phi(y) \rangle = \langle x, y \rangle \qquad \forall x, y \in V$$

gilt.

Φ Isometrie $\Rightarrow$ Φ injektiv, aber im Allgemeinen nicht surjektiv. Falls Φ surjektiv ist, sagt man, dass V und W *isometrisch isomorph* sind.

Satz 5.15. Für $\Phi : V \to W$ sind äquivalent:

(i) Φ Isometrie

(ii) $\|\Phi(x)\| = \|x\|$ für alle $x \in V$

(iii) $d(\Phi(x), \Phi(y)) = d(x, y)$ für alle $x, y \in V$

Beweis:

(i) $\Rightarrow$ (ii): $\|\Phi(x)\| = \sqrt{\langle \Phi(x), \Phi(x) \rangle} = \sqrt{\langle x, x \rangle} = \|x\|$

(ii) $\Rightarrow$ (iii): Es gilt

$$\begin{aligned} d(\Phi(x), \Phi(y)) &= \|\Phi(x) - \Phi(y)\| \\ &= \|\Phi(x - y)\| \\ &= \|x - y\| \\ &= d(x, y) \end{aligned}$$

(iii) $\Rightarrow$ (i): Es gilt

$$\begin{aligned} \langle \Phi(x), \Phi(y) \rangle &= \frac{1}{4}\big(\|\Phi(x) + \Phi(y)\|^2 - \|\Phi(x) - \Phi(y)\|^2\big) \\ &= \frac{1}{4}\big(d(x, -y)^2 - d(x, y)^2\big) \\ &= \langle x, y \rangle \end{aligned}$$

□

Satz 5.16. Seien V, W euklidische Vektorräume mit $\dim V = \dim W = n \in \mathbb{N}_0$ und $\Phi \in \mathrm{Hom}(V, W)$. Dann sind äquivalent:

(i) Φ Isometrie

(ii) Für jede ONB $(x_1, \ldots, x_n)$ von V ist $(\Phi(x_1), \ldots, \Phi(x_n))$ ONB von W

(iii) Es gibt eine ONB $(x_1, \ldots, x_n)$ von V, für die $(\Phi(x_1), \ldots, \Phi(x_n))$ ONB von W ist

(iv) $\Phi^* \circ \Phi = \mathrm{id}_V$ und $\Phi \circ \Phi^* = \mathrm{id}_W$

(v) Bezüglich jeder ONB von V und jeder ONB von W ist A_Φ orthogonal

(vi) Es existieren ONBs in V und W, so dass A_Φ orthogonal ist

Beweis:

(i) $\Rightarrow$ (ii): Φ ist injektiv, also wegen $\dim V = \dim W = n$ auch surjektiv, das heißt bijektiv.
Sei $(x_1, \ldots, x_n)$ ONB $\Rightarrow$ $(\Phi(x_1), \ldots, \Phi(x_n))$ Basis. Wegen

$$\langle \Phi(x_i), \Phi(x_j) \rangle = \langle x_i, x_j \rangle = \delta_{ij}$$

folgt ONB.

(ii) $\Rightarrow$ (iii): Folgt aus Satz 5.7.

(iii) $\Rightarrow$ (vi): Bezüglich ONB $(x_1, \ldots, x_n)$ und $(\Phi(x_1), \ldots, \Phi(x_n))$ ist $A_\Phi = E_n$ $\Rightarrow$ $A_\Phi^\top A_\Phi = E_n$, also A_Φ orthogonal.

(vi) $\Rightarrow$ (iv): Bezüglich der ONBs in V und W gilt:

$$\begin{aligned} A_{\Phi^* \circ \Phi} &= A_{\Phi^*} \cdot A_\Phi \\ &= A_\Phi^\top \cdot A_\Phi \\ &= E_n \\ &= A_{\mathrm{id}_V} \end{aligned}$$

$\Rightarrow$ $\Phi^* \circ \Phi = \mathrm{id}_V$. Analog: $\Phi \circ \Phi^* = \mathrm{id}_W$.

(iv) $\Rightarrow$ (i): Es gilt

$$\begin{aligned} \langle \Phi(x), \Phi(y) \rangle &= \langle x, (\Phi^* \circ \Phi)(y) \rangle \\ &= \langle x, y \rangle \end{aligned}$$

(iv) $\Rightarrow$ (v): Es gilt $\Phi^* \circ \Phi = \mathrm{id}_V \overset{\text{Bzgl. ONBs}}{\Rightarrow} E_n = A_{\mathrm{id}_V} = A_{\Phi^* \circ \Phi} = A_\Phi^\top \cdot A_\Phi$. Analog $A_\Phi \cdot A_\Phi^\top = E_n$.
$\Rightarrow$ A_Φ orthogonal.

(v) $\Rightarrow$ (vi): Folgt aus Satz 5.7.

□

Ab jetzt $V = W$ mit $\dim V = n$. $\Phi : V \to V$ Isometrie.

Eigenwerte? $\Phi(x) = cx$, $x \neq 0$

$$\Rightarrow \underbrace{\|\Phi(x)\|}_{\|x\| \neq 0} = |c| \|x\| \Rightarrow |c| = 1 \Rightarrow c = \pm 1$$

$\Rightarrow$ Bis auf triviale Fälle keine Jordannormalform (im Reellen). Andere Normalform?

Satz 5.17 (Normalform von Isometrien)**.** Sei V euklidischer Vektorraum, $\dim V = n$ und $\Phi : V \to V$ Isometrie. Dann existiert eine ONB von V bezüglich der A_Φ die folgende Gestalt hat:

$$A_\Phi = \begin{pmatrix} 1 & & & & & & & & & 0 \\ & \ddots & & & & & & & & \\ & & 1 & & & & & & & \\ & & & -1 & & & & & & \\ & & & & \ddots & & & & & \\ & & & & & -1 & & & & \\ & & & & & & \cos\omega_1 & -\sin\omega_1 & & \\ & & & & & & \sin\omega_1 & \cos\omega_1 & & \\ & & & & & & & & \ddots & \\ & & & & & & & & \cos\omega_k & -\sin\omega_k \\ 0 & & & & & & & & \sin\omega_k & \cos\omega_k \end{pmatrix}$$

mit $\omega_i \in [0, \pi]$, $i = 1, \ldots, k$.

Definition 5.11. Isometrien $\Phi : \mathbb{R}^n \to \mathbb{R}^n$ heißen auch *Drehungen*, genauer *eigentliche Drehungen* für $\det \Phi = 1$. Ist $\det \Phi = -1$, so heißt Φ *Drehspiegelung* (uneigentliche Drehung). Die Isometrien bilden eine Gruppe, die orthogonalen Matrizen also auch:

- $O(n)$ – *Orthogonale Gruppe*
- $SO(n)$ – *Spezielle Orthogonale Gruppe* $\{A \in O(n) \mid \det A = 1\}$

Interpretation von 5.17:

Drehkästchen

$$\boxed{\begin{pmatrix} \cos\omega & -\sin\omega \\ \sin\omega & \cos\omega \end{pmatrix}} =: \tilde{A}$$

$\tilde{A} : \mathbb{R}^2 \to \mathbb{R}^2$

$$x = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} r\cos\alpha \\ r\sin\alpha \end{pmatrix}$$

$$\Rightarrow \tilde{A}x = \begin{pmatrix} \cos\omega & -\sin\omega \\ \sin\omega & \cos\omega \end{pmatrix} \begin{pmatrix} r\cos\alpha \\ r\sin\alpha \end{pmatrix} = \begin{pmatrix} r\cos(\alpha+\omega) \\ r\sin(\alpha+\omega) \end{pmatrix}$$

$\Rightarrow$ $\tilde{A}$ bewirkt eine Drehung um den Winkel ω.

$n = 2$: $\det A = -1$:

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

$\Rightarrow$ Spiegelung an einer Geraden durch 0.

$\det A = 1$:

$$\tilde{A} = \begin{pmatrix} \cos\omega & -\sin\omega \\ \sin\omega & \cos\omega \end{pmatrix}$$

$\Rightarrow$ Drehung um $\omega \in [0, \pi]$.

$n = 3$: Drehung:

$$\tilde{A} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos\omega & -\sin\omega \\ 0 & \sin\omega & \cos\omega \end{pmatrix} = \begin{pmatrix} u & v & w \end{pmatrix}$$

oder Drehspiegelung:

$$\tilde{A} = \begin{pmatrix} -1 & 0 & 0 \\ 0 & \cos\omega & -\sin\omega \\ 0 & \sin\omega & \cos\omega \end{pmatrix}$$

$\omega \in [0, \pi]$.

$[u] = U$ Drehachse, $[v, w] = U^\perp$ Drehebene, ω Drehwinkel

Vorlesung: 2005-07-13

Beweis: (Beweis zu Satz 5.17)

„⇐“: $A_\Phi \cdot A_\Phi^\top \overset{\text{Satz 5.16}}{=} E_n \Rightarrow \Phi$ Isometrie

„⇒“: Setze $\Psi := \Phi + \underbrace{\Phi^*}_{\Phi^{-1}} : V \to V$. Ψ ist selbstadjungiert.

$\overset{\text{Satz 5.14}}{\Rightarrow}$ Es existiert eine orthogonale Zerlegung von V in Eigenräume von Ψ.

1.) Ψ hat Eigenwert $2 \Leftrightarrow \Phi$ hat Eigenwert 1.

„⇐“: $\Phi(x) = 1 \cdot x, x \neq 0$

$$\begin{aligned} \Rightarrow \Psi(x) &= \Phi(x) + \Phi^{-1}(x) \\ &= x + x \\ &= 2x \end{aligned}$$

$\Rightarrow x$ Eigenvektor von Ψ zum Eigenwert 2.

„⇒“: Sei $x \neq 0$ mit $\Psi(x) = 2x \Rightarrow \Phi(x) + \Phi^*(x) = 2x \Rightarrow 2\langle \Phi(x), x\rangle = 2\langle x, x\rangle$

$$\begin{aligned} \Rightarrow \|\Phi(x) - x\|^2 &= \langle \Phi(x) - x, \Phi(x) - x\rangle \\ &= \langle \Phi(x), \Phi(x)\rangle + \langle x, x\rangle - 2\langle \Phi(x), x\rangle \\ &= 0 \end{aligned}$$

$\Rightarrow \Phi(x) = x$.

2.) Ψ hat Eigenwert $-2 \Leftrightarrow \Phi$ hat Eigenwert -1 analog.

$$\Rightarrow V = E_2 \oplus E_{-2} \oplus E_{c_1} \oplus \ldots \oplus E_{c_k} \qquad c_i \neq \pm 2$$

E_2 und E_{-2} können unter Umständen $\{o\}$ sein.

3.) Alle Eigenräume E_c von Ψ sind Φ-invariant:

$$\Psi(x) = cx \qquad \forall x \in E_c$$

$\Phi(x)$?

$$\begin{aligned} \Psi(\Phi(x)) &= \Phi^2(x) + x \\ &= \Phi(\Psi(x)) \\ &= \Phi(cx) \\ &= c\Phi(x) \end{aligned}$$

$\Rightarrow \Phi(x) \in E_c$ ($\Rightarrow \Phi(E_c) = E_c$)

Sei nun $c \neq \pm 2$ Eigenwert von Ψ, Eigenraum E_c

4.) $\dim E_c$ ist gerade und E_c ist die orthogonale Summe von $l = \frac{1}{2}\dim E_c$ zweidimensionalen Unterräumen U_i, die Φ-invariant sind.

Angenommen $\dim E_c$ ungerade $\Rightarrow \Phi|_{E_c}$ hat einen Eigenwert weil charakteristisches Polynom eine Nullstelle besitzt.

$\Rightarrow \exists x \in E_c, x \neq 0$ mit $\Phi(x) = x$ oder $\Phi(x) = -x$

$\Rightarrow x \in E_2$ oder $x \in E_{-2}$ - Widerspruch

$\Rightarrow \dim E_c$ gerade.

Sei $x \neq 0$ aus E_c beliebig.

Behauptung: $U = [x, \Phi(x)]$ ist Φ-invariant. Es gilt $\dim U = 2$ und

$$x \mapsto \Phi(x) \in U$$

$\Phi(x) \mapsto \Phi(x) \in U$?

Betrachte $\Psi(x) = cx \Rightarrow \Phi(x) + \Phi^{-1}(x) = cx \Rightarrow \Phi^2(x) + x = cx$

$$\Phi^2(x) = c\Phi(x) - x \tag{15}$$

$\Rightarrow \Phi(U) \subset U$ ($\Rightarrow \Phi(U) = U$). Setze $U_i = U$.

Nun betrachten wir $U^\perp \cap E_c$ und wählen $x \in U^\perp \cap E_c$, $x \neq 0$.

Einschub. $U_1^\perp \cap E_c$ ist wieder Φ-invariant:
Sei $x \in U_1^\perp \cap E_c \Rightarrow \Phi(x) \in E_c$ und wenn $y \in U_1$, dann

$$\begin{aligned}\langle \Phi(x), y\rangle &= \langle x, \Phi^*(y)\rangle \\ &= \langle x, \underbrace{\Phi^{-1}(y)}_{\in U}\rangle \\ &= 0\end{aligned}$$

$\Rightarrow U_2 = [x, \Phi(x)] \Rightarrow \Phi(U_2) = U_2$ und $U_1 \perp U_2$. Analog: Wähle $x \in (U_1 \oplus U_2)^\perp \cap E_2$, $U_3 = [x, \Phi(x)]$, usw.
Verfahren bricht nach l Schritten ab und liefert

$$E_c = U_1 \oplus \cdots \oplus U_l$$

5.) Sei nun $U = [x, \Phi(x)]$, $x \in E_c$, $c \neq \pm 2$, $x \neq 0$, $\|x\| = 1$.
Wähle ONB in U mit erstem Vektor x und

$$y = \frac{\Phi(x) - \langle x, \Phi(x)\rangle x}{\|\Phi(x) - \langle x, \Phi(x)\rangle x\|}$$

Damit folgt

$$\begin{aligned}\langle x, \Phi(x)\rangle &= \langle \Phi^*(x), x\rangle \\ &= \langle \Phi^{-1}(x), x\rangle \\ &= c\langle x, x\rangle - \langle x, \Phi(x)\rangle\end{aligned}$$

also $\langle x, \Phi(x)\rangle = \frac{c}{2}\langle x, x\rangle = \frac{c}{2}$.
$\Rightarrow \exists \omega \in (0, \pi)$ mit ´

$$\cos\omega = \langle x, \Phi(x)\rangle = \frac{c}{2}$$

und

$$\sin\omega = \sqrt{1 - \frac{c^2}{4}}$$

Damit

$$\begin{aligned}\|\Phi(x) - \langle x, \Phi(x)\rangle x\|^2 &= \|\Phi(x)\|^2 + \langle x, \Phi(x)\rangle^2\|x\|^2 - 2\langle x, \Phi(x)\rangle\Phi(x)x \\ &= 1 - \langle x, \Phi(x)\rangle^2 \\ &= 1 - \cos^2\omega \\ &= \sin^2\omega\end{aligned}$$

$\Rightarrow y = \frac{1}{\sin\omega}(\Phi(x) - \cos\omega x)$

$$\begin{aligned}\Rightarrow \Phi(y) &= \frac{1}{\sin\omega}(\Phi^2(x) - \cos\omega\Phi(x)) \\ &\overset{(15)}{=} \frac{1}{\sin\omega}(2\cos\omega\Phi(x) - x - \cos\omega\Phi(x)) \\ &= \frac{1}{\sin\omega}(\cos^2\omega x + \cos\omega\sin\omega y - x) \\ &= -\sin\omega x + \cos\omega x\end{aligned}$$

ONB (x, y). Darstellung von $\Phi|_U$ bezüglich dieser ONB

$$\Phi(x) = \cos\omega x + \sin\omega y$$
$$\Phi(y) = -\sin\omega x + \cos\omega x$$

Damit folgt

$$A_{\Phi|U} = \begin{pmatrix} \cos\omega & -\sin\omega \\ \sin\omega & \cos\omega \end{pmatrix}$$

□

Satz 5.18 (Matrix-Version von Satz 5.17)**.** Sei $A \in \mathbb{R}^{n\times n}$. Dann gilt:

A orthogonal $\Leftrightarrow$ $\exists$ orthogonale Matrix S mit

$$\tilde{A} = S^\top A S = \begin{pmatrix} 1 & & & & & & & & & 0 \\ & \ddots & & & & & & & & \\ & & 1 & & & & & & & \\ & & & -1 & & & & & & \\ & & & & \ddots & & & & & \\ & & & & & -1 & & & & \\ & & & & & & \cos\omega_1 & -\sin\omega_1 & & \\ & & & & & & \sin\omega_1 & \cos\omega_1 & & \\ & & & & & & & & \ddots & \\ & & & & & & & & \cos\omega_k & -\sin\omega_k \\ 0 & & & & & & & & \sin\omega_k & \cos\omega_k \end{pmatrix}$$

Beispiel:

$$A = \frac{1}{9\sqrt{2}} \begin{pmatrix} 9 & 4 & 8 & 1 \\ -4 & 9 & -1 & 8 \\ -8 & 1 & 9 & -4 \\ -1 & -8 & 4 & 9 \end{pmatrix}$$

Damit gilt

$$A + A^\top = \frac{1}{9\sqrt{2}} \begin{pmatrix} 18 & 0 & 0 & 0 \\ 0 & 18 & 0 & 0 \\ 0 & 0 & 18 & 0 \\ 0 & 0 & 0 & 18 \end{pmatrix}$$

$\Rightarrow$ $c = \sqrt{2}$ $\Rightarrow$ $\cos\omega = \frac{1}{2}\sqrt{c}$, $\sin\omega = \frac{1}{2}\sqrt{2}$

$\Rightarrow$ $E_c = \mathbb{R}^4$, U_1, U_2?

$x \in \mathbb{R}^4$ mit $\|x\| = 1$ beliebig, zum Beispiel $x = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}$

$\Rightarrow$ Ax mit Gram-Schmidt orthogonalisieren

$$U_1 = [\begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \frac{1}{9}\begin{pmatrix} 0 \\ 4 \\ -8 \\ -1 \end{pmatrix}]$$

$\Rightarrow$ $U_1^\perp$ bestimmen, $x \in U_1^\perp$, $\|x\| = 1$ beliebig, usw.

ENDE!

6 Anhang

§1 Klausurvorbereitung

Dies ist der Mitschrieb der Klausurvorbereitungsaufgaben die Herr Hoffmann in der großen Saalübung jeden Montag durchführt.

Übung: 2005-04-18

Wiederholung (Gruppe). $(G, \circ)$ heißt *Gruppe* falls G Menge und $\circ : G \times G \to G$ mit folgenden Eigenschaften

(i) $\forall a, b, c, \in G : a \circ (b \circ c) = (a \circ b) \circ c$

(ii) $\exists e \in G : \forall a \in G : a \circ e = e \circ a = a$

(iii) $\forall a \in G : \exists a^{-1} \in G : a \circ a^{-1} = e = a^{-1} \circ a$

G heißt *abelsch* falls zusätzlich gilt

(iv) $\forall a, b \in G : a \circ b = b \circ a$

Wiederholung (Untergruppe). Sei $M \subseteq G$. M heißt *Untergruppe* von G, falls $(M, \circ)$ eine Gruppe ist.

Wiederholung (Untergruppenkriterium). $M \subseteq G$ ist Untergruppe $\Leftrightarrow$

(i) $M \neq \emptyset$

(ii) $\forall x, y \in M : x^{-1} \circ y \in M$

oder $\Leftrightarrow$

(i) $M \neq \emptyset$

(ii) $\forall x \in M : x^{-1} \in M$

(iii) $\forall x, y \in M : x \circ y \in M$

Aufgabe 1. Es sei $(G, \circ)$ eine Gruppe mit Neutralelement e. Weiter sei

$$M := \{x \in G \mid x \circ x = e\}$$

Zeigen Sie

(a) Ist G kommutativ, so ist M eine Untergruppe von G.

(b) Sei $n \geq 3$ und $G := S_n$, dann ist M keine Untergruppe von G.

Lösung von Aufgabe 1:

(a) Zu Zeigen:

1) $M \neq \emptyset$, da $e \circ e = e$ ist $e \in M$.

2) $\forall x \in M : x^{-1} \in M$, denn

$$\begin{aligned} x \in M &\Leftrightarrow x \circ x = e \\ &\Leftrightarrow (x^{-1} \circ x) \circ x = x^{-1} \circ e \\ &\Leftrightarrow x = x^{-1} \\ &\Leftrightarrow x^{-1} \circ x = x^{-1} \circ x^{-1} \\ &\Leftrightarrow e = x^{-1} \circ x^{-1} \\ &\Leftrightarrow x^{-1} \in M \end{aligned}$$

3) $\forall x, y \in M : x \circ y \in M$, denn

$$\begin{aligned} (x \circ y) \circ (x \circ y) &= \underbrace{(x \circ x)}_{e} \circ \underbrace{(y \circ y)}_{e} \\ &= e \circ e \\ &= e \end{aligned}$$

Also ist M eine Untergruppe von G.

(b) Sei $n \geq 3$ und $G = S_n$, dann ist M keine Untergruppe von G.

$$S_n := \{\pi : \{1, \ldots, n\} \rightarrow \{1, \ldots, n\} : \pi \text{ bijektiv}\}$$

und „$\circ$“ ist die Verkettung von Abbildungen. Seien

$$\tau_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & \cdots & n \\ 3 & 2 & 1 & 4 & \cdots & n \end{pmatrix}$$

$$\tau_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & \cdots & n \\ 2 & 1 & 3 & 4 & \cdots & n \end{pmatrix}$$

Da $\tau_1 \circ \tau_1 = \tau_2 \circ \tau_2 = \left(\begin{smallmatrix} 1 & 2 & 3 & \cdots & n \\ 1 & 2 & 3 & \cdots & n \end{smallmatrix}\right) = \mathrm{id}_{1,\ldots,n} \Rightarrow \tau_1, \tau_2 \in M$.
Aber $(\tau_1 \circ \tau_2) \circ (\tau_1 \circ \tau_2)(1) = 3 \neq 1$, also ist $(\tau_1 \circ \tau_2) \circ (\tau_1 \circ \tau_2) \neq \mathrm{id}_{1,\ldots,n}$ d.h. $\tau_1 \circ \tau_2 \notin M$.
Also ist M keine Untergruppe.

Übung: 2005-04-25

Wiederholung. Eine Abbildung $\Phi : V \rightarrow V$ heißt *Projektion*, falls

$$\Phi^2 = \Phi$$

also $\Phi^2(x) = \Phi(x)$ für alle $x \in V$.

Aufgabe 2. Sei V ein Vektorraum und Φ ein Endomorphismus von V, so dass

$$\Phi^2(\mathrm{id}_V - \Phi) \;=\; \Phi(\mathrm{id}_V - \Phi)^2 \;=\; 0$$

(a) Zeigen Sie, dass Φ eine Projektion ist.

(b) Geben Sie ein Beispiel für ein Vektorraum V und ein Endomorphismus Φ von V an, so dass

$$\Phi^2(\mathrm{id}_V - \Phi) = 0$$

aber

$$\Phi^2 \neq \Phi$$

Lösung von Aufgabe 2:

(a) Es gilt

$$\Phi^2 - \Phi^3 \Leftrightarrow \Phi^3 = \Phi^2 \tag{16}$$

$$\Phi(\mathrm{id}_V - 2\Phi + \Phi^2) = 0 \Leftrightarrow \Phi - 2\Phi^2 + \Phi^3 = 0 \tag{17}$$

Mit (16) in (17)

$$\Phi - 2\Phi^2 + \Phi^2 = \Phi - \Phi^2 = 0 \Leftrightarrow \Phi = \Phi^2$$

(b) $V = \mathbb{R}^2$, so suchen wir $A \in \mathbb{R}^{2\times 2}$ mit

$$A^2(E_2 - A) = 0$$

aber $A^2 \neq A$.

Gesucht $A \in \mathbb{R}^{2\times 2}$ mit $A^2 = 0$ aber $A \neq 0$.

$$A^2 = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}^2 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

erfüllt die Voraussetzung.

Ist Φ die lineare Abbildung mit Abbildungsmatrix A bezüglich der Standardbasis, so gilt

$$\underbrace{\Phi^2}_{=0}(\mathrm{id}_V - \Phi) = 0$$

aber $\Phi^2 = 0 \neq \Phi$.

Übung: 2005-05-02

Wiederholung.

$$\mathrm{Kern}\,\Phi := \{x \in V \mid \Phi(x) = 0\}$$
$$\mathrm{Bild}\,\Phi := \{y \in V \mid \exists x \in V : \Phi(x) = y\} = \Phi(V)$$

U, W Untervektorräume von V.

$$U + W := \{u + w | u \in U, w \in W\}$$

$U + W$ direkt, falls gilt

$$U \cap W = \{o\}$$

Falls $U \oplus W$ direkt ist, gilt: Für alle $x \in U \oplus W$ existieren endlich bestimmte $u \in U$ und $w \in W$ mit $x = u + w$. Es gilt

- $\dim(U + W) = \dim U + \dim W - \dim(U \cap W)$
- $\dim V = \dim \mathrm{Bild}\,\Phi + \dim Kern\Phi$

Aufgabe 3. Sei V ein $\mathbb{K}$-Vektorraum mit $\dim V < \infty$ und $\Phi : V \to V$ ein Endomorphismus mit

$$\mathrm{Kern}\,\Phi = \mathrm{Kern}(\Phi^2) \tag{18}$$

(a) Zeigen Sie, dass $V = \mathrm{Kern}(\Phi) \oplus \mathrm{Bild}(\Phi)$

(b) Zeigen Sie, dass a ohne Voraussetzung 18 im allgemeinen nicht gilt.

Lösung von Aufgabe 3:

(a) Seien

$$\operatorname{Kern}\Phi \cap \operatorname{Bild}\Phi = \{o\} \tag{19}$$
$$\dim V = \dim \operatorname{Bild}\Phi + \dim \operatorname{Kern}\Phi \tag{20}$$

Damit folgt

$$\dim \operatorname{Bild}\Phi + \dim \operatorname{Kern}\Phi - \dim(\operatorname{Bild}\Phi \cap \dim \operatorname{Kern}\Phi) \overset{(19)}{=} \dim \operatorname{Bild}\Phi + \dim \operatorname{Kern}\Phi$$

Es bleibt zu zeigen: $\operatorname{Kern}\Phi \cap \operatorname{Bild}\Phi = \{o\}$.

Sei $x \in \operatorname{Kern}\Phi \cap \operatorname{Bild}\Phi$, das heißt

1. $\Phi(x) = 0$
2. $\exists y \in V : \Phi(y) = x$

$$\Phi^2(y) = \Phi(\Phi(y)) = \Phi(x) = o$$

Also gilt $y \in \operatorname{Kern}\Phi^2$. Also $y \in \operatorname{Kern}\Phi$.

$\Rightarrow\ \Phi(y) = 0 = x$, das heißt $x = 0$. Also gilt $\operatorname{Kern}\Phi \cap \operatorname{Bild}\Phi = \{o\}$.

(b) Gesucht: V und $\Phi : V \to V$ mit $\operatorname{Kern}\Phi \subsetneqq \operatorname{Kern}(\Phi^2)$. Z.B.: $V = \mathbb{R}^2$.

Sei A_Φ die Abbildungsmatrix von Φ bzgl. der Standardbasis

$$A_\Phi := \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$$

Dann folgt

$$\operatorname{Kern}\Phi = [\begin{pmatrix} 0 \\ 1 \end{pmatrix}] \quad \operatorname{Kern}(\Phi^2) = \mathbb{R}^2$$
$$\operatorname{Bild}\Phi = [\begin{pmatrix} 0 \\ 1 \end{pmatrix}]$$
$$\operatorname{Kern}\Phi + \operatorname{Bild}\Phi = [\begin{pmatrix} 0 \\ 1 \end{pmatrix}] \neq V$$

Übung: 2005-05-09

Wiederholung.

- $\Phi : V \to \mathbb{K}$ linear heißt *Linearform*
- $V^* = \{\Phi : V \to \mathbb{K} \mid \Phi\text{linear}\}$ heißt *Dualraum*
- Sei $\dim V = n$ und $(b_1, \ldots, b_n)$ eine Basis von V. $(b_1^*, \ldots, b_n^*)$ heißt zugehörige *Dualbasis* falls gilt

$$b_i^*(b_j) = \delta_{ij} = \begin{cases} 1 & \text{falls} \quad i = j \\ 0 & \text{falls} \quad i \neq j \end{cases}$$

- $x_1, \ldots, x_k \in V$ heißen *linear unabhängig* genau dann wenn

$$\sum_{i=0}^{k} a_i x_i = 0 \ \Rightarrow\ a_1, \ldots, a_k = 0$$

Aufgabe 4. Sei V ein n-dimensionaler $\mathbb{K}$-Vektorraum und $\Phi_1, \ldots, \Phi_n$ Linearformen auf V.

Zeigen Sie: $\Phi_1, \ldots, \Phi_n$ linear unabhängig genau dann wenn

$$\forall x_1, \ldots, x_n \in V : \det \begin{pmatrix} \Phi_1(x_1) & \cdots & \Phi_n(x_1) \\ \vdots & & \vdots \\ \Phi_1(x_n) & \cdots & \Phi_n(x_n) \end{pmatrix} = 0$$

Lösung von Aufgabe 4:

$\Rightarrow$: $\Phi_1, \ldots, \Phi_n$ linear abhängig, das heißt es existieren $a_1, \ldots, a_n \in \mathbb{K}$ nicht alle Null mit

$$a_1\Phi_1 + \ldots + a_n\Phi_n = 0 \in V^*$$

Seien $x_1, \ldots, x_n \in V$. Dann gilt

$$\begin{array}{ccccccc} a_1\Phi_1(x_1) & + & \ldots & + & a_n\Phi_n(x_1) & = & 0 \quad \in \mathbb{K} \\ \vdots & & & & \vdots & & \vdots \\ a_1\Phi_n(x_n) & + & \ldots & + & a_n\Phi_n(x_n) & = & 0 \quad \in \mathbb{K} \end{array}$$

In Matrixschreibweise

$$\begin{pmatrix} \Phi_1(x_1) & \cdots & \Phi_n(x_1) \\ \vdots & & \vdots \\ \Phi_1(x_n) & \cdots & \Phi_n(x_n) \end{pmatrix} \cdot \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix} \in \mathbb{K}^n$$

$(a_1, \ldots, a_n)^\top \in \mathbb{K}^n$ ist nicht der Nullvektor, das heißt zur Matrix A gehörende homogene LGS ist nicht trivial lösbar. Damit ist A nicht invertierbar, also $\det A = 0$.

$\Leftarrow$: Seien $x_1, \ldots, x_n \in V$. Nach Voraussetzung existieren $a_1, \ldots, a_n \in \mathbb{K}$, so dass

$$a_1\Phi_1(x_i) + \ldots + a_n\Phi_n(x_i) = 0 \in \mathbb{K} \qquad i = 1, \ldots, n$$

Wäre $\{x_1, \ldots, x_n\}$ eine Basis von V, so müsste

$$a_1\Phi_1 + \ldots + a_n\Phi_n = 0 \in V^*$$

Da $x_1, \ldots, x_n \in V$ beliebig waren, können wir sie speziell also linear unabhängig wählen. Da nicht alle a_i Null sein müssen sind $\Phi_1, \ldots, \Phi_n$ linear unabhängig.

Übung: 2005-05-23

Aufgabe 5. Seien

$$A := \begin{pmatrix} -\frac{1}{2} & 0 & \frac{1}{2} \\ -\frac{1}{2} & 1 & \frac{1}{2} \\ \frac{1}{2} & 0 & -\frac{1}{2} \end{pmatrix} \qquad \Phi : \mathbb{R}^3 \underset{x \mapsto Ax}{\to} \mathbb{R}^3$$

(a) Zeigen Sie, dass Φ diagonalisierbar ist und bestimmen Sie eine Matrix S, für die $S^{-1}AS$ Diagonalgestalt hat.

(b) Für welche $n \in \mathbb{N}$ ist Φ^n eine Projektion?

Lösung von Aufgabe 5:

(a) Berechne $\det(A - X \cdot E_3)$

$$\begin{vmatrix} -\frac{1}{2} - X & 0 & \frac{1}{2} \\ -\frac{1}{2} & 1 - X & \frac{1}{2} \\ \frac{1}{2} & 0 & -\frac{1}{2} - X \end{vmatrix} = (1 - X) \begin{vmatrix} -\frac{1}{2} - X & \frac{1}{2} \\ \frac{1}{2} & -\frac{1}{2} - X \end{vmatrix} \quad \hookleftarrow +$$

$$\underline{-1} \quad \downarrow \quad + \text{ (Diagonale)}$$

$$= (1 - X) \begin{vmatrix} -X & -X \\ \frac{1}{2} & -\frac{1}{2} - X \end{vmatrix}$$

$$= (1 - X) \begin{vmatrix} -X & 0 \\ \frac{1}{2} & -1 - X \end{vmatrix}$$

$$= -X(1 - X)(-1 - X)$$

$-1, 0, 1$ sind die Eigenwerte von Φ. Also ist Φ diagonalisierbar, weil das Minimalpolynom in einfache Linearfaktoren zerfällt.

- Eigenraum zum Eigenwert 0, d.h. Lösungsraum des LGS $Ax = 0$

$$E_0 = [\begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}]$$

- Eigenraum zum Eigenwert 1, d.h. Lösungsraum des LGS $(A - E)x = 0$

$$E_1 = [\begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}]$$

- Eigenraum zum Eigenwert -1, d.h. Lösungsraum des LGS $(A + E)x = 0$

$$E_{-1} = [\begin{pmatrix} 0 \\ 1 \\ -2 \end{pmatrix}]$$

Damit folgt

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

(b) Φ Projektion $\Rightarrow$ $\Phi^2 = \Phi$

$$\overset{\dim V < \infty}{\Rightarrow} V = \operatorname{Kern} \Phi \oplus \operatorname{Bild} \Phi$$

Die Eigenwerte von Φ^n sind $(-1)^n, 0^n, 1^n$, also $-1, 0, 1$ falls n ungerade und $0, 1$ falls n gerade.

Bzgl. $(\begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 2 \\ 1 \\ -2 \end{pmatrix})$ hat Φ die Abbildungsmatrix

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

Φ^n hat dann die Abbildungsmatrix $\widetilde{A}^n$

$$\widetilde{A}^n = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 1^n & 0 \\ 0 & 0 & (-1)^n \end{pmatrix}$$

Ist n ungerade, so ist -1 Eigenwert $\Rightarrow$ Φ^n keine Projektion. Ist n gerade $\Rightarrow$ Φ^n Projektion.

Übung: 2005-05-30

Aufgabe 6. Es sei $V = \mathbb{R}^{2\times 3}$ und

$$\begin{array}{rccc} \Phi: & V & \to & V \\ & \left(\begin{smallmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \end{smallmatrix}\right) & \mapsto & \left(\begin{smallmatrix} a_{11}-a_{21} & a_{12}+a_{22} & 2a_{13}+a_{23} \\ a_{11}+a_{21} & -a_{12}+2a_{22} & a_{13}+4a_{23} \end{smallmatrix}\right) \end{array}$$

Bestimmen Sie $\det(\Phi)$.

Lösung von Aufgabe 6:

Gesucht ist eine Wyrre-Basis[2] von V. Idee:

$$B = (\underbrace{\begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}}_{M_1}, \underbrace{\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix}}_{M_2}, \underbrace{\begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}}_{M_3}, \underbrace{\begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \end{pmatrix}}_{M_4}, \underbrace{\begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}}_{M_5}, \underbrace{\begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}}_{M_6})$$

Bilder der Basisvektoren:

$$\begin{aligned} \Phi(M_1) &= \begin{pmatrix} 1 & 0 & 0 \\ 1 & 0 & 0 \end{pmatrix} = 1 \cdot M_1 + 1 \cdot M_4 \\ \Phi(M_2) &= \begin{pmatrix} 0 & 1 & 0 \\ 0 & -1 & 0 \end{pmatrix} = 1 \cdot M_2 - 1 \cdot M_5 \\ \Phi(M_3) &= \begin{pmatrix} 0 & 0 & 2 \\ 0 & 0 & 1 \end{pmatrix} = 2 \cdot M_3 + 1 \cdot M_6 \\ \Phi(M_4) &= \begin{pmatrix} -1 & 0 & 0 \\ 1 & 0 & 0 \end{pmatrix} = -1 \cdot M_1 + 1 \cdot M_4 \\ \Phi(M_5) &= \begin{pmatrix} 0 & 1 & 0 \\ 0 & 2 & 0 \end{pmatrix} = 1 \cdot M_2 + 2 \cdot M_5 \\ \Phi(M_6) &= \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 4 \end{pmatrix} = 1 \cdot M_3 + 4 \cdot M_6 \end{aligned}$$

Damit folgt

$$A_\Phi = \begin{pmatrix} 1 & 0 & 0 & -1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & -1 & 0 & 0 & 2 & 0 \\ 0 & 0 & 1 & 0 & 0 & 4 \end{pmatrix}$$

[2] Vgl. http://www.ru-eschweilerhof.de/cs/fb17/algodat/vortrag/img17.html

Also

$$
\begin{aligned}
\det A_\Phi &= \begin{vmatrix} 1 & 0 & 0 & -1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & -1 & 0 & 0 & 2 & 0 \\ 0 & 0 & 1 & 0 & 0 & 4 \end{vmatrix} \\
&= \begin{vmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 & 0 \\ 1 & 0 & 0 & 2 & 0 & 0 \\ 0 & -1 & 0 & 0 & 3 & 0 \\ 0 & 0 & 1 & 0 & 0 & \frac{7}{2} \end{vmatrix} \\
&= 2 \cdot 3 \cdot 7 \\
&= 42
\end{aligned}
$$

Übung: 2005-06-06

Aufgabe 7. Es seien G, G' Gruppen und $\Phi : G \to G'$ und $\Psi : G \to G'$ Gruppenhomomorphismen.
Zeigen Sie: Ist $H \subsetneq G$ eine echte Untergruppe von G und gilt $\Phi(a) = \Psi(a)$ für alle $a \in G \setminus H$, so ist $\Phi = \Psi$.

Lösung von Aufgabe 7: Sei $a \in G \setminus H$ und $b \in H$.

$$
\begin{aligned}
\Phi(a \circ b) &= \Phi(a) \circ' \Phi(b) \\
&= \Psi(a) \circ' \Phi(b)
\end{aligned}
$$

Ist $a \circ b \in G \setminus H$? Ja, denn Annahme

$$
\left.\begin{array}{r} a \circ b \in H \\ b^{-1} \in H \end{array}\right\} \Rightarrow \underbrace{(a \circ b)}_{\in H} \circ \underbrace{b^{-1}}_{\in H} = a \circ (b \circ b^{-1}) = a \in H \quad \text{Widerspruch!}
$$

Also gilt

$$
\Phi(a \circ b) \overset{\text{Vor.}}{=} \Psi(a \circ b) = \Psi(a) \circ' \Psi(b)
$$

Insgesamt:

$$
\begin{aligned}
& \Psi(a) \circ' \Phi(b) = \Psi(a) \circ' \Psi(b) \\
\Rightarrow\ & \Psi(a)^{-1} \circ' \Psi(a) \circ' \Phi(b) = \Psi(a)^{-1} \circ' \Psi(a) \circ' \Psi(b) \\
\Leftrightarrow\ & \Phi(b) = \Psi(b)
\end{aligned}
$$

Also gilt $\Phi = \Psi$.

Wiederholung.

$$\mathbb{Z}_m := \{[Z]_\sim \mid z \in \mathbb{Z}\}$$

$\forall z_1, z_2 \in \mathbb{Z}$:

$$z_1 \sim z_2 \ :\Leftrightarrow \ z_1 - z_2 = k \cdot m$$

für ein $k \in \mathbb{Z}$. Es gilt

$$[z_1]_\sim + [z_2]_\sim := [z_1 + z_2]_\sim$$

(„+“ ist wohldefiniert).
Sei $z_1' \in [z_1]_\sim$ und $z_2' \in [z_2]_\sim$, $z_1' = z_1 + km$ und $z_2' = z_2 + lm$, dann

$$\begin{aligned}[z_1' + z_2']_\sim &= [z_1 + km + z_2 + lm]_\sim \\ &= [z_1 + z_2 + (k+l)m]_\sim \\ &= [z_1 + z_2]_\sim\end{aligned}$$

Für alle $m \in \mathbb{N}$ ist $\mathbb{Z}_m$ eine Gruppe.

Aufgabe 8. Geben Sie alle Guppenhomomorphismen von $(\mathbb{Z}_6, +)$ nach $(\mathbb{Z}_7, +)$ an.

Lösung von Aufgabe 8:

$$\mathbb{Z}_6 = \{[z]_6 \mid z \in \mathbb{Z}\} \qquad \mathbb{Z}_7 = \{[z]_7 \mid z \in \mathbb{Z}\}$$

Für alle $m \in \mathbb{N}$ gilt $(\mathbb{Z}_m, +)$ ist zyklisch:

$$[k]_m = \underbrace{[1]_m + \ldots + [1]_m}_{k\text{Mal}}$$

Für jede Gruppe G' gilt $\Phi : \mathbb{Z}_m \to G'$ ist eindeutig durch $\Phi([1])$ festgelegt.

$$\Phi([0]_m) = e_G$$

$\Phi : \mathbb{Z}_6 \to \mathbb{Z}_7$ Gruppenhomomorphismus.
Dann muss gelten

$$\Phi([0]_6) = [0]_7 \quad \text{(Eigenschaft eines Gruppenhomomorphismus)}$$

Nun

$$[3]_6 + [3]_6 = [6]_6 = [0]_6$$

das heißt $[3]_6$ ist selbstinvers.

Einschub. $\Phi(x^{-1}) = \Phi(x)^{-1}$, das heißt $x = x^{-1}$, so ist $\Phi(x^{-1}) = \Phi(x)$. Also selbstinverse Elemente werden auf selbstinverse Elemente abgebildet.

Somit gilt

$$\Phi([3]_6) = [0]_7$$

$\Phi([1]_6) = [k]_7$ für ein $k \in \{0, \ldots, 6\}$

$$\begin{aligned}\Phi([3]_6) &= \Phi([1]_6 + [1]_6 + [1]_6) \\ &= \Phi([1]_6) + \Phi([1]_6) + \Phi([1]_6) \\ &= [k]_7 + [k]_7 + [k]_7 \\ &= [3 \cdot k]_7 \\ &= [3]_7 \cdot [k]_7 \\ &= [0]_7\end{aligned}$$

Da $\mathbb{Z}_7$ ein Körper und somit nullteilerfrei ist, gilt $k = 0$, also $\Phi([1]_6) = [0]_7$. Also ist

$$\begin{array}{rccc}\Phi: & \mathbb{Z}_6 & \to & \mathbb{Z}_7 \\ & [k]_6 & \mapsto & [0]_6\end{array}$$

Es gibt also nur einen Gruppenhomomorphismus von $\mathbb{Z}_6$ nach $\mathbb{Z}_7$.

Übung: 2005-06-13

Aufgabe 9. Sei $B = (b_1, \ldots, b_5)$ eine Basis des reellen Vektorraums V und $\Phi : V \to V$ ein Endomorphismus mit folgenden Eigenschaften

$$\Phi(b_1) = 2b_1 + 3b_4 \tag{21}$$
$$\Phi(b_2) = -b_1 + b_2 + 3b_3 + b_5 \tag{22}$$
$$\Phi(b_3) = -b_1 + 2b_3 - 4b_4 \tag{23}$$
$$\Phi(b_4) = b_1 - 2b_3 \tag{24}$$
$$\Phi(b_5) = -3b_1 - 2b_2 + 2b_4 + 4b_5 \tag{25}$$

(a) Bestimmen Sie die Abbildungsmatrix von Φ bezüglich B.

(b) Zeigen Sie, dass

$$\begin{aligned}c_1 &= b_1 + b_3 + b_4 \\ c_2 &= b_1 - b_3 \\ c_3 &= b_1 + b_4\end{aligned}$$

linear unabhängig sind.

(c) Zeigen Sie, dass $U = [c_1, c_2, c_3]$ Φ-invariant ist.

(d) Bestimmen Sie die Abbildungsmatrix von $\Phi_U : U \to U$ bezüglich (c_1, c_2, c_3).

Lösung von Aufgabe 9:

(a)

$$A_\Phi = \begin{pmatrix} 2 & -1 & -1 & 1 & -3 \\ 0 & 1 & 0 & 0 & -2 \\ 0 & 3 & 2 & -2 & 0 \\ 3 & 0 & -4 & 0 & 2 \\ 0 & -2 & 0 & 0 & 4 \end{pmatrix}$$

(b) c_1, c_2, c_3 linear unabhängig $\Leftrightarrow$ $\begin{pmatrix}1\\0\\1\\1\\0\end{pmatrix}, \begin{pmatrix}1\\0\\-1\\0\\0\end{pmatrix}, \begin{pmatrix}1\\0\\0\\1\\0\end{pmatrix}$ linear unabhängig

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

Die Matrix hat Rang 3, das heißt c_1, c_2, c_3 linear unabhängig.

(c) Außerdem haben wir gezeigt

$$U = [b_1, b_3, b_3]$$

Zu zeigen: $\Phi(U) \subset U$. Wir zeigen $\Phi(b_i) \in U$ für $i = 1, 2, 3$. Dies stimmt nach Voraussetzung wegen (21) (23) und (24).

(d) Bezüglich b_1, b_3, b_4 hat Φ_U die Abbildungsmatrix

$$A_{\Phi_U} = \begin{pmatrix}2&-1&1\\0&2&-2\\3&-4&0\end{pmatrix}$$

Es gilt

$$S = \begin{pmatrix}1&1&1\\1&-1&0\\1&0&1\end{pmatrix}$$

Also hat Φ_U bezüglich (c_1, c_2, c_3) die Abbildungsmatrix $S^{-1}AS$.

Übung: 2005-06-20

Wiederholung. Sei V ein $\mathbb{K}$-Vektorraum und $U \subset V$ ein Untervektorraum von V.

$$V/_U = \{[x]_\sim \mid x \in V\} \qquad x \sim y \Leftrightarrow x - y \in U$$

Für $a \in \mathbb{K}$, $x, y \in V$ gilt

$$a \cdot [x]_\sim = [a \cdot x]_\sim$$

und

$$[x]_\sim + [y]_\sim = [x + y]_\sim$$

sind wohldefiniert.

Aufgabe 10. Im Vektorraum

$$V = \{p \in \mathbb{R}[X] \mid \operatorname{Grad} p \leq 4\}$$

sei der Untervektorraum U erzeugt von den 4 Polynomen

$$p_1 := 1 + 2X - X^2 + X^3 - X^4 \tag{26}$$
$$p_2 := 2 - 2X + X^2 - 2X^3 \tag{27}$$
$$p_3 := 1 + 2X - X^2 - X^3 - 2X^4 \tag{28}$$
$$p_4 := -6X + 3X^2 - 2X^3 + 3X^4 \tag{29}$$

(a) Bestimmen Sie $\dim U$ und $W_1 \subset V$ mit $U \oplus W_1 = V$.

(b) Bestimmen Sie eine Basis von $V/_U$.

(c) Bestimmen Sie W_2 mit $U \oplus W_2 = V$ und $W_1 \cap W_2 = \{o\}$.

Lösung von Aufgabe 10:

(a) Wir wählen $B = (1, X, X^2, X^3, X^4)$ als Basis von V. Dann sind

$$\hat{p_1} = \begin{pmatrix} 1 \\ 2 \\ -1 \\ 1 \\ -1 \end{pmatrix}, \quad \hat{p_2} = \begin{pmatrix} 2 \\ -2 \\ 1 \\ -2 \\ 0 \end{pmatrix}, \quad \hat{p_3} = \begin{pmatrix} 1 \\ 2 \\ -1 \\ -1 \\ -2 \end{pmatrix}, \quad \hat{p_4} = \begin{pmatrix} 0 \\ -6 \\ 3 \\ -2 \\ 3 \end{pmatrix}$$

Berechne einfache Basis von U

$$\begin{pmatrix} 1 & 2 & -1 & 1 & -1 \\ 2 & -2 & 1 & -2 & 0 \\ 1 & 2 & -1 & -1 & -2 \\ 0 & -6 & -3 & -2 & 3 \end{pmatrix} \overset{\text{Gauß}}{\rightsquigarrow} \begin{pmatrix} 1 & 2 & -1 & 1 & -1 \\ 0 & -6 & 3 & -4 & 2 \\ 0 & 0 & 0 & 2 & 1 \end{pmatrix}$$

Also ist

$$C = \{1 + 2X + X^2 + X^3 - X^4, -6X + 3X^2 - 4X^3 + 2X^4, 2X^3 + X^4\}$$

eine Basis von U. $\Rightarrow$ Es gilt $\dim U = 3$.

Ergänze nun das Ergebnis des Gauß-Verfahren

$$\begin{pmatrix} 1 & 2 & -1 & 1 & -1 \\ 0 & -6 & 3 & -4 & 2 \\ 0 & 0 & 0 & 2 & 1 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 1 & 2 & -1 & 1 & -1 \\ 0 & -6 & 3 & -4 & 2 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 2 & 1 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

Diese Matrix hat $\mathrm{Rang}\, 5$, also $\{X^2, X^4\}$ linear unabhängig von U, also ist W_1 zum Beispiel gegeben durch

$$W_1 = [x2, X4]$$

(b) Sei $W \subset V$ Untervektorraum so, dass $U \oplus W = V$. Weiter sei $\{x_1, \ldots, x_n\}$ eine Basis von W.
Dann gilt $[x_1]_\sim, \ldots, [x_n]_\sim$ bilden eine Basis von $V/_U$.
Also sind $\{[X^2]_\sim, [X^4]_\sim\}$ eine Basis von $V/_U$.

(c) Ergänze die Matrix aus dem Ergebnis des Gauß-Verfahrens aus Aufgabenteil (a) zu

$$\begin{pmatrix} 1 & 2 & -1 & 1 & -1 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & -6 & 3 & -4 & 2 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 2 & 1 \end{pmatrix}$$

Auch diese Matrix hat $\mathrm{Rang}\,5$, also ist $\{X, X^3\}$ linear unabhängig von U und $W_1 \cap \{X, X^3\} = \{o\}$.
Also ist

$$W_2 = \{X, X^3\}$$

Index

Äquivalenzklasse, 9
Übung (LA II)
    2005-04-18, 137
    2005-04-25, 138
    2005-05-02, 139
    2005-05-09, 140
    2005-05-23, 141
    2005-05-30, 142
    2005-06-06, 144
    2005-06-13, 146
    2005-06-20, 147

Abbildung, 5
    adjungierte, 127
    alternierend, 83
    bijektiv, 6
    duale, 74
    eingeschränkt, 7
    fortgesetzt, 7
    identische, 7
    injektiv, 6
    inverse, 7
    kanonisch, 10
    linear, 67
    lineare, 44
    multilinear, 83
    normiert, 83
    Projektion, 138
    selbstadjungiert, 129
    surjektiv, 6
    transponierte, 74
    Umkehrung, 7
    zusammengesetzte, 7
Abbildungsmatrix, 75
Abstand, 124
Algebra, 71
Assoziativgesetz, 12
Automorphismus
    Gruppen-, 18
    Vektorraum-, 67

Basis, 50
    duale, 72, 140
    geordnet, 75
    Orthogonal-, 117
    Orthonormal-, 117
    Wyrre-, 143
Bild, 6
Bilinearform, 108
    positiv definit, 108
    symmetrisch, 108

Charakteristik, 23
Cholesky-Zerlegung, 117

Darstellung
    Parameter-, 65
definit
    positiv, 108, 112
Definitionsbereich, 6
Determinante, 81, 88
Dimension, 52
Distanz, 108
Drehspiegelung, 133
Drehung
    eigentliche, 133
    uneigentliche, 133
Dualbasis, 72
Dualraum, 72, 140

Ebene, 64
Eigenraum, 89
Eigenvektor, 89
Eigenwert, 89
Einschränkung, 7
Elementare Zeilenumformungen, 39
endlich dimensional, 52
Endomorphismus
    diagonalisierbar, 92
    Vektorraum-, 67
Erzeugendensystem, 46
    minimal, 50
Eulerschie φ-Funktion, 27

Faktormenge, 9
Faktorraum, 61
Fehlstand, 81
Fortsetzung, 7
Funktional
    lineares, 72

Gaußsche Normalform, 40
Gerade, 64
Grad, 34
Gruppe, 13, 137
    abelsch, 13
    allgemeine Lineare, 32
    Faktor-, 20
    ntafel, 14
    orthogonale, 133
    permutations, 15
    spezielle orthogonale, 133
    symmetrische, 15
    unter, 17

Halbgruppe, 12
    kommutativ, 12
Hauptminor, 114
Hauptraum, 99

Homomorphiesatz
Grundform, 10
Homomorphismus
Gruppen-, 18
Körper, 23
Ring-, 26
Vektorraum-, 44, 67
Hyperebene, 64

Ideal, 37
Identität, 7
Imaginärteil, 24
Index, 100
Inverses (Gruppen), 12
Isometrie, 131
isomorph
bei Gruppen, 18
bei Körpern, 23
bei Vektorräumen, 67
isometrisch, 131
Isomorphismus
Gruppen-, 18
Körper, 23
Vektorraum, 67

Jordan
Block, 105
Kästchen, 105

Körper, 20
der komplexen Zahlen, 24
Kodimension, 64
Kommutativgesetz, 12
Komplement
orthogonales, 109
Komplementärraum, 60
Komposition, 7
Kongruenz, 22
konjugiert komplexe Zahl, 25
Koordinate, 75
Kreuzprodukt, 5

Länge, 108
LGS, 11
homogen, 11
inhomogen, 11
linear
unabhängig, 140
Linear abhängig, 46, 48
Linear unabhängig, 46, 48
linear unabhängig
maximale Menge, 50
Lineare Hülle, 46
Linearer Teilraum, 44
Lineares Gleichungssystem, 11
Linearfaktor, 93
Linearform, 72, 140
Linearkombination, 46
Lotfußpunkt, 125

Matrix, 29
ähnlich, 80
äquivalent, 79
Abbildungs-, 75
diagonalisierbar, 92
Einheits-, 30
Inverses, 32
orthogonal, 130
positiv definit, 112
quadratische, 29
regulär, 32
singulär, 32
Spalten-, 30
Spur, 72
symmetrisch, 33
transponierte, 32
Zeilen-, 30
Menge, 4
Metrik, 108, 111

Neutralelement, 12
Norm, 108, 110
Normalteiler, 20
Nullstelle, 36
Vielfachheit, 93

orthogonal, 109
Orthogonalsystem, 117
Orthonormalsystem, 117

parallel, 66
Partition, 9
Permutation, 15
gerade, 17
ungerade, 17
Polynom, 34
charakteristisches, 90
Grad von, 34
konstante, 34
Minimal-, 98
normiert, 34
Null-, 34
Produkt
inneres, 108
Kreuz, 5
Matrix-, 30
Projektion, 68, 120, 138
Orthogonal-, 120
Punkt, 64

Quotientenraum, 61

Rang, 56
Spalten-, 56

Zeilen-, 56
Realteil, 24
Relation, 8
äquivalenz, 9
reflexiv, 9
symmetrisch, 9
transitiv, 9
Repräsentant, 9
Restriktion, 7
Richtungsraum, 64
Ring, 25
mit Eins, 26

Skalarprodukt, 108
Standard-, 73, 108
Spur, 72
Summe, 59
direkte, 59

Teiler, 37
teilerfremd, 27, 37
Teilmenge, 4
echte, 4
Transposition, 16
Treppennormalform, 40

Umkehrabbildung, 7
unendlich dimensional, 52
Untergruppe, 17, 137
Unterraum, 44
affiner, 64
aufspannen, 46
Untervektorraum, 44
erzeugter, 46
Urbild, 6

Vektor, 44
Koordinaten-, 75
Vektorraum, 44
dualer, 72
euklidischer, 108
komplementärer, 60
komplexer, 44
reller, 44
Verknüpfung
assoziativ, 12
kommutativ, 12
Verknüpfungstafel, 14
Vielfachheit, 93
Vorlesung (LA I)
2004-10-20, 4
2004-10-22, 6
2004-10-27, 9
2004-10-29, 12
2004-11-03, 14
2004-11-05, 16
2004-11-10, 18
2004-11-12, 21
2004-11-17, 24
2004-11-19, 27
2004-11-24, 29
2004-11-26, 32
2004-12-01, 34
2004-12-03, 37
2004-12-08, 40
2004-12-10, 44
2004-12-15, 45
2004-12-17, 48
2004-12-22, 51
2005-01-07, 53
2005-01-12, 56
2005-01-14, 58
2005-01-19, 61
2005-01-21, 64
2005-01-26, 67
2005-01-28, 69
2005-02-02, 72
2005-02-04, 74
2005-02-09, 78
2005-02-11, 81
2005-02-16, 84
2005-02-18, 88
Vorlesung (LA II)
2005-04-13, 90
2005-04-20, 92
2005-04-27, 95
2005-05-04, 98
2005-05-11, 101
2005-05-18, 104
2005-05-25, 107
2005-06-01, 110
2005-06-04, 127
2005-06-07, 130
2005-06-08, 114
2005-06-15, 118
2005-06-22, 120
2005-06-29, 123
2005-07-13, 133

Wertebereich, 6
windschief, 66
Winkel, 111