

## 1. Grundlagen

TODO: Modulo und  $\mathbb{Z}_n$

### 1.1. Mengenlehre

#### 1.1.1 Für alle Mengen A,B,C gilt:

- $\emptyset \subset B$
- $A \setminus (B \cup C) = (A \setminus B) \cap (A \setminus C)$
- $(A \cap B) \cap C = A \cap (B \cap C)$   
 $(A \cup B) \cup C = A \cup (B \cup C)$
- $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$   
 $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$
- $A \Delta B = (A \cup B) \setminus (A \cap B)$   
symmetr. Differenz zweier Mengen: Alle Elemente, die entweder in A oder B enthalten sind.
- $A \times B = \{(a_1, b_1), \dots, (a_1, b_n), (a_2, b_1), \dots\}$   
direktes Produkt zweier Mengen, ordnet jedem Element aus A jedes Element aus B zu (Tupel)

### 1.2. Abbildungen

$f: A \rightarrow B$

#### Surjektivität

$\forall y \in B \exists x \in A : f(x) = y$ . Es wird auf alle Werte der Wertemenge abgebildet

Beweisstruktur:

- Sei  $y \in B$ , finde  $x \in A$  mit  $f(x) = y$
- Durch Einsetzen ergibt sich  $y = f(x)$ , kann man dies nach  $x$  auflösen, so ist  $f$  surjektiv.  
Ist  $B = K^n$ , z.B.  $n = 2$ , so wählt man  $(a, b) \in K^2$ ,  $f(x, y) = (a, b)$  und löst das lin. Gleichungssystem nach  $x$  und  $y$  auf

$f$  surjektiv  $\iff$  Bild  $f = B$

#### Injektivität

$f(x_1) = f(x_2) \Rightarrow x_1 = x_2$ . Zwei verschiedene Elemente der Definitionsmenge bilden nicht auf gleiche Elemente der Wertemenge ab.

Beweisstruktur:

- $x_1, x_2 \in A$  mit  $x_1 \neq x_2$
- Gibt es eine Kombination von  $x_1, x_2$ , sodass  $f(x_1) = f(x_2)$ , so ist  $f$  nicht injektiv  
Ist  $A = K^n$ , z.B.  $n = 2$ , so wählt man  $(x_1, y_1), (x_2, y_2) \in K^2$  und vergleicht  $f(x_1, y_1) = f(x_2, y_2)$ . Hier erhält man zwei Gleichungen, setzt man die eine in die andere ein, so muss  $x_1 = x_2$  bzw.  $y_1 = y_2$  rauskommen.

$f$  injektiv  $\iff$  Kern  $f = \{0\}$

$f$  injektiv  $\iff f$  streng monoton steigend

#### 1.2.1 Schnitt-/Vereinigungsbeweis von (Ur-)Bildern

- $f^{-1}(N_1 \cup N_2) = f^{-1}(N_1) \cup f^{-1}(N_2)$ 
  - Sei  $x \in f^{-1}(N_1 \cup N_2) \iff f(x) \in N_1 \cup N_2$
  - Beweis weiterführen, bis man auf  $x \in f^{-1}(N_1) \cup f^{-1}(N_2)$  kommt
- $f(M_1 \cup M_2) = f(M_1) \cup f(M_2)$ 
  - Sei  $y \in f(M_1 \cup M_2) \iff x \in M_1 \cup M_2$
  - Beweis weiterführen, bis man auf  $y \in f(M_1) \cup f(M_2)$  kommt

## 2. Algebraische Strukturen

### 2.1. Gruppen

Menge mit einer Verknüpfung  $\circ$  (z.B.  $+$ ,  $\cdot$ )  $\Rightarrow (M, \circ)$

#### 2.1.1 Halbgruppe

Falls für alle  $a, b, c \in M$  das Assoziativgesetz gilt:

$(ab)c \stackrel{!}{=} a(bc)$ , hierbei beschreibt  $ab$  die Verknüpfung von  $a$  und  $b$  ( $\circ$ )

#### 2.1.2 Monoid

Halbgruppe mit neutralem Element  $e: ae = ea = a$

#### 2.1.3 abelsche/kommutative (Halb-)Gruppe

(Halb-)Gruppe, wobei das Kommutativgesetz gilt:  $ab = ba$

#### 2.1.4 Gruppe

Eine Halbgruppe  $(G, \circ)$  heißt Gruppe mit neutralem Element  $e$ , falls:

- Die Gruppe abgeschlossen ist:  $\forall a, b \in G : a \circ b \in G$
- es zu jedem  $a \in G$  ein  $b \in G$  gibt mit  $ab = ba = e$ .  
 $b$  ist das Inverse von  $a$  und ist eindeutig. Man schreibt  $b = a^{-1}$

**symmetrische Gruppe  $S_n$ :** Gruppe der Permutationen:

$\begin{smallmatrix} 1 & 2 & 3 & 1 & 2 & 3 \\ (1, 3, 2) & (2, 3, 1) \end{smallmatrix} = (3, 2, 1)$ . Von rechts nach links gelesen:

- Die Stelle **1** wird auf die 2 abgebildet, die Stelle **2** wird auf die 3 abgebildet. 1. Element des Ergebnisses, usw...

#### 2.1.5 Untergruppe

Gruppe  $(U, \circ)$ , wobei  $U \subset G$ . Dann ist  $U$  Untergruppe von  $G$

**Axiome zum Beweis von Untergruppe:**

- $e \in U$
- $v, w \in U \Rightarrow v \circ w \in U$
- $v \in U \Rightarrow v^{-1} \in U$

### 2.2. Ring

Menge  $R$  mit zwei Verknüpfungen  $(R, +, \cdot)$ , falls gilt:

- $(R, +)$  kommutative Gruppe mit neutralem Element **e**
- $(R, \cdot)$  Halbgruppe
- $\forall a, b, c \in R$  gilt  $a(b + c) = ab + ac$  und  $(b + c)a = ba + ca$  (Distributivgesetz)

### 2.3. Körper

- $(R, +, \cdot)$  ist ein Ring
- $(R \setminus \{\mathbf{e}\}, \cdot)$  der kommutativen Gruppe des Rings,  $\cdot$  ist kommutative Gruppe

#### Wichtige Beispiele

- $\mathbb{Q}$  und  $\mathbb{R}$  sind Körper
- $(\mathbb{Z}_p, \oplus_p, \odot_p)$  ist für jede Primzahl  $p$  ein Körper

### 2.4. Vektorraum

Eine Menge  $V$  ist  $K$ -Vektorraum (VR über Körper  $K$ ) mit

- Vektoraddition:  $V \times V \rightarrow V, (v, w) \mapsto v + w$
- Skalarmultiplikation:  $K \times V \rightarrow V, (\lambda, v) \mapsto \lambda v$   
wobei  $\forall \lambda, \mu \in K$  und  $\forall v, w \in V$  gilt:

- $(\lambda \mu)v = \lambda(\mu v)$
- $\lambda(v + w) = \lambda v + \lambda w$  und  $(\lambda + \mu)v = \lambda v + \mu v$
- $1v = v$

#### 2.4.1 Untervektorraum

$U$  ist Untervektorraum von  $V$ , wenn  $U \subset V$ , bzw.  $\forall v, w \in U, \lambda \in K$

- $v + w \in U$
- $\lambda v \in U$
- $U \neq \emptyset$  bzw.  $e \in U$  (**e** der kommut. Gruppe des Ringes)

#### 2.4.2 direkte Summe zweier UVRs

Zwei UVRs  $U_1, U_2$  heißen direkte Summe  $U_1 \oplus U_2$ , wenn  $U_1 \cap U_2 = \{0\}$ . D.h. zwei UVRs treffen sich nur im Ursprung (zwei Geraden (UVR vom  $\mathbb{R}^3$ ) schneiden sich nur im Ursprung)

In der Summe  $U_1 + U_2 = \{u_1 + u_2 | u_1 \in U_1, u_2 \in U_2\}$  ist die Darstellung  $u = u_1 + u_2$  eindeutig. Es gibt nur eine mögliche Linearkombination! (Aus ) Z.B.  $\{(x, 0) | x \in \mathbb{R}\} \oplus \{(0, y) | y \in \mathbb{R}\} = \mathbb{R}^2$ , da  $(x, y) = (x, 0) + (0, y)$

#### 2.4.3 Neue UVRs aus Alten

- $U_1 \cap U_2$  ist UVR
- $U_1 + U_2$  ist UVR
- $\Phi: V \rightarrow W$  linear mit  $U \subset V, T \subset W$ :  
 $\Phi(U) = \{\Phi(u) | u \in U\}$  UVR von  $W$   
 $\Phi(T) = \{v \in V | \Phi(v) \in T\}$  UVR von  $V$

### 2.5. Spann

Menge aller Vektoren, die aus Linearkombination der Argumente (hier  $v_1, v_2$ ) hervorgehen,

z.B.:  $\text{spann}(v_1, v_2) = \{av_1 + bv_2 | a, b \in \mathbb{R}\}$

- $\text{spann } M$  ist UVR von  $V$ , wenn  $M \subset V$
- Sind  $U_1$  und  $U_2$  UVR von  $V$ :  $\text{spann}(U_1 \cup U_2) = U_1 + U_2$
- $\text{spann } \emptyset = \{0\}$
- $\Phi: V \rightarrow W$  linear:  $\text{spann}(\Phi(V)) = \Phi(\text{spann } V)$

## 3. Lineare Abbildungen

Seien  $V, W$   $K$ -Vektorräume. Eine Abbildung  $\Phi: V \rightarrow W$  heißt **Vektorraumhomomorphismus** oder **linear**, falls  $\forall v, w \in V$  und  $\forall \lambda \in K$  gilt:

- $\Phi(0) = 0$
- $\Phi(\lambda v + w) = \lambda \Phi(v) + \Phi(w)$

$L(V, W) := \{\Phi: V \rightarrow W | \Phi \text{ linear}\}$

**Endomorphismen:** VR-Homomorphismen von  $V$  auf sich selbst ( $\Phi: V \rightarrow V$ )

**Isomorphismen:** Bijektive VR-Homomorphismen

**Automorphismen:** Bijektive Endomorphismen

### 3.1. Kern

Sei  $\Phi: V \rightarrow W$  eine lineare Abbildung, der Kern  $\Phi$  ist die Menge aller Elemente aus  $V$ , die auf die 0 abgebildet werden.

Kern  $\Phi := \{v \in V | \Phi(v) = 0\} = \Phi^{-1}(\{0\})$

### 3.2. Bild

Sei  $\Phi: V \rightarrow W$  eine lineare Abbildung, das Bild  $\Phi$  ist die Menge aller Elemente aus  $W$ , auf die abgebildet wird.

Bild  $\Phi := \{\Phi(v) | v \in V\}$

### 3.3. Dimension

Menge an lin. unabh. Vektoren eines VRs ( $f: V \rightarrow W$  lin.)

**Rang:**  $\text{Rang } f := \dim(\text{Bild } f)$

**Dimensionssatz:**  $\dim V = \dim(\text{Kern } f) + \dim(\text{Bild } f)$

- $\dim V = 0 \iff V = \{0\}$

### 3.4. Vektorraumisomorphismus

Zwei VRs sind isomorph  $V \cong W$  genau dann, wenn

- Man eine bijektive lin. Abb. finden kann, die eine Basis von  $V$  auf eine Basis von  $W$  abbildet
- $\dim V = \dim W$

**Koordinatensystem:** Isomorphismus  $\Phi: K^n \rightarrow V$

CONTINUE: Determinanten und Bilinearform

## 3.5. Basiswechsel

### 3.5.1 Basiswechselmatrix allg.

$$[v]_{B_{neu}} = P_{B_{neu} \leftarrow B_{alt}} [v]_{B_{alt}}$$

Basiswechselmatrix finden, die  $B_{alt}$  zu  $B_{neu}$  abbildet:

1. Nimm den  $j$ -ten ( $v_j$ ) Basisvektor aus  $B_{alt}$
2. Schreibe ihn in der neuen Basis mithilfe Linearkombination der neuen Basisvektoren  
 $v_j = a_1 w_1 + \dots + a_n w_n$
3. Die  $j$ -te Spalte von  $P_{B_{neu} \leftarrow B_{alt}}$  ist der Vektor der Koeffizienten  $(a_1, \dots, a_n)^T$

### 3.5.2 Basiswechselmatrix $R^n$

Basiswechselmatrix von  $B_{alt}$  zu  $B_{neu}$ :

1. Basisvektoren von  $B_{alt}$  und  $B_{neu}$  als Matrix nebeneinander schreiben
2.  $P_{B_{neu} \leftarrow B_{alt}} = B_{neu}^{-1} B_{alt}$   
 $P_{B_{alt} \leftarrow B_{neu}} = B_{alt}^{-1} B_{neu}$

## 3.6. Darstellungsmatrix $D$

Beschreibt die Bilder der Basisvektoren einer lin. Abb.

### 3.6.1 Basiswechsel mit Basiswechselmatrix

Basiswechsel im Definitionsraum mit neuer Basis  $B_{neu}$ :

$$D_{B_{neu}, B} = D_{B_{alt}, B} \times P_{B_{alt} \leftarrow B_{neu}}$$

Basiswechsel im Bildraum mit neuer Basis  $B_{neu}$ :

$$D_{B, B_{neu}} = P_{B_{neu} \leftarrow B_{alt}} \times D_{B, B_{alt}}$$

### 3.6.2 Spezialfälle

Basiswechsel im Definitionsraum mit Standard-Basis im Bildraum:

Bilder der neuen Basisvektoren sind die Spalten der Darstellungsmatrix

Basiswechsel im Bildraum mit Standard-Basis im Definitionsraum:

Die Bilder der Standard-Basisvektoren ausgedrückt in der neuen Basis  $\{b_1, \dots, b_n\}$  bilden die Spalten der Darstellungsmatrix:  $f(e_n) \stackrel{!}{=} a_1 b_1 + \dots + a_n b_n$ . Die Koeffizienten bilden die Spalten der Darstellungsmatrix.

## 3.7. Determinanten

$f: V \rightarrow V$ ,  $\omega$  Determinantenform:

$$(\det f) \omega(v_1, \dots, v_n) = \omega(f(v_1), \dots, f(v_n))$$

### 3.7.1 Eigenschaften

- Vertauscht man zwei Spalten/Zeilen von  $A \rightarrow A' \implies \det A = -\det A'$
- Skaliert man  $n$  Spalten mit  $\lambda$ ,  $A \rightarrow A' \iff \det A = \lambda^n \det A'$
- Addiert man zwei Spalten aufeinander:  $\det A$  bleibt gleich
- $\det(f \circ g) = \det(AB) = \det f \det g = \det A \det B$
- $\det A^{-1} = \frac{1}{\det A}$
- $\det A = \det A^T$

### 3.7.2 Laplace-Formel

Vorzeichenwechsel beispielhaft erklärt für  $K^{3 \times 3}$

Term	Spalte	sign	# Vertauschungen
$aei$	(1, 2, 3)	+	0
$afg$	(1, 3, 2)	-	1
$bfg$	(2, 3, 1)	-	2

## 3.8. euklidische Vektorräume

Cauchy-Schwarz-Ungl.:  $|\langle v, w \rangle| \leq \|v\| \|w\|$

Sei  $(V, \langle \cdot, \cdot \rangle)$  euklid. VR. Dann gilt  $\forall v, w \in V$ :

1. **Polarisation:**  $\langle v, w \rangle = \frac{1}{4}(\|v+w\|^2 - \|v-w\|^2)$
2. **Parallelogrammgleichung:**  
 $2(\|v\|^2 + \|w\|^2) = \|v+w\|^2 + \|v-w\|^2$

Für eine bel. Norm gilt: Die Parallelogrammgleichung gilt  $\iff$  Die Norm kommt von einem Skalarprodukt. Dann erhält man das Skalarprodukt durch Polarisation.

### 3.8.1 Skalarprodukt

- bilinear:  $\langle a, b+c \rangle = \langle a, b \rangle + \langle a, c \rangle$
- symmetr.:  $\langle a, b \rangle = \langle b, a \rangle$
- pos. definit:  $\langle v, v \rangle > 0$  oder  $\langle v, v \rangle = 0 \implies v = 0$

### 3.8.2 Norm

Abbildung  $\|\cdot\|: V \rightarrow \mathbb{R}$  mit den Eigenschaften:

- $\|\lambda v\| = |\lambda| \|v\| \quad \forall \lambda \in \mathbb{R}, v \in V$
- $\|a\| > 0$  oder  $\|a\| = 0 \implies a = 0$
- $\forall v, w \in V$  gilt die Dreiecksungleichung:  
 $\|v+w\| \leq \|v\| + \|w\|$

## 4. Matrix-Lookup-Table

### 4.1. Rechenregeln

- $A \in \mathbb{R}^{m \times n}$ ,  $B \in \mathbb{R}^{n \times k} \rightarrow AB$  definiert:  $AB \in \mathbb{R}^{m \times k}$
- $\det A = a_{11}a_{22} - a_{12}a_{21}$ ,  $A \in \mathbb{R}^{2 \times 2}$
- $\det A = a_{11}(a_{22}a_{33} - a_{23}a_{32}) - a_{12}(a_{21}a_{33} - a_{23}a_{31}) + a_{13}(a_{21}a_{32} - a_{22}a_{31})$

## 4.2. Standard-Matrix

- Menge an lin. unabh. Spalten/Zeilen von  $A$ :  $\text{Rang } A$
- $\dim(\text{Kern } A) = \text{Spaltenanzahl} - \text{Rang } A$
- $f: V \rightarrow W$ :  $\dim V = \text{Spaltenanzahl}$ ,  $\dim W = \text{Zeilenanzahl}$
- $\text{Rang}(AB) \leq \min(\text{Rang } A, \text{Rang } B)$

### 4.2.1 Invertierbarkeit $A \in \text{Mat}(n, n, K)$

- $A$  invertb.  $\iff \text{Rang } A = n \iff \dim(\text{Kern } A) = 0 \rightarrow A$  besitzt keine Nullzeile/-spalte
- $A$  invertierbar  $\iff A$  bijektiv
- $A$  invertierbar  $\iff \det A \neq 0$
- $A$  Nullzeile/-spalte  $\iff A$  nicht invertb.

### 4.2.2 Transposition

- $\text{Rang } A = \text{Rang } A^T$  (Zeilenrang = Spaltenrang)
- symmetr. Matrix:  $A^T = A$ :  $a_{ji} = a_{ij}$
- schiefssymmetr. Matrix:  $A^T = -A$ :  $a_{ji} = -a_{ij}$
- $(A^T)^{-1} = (A^{-1})^T$

## 4.3. Gauß

- Anzahl der lin. unabh. Nicht-Nullzeilen  $\iff \text{Rang } A$

### 4.3.1 Lösbarkeit der erw. Matrix $[A|b]$

- Unlösbar: Es existiert Nullzeile links und ein Nicht-Null Eintrag rechts
- Eindeutig lösbar:  $\text{Rang } A = \text{Anzahl der Variablen}$  und  $b \in \text{Bild } A$
- Unendl. viele Lösungen:  $\text{Rang } A < \text{Anzahl der Variablen} \rightarrow$  Nullzeile rechts und Nulleintrag links
- Homog. System  $b = 0$ : Lösungsmenge ist VR - der Kern  $A \implies \dim L = \dim V - \text{Rang } A$
- Inhomog. System: Lösungsmenge ist Partikulärlösung + Kern (affiner Unterraum)