1. Grundlagen

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

1.1. Abbildungen

$f: A \to B$
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.

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

f injektiv $\Longleftrightarrow f$ streng monoton steigend

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

2.1.2 Gruppe

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

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

2.1.3 Untergruppe

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

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

2.2. Ring

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

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

2.3. Körper

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

Wichtige Beispiele

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

2.4. Vektorraum

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

1. Vektoraddition: $V \times V \to V, (v, w) \mapsto v + w$
2. Skalarmultiplikation: $K \times V \to V, (\lambda, v) \mapsto \lambda v$

wobei $\forall \lambda, \mu \in K$ und $\forall v, w \in V$ gilt:

1. $(\lambda\mu)v = \lambda(\mu v)$
2. $\lambda(v + w) = \lambda v + \lambda w$ und $(\lambda + \mu)v = \lambda v + \mu v$
3. $1v = v$

2.4.1 Untervektorraum

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

1. $v + w \in U$
2. $\lambda v \in U$
3. $U \neq \emptyset$ 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

2.4.3 Neue UVRs aus Alten

- $U_1 \cap U_2$ ist UVR
- $U_1 + U_2$ ist UVR
- $\Phi: V \to W$ 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: $\text{spann}(U_1 \cup U_2) = U_1 + U_2$
- $\text{spann}\, \emptyset = \{0\}$
- $\Phi: V \to W$ linear: $\text{spann}(\Phi(V)) = \Phi(\text{spann}\, V)$

3. Lineare Abbildungen

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

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

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

Endomorphismen: VR-Homomorphismen von V auf sich selbst ($\Phi: V \to V$)
Isomorphismen: Bijektive VR-Homomorphismen
Automorphismen: Bijektive Endomorphismen

3.1. Dimension

Menge an lin. unabh. Vektoren eines VRs ($f: V \to W$ lin.)
Dimensionssatz: $\dim V = \dim(\text{Kern}\, f) + \dim(\text{Bild}\, f)$

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

3.2. Vektoraumisomorphismus

Zwei VRs sind isomorph $V \tilde{=} W$ 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 $\Phi: K^n \to V$

3.3. Basiswechsel

3.3.1 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
   $v_j = a_1 w_1 + ... + a_n w_n$
3. Die j-te Spalte von $P_{B_{neu} \leftarrow B_{alt}}$ ist der Vektor der Koeffizienten $(a_1, ..., a_n)^T$

3.3.2 Basiswechselmatrix R^n

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

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

3.4. Darstellungsmatrix D

Beschreibt die Bilder der Basisvektoren einer lin. Abb.

3.4.1 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}:
$D_{B, B_{neu}} = P_{B_{neu} \leftarrow B_{alt}} \times D_{B, B_{alt}}$

3.4.2 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 $\{b_1, ..., b_n\}$ bilden die Spalten der Darstellungsmatrix: $f(e_n) \overset{!}{=} a_1 b_1 + ... + a_n b_n$. Die Koeffizienten bilden die Spalten der Darstellungsmatrix.

3.5. Determinanten

$f: V \to V$, $\quad \omega$ Determinantenform:
$(\det f)\omega(v_1, ..., v_n) = \omega(f(v_1), ..., f(v_n))$

3.5.1 Eigenschaften

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

4. 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 und es gilt: $||v|| = \sqrt{\langle v, v\rangle}$.

4.0.1 Skalarprodukt

$\langle x, y\rangle = x^T Ey$

- 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 $\langle v, v\rangle = 0 \Rightarrow v = 0$

4.0.2 Norm

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

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

4.1. Gram-Schmidt-Orthonormalisierung

w_n Ausgangsvektoren, v_n Orthonormale Vektoren:
$\tilde{v_3} = w_3 - \langle w_3, v_1\rangle v_1 - \langle w_3, v_2\rangle v_2$

4.1.1 orthogonale Projektion

Für eine Orthonormalbasis $u_1, ..., u_k$ von U gilt:
$\pi_U(v) = \sum_{i=1}^{k} \langle v, u_i\rangle u_i$

4.1.2 orthogonales Komplement $U^\perp$

Vektoren, die senkrecht zu einem Unterraum U sind.

- $U^\perp = \operatorname{Kern} \pi_U$
- $U^\perp$ sind alle Vektoren, dessen Skalarprodukt mit Vektoren aus dem Unterraum 0 ist

4.1.3 Adjungierte f^* von $f \in \operatorname{End}(V)$

$\langle f(v), w\rangle = \langle v, f^*(w)\rangle$
Ist B ON-Basis von V, so gilt: $D_{B,B}(f^*) = D_{B,B}(f)^T$

5. Matrix-Lookup-Table

5.1. Rechenregeln

- $A \in \mathbb{R}^{m\times n}$, $B \in \mathbb{R}^{n\times k}$ $\to$ AB definiert: $AB \in \mathbb{R}^{m\times k}$
- $\det A = a_{11}a_{22} - a_{12}a_{21}$, $A \in \mathbb{R}^{2\times 2}$

5.2. Standard-Matrix

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

5.2.1 Invertierbarkeit $A \in \operatorname{Mat}(n, n, K)$

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

5.2.2 Transposition

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

5.3. Gauß

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

5.3.1 Lösbarkeit der erw. Matrix $[A|b]$

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