

# A quick guide to Lineare Algebra

## Mengen

- $X \cap Y = Y \cap X$
- $X \cup Y = Y \cup X$
- $(X \cap Y) \cap Z = X \cap (Y \cap Z)$
- $(X \cup Y) \cup Z = X \cup (Y \cup Z)$
- $X \cap (Y \cup Z) = (X \cap Y) \cup (X \cap Z)$
- $X \cup (Y \cap Z) = (X \cup Y) \cap (X \cup Z)$
- $X \setminus Y = X \setminus (X \cap Y)$
- $X \cap Y = X \Leftrightarrow X \subseteq Y$
- $X \cup Y = Y \Leftrightarrow X \subseteq Y$
- $b \in X$  ist obere Schranke von  $A \subseteq X$ , wenn  $x \leq b \forall x \in A$
- $b \in X$  ist Supremum von  $A \subseteq X$ , wenns die kleinste obere Schranke ist. (ist eindeutig)
- $b \in X$  ist Maximales Element von  $A \subseteq X$ , wenn  $b \in A$  und  $\forall x \in A: b \leq x \Rightarrow x = b$  (Kein Element von A ist Größer).
- $b \in X$  ist Maximum von  $A \subseteq X$ , wenn  $b \in A$  und  $\forall x \in A: x \leq b$  (Maximum ist eindeutig)
- $a \in X$  ist Untere Schranke von  $A \subseteq X$ , wenn  $a \leq x \forall x \in A$
- $b \in X$  ist Infimum von  $A \subseteq X$ , wenns die größte untere Schranke ist. (ist eindeutig)
- $b \in X$  ist Minimales Element von  $A \subseteq X$ , wenn  $a \in A, \forall x \in A: x \leq a \Rightarrow x = a$
- $b \in X$  ist Minimum von  $A \subseteq X$ , wenn  $a \in A, \forall x \in A: a \leq x$  (Minimum ist eindeutig)

## Weiteres

$x|y \Rightarrow \exists n \in \mathbb{Z}: y = nx$

## Tupel

$A \times B := \{(a, b) | a \in A \wedge b \in B\}$

## Relationen

- (R, X, X). R ist:
- reflexiv  $\rightarrow (x, x) \in R \quad \forall x \in X$
- symmetrisch  $\rightarrow (x, y) \in R \Rightarrow (y, x) \in R$
- antisymmetrisch  $\rightarrow (x, y) \in R$  und  $(y, x) \in R \Rightarrow x = y$
- transitiv  $\rightarrow (x, y) \in R$  und  $(y, z) \in R \Rightarrow (x, z) \in R$
- total  $\rightarrow (x, y)$  oder  $(y, x) \in R \forall x, y \in X$
- **Ordnungsrelation** → reflexiv, antisymmetrisch, transitiv
- **Äquivalenzrelation** → reflexiv, symmetrisch, transitiv
- Äquivalenzrelationen erzeugen Partitionen von Mengen.

## Funktionen

- linkstotal → jedes x hat y
- rechtseindeutig → 1 x hat keine 2 y
- Bild u. Urbild Dinger**
- $f(\bigcup_{i \in I} X_i) = \bigcup_{i \in I} f(X_i)$
- $f(\bigcap_{i \in I} X_i) \subseteq \bigcap_{i \in I} f(X_i)$
- $f^{-1}(\bigcup_{j \in J} Y_j) = \bigcup_{j \in J} f^{-1}(Y_j)$
- $f^{-1}(\bigcap_{j \in J} Y_j) = \bigcap_{j \in J} f^{-1}(Y_j)$

### Kompositionen

- $f: X \rightarrow Y; \quad g: Y \rightarrow Z; \quad h: Z \rightarrow W$
- $(h \circ g) \circ f = h \circ (g \circ f)$
- **Assoziativ** → f, g sind injektiv → g ∘ f ist injektiv
- f, g sind surjektiv → g ∘ f ist surjektiv
- go f injektiv → f ist injektiv
- gof surjektiv → g ist surjektiv
- $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$
- $f: X \rightarrow Y; X, Y$  sind endlich und gleichmächtig ⇒ Äquivalent: f ist injektiv, f ist surjektiv, f ist bijektiv

## Strukturen

### Halbgruppe

Menge H mit assoziativer Verknüpfung:  
 $(a * b) * c = a * (b * c)$

### Monoid

Halbgruppe mit e:  $e * x = x * e = x$  → Einheitsgruppe ist Teilmenge eines Monoids, welche eine Gruppe ist.

### Translation

- $*_a: H \ni x \mapsto x * a \in H$
- $a*: H \ni x \mapsto a * x \in H$
- a ist fest und x läuft durch

### Inverse

$a * b = e = b * a$  → Inverse sind eindeutig

## Gruppe

- assoziative Verknüpfung
- Monoid
- jedes Element hat ein Inverses
- Es gilt:
- $a * b_1 = a * b_2 \Rightarrow b_1 = b_2$
- Egal ob abelsch, muss man nur eine Sache testen, entweder  $a * b = e$  oder andersrum
- $(a')' = a$
- $(a * b)' = b' * a'$
- Translationen in Gruppen sind bijektiv
- Abelsche Gruppe, wenn  $a * b = b * a \quad \forall a, b \in G$
- $ord(a) = n, f \text{ür } n \in \mathbb{N}$  kleinstes n für das gilt:  $a^n = 1_{bw}.na = 0$  (n-mal verknüpfen ist neutrales Element)
- In einer Gruppe sind alle links- und rechtstranlationen bijektive Abbildungen. von  $G \rightarrow G$
- Eine nichtleere Halbgruppe mit surjektiven links und rechtstranlationen ist eine Gruppe.

## Symmetrische Gruppe

- $S(X) = \{f: X \rightarrow X | f \text{ ist bijektiv}\}$
- $(S(X), \circ) \rightarrow$  Symmetrische Gruppe
- Elemente aus S(X) heißen Permutationen  $\sigma$  von X
- *Speziell* wenn  $X_1 = [1, n] \Rightarrow S_n$
- $\tau(i, j)$  ist eine Funktion, die nur zwei Elemente aus  $X_1$  vertauscht
- Fehlstand:  $i < j$  und  $\sigma(i) > \sigma(j)$
- $sgn \sigma = (-1)^{\text{Anzahl der Fehlstaende}}$
- $sgn \tau = -1$
- $sgn(\sigma_1 \circ \sigma_2) = (sgn \sigma_1) \cdot (sgn \sigma_2)$

## Untergruppenkriterium

Wenn  $U \subseteq G$  und  $U \neq \emptyset$  und  $\forall a, b \in U$  gilt  $a * b' \in U$  dann ist U Untergruppe

## Erzeugnis

- $E \subseteq G$
- $\langle E \rangle = \bigcap \{U | U \text{ ist UG und } E \subseteq U\}$

## Untergruppeninduzierte Äquivalenzrelation

- $a \sim_U b \Leftrightarrow b \in a * U \Leftrightarrow a' * b \in U$
- $a \sim_U b \Leftrightarrow a \in U * b \Leftrightarrow a * b' \in U$

$[a]_{\sim U} = a * U$

$[a]_{U \sim} = U * a$

## Satz von Lagrage

$\#U | \#G$ ; G ist Gruppe, U ist Untergruppe

## Gruppenmorphismus

- $f(a * b) = f(a) \square f(b)$
- $f(e_1) = e_2$
- $f((a'))' = f(a')$
- Bild(f), Kern(f) sind jeweils Untergruppen
- Wenn Kern(f) =  $\{e_1\}$ , ist f injektiv

## Normalteiler

- N ist Untergruppe von G
- wenn  $a * N = N * a$
- Wobei nur die Mengen gleich sein muessen, dann ist N ein Normalteiler
- Kern(f) ist immer Normalteiler

## Faktorgruppe

- $G/N = \{[a] = a * N | a \in G\}$
- $\tilde{\tau} = [a] \tilde{\tau} \quad [b] = [a * b]$
- kanonsiche Surjektion:  $\pi: \begin{cases} G \rightarrow G/N \\ a \rightarrow [a] \end{cases}$

## Homomorphiersatz

$G / \text{Kern}(f) \cong \text{Bild}(f)$

## Ring

- $(R, +, \cdot)$
- $(R, +)$  ist abelsche Gruppe
- $(R, \cdot)$  ist Halbgruppe
- Distributivgesetze müssen gelten:  
→  $(a + b) \cdot c = (a \cdot c) + (b \cdot c)$
- kommutativer Ring →  $(R, \cdot)$  kommutiert
- Ring mit Eins →  $(R, \cdot)$  ist Monoid
- Charakteristik ist die kleinste Zahl  $n \in \mathbb{N}$  für die im Ring gilt:  $n \cdot 1_R = 0_R$  (Char(R))
- char(R) = 0 wenn  $n \cdot 1_R = 0 \forall n \in \mathbb{N}$
- Nullteiler  $a \cdot b = 0_R$  für  $b \in R \setminus \{0_R\}$  Es gibt wieder links und rechtsnullteiler, je nach kommutativität.
- Nullteilerfrei:  $\forall a, b \in R (a \cdot b = 0_R \Rightarrow a = 0_R \text{ oder } b = 0_R)$
- Integritätsring = Ring mit Eins, kommutativ, Nullteilerfrei
- Restklassenring modulo m ist ein Integritätsring wenn m eine Primzahl ist

## Ringmorphismen

- $f(a +_1 b) = f(a) +_2 f(b)$
- $f(a \cdot_1 b) = f(a) \cdot_2 f(b)$
- wenn beide Ringe eine 1 haben:  $f(1_{R1}) = 1_{R2}$

## Körper

- $(K, +)$  ist abelsche Gruppe
- $(K \setminus \{0_K\}, \cdot)$  ist abelsche Gruppe
- Es gelten die Distributivgesetze ( wie im Ring)
- Da  $0_K \neq 1_K$  hat ein Körper immer min. 2 Elemente
- Jeder Körper ist ein Integritätsring
- Ringregeln gelten hier auch
- endliche Integritätsringe sind Körper

## Körpermorphismen

- $f(a +_1 b) = f(a) +_2 f(b)$
- $f(a \cdot_1 b) = f(a) \cdot_2 f(b)$
- $f(1_{K1}) = 1_{K2}$
- $f(0_{K1}) = 0_{K2}$
- Körpermorphismen sind automatisch injektiv

## Polynome

$$p = \sum_{i=0}^m a_i \cdot t^i; \quad q = \sum_{i=0}^n b_i \cdot t^i$$

**Addition:**  
 $p + q = \sum_{i=0}^{\max(m,n)} (a_i + b_i) \cdot t^i$

- Multiplikation:**  
 $p \cdot q = \sum_{k=0}^{m+n} c_k \cdot t^k; \quad c_k = \sum_{i=0}^k a_i \cdot b_{k-i}$
- Polynome bilden einen Ring  $(R[t], +, \cdot)$
- monisch, normiert = Leitkoeffizient ist 1<sub>R</sub>
- $\deg(p+q) \leq \max(\deg(p), \deg(q))$
- $\deg(p \cdot q) \leq \deg(p) + \deg(q)$
- Wenn R Nullteilerfrei wird  $\leq 1$  zu =
- ist R ein Integritätsring, dann auch R[t]

## Polynomdivision

- R[t] ist niemals ein Körper. Aber R muss für die Polynomdivision ein Körper sein (multiplikative Inverse).
- $p_2$  ist Teiler von  $p_1$ , wenn q existiert, mit  $p_1 = q \cdot p_2$
- $p_1 = q \cdot p_2 + r$  mit  $\deg(r) < \deg(p_2)$
- q ist eindeutig
- Beispiel Division:

$$\begin{array}{r} 3t^3 \phantom{+ 2t} + 1 = (t^2 - 4t)(3t + 12) + 50t + 1 \\ - 3t^3 + 12t^2 \\ \hline 12t^2 + 2t \\ - 12t^2 + 48t \\ \hline 50t + 1 \end{array}$$

## Nullstelle

- $\lambda$  ist Nullstelle, wenn  $p(\lambda) = 0_R$
- Folgendes ist äquivalent:
  - $\lambda \in K$  ist Nullstelle von K
  - $(t - \lambda) \in K[t]$  ist Teiler von p
- **Zerlegung**
  - K sei Körper,  $p \in K[t]$
  - $p = (t - \lambda_1)^{s_1} \dots (t - \lambda_s)^{s_s} \cdot q$ , wobei q keine Nullstelle in K hat.
  - p hat höchstens deg(p) verschiedene Nullstellen s ≤ p)
  - Ist K ein unendlicher Körper,  $\Phi: K[t] \rightarrow K^K$  ist injektiv

## Vektorraum

- $(V, +)$  → abelsche Gruppe
- Für  $\cdot$  mit Skalar aus Skalarkörper muss gelten:
  - $\alpha \circ (u \oplus v) = (\alpha \circ u) \oplus (\alpha \circ v)$
  - $(\alpha + \beta) \circ v = (\alpha \circ v) \oplus (\beta \circ v)$
  - $(\alpha \cdot \beta) \circ v = \alpha \circ (\beta \circ v)$
  - $1_K \circ v = v$
  - $0_K \circ v = 0_V \cdot \alpha \circ 0_V = 0_V$

## Linearkombination

$$\sum_{j=1}^n a_j \cdot v_j$$

## Unterraumkriterium

- $U \neq \emptyset; \forall u, v \in U; \alpha \in K$  gilt  $u + v \in U; \alpha \cdot v \in U$
- $U \neq \emptyset; \forall u, v \in U; \alpha, \beta \in K$  gilt  $\alpha \cdot u + \beta \cdot v \in U$
- $\langle E \rangle$  erzeugter Unterraum, wie bei der Gruppe, kann man sich vorstellen, als alle möglichen Linearkombinationen mit Vektoren aus E.
- Es gilt weiter:
  - $\langle E_1 \cup E_2 \rangle = \langle \langle E_1 \rangle \cup \langle E_2 \rangle \rangle$
  - $\langle E_1 \cap E_2 \rangle = \langle \langle E_1 \rangle \cap \langle E_2 \rangle \rangle$

## Lin. Unabhängigkeit

- $\sum_{i=1}^n \alpha_i \cdot v_i = 0$  nur wenn alle  $\alpha_i = 0$  sind.
- Menge/Familie an Vektoren, die den Nullvektor enthält sind immer linear abhängig.

## Basis

- Sei  $B \subseteq V$ , B ist lin. unabhängig,  $\langle B \rangle = V$
- Sei A lin unabhängig Menge und  $A \subseteq V$  und  $A \subseteq E$ , wobei  $E \rightarrow \langle E \rangle = V$ , dann existiert eine Basis B mit  $A \subseteq B \subseteq E$
- Jeder Vektorraum besitzt eine Basis.
- aus E mit  $\langle E \rangle = V$  lässt sich eine Basis auswählen.
- jede lin. unabhängige  $A \subseteq V$  kann zu einer Basis erweitert werden.

## Dimension

- Kardinalität der Basis,  $\dim(V) = \#B$ , wenn B endlich
- Wenn B unendlich, ist  $\dim(V) = \infty$
- Austauschlemma, Sei  $B = \{v_1, \dots, v, \dots, v_n\}$  eine Basis

Sei  $w = \sum_{i=1}^n \alpha_i \cdot v_i$  wobei nicht alle  $\alpha_i = 0$  sein dürfen.

- Dann ist  $B_0 = \{v_1, \dots, v, \dots, v_n\}$  auch nh Basis
- Sei B eine Basis von V mit  $\#B = n$ , und A eine lin. unabhängige Untermenge von V mit  $\#A = m$ , dann gilt:  $m \leq n$
- alle Basen eines endlich erzeugten Vektorraums V sind gleichmächtig.

## Summe von Unterräumen

- $\langle U \cup W \rangle = U + W$
- $\dim(U+W) = \dim(V) + \dim(W) - \dim(U \cap W)$
- wenn  $U \cap W = 0$ , dann ist die Summe direkt  $\oplus$
- Es ist Äquivalent:
  - $V = U \oplus W$
  - $\forall v \in V$  existieren eindeutige Vektoren u,w, sodass  $v = u + w$
  - Sind U und W endlich dimensional gilt weiterhin:
    - $\dim(V) = \dim(U) + \dim(W)$  und  $\dim(U \cap W) = 0$
    - Sei B eine Basis von V,  $B = \{B_1, B_2\}$  eine Partition, es gilt:  $V = \langle B_1 \rangle \oplus \langle B_2 \rangle$
    - $U_1, U_2$  sind UR von U und haben die Basen  $B_1, B_2, V = U_1 \oplus U_2$ , so ist  $B_1 \cup B_2$  eine Basis von V
    - Wenn  $V = U \oplus W$ , ist W ein komplementärer Unterraum von U.
    - Dimension des komplementären Unterraums heißt Kodimension von U, also  $\dim(W) = \text{codim}(U)$ .

## Summe von Familien von Unterräumen

- $\sum_{i \in I} U_i = \langle \bigcup_{i \in I} U_i \rangle$
- Direkt, wenn  $U_j \cap \sum_{i \in I \setminus \{j\}} U_i = \{0\} \quad \forall j \in I$

## Matrizen

- $K^{n \times m}$  ist Matrize über K
- k-te Diagonale ist j=i=k, für i = Zeilenindex, j = Spaltenindex
- Addition  $(A + B)_{ij} = a_{ij} + b_{ij}$
- Skalare Multiplikation:  $(\alpha \cdot A)_{ij} = \alpha \cdot a_{ij}$
- $(K^{n \times m}, +, \cdot)$  ist Vektorraum mit Standardbasis  $E_{ij}$

