LINEARE ALGEBRA

2.1 - **Notwendige Eigenschaften eines Vektorraums** sind Gruppenstruktur der Addition, $(k_1 + k_2) \cdot v = k_1 \cdot v + k_2 \cdot v$, $k \cdot (v_1 + v_2) = k \cdot v_1 + k \cdot v_2$ (Distributivität), $(k_1 \cdot k_2) \cdot v = k_1 \cdot (k_2 \cdot v)$ (Assoziativität), $1 \cdot v = v$ (Neutrales Element)

2.7 - Der **Schnitt von beliebig vielen K-Untervektorräumen** von V ist wieder ein K-Untervektorraum von V

2.? - Ein **Homomorphismus** erfüllt im Allgemeinen $\phi(v_1 + v_2) = \phi(v_1) + \phi(v_2)$. Ein **Vektorraumhomomorphismus** erfüllt auch $\phi(k \cdot v) = k \cdot \phi(v)$

2.52 - Seien U, V, W Vektorräume mit Basen B_U, B_V, B_W. Sei $\phi : U \to V$ und $\psi : V \to W$. Dann gilt ${}_{B_W}(\psi \circ \phi)_{B_U} = ({}_{B_W}\psi_{B_V}) \cdot ({}_{B_V}\phi_{B_U})$, wobei $({}_{B_V}\phi_{B_U})$ nur genauere Notation für ϕ ist.

2.63, 2.65 - $\phi : V \to W$. $\dim(Kern(\phi)) + \dim(Bild(\phi)) = \dim(V)$. ϕ ist **injektiv** gdw. $\dim(\text{Kern}(\phi)) = 0$. Sie ist **surjektiv** gdw. $\dim(\text{Bild}(\phi)) = \dim(W)$. Es folgt, dass Funktionen $\mathbb{R}^n \to \mathbb{R}^m$, also $n \times m$-Matrizen, nicht invertierbar sind.

2.73 Spalten von ϕ, die nach Umformung zu **Pivots** werden, bilden eine Basis des Bildes.

2.78 - 2.81 $(A^T)^{-1} = (A^{-1})^T$. $(A \cdot B)^T = B^T \cdot A^T$. $rg(A) = rg(A^T)$. $rg(A^T \cdot A) = rg(A)$.

2.82 **Normen:** $||v|| = 0 \Leftrightarrow v = 0$; $||kv|| = |k| \cdot ||v||$; $||v + w|| \leq ||v|| + ||w||$
Metriken: $d(u, v) = 0 \Leftrightarrow u = v$; $d(u, v) = d(v, u)$; $d(u, w) \leq d(u, v) + d(v, w)$

2.83 **Jede Norm erzeugt eine Metrik** durch $d(u, v) = ||u - v||$

2.88 $\langle v, w\rangle = ||v|| \cdot ||w|| \cdot \cos(\alpha)$

2.89 **Orthogonale Projektion** $w_v = \frac{\langle w,v\rangle}{\langle v,v\rangle} = \frac{\langle w,v\rangle}{||v||} \cdot \frac{v}{||v||}$

2.91 Ist $v_1, \ldots, v_n$ eine Orthogonalbasis gilt $w = \sum_{i=1}^{n} \langle w, v_i\rangle \cdot v_i \ \forall w$

2.92 **Graham Schmidt** Induktiv mit einem Vektor v starten und dann von den anderen Vektoren die Orthogonalprojektion auf die bisherigen Vektoren abziehen. Danach alle Vektoren normalisieren.

2.93 Ist U ein Untervektorraum von V, so ist $U^\perp$ die Menge der Vektoren aus V welche zu allen Vektoren aus U orthogonal sind (**Orthogonales Komplement von U in V**)

2.96 $\langle A \cdot v, w\rangle = \langle v, A^T \cdot w\rangle$

2.99 **Determinanten sind multilinear** $\left(\det\begin{pmatrix}\dots\\ ka+b\\ \dots\end{pmatrix} = k\det\begin{pmatrix}\dots\\ a\\ \dots\end{pmatrix} + \det\begin{pmatrix}\dots\\ b\\ \dots\end{pmatrix}\right)$

Determinanten sind alternierend (sind zwei Zeilen idenisch ist det 0)
Kofaktoren: $A_{ij} = -1^{i+j}\det(<\textit{Matrix A ohne Zeile i und Spalte j}>)$

2.102 $A^{-1} = \frac{1}{\det A}\begin{pmatrix}A_{11} & \dots & A_{1n}\\ \vdots & & \vdots\\ A_{n1} & \dots & A_{nn}\end{pmatrix}^T$

2.105 **Charakteristisches Polynom** - $\det(A-\lambda I_n) = 0$

2.107, 2.111 Eine Matrix ist **Diagonalisierbar**, wenn eine Basis aus Eigenvektoren existiert. Dies ist gegeben wenn n Eigenwerte existieren, da Eigenvektoren mit verschiedenen Eigenwerten orthogonal zueinander sind.

2.108 A und B sind **ähnlich**, wenn sie als $B = C^{-1}\cdot A\cdot C$ geschrieben werden können.

2.114 $U \leq V$ ist ϕ **- invariant**, wenn $\phi(u)\in U\ \forall u\in U$

2.116 **Spektralsatz** - ist A symmetrisch so hat sie Eigenvektoren $v_1,\dots,v_n$ und es ist

$$(v_1|\dots|v_n)\cdot A\cdot(v_1|\dots|v_n)^T = \begin{pmatrix}\lambda_1 & & \\ & \ddots & \\ & & \lambda_n\end{pmatrix}$$

2.118 **Singulärwertzerlegung**

- $B := A^T\cdot A$, B hat n Eigenvektoren v_i geordnet nach Größe der Eigenwerte
- $u_i := \frac{1}{\sqrt{\lambda_1}}\cdot A\cdot v_i$. Wenn nötig durch weitere Orthogonale Vektoren ergänzen (Orthonormalbasis von $U^\perp$)
- $U := (u_1|\dots|u_m)$; $V := (v_1|\dots|v_n)$; $\Sigma_{ij} := \sqrt{\lambda_i}$ falls $i = j \leq rg(A)$
- Dann ist $A = U\cdot\Sigma\cdot V^T$

2.122 **Prüfziffern** - Ergänzung der Nachricht A um ein Zeichen s.d. $\Pi a_i = c$ für ein konstantes c

2.124 Prüfziffern erkennen Vertauschungen falls $x\cdot\pi_{i+1}(\pi_1^{-1}(y)) \neq y\cdot\pi_{i+1}(\pi_1^{-1}(x))$

2.128 Ein **q-ärer Code C der Länge n über A / einem Alphabet mit q Wörtern** ist eine nichtleere Teilmenge von H(n,A) bzw. H(n,q). Ein linearer q-ärer [n,k,d]-Code ist ein Untervektorraum von $\mathbb{F}_q^n$ mit Dimension k und Minimalabstand d. Das Minimalgewicht ist dann $min(d(c,0)|c\neq 0)$.

2.131 Ein Code mit Minimalabstand d erkennt Fehler bis $d-1$ und korrigiert bis $\lfloor\frac{d-1}{2}\rfloor$

2.133 Ein **Ball mit Radius e** enthält $\sum_{i=0}^{e}\binom{n}{i}\cdot(q-1)^i$ Wörter

2.136 Ein **perfekter Code** enthält $\frac{q^n}{\sum_{i=0}^{\lfloor \frac{d-1}{2} \rfloor} \begin{pmatrix} n \\ i \end{pmatrix} \cdot (q-1)^i}$ Wörter

2.140 Eine **Erzeugermatrix G** für einen linearen [n,k] Code ist eine $(k \times n)$-Matrix, deren Zeilen eine Basis von C bilden. Es existiert immer eine Erzeugermatrix der Form $(I_k|A)$.

2.142,5 **Codierung** eines Vektors erfolgt durch $v \cdot G$

2.145 Eine **Prüfmatrix H** für einen linearen [n,k] Code ist eine $((n-k) \times n)$-Matrix, welche $C = Kern(H)$ erfüllt.

2.146 H ist eine Prüfmatrix von C $\Leftrightarrow H \cdot c^T = 0 \; \forall c \in C$ und Zeilen von H sind linear unabhängig $\Leftrightarrow G \cdot H^T = 0$ und Zeilen von H sind linear unabhängig

2.148 Hat G die Form $(I_n|A)$, so hat H die Form $(-A^T|I_{n-k})$

2.150 C hat ein **Minimalgewicht** $\geq d$ gdw. je $d-1$ Spalten der Prüfmatrix linear unabhängig sind

2.152 Ein **Hamming-Code** ist ein Code mit Minimalgewicht 3 und der Maximalen Anzahl an Spalten

2.153 Bei gegebener Zeilenzahl m der Prüfmatrix existiert ein Hamming-Code mit Wortlänge $n = \frac{q^m-1}{q-1}$ und Dimension $k = n - m$

ALGEBRA

3.7 Eine **Untergruppe** enthält das neutrale Element und ist bzgl. Gruppenoperation und Inversion abgeschlossen

3.10 Kerne und Bilder von Gruppenhomomorphismen sind Untergruppen

3.18 - 3.20 **Zyklische Gruppen** sind kommutativ, ebenso ihre Untergruppen und homomorphe Bilder. Zyklische Gruppen der Ordnung m sind isomorph zu $\mathbb{Z}_m$.

3.23 Die **Automorphismen einer zyklischen Gruppe** $G = \langle g \rangle$ sind genau die Homomorphismen $\phi : G \to G$, für die $\phi(g)$ ein Erzeuger von G ist. Bei Z_m sind dies die zu m teilerfremden Zahlen.

3.27 $Z_m \times Z_n$ ist zyklisch gdw. m und n Teilerfremd sind. Die Gruppe ist dann isomorph zu Z_{mn}. Bei Produkten von Gruppen kann man dementsprechend Teilerfremde Gruppen zusammenfassen aber nicht Gruppen mit gemeinsamen Teilern.

3.29 - 3.31 Die **Linksnebenklassen von U in G** sind die Äquivalenzklassen der Relation $g_1 \ {}_U\!\sim g_2 \Leftrightarrow g_1^{-1} \circ g_2 \in U$.
Die **Rechtsnebenklassen von U in G** sind die Äquivalenzklassen der Relation $g_1 \sim_U g_2 \Leftrightarrow g_1 \circ g_2^{-1} \in U$.
Man schreibt dann gU bzw. Ug für die Links- bzw. Rechtsnebenklasse welche g enthält.
Die **Menge der Linksnebenklassen** ist G/U, die Menge der Rechtsnebenklassen ist $U \backslash G$

3.32 Alle Nebenklassen einer Untergruppe U von G haben gleich viele Elemente wie die Untergruppe. Die Anzahl an Nebenklassen pro Seite ist der **Index [G:U]**.

3.33 Für eine endliche Gruppe G gilt $|G| = |U| \cdot [G : U]$

3.34 Eine Untergruppe heißt **normale Untergruppe** oder **Normalteiler**, falls ihre Links- und Rechtsnebenklassen identisch sind. Man Schreibt $U \trianglelefteq G$.

3.35 Kerne von Gruppenhomomorphismen sind normale Untergruppen, e und G sind normale Untergruppen,

3.36 Eine Äquivalenzrelation auf einer Gruppe heißt **Kongruenzrelation**, falls $g \to g/\sim$ ein Homomorphismus ist. Das gilt gdw. $(g/\sim) \circ (h/\sim) := (g \circ h)/\sim$, also wenn die Äquivalenzklasse von $g \circ h$ nur von den Äquivalenzklassen von g und h abhängen (und nicht von g und h selbst)

3.37 Die **Kongruenzrelationen von Gruppen** sind die Nebenklassenrelationen normaler Untergruppen.

3.38 ist $N \leq G$, so ist die Gruppenstruktur auf der Menge G/N der Nebenklassen von N in G die **Faktorgruppe von G nach N**

3.49 Ein **Ideal eines Rings R** ist eine additive Untergruppe I mit $r \cdot i \in I$ und $i \cdot r \in I$. Man schreibt $I \trianglelefteq R$.

3.51 Kerne von Ringhomomorphismen sind Ideale und umgekehrt, genauer wird R/I durch $(r_1 + I) \cdot (r_2 + I) = (r_1 \cdot r_2) + I$ zu einem Ringhomomorphismus mit Kern I

3.55 Eine **Einheit** ist ein Ringelement mit multiplikativen Inversen. Dies sind genau die Teiler des Einselements. Einheiten Teilen jedes andere Element. Die Menge der Einheiten von $\mathbb{Z}$ ist $\mathbb{Z}_m^*$

3.57 Jeder gemeinsame Teiler zweier Zahlen ist ein Teiler des ggT. (Es ist auch jedes gemeinsame Vielfache zweier Zahlen ein Vielfaches des kgV, dies wurde jedoch in der Vorlesung nicht bewiesen).

3.58 Für alle a, b gibt es $k, l \in \mathbb{Z}$ sd. $k \cdot a + l \cdot b = \text{ggT}(a, b)$

3.60 Sei $a \neq 0 \in \mathbb{Z}_m$. Dann: a ist eine Einheit $\Leftrightarrow$ a ist kein Nullteiler $\Leftrightarrow$ Multiplikation mit a ist ein Isomorphismus $\Leftrightarrow$ a und m sind Teilerfremd

3.61 Inverses per Euklid: $1 = \text{ggT}(a, m) = k \cdot a + l \cdot m$, dann ist $k \mod m$ das Inverse

3.64 **Kongruenzsysteme** haben immer eine Lösung wenn die m_i paarweise teilerfremd sind.

$$a = r_1 \mod m_1$$
$$a = r_2 \mod m_2$$

3.64.1 Erster Schritt bei Kongruenzsystemen: Finde a_1 und a_2 sd. $a_1 m_1 + a_2 m_2 = 1$. Dann ist $a = r_2 a_1 m_1 + r_1 a_2 m_2$ eine Lösung.

3.64.2 Sei bereits $b_{k-1} \equiv r_1 \mod m_1 \equiv r_{k-1} \mod m_{k-1}$. Dann sucht man im nächsten Schritt ein $b_k \equiv b_{k-1} \mod m_1 \cdot \ldots \cdot m_{k-1} \equiv r_k \mod m_k$

3.67 Die **Eulersche φ-Funktion** zählt die Anzahl an Zahlen $< m$ die teilerfremd mit m sind

3.71 + 3.72 Aus 3.33 folgt $g^{|G|} = e$. Daraus folgt: Für a welches m nicht teilt (also $a \in \mathbb{Z}_m^*$) gilt $a^{\varphi(m)} \equiv 1 \mod m$. Daraus folgt wiederum der **kleine Satz von Fermat** $a^{p-1} \equiv 1 \mod m$ für Primzahlen p die a nicht teilen.

3.? **Schnelle Exponentiation** $a^b \mod c$:

1	1	0	1	$\leftarrow$ Binärdarstellung von b
$a_4 = a_3^2$	$a_3 = a_2^2$	$a_2 = a_1^2$	$a_1 = a^2$	$\leftarrow$ $a_n = a_{n-1}^2 \mod c$

Dann einfach alle a_n aus Spalten mit Eintrag 1 multiplizieren.

3.?? **RSA**

- Man finde zwei Primzahlen p und q. $n = p \cdot q$, $\varphi(n) = (p-1) \cdot (q-1)$.
- Man wähle ein großes, zu $\varphi(n)$ teilerfremdes e und finde das Inverse d in $Z_{\varphi(n)}$
- Man veröffentlicht e und n
- Verschlüsselung eines Zeichens a durch $a_* = a^e \mod n$
- Entschlüsselung durch $a_*^d \mod n = a$

ANALYSIS

4.2 Die **offene Kugel** $B_r(x)$ mit Radius r und Mittelpunkt x ist $\{y \mid d(x, y) < r\}$. Eine Umgebung um x enthält eine Kugel $B_\varepsilon(x)$ mit $\varepsilon > 0$

4.2 Alle Normen sind asymptotisch äquivalent

4.11, 4.12 Konvergenz und Stetigkeit sind äquivalent zum eindimensionalen Fall (also Stetigkeit durch Folgenstetigkeit)

4.13 Für f, g stetig und $g(x) \neq 0$ ist $\frac{f(x)}{g(x)}$ stetig

4.17, 4.18 Die **Matrixnorm** einer linearen Abbildung $V \to W$ mit Matrix A ist die Norm $||A|| := \sup\{||A \cdot v||_W \mid v \in V, ||v||_V = 1\}$. Es gilt $\max|a_{ij}| \leq ||A|| \leq \sqrt{mn} \max|a_{ij}|$

4.20 Die **Richtungsableitung** $D_v f(x)$ in Richtung v ist der Grenzwert $D_v f(x) = f'_v(x) = \lim_{h \to 0} \frac{f(x+hv)-f(x)}{h}$

4.21 Die **partielle Ableitung** $\frac{\partial f(x)}{\partial x_i}$ ist die Richtungsableitung in die Koordinatenrichtung x_i. f heißt partiell differenzierbar wenn partielle Ableitungen an jedem Punkt in jede Richtung existieren und stetig partiell differenzierbar ($f \in C^n$) falls sie stetig sind.

4.24 **Gradient:** $f : D \to \mathbb{R}$, dann $\text{grad} f(x) = \nabla f(x) = \left(\frac{\partial f(x)}{\partial x_1}, \ldots, \frac{\partial f(x)}{\partial x_n}\right)$. Auf Gradienten gelten die selben Rechenregeln wie für Ableitungen generell.

4.26 Die **Divergenz** einer Funktion $g : D \to \mathbb{R}^n$ ist $\text{div } g := \langle \nabla, g \rangle := \frac{\partial g_1}{\partial x_1} + \ldots + \frac{\partial g_n}{\partial x_n}$

4.29 $D_j D_i f(x) = D_i D_j f(x)$

4.32 $\Delta f := \text{div grad } f = \frac{\partial^2 f}{\partial x_1^2} + \ldots + \frac{\partial^2 f}{\partial x_n^2}$

4.34 $f : D \subseteq \mathbb{R}^n \to \mathbb{R}^m$ heißt **total differenzierbar** im Punkt x_0, falls eine $(m \times n)$-Matrix A existiert, sodass

$$\lim_{h \to 0} \frac{||f(x_0 + h) - f(x_0) - A \cdot h||}{||h||} = 0$$

4.38 Sind alle partiellen Ableitungen von f in x stetig, so ist f in x total differenzierbar.

4.? Totale Differenzierbarkeit $\Rightarrow$ Richtungsdifferenzierbarkeit in alle Richtungen $\Rightarrow$ partielle Differenzierbarkeit

4.45 f ist **konkav** falls $f(\lambda x + (1-\lambda)y) \geq \lambda f(x) + (1-\lambda) f(y)\ \forall x, y \in S, \lambda \in [0, 1]$.

4.46 Sei $A \in \text{Mat}_{(n \times n)}(\mathbb{R})$ und $q(x) := \langle x, A \cdot x \rangle$. Dann ist A:

- positiv semidefinit, falls $q(x) \geq 0 \quad \forall x \neq 0$
- negativ semidefinit, falls $q(x) \leq 0 \quad \forall x \neq 0$
- ansonsten indefinit

4.47 Ist A symmetrisch, so kann man in den Ungleichungen $q(x)$ durch die Eigenwerte von A ersetzten

4.49 **Hurwitz-Kriterium**: Seien die Hauptminoren $A_k k$ die Matrizen mit den ersten k Zeilen und Spalten von A, dann ist A positiv definit, wenn $\det A_{kk} > 0 \quad \forall k$ und negativ definit, wenn $(-1)^k \det A_{kk} > 0$

4.51 $\text{Hess} f(x) := \left(\frac{\partial^2 f(x)}{\partial x_i \partial x_j}\right)$. Nach Satz 4.29 ist Hess symmetrisch.

4.52 f **ist konvex gdw. Hess** $f(x)$ **positiv semidefinit ist** und konkav falls negativ. Ist sie nicht nur semidefinit sondern definit ist f strikt konvex bzw. konkav.

4.54 $f \in C^1(D)$ **ist konkav** gdw. $f(x) - f(y) \leq \langle \nabla f(y), x - y \quad \forall x, y$

4.55 x ist ein **stationärer Punkt** von f falls $\nabla f(x) = 0$

4.57 Ist f konkav, so ist jeder stationäre Punkt ein Maximum. Ist f konvex, so ist jeder stationäre Punkt ein Minimum.

4.58 Ist **Hess** $f(x*)$ **positiv definit**, so ist $x*$ ein Minimum und umgekehrt. Ist Hess indefinit ist $x*$ ein Sattelpunkt.