Mathematik für Informatik 3

Klausurvorbereitung

Marvin Borner

Wintersemester 2022/23

Dies ist meine WIP Zusammenfassung, welche hauptsächlich mir dienen soll. Ich schreibe außerdem ein inoffizielles Skript, welches auf https://marvinborner.de/mathe3.pdf zu finden ist.

Inhalt

1 Sinnvolle Rechenregeln **4**
1.1 Potenzregeln 4
1.2 Toll 4

2 Euklidischer Algorithmus **4**

3 Erweiterter Euklidischer Algorithmus **4**

4 Inverse prüfen **4**

5 Zykel **5**

6 Fundamentalsatz **5**

7 Chinesischer Restsatz **5**

8 Reduzibilität **5**

9 Lösen von $a^b \pmod n$ **5**

10 Eulersche φ-Funktion **5**

11 RSA-Verfahren **5**

12 Konvergenz **6**

13 Eigenschaften von Mengen **6**

14 Stetigkeit **6**
14.1 Polarkoordinaten 7
14.2 Prüfen 7

15 Weierstraß Minimax-Theorem **7**

16 TODO: Zeug? **7**

17 Differenziation **7**
17.1 Prüfen 8

18 Ableitungsregeln **8**

19 Richtungsableitung **8**

20 Satz von Schwarz **8**

21 Definitheit **8**
21.1 Matrix 8

22 Extrema **9**

23 Taylor **9**

24 Höhenlinien **9**

25 Implizite Funktionen **9**

26 Umkehrfunktionen **9**

27 Lagrange **9**

1 Sinnvolle Rechenregeln

1.1 Potenzregeln

- $a^n \cdot a^m = a^{n+m}$
- $a^n \cdot b^n = (a \cdot b)^n$
- $(a^n)^m = a^{n \cdot m}$
- $\frac{a^n}{b^n} = \left(\frac{a}{b}\right)^n$
- $\frac{a^n}{b^m} = a^{n-m}$

1.2 Toll

- $\sin^2(x) + \cos^2(x) = 1$

2 Euklidischer Algorithmus

Zur Berechnung des ggT.

Beispiel

Berechnung von $\text{ggT}(48, -30)$:

$$\begin{aligned} 48 &= -1 \cdot -30 + 18 \\ -30 &= -2 \cdot 18 + 6 \\ 18 &= 3 \cdot 6 + 0 \end{aligned}$$

$\text{ggT}(48, -30) = 6$

TODO: kgV mit Primfaktorzerlegung

3 Erweiterter Euklidischer Algorithmus

Zur Berechnung von s, t, da:

$$0 \neq a, b \in \mathbb{Z} \implies \exists s, t \in \mathbb{Z} : \text{ggT}(a, b) = sa + tb$$

ggT gleichsetzen, rückwärts einsetzen und je ausmultiplizieren.

Beispiel

Mit vorigem Beispiel:

$$\begin{aligned} 6 &= -30 + 2 \cdot 18 \\ &= -30 + 2 \cdot (48 + 1 \cdot -30) \\ &= 2 \cdot 48 + 3 \cdot -30 \end{aligned}$$

TODO: Polynome.

4 Inverse prüfen

$$a \in \mathbb{Z}_n \text{ invertierbar} \iff \text{ggT}(a, n) = 1$$

a^{-1} ist dann s aus $sa + tn = 1$ des EEA.

5 Zykel

- zyklische Gruppe, von a erzeugt: $\langle a \rangle := \{a^n \mid n \in \mathbb{Z}\}$

6 Fundamentalsatz

Mit $2 \leq n \in \mathbb{N}$ gibt es endlich viele paarweise verschiedene $p_1, ..., p_k \in \mathbb{P}$ und $e_1, ..., e_k \in \mathbb{N}$, sodass

$$n = p_1^{e_1} \cdot ... \cdot p_k^{e_k}.$$

7 Chinesischer Restsatz

Lösen von simultaner Kongruenz.

TODO: Beispiel.

8 Reduzibilität

- TODO: Nullstellen und so
- TODO: Mit Primzahlen ez

9 Lösen von $a^b \pmod n$

- falls n groß: Primfaktorzerlegung von n und für jeden Faktor durchführen.
- Modulo in Potenzen aufnehmen (Trick: $2 \pmod 3 = -1$)
- Satz von Euler: $a^{\varphi(n)} \equiv 1 \pmod n$
- sonst schlau Potenzregeln anwenden

10 Eulersche φ-Funktion

- $\varphi(p) = p - 1$ für $p \in \mathbb{P}$
- $\varphi(M) = m_1 \cdot ... \cdot m_n$ mit $m_i \in \mathbb{N}$ paarweise teilerfremd (bspw. über chinesischen Restsatz)
- $\varphi(M) = (p_1 - 1)p_1^{a_1 - 1} \cdot ... \cdot (p_k - 1)p_k^{a_k - 1}$, mit Primfaktorzerlegung $M = p_1^{a_1} \cdot ... \cdot p_k^{a_k}$

Beispiel

$\varphi(100) = \varphi(4 \cdot 5^2) = \varphi(4) \cdot \varphi(5^2) = 2 \cdot (5 - 1) \cdot 5^{2-1} = 40$

11 RSA-Verfahren

Bob (Schlüsselerzeugung)

1. wählt zwei große $p, q \in \mathbb{P} : p \neq q$ und bildet $n = pq$
2. berechnet $\varphi(n) = (p - 1)(q - 1)$
3. wählt e teilerfremd zu $\varphi(n)$
4. bestimmt $0 < d < \varphi(n)$ mit $e \cdot d \pmod{\varphi(n)} = 1$. Verwendet dazu EEA: $ed \pmod{\varphi(n)}$
5. Public key: (e, n). Private key: d

Alice (Verschlüsselung)

1. kodiert Nachricht als Zahl und zerlegt sie anschließend in Blöcke gleicher Länge, sodass jeder Block m_i als Zahl $0 \leq m_i < n$ ist. Blöcke werden einzeln verschlüsselt. Sei m ein solcher Block.

2. berechnet $c = m^e \pmod n$
3. sendet c an Bob.

Bob (Entschlüsselung)

1. berechnet $c^d \pmod n = m$ für alle Blöcke

Beispiel

Gegeben $(n, e) = (33, 3)$ public key

1. Verschlüsseln Sie die Nachricht $m = 6$.
   $c = m^e \pmod n = 6^3 \pmod{33} = 3 \cdot 6 = 18$
2. Faktorisieren Sie $n = 33$, berechnen Sie $\varphi(n)$ und d.
   $\varphi(n) = 2 \cdot 10 = 20$, $ed \pmod{20 = 1}$. Man erkennt $d = 7$.
3. Entschlüsseln Sie die Nachricht $c = 2$: $m = c^d \pmod n = 2^7 \pmod{33} = 2^5 \cdot 2^2 \pmod{33} = -4 \pmod{33} = 29$.

12 Konvergenz

Sei $(x_k)_{k\in\mathbb{N}}$ eine Folge im $\mathbb{R}^n$. $(x_k)_{k\in\mathbb{N}}$ konvergiert gegen $a \in \mathbb{R}^n$ ($x_k \to a$ oder $\lim_{k\to\infty} x_k = a$) wenn gilt

$$\forall \varepsilon > 0 \; \exists N \in \mathbb{N} \; \forall k \geq N : \|x_k - a\| < \varepsilon.$$

13 Eigenschaften von Mengen

- Sei $x_0 \in \mathbb{R}^n,\ \varepsilon > 0$. $K_\varepsilon(x_0) = \{x \in \mathbb{R}^n \mid \|x - x_0\| < \varepsilon\}$ heißt offene ε-Kugel um x_0.
- $D \subseteq \mathbb{R}^n$ **beschränkt** $:\iff \exists K > 0 : \|x\| < K \quad \forall x \in D$
- $U \subseteq \mathbb{R}^n$ **offen** $:\iff \forall x \in U \exists \varepsilon > 0 : K_\varepsilon(x) \subseteq U$
- $A \subseteq \mathbb{R}^n$ **abgeschlossen** $:\iff A^C = \mathbb{R}^n \setminus A$ offen
- Sei (x_k) Folge in $A \subseteq \mathbb{R}^n$ mit Grenzwert $a \in \mathbb{R}^n$. A **abgeschlossen** $\iff a \in A$.
- $x \in \mathbb{R}^n$ Randpunkt von $D \subseteq \mathbb{R}^n :\iff K_\varepsilon(x) \cap D \neq \emptyset$ und $K_\varepsilon(x) \cap D^C \neq \emptyset \quad \forall \varepsilon > 0$.
- ∂D ist die (abgeschlossene) Menge aller Randpunkte von D.
- $D \subseteq \mathbb{R}^n$ **kompakt** $:\iff$ Jede Folge in D besitzt eine in D konvergente Teilfolge.
- $D \subseteq \mathbb{R}^n$ **kompakt** $\iff$ D beschränkt und abgeschlossen.
- $\bar{D} := D \cup \partial D$ ist abgeschlossen und heißt **Abschluss** von D.
- $\mathring{D} := D \setminus \partial D$ ist offen und heißt **Innneres** von D.

14 Stetigkeit

Sei $f : D \subset \mathbb{R}^n \to \mathbb{R}^m$.

- f stetig in $a \in D :\iff \lim_{x\to a} f(x) = f(a)$
- f stetig auf $D :\iff f$ stetig in $a \quad \forall a \in D$

Mit $f : D \subseteq \mathbb{R}^n \to \mathbb{R}^n, v \subseteq f(0)$, V offen:

$$f \text{ stetig} \iff f^{-1}(V) \text{ offen.}$$

TODO: Stetige Fortsetzbarkeit

14.1 Polarkoordinaten

- $x = r \cdot \cos(\alpha)$
- $y = r \cdot \sin(\alpha)$
- statt (x, y) (r, α) gegen a laufen lassen (TODO!)

14.2 Prüfen

- In Punkt: $\lim_{v \to v_0} f(v) = f(v_0)$
  - bspw. mit Polarkoordinaten
  - oder mit $0 \leq |f(x,y)| \leq ... \implies \lim_{(x,y)\to(0,0)} f(x,y) = 0$
    - bspw. x aus Nenner nehmen

15 Weierstraß Minimax-Theorem

$f : D \subseteq \mathbb{R}^n \to \mathbb{R}$ stetig, D kompakt.

$$\implies \exists x_\star, x^\star \in D : \underbrace{f(x_\star)}_{\min} \leq f(x) \leq \underbrace{f(x^\star)}_{\max} \quad \forall x \in D$$

Beispiel

$f : \mathbb{R}^2 \to \mathbb{R}$, $f(x,y) = xy$

$S = \left\{ \begin{pmatrix} x \\ y \end{pmatrix} \in \mathbb{R}^2 \mid x^2 + y^2 = 1 \right\}$

$\implies$ f hat Maximum und Minimum auf S

16 TODO: Zeug?

17 Differenziation

Sei $D \subseteq \mathbb{R}^n$ offen, $f : D \to \mathbb{R}^m$, $f(x) = (f_1(x), ..., f_m(x))$ und $a = (a_1, ..., a_n)^\top \in D$.

- Jacobimatrix:
$$f'(a) := \begin{pmatrix} \frac{\partial f_1}{\partial x_1}(a) & ... & \frac{\partial f_1}{\partial x_n}(a) \\ \frac{\partial f_m}{\partial x_1}(a) & ... & \frac{\partial f_m}{\partial x_n}(a) \end{pmatrix} \in \mathcal{M}_{m,n}(\mathbb{R})$$
- Gradient:
$$f'(a)^\top = \begin{pmatrix} \frac{\partial f}{\partial x_1}(a) \\ \vdots \\ \frac{\partial f}{\partial x_n}(a) \end{pmatrix} =: \nabla f(a) = \operatorname{grad}(f(a)) \in \mathbb{R}^n$$

Sei $D \subseteq \mathbb{R}^n$ offen, $a \in D$, $f : D \to \mathbb{R}^m$.

- f heißt in $a \in D$ (total) differenzierbar, wenn f geschrieben werden kann als
$$f(x) = \underbrace{f(a)}_{\in \mathbb{R}^m} + \underbrace{A}_{\in \mathcal{M}_{m,n}(\mathbb{R})} \cdot \underbrace{(x-a)}_{\in \mathbb{R}^m} + \underbrace{R(x)}_{\in \mathbb{R}^m},$$
  wobei $A \in \mathcal{M}_{m,n}(\mathbb{R})$ und $R : D \to \mathbb{R}^m$ mit $\lim_{x \to a} \frac{R(x)}{\|x-a\|} = 0$
- f heißt (total) differenzierbar, wenn in jedem Punkt von D differenzierbar.

Anderes:

- $f : D \subseteq \mathbb{R}^n \to \mathbb{R}^m$ differenzierbar in $a \in D$ (D offen) $\implies$ f stetig in a.

- **Tangentialebene**: $g(x) = f(a) + f'(a) \cdot (x - a)$
- f differenzierbar in $a \in D \iff f_i$ differenzierbar in $a \in D \quad \forall i \in \{1, ..., n\}$.

17.1 Prüfen

- ob in Punkt p partiell differenzierbar: partielle Ableitungen bilden
  - falls bspw. Fallunterscheidung und $(0,0)$-Punkt: h-Definition für x/y anwenden
  - Richtungsableitung: $f_v(x,y) = \frac{(x+hv_1, 0+hv_2) - f(0,0)}{h}$
- total differenzierbar
  - je partiell ableiten und prüfen ob Ableitungen stetig
  - mit Richtungsleitung versuchen Gegenteil zu beweisen (TODO)

18 Ableitungsregeln

- $(g \circ f)'(a) = g'(f(a)) \cdot f'(a)$
- $(f + g)'(a) = f'(a) + g'(a)$
- $(\lambda f)'(a) = \lambda f'(a)$
- $(f^\top g)'(a) = f(a)^\top g'(a) + g(a)^\top f'(a)$

TODO: lhopital

Anderes:

- $(\ln x)' = \frac{1}{x}$
- $\left(\frac{g}{h}\right)' = \frac{h \cdot g' - g \cdot h'}{h^2}$
- $\left(\frac{a}{x^k}\right)' = -\frac{ka}{x^{k+1}}$ bzw. unten Kettenregel

19 Richtungsableitung

Sei $D \subseteq \mathbb{R}^n$ offen, $f : D \to \mathbb{R}$, $v \in \mathbb{R}^n$ mit $\|v\| = 1$.

f heißt in $a \in D$ differenzierbar in Richtung v, falls $\lim_{h \to 0} \frac{f(a+hv) - f(a)}{h}$ exisitert. Der Grenzwert heißt Richtungsableitung von f in Richtung v in a, $\frac{\partial f}{\partial v}(a)$.

20 Satz von Schwarz

TODO.

21 Definitheit

1. Partielle Ableitungen
2. Gradienten mit 0 gleichsetzen
3. Hessematrix und Punkte einsetzen (falls x/y vorhanden)
4. Über Eigenwerte oder Determinante bestimmen

21.1 Matrix

Eine symmetrische Matrix $A \in \mathcal{M}_n(\mathbb{R})$ ist

- positiv definit $\iff \det(A_k) > 0 \quad \forall k \in \{1, ..., n\}$
- negativ definit $\iff \det(A_k) \begin{cases} < 0 & k \text{ ungerade} \\ > 0 & k \text{ gerade} \end{cases}$ (-+-+..)

TODO: über Eigenwerte

22 Extrema

Sei $D \subseteq \mathbb{R}^n$ offen, $f \in \varphi^2(D, \mathbb{R}),\ a \in D,\ \nabla f(a) = 0$.

- $H_f(a)$ positiv definit $\implies$ a Stelle eines lokalen Minimums.
- $H_f(a)$ negativ definit $\implies$ a Stelle eines lokalen Maximums.
- $H_f(a)$ indefinit $\implies$ a ist Sattelpunkt
- Ist $H_f(a)$ positiv/negativ semidefinit, so ist keine Aussage möglich.

23 Taylor

- Taylorpolynom: $T_n(x) = \sum_{k=0}^{n} \frac{f^{(k)}(x_0)}{k!}(x - x_0)^k$
- Satz: $f(x) = T_n(x) + R_n(x)$
  - $R_n(x) = \frac{f^{(n+1)}(\xi)}{(n+1)!}(x - x_0)^{n+1}$

24 Höhenlinien

- $f(x, y) = c$ setzen
- nach $y = ...$ umformen
- entweder verschiedene c einsetzen oder geg. $N_c(f)$

25 Implizite Funktionen

TODO.

26 Umkehrfunktionen

TODO.

27 Lagrange

1. Nebenbedingung mit 0 gleichsetzen
2. Lagrange-Funktion, bspw. $\mathcal{L}(x, y, \lambda) = f(x, y) + \lambda g(x, y)$ mit g Nebenbedingung
3. Erste partielle Ableitungen der Lagrange Funktion ($\mathcal{L}_\lambda = g$)
4. Ableitungen mit 0 gleichsetzen und lösen (Additionsverfahren gut)
5. Mehrere Ergebnisse dann Extrempunkte
6. Definitheit überprüfen (geränderte Matrix TODO?)