Mathematik für Informatik 3

Inoffizielles Skript

Marvin Borner

WARNUNG WIP: Fehler zu erwarten!
Stand: 20/01/2023, 13:52:03
Bitte meldet euch bei mir, falls ihr Fehler findet.

Vorlesung gehalten von
Rüdiger Zeller

EBERHARD KARLS UNIVERSITÄT TÜBINGEN

Wintersemester 2022/23

Inhalt

1 Ergänzungen zur elementaren Zahlentheorie

1.1 Teiler, Vielfaches

Sei $a, b \in \mathbb{Z},\ b \neq 0$. b heißt Teiler von A $(b \mid a) \iff \exists q \in \mathbb{Z} : a = qb$.

Beispiel

$$6 \mid 24$$

$$1 \mid 0$$

$$6 \nmid 5$$

1.2 Division mit Rest

Sei $a, b \in \mathbb{Z},\ b \neq 0$. Es gibt eindeitig bestimmbare $q, r \in \mathbb{Z}$ mit

1. $a = qb + r$
2. $0 \leq r < |b|$.

Bemerkung

q heißt Quotient, r heißt Rest.

Beweis

Beweis. Folgerung aus Fundamentalsatz der Arithmetik. Siehe Mathe 2. Q.E.D.

Beispiel

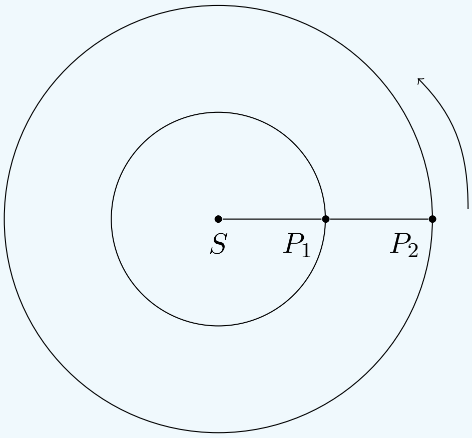
1. $a = 22,\ b = 5$
$$22 \pmod{5} \text{ (div 5)} $$

$$22 \quad (\text{div } 5) = 4, \quad 22 \quad (\text{mod } 5) = 2$$
2. $a = -22,\ b = 5$
$$-22 \quad (\text{div } 5) = -5, \quad -22 \quad (\text{mod } 5) = 3$$
3. Für $a \in \mathbb{R}$ und $b \in \mathbb{Z}$ gilt mit $q \in \mathbb{Z}$ und $r \in \mathbb{R}$ gilt z.B.:
$$a = \frac{8}{3},\ b = 1 \quad \Longrightarrow \quad \frac{8}{3} = 2 \cdot 1 + \frac{2}{3}$$

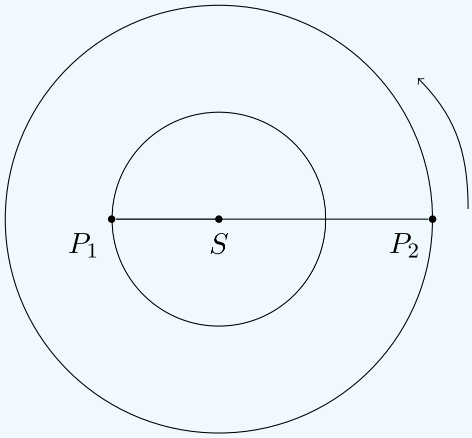
1.3 Zyklische Strukturen in Planetenbewegungen

Für die langfristige Stabilität der Planetenbewegungen sind Konjunktions- und Oppostionsstellungen von Bedeutung:

Visualisation



Konjunktion der Planeten P_1, P_2: Von P_1, P_2 geht gemeinsam größt mögliche gravitative Kraft aus.



Opposition von P_1, P_2: Die gravitativen Kräfte von P_1, P_2 gleichen sich einigermaßen aus.

Saturn und Jupiter sind mit Abstand die beiden massereichsten Planeten des Sonnensystems. Stehen Jupiter und Saturn in Konjunktion, so vollzieht sich eine Ausgleichsbewegung, bei der die Sonne um ihren eigenen Durchmesser aus dem Baryzentrum wandert. Insgesamt sind die Konjunktionstermine aller Planeten so verteilt, dass das Sonnensystem stabil bleibt.

Betrachte exemplarisch Venus und Erde. Es gilt:

$$8 \text{ Erdjahre} \approx 13 \text{ Venusjahre}.$$

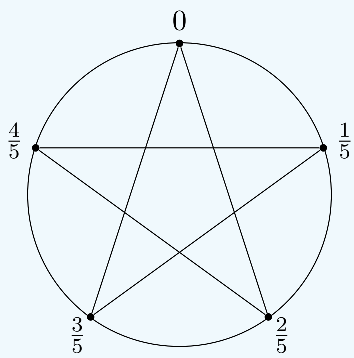
Genauer: $8 : 13{,}0042$. Abweichung von $8 : 13$ um ca. 0.032. Nehme zunächst an, dass das Verhältnis von $8 : 13$ exakt ist. In 8 Jahren überholt die Venus die Erde fünfmal.

$\implies$ In 8 Jahren finden 5 Konjunktionen zwischen Venus und Erde statt.

$\implies$ Findet zum Zeitpunkt $t = 0$ eine Konjunktion statt, so findet nach $\frac{8}{5} = 1\frac{3}{5}$ Jahren die nächste Konjunktion statt. In $\frac{8}{5}$ Erdjahren finden $\frac{13}{5} = 2\frac{3}{5}$ Venusjahre statt. Beide Planeten befinden sich demzufolge bei $\frac{3}{5}$ ihrer Umlaufbahn:

Visualisation

Positionen der Erde zu Konjunktionsterminen mit Venus (chronologisch verbunden).



$$0 \xrightarrow{+\frac{8}{5} \pmod 1} \frac{3}{5} \xrightarrow{+\frac{8}{5} \pmod 1} \frac{1}{5} \xrightarrow{+\frac{8}{5} \pmod 1} \frac{4}{5} \xrightarrow{+\frac{8}{5} \pmod 1} \frac{2}{5} \xrightarrow{+\frac{8}{5} \pmod 1} 0$$

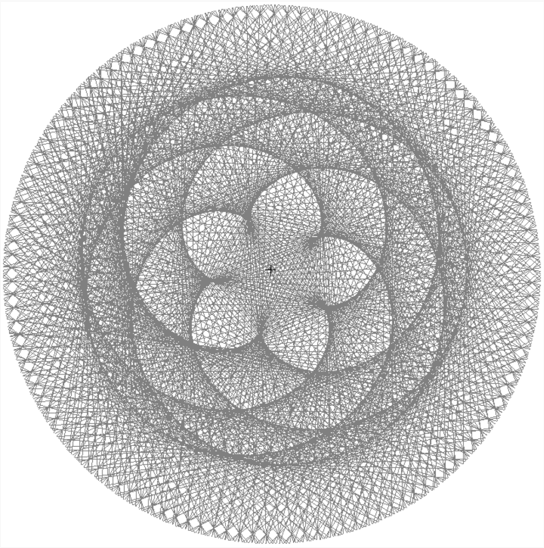
Man kann bei allen Zahlen den Nenner weglassen und stattdessen mod 5 rechnen. Es ist außerdem $8 \equiv 3 \pmod 5$.

$$0 \xrightarrow{+3 \pmod 5} 3 \xrightarrow{+3 \pmod 5} 1 \xrightarrow{+3 \pmod 5} 4 \xrightarrow{+3 \pmod 5} 2 \xrightarrow{+3 \pmod 5} 0$$

Die Abfolge der Konjunktion wird demnach durch die zyklische Gruppe $\langle 3 \rangle$ beschrieben, $3 \in (\mathbb{Z}_5, \oplus)$, vgl. Mathe 2.

Bemerkung

Das Pentagramm entstünde bei einem exakten Verhältnis von 8 : 13. Tatsächliche Figur:



1.4 Größte/kleinste gemeinsame Teiler

Seien $a_1, ..., a_r \in \mathbb{Z}$.

1. Ist mindestens ein $a_i \neq 0$, so ist der größte gemeinsame Teiler die größte natürliche Zahl, die alle a_i teilt. Schreibweise: $\text{ggT}(a_1, ..., a_r)$
2. Sind alle $a_i \neq 0$, so ist das kleinste gemeinsame Vielfache die kleinste natürliche Zahl, die von allen a_i geteilt wird. Schreibweise: $\text{kgV}(a_1, ..., a_r)$.
3. Ist $\text{ggT}(a_1, ..., a_r) = 1$, so heißen $a_1, ..., a_r$ teilerfremd. Ist $\text{ggT}(a_i, a_j) = 1 \ \forall i \neq j$, so heißen $a_1, ..., a_r$ paarweise teilerfremd.

Beispiel

Im 3. Punkt stärkere Bedingung: $\text{ggT}(3, 7, 9) = 1$, aber $\text{ggT}(3, 9) = 3$

1.5 Euklidischer Algorithmus zur Berechnung des ggT

1.5.1 Herleitung

Beweis

Zu zeigen: Seien $q, v, w \in \mathbb{Z},\ v \neq 0$. Dann:

$$t \mid v \wedge t \mid w \iff t \mid v \wedge t \mid qv + w$$

Beweis. Der vorigen Aussage.

$$\begin{aligned}
\Longrightarrow: \quad & t \mid v \wedge t \mid w \implies \exists k_1, k_2 \in \mathbb{Z} : v = tk_1,\ w = k_2 t \\
& \implies qv + w = qtk1 + tk_2 = t(\underbrace{qk_1 + k_2}_{\in\mathbb{Z}}) \implies t \mid qv + w \\
\Longleftarrow: \quad & t \mid v \wedge t \mid qv + w \implies \exists k_1, k_2 \in \mathbb{Z} : v = k_1 t,\ qv + w = k_2 t \\
& \implies w = k_2 t - qv = t(\underbrace{k_2 - qk_1}_{\in\mathbb{Z}}) \implies t \mid w
\end{aligned}$$

Q.E.D.

Es folgt $\mathrm{ggT}(v, w) = \mathrm{ggT}(v, q + v + w)$. damit lässt sich der euklidische Algorithmus formulieren. Seien $a, b \in \mathbb{Z},\ b \neq 0,\ b \nmid a$. **Frage**: Wie findet man $\mathrm{ggT}(a, b)$?

Idee: Verwende Division mit Rest und

$$\begin{aligned}
a_0 &= a, a_1 = b \\
a_0 &= q_1 a_1 + a_2 && |a_2| < |a_1| \\
a_1 &= q_2 a_2 + a_3 && |a_3| < |a_2| \\
&\vdots \\
a_{n-1} &= q_n a_n + \underbrace{0}_{\text{erstmals Rest } 0} && |a_n| < |a_{n-1}|
\end{aligned}$$

Es folgt:

$$\begin{aligned}
\mathrm{ggT}(a, b) &= \mathrm{ggT}(a_1, a_0) = \mathrm{ggT}(a_1, q_1 a_1 + a_2) \\
&= \mathrm{ggT}(a_1, a_2) = \mathrm{ggT}(a_2, \underbrace{q_2 a_2 + a_3}_{=a_1}) \\
&= \mathrm{ggT}(a_2, a_3) \\
&\vdots \\
&= \mathrm{ggT}(\underbrace{a_{n-1}}_{q_n a_n}, a_n) = a_n
\end{aligned}$$

1.6 Euklidischer Algorithmus

```
Eingabe: a,b ∈ ℤ, nicht beide =0
if b=0 then y=|a| endif
if b|a then y=|b| endif
if b≠0 and b∤a then
  x = a, y = b
  while (x mod y)≠0 do
    r=(x mod y), x=y, y=r
  endwhile
endif
Ausgabe: y (=ggT(a,b))
```

Beispiel

EA mit $a = 48$ und $b = -30$:

x	y	r
48	-30	18
-30	18	6
18	**6**	0

Damit ist der größte gemeinsame Teiler mit 6 gefunden.

1.7 Satz von Méziriac

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

Beweis

Beweis.

$$
\begin{aligned}
b = 0 :&\quad \text{ggT}(a,b) = |a| = sa + 0b, \quad s = \text{sgn}(a) \\
b \neq 0,\ b \mid a :&\quad \text{ggT}(a,b) = |b| = 0a + tb, \quad t = \text{sgn}(b) \\
b \neq 0,\ b \nmid a :&\quad a_0 := a, a_1 := b \implies \text{EA} \implies \text{ggT}(a,b) = a_n, \quad n \geq 2 \\
&\quad \text{Zeige mit vollst. Induktion: } \exists s_j, t_j \in \mathbb{Z} : a_j = s_j a_0 + t_j a_1 \quad \forall j = 0, .., n
\end{aligned}
$$

Q.E.D.

1.8 Erweiterter Euklidischer Algorithmus (EEA)

Dient der Berechnung von s, t im *Satz des Méziriac*.

```
Eingabe: a,b ∈ ℤ, nicht beide =0
if b=0 then y=|a|, t=0
  if a>0 then s=1 else s=-1 endif
endif
if b|a then y=|b|, s=0
  if b>0 then t=1 else t=-1 endif
endif
if b≠0 and b∤a then x=a, y=b
  s1=1, s2=0
  t1=0, t2=1
  while (x mod y)≠0 do
    q=(x div y), r=(x mod y)
    s=(s1-qs2), t=t1-qt2
    s1=s2, s2=s
    t1=t2, t2=t
    x=y, y=r
  endwhile
endif
Ausgabe y (=ggT(a,b)), s,t (y=sa+tb)
```

Beispiel

$a = 48$, $b = -30$

x	y	s_1	s_2	s	t_1	t_2	t	q	r
48	-30	1	0	/	0	1	/	/	/
-30	18	0	1	1	1	1	1	-1	18
18	6	/	/	2	/	/	3	-2	6

$\implies \operatorname{ggT}(48, -30) = 6 = 2 \cdot 48 + 4 \cdot (-30)$

Bemerkung

Darstellung des ggT nicht eindeutig, z.B. ist auch $\operatorname{ggT}(48, -38) = 6 = 7 \cdot 48 + 11 \cdot (-30)$

1.9 Die Gruppe $(\mathbb{Z}_n^*, \odot)$

Ist $(\mathbb{Z}_n^*, \odot)$ eine Gruppe? $(\mathbb{Z}_n, \odot)$

- ist abgeschlossen: $a, b \in \mathbb{Z}_n \implies a \odot b \in \mathbb{Z}_n$
- ist assoziativ
- besitzt Neutralelement: $a \odot 1 = 1 \odot a = a \quad \forall a \in \mathbb{Z}_n$
- enthält im Allgemeinen keine Inversen, z.B. hat 0 keine Inverse

Welche Elemente haben Inversen?

Beispiel

$5 \in \mathbb{Z}_{10}$ hat keine Inverse, da $t \cdot x \pmod{10} = \begin{cases} 0 & x \text{ gerade} \\ 5 & x \text{ ungerade} \end{cases}$, d.h. $5 \odot x \neq 1 \quad \forall x \in \mathbb{Z}_{10}$

Dagegen hat $3 \in \mathbb{Z}_{10}$ Inverse $x = 7$.

Aus Mathe 2: $a \in \mathbb{Z}_n$ invertierbar $\iff \operatorname{ggT}(a, n) = 1$

Es ist $Z_n^* = \{a \in \mathbb{Z}_n \mid \operatorname{ggT}(a, n) = 1\}$ die Menge aller invertierbaren Elemente in $\mathbb{Z}_n$ und ist bezüglich $\odot$ eine Gruppe. $\varphi(n) = |\mathbb{Z}_n^*|$ heißt Eulersche Phi-Funktion.

Berechnung von $a^{-1} \in \mathbb{Z}_n$: Wegen EEA gibt es $s, t \in \mathbb{Z} : sa + tn = 1 \implies sa \equiv 1 \pmod{n} \implies a^{-1} \equiv s \pmod{n}$

Beispiel

Inverse von $5 \in \mathbb{Z}_{21}$ durch EEA: $(-4) \cdot 5 + 1 \cdot 21 = 1$
$\implies 5^{-1} \equiv -4 \equiv 17 \pmod{21}$

Falls man $s, t \in \mathbb{Z}$ nicht unmittelbar sieht: EEA.

1.9.1 Korollar

$a, b \in \mathbb{Z}$, nicht beide $= 0$, $\ c \in \mathbb{Z}$

1. $\operatorname{ggT}(a, b) = 1 \iff \exists s, t \in \mathbb{Z} : sa + tb = 1$
2. $\operatorname{ggT}(a, b) = 1 \implies$ falls $a \mid bc$, dann $a \mid c$

Beweis

Beweis. In beide Richtungen:

- „ $\implies$ “: Gelte $sa + tb = 1$. Annahme: $\operatorname{ggT}(a, b) > 1$
  $d := \operatorname{ggT}(a, b) \implies d \mid a, \quad d \mid b \implies \exists k_1, k_2 \in \mathbb{Z} : a = k_1 d,\ b = k_2 d \implies sa + tb = d(sk_1 + tk_2) \neq 1$, da $d > 1$ ↯, also $d = 1$
- „ $\impliedby$ “: $\exists s, t \in \mathbb{Z} : 1 = sa + tb \implies c = sac + tbc$, also $a \mid a$ und $a \mid bc$ $\implies a \mid (\underbrace{sac + tbc}_{=c})$

Q.E.D.

1.10 Primzahlen

$p \in \mathbb{N},\ p \geq 2$ heißt Primzahl, wenn 1 und p die einzigen gemeinsamen Teiler von p sind, d.h. $\operatorname{ggT}(k, p) = 1 \quad \forall k \in \{1, ..., p - 1\}$

1.10.1 Lemma von Euklid

Sei $p \in \mathbb{P},\ a_1, ..., a_k \in \mathbb{Z}$.

$p \mid a_1, ..., a_n \implies \exists j \in \{1, ..., k\} : p \mid a_j$

Gegenbeispiel: 6 keine Primzahl: $6 \mid 3 \cdot 4$, aber $6 \nmid 3 \wedge 6 \nmid 4$

Beweis

Beweis. Durch vollständige Induktion über k:
IA: $k = 1 : p \mid a_1 \implies p \mid a_1$
IV: Lemma gelte für $k - 1$ beliebige, ganzzahlige Faktoren
IS: $k - 1 \to k$: **Zu zeigen:** Lemma gilt für k Faktoren $a_1, ..., a_k$.
Fallunterscheidung:

$$\begin{aligned}
p \mid a_k : \quad &\implies \text{fertig} \\
p \nmid a_k : \quad &\implies \operatorname{ggT}(g, a_k) = 1, \text{ da } p \in \mathbb{P} \\
&\implies p \mid a_1, ..., a_{k-1} \\
&\implies \exists j \in \{1, ..., k - 1\} : p \mid a_j
\end{aligned}$$

Q.E.D.

1.11 Fundamentalsatz der elementaren Zahlentheorie

Zu jeder natürlichen Zahl $n \geq 2$ gibt es endlich viele paarweise verschiedene Primzahlen $p_1, ..., p_k$ und natürliche Zahlen $e_1, ..., e_k$ mit

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

Die p_i heißen Primfaktoren von n. Die Darstellung von n als Produkt von Primzahlen ist bis auf die Reihenfolge eindeutig.

Beweis

Beweis.

- **Existenz:** Durch vollständige Induktion.

IA: $n = 2 \in \mathbb{P}$
IV: Aussage gelte für $2, ..., n$
IS: $2, 3, ..., n \to n+1$: **Zu zeigen:** Aussage gilt dann auch für $n+1$
Ist $n+1 \in \mathbb{P} \implies$ fertig.
Ist $n+1 \notin \mathbb{P} \implies n+1 = a \cdot b, \quad a, b \in \{2, ..., n\}$
$\implies a, b$ Produkte von Primfaktoren

- **Eindeutigkeit:** Sei $n \geq 2$.
  (i) Falls $n \in \mathbb{P}$: Behauptung erfüllt.
  (ii) Falls $n \notin \mathbb{P}$: sei n die kleinste natürliche Zahl mit 2 verschiedenen Zerlegungen
  $n = p_1^{e_1} \cdot ... \cdot p_k^{e_k} = q_1^{f_1} \cdot ... \cdot q_e^{f_e}$
  Zu zeigen: $\{p_1, ..., p_k\} \cap \{q_1, ..., q_e\} = \emptyset$
  Angenommen nicht: O.B.d.A. $p_1 = q_1$
  $\frac{n}{p_1} < n$ und $\frac{n}{p_1}$ hat 2 verschiedene Zerlegungen $\lightning$
  (iii) $p_1 \mid q_1^{f_1}, ..., q_e^{f_e} \implies \exists j \in \{1, ..., k\} : p_i \mid q_j \implies p_1 = q_j$, da $p_1 \neq 1 \wedge q_j \in \mathbb{P} \lightning$

Q.E.D.

1.12 Euklid

Es gibt unendlich viele Primzahlen.

Beweis

Beweis. Angenommen es gibt nur endlich viele Primzahlen $p_1, ..., p_n$. Sei $a = p_1 \cdot ... \cdot p_n + 1$
$\implies \exists q \in \mathbb{P} : q \mid a$
$\implies q = p_i$ für ein $i \in \{1, ..., n\}$
$\implies q \mid \underbrace{(a - p_1, ..., p_n)}_{1} \lightning$ (da $q > 1$) Q.E.D.

1.13 Chinesischer Restsatz

Gegeben: $m_1, ..., m_n \in \mathbb{N}, \quad a \in \mathbb{Z}$ und $M = m_1 \cdot ... \cdot m_n$. Dann: $\underbrace{(a \pmod{M})}_{=r} \pmod{m_i} = a \pmod{m_i} \quad \forall i$

Beweis

Beweis. Zu zeigen: $r \equiv a \pmod{m_i}$.
Division mit Rest: $\exists q \in \mathbb{Z} : a = qM + r = q \underbrace{\left(\frac{M}{m_i}\right)}_{\in \mathbb{Z}} m_i + r$

$\implies a \equiv r \pmod{m_i}$ Q.E.D.

Gegeben:

- $m_1, ..., m_n \in \mathbb{N}$ paarweise teilerfremd,
- $M = m_1 \cdot ... \cdot m_n$
- $a_1, ..., a_n \in \mathbb{Z}$

Dann existiert $0 \leq x < M$ mit *simultaner Kongruenz*

$$x \equiv \begin{cases} a_1 \pmod{m_1} \\ \vdots \\ a_n \pmod{m_n} \end{cases}$$

Beweis

Beweis. Setze $M_i := \frac{M}{m_i} \in \mathbb{Z} \implies \mathrm{ggT}(m_i, M_i) = 1 \quad \forall i = 1, ..., n$
$\implies \exists s_i, t_i \in \mathbb{Z} : s_i \cdot m_i + t_i M_i = 1$
Setze $e_i := t_i M_i \implies e_i \equiv \begin{cases} 0 \pmod{m_j} & j \neq i \\ 1 \pmod{m_i} \end{cases}$
$\implies x = (\sum_{i=1}^n a_i e_i) \pmod M$ Lösung, da:

$$\begin{aligned} x \pmod{m_j} &= \left(\left(\sum_{i=1}^n a_i e_i\right) \pmod M\right) \pmod{m_j} \\ &= \left(\sum_{i=1}^n a_i e_i\right) \pmod{m_j} \\ &= a_j \pmod{m_j} \end{aligned}$$

Q.E.D.

Beispiel

1. Finde $0 \leq x < M$ mit $m_1 = 3,\ m_2 = 4,\ m_3 = 5 \implies M = 60$. $M_1 = \frac{M}{m_1} = 20,\ M_2 = \frac{60}{4} = 15,\ M_3 = \frac{60}{5} = 12$
   EEA:

   $$\begin{aligned} 7 \cdot 3 - 20 &= 1 \\ 4 \cdot 4 - 15 &= 1 \\ 5 \cdot 5 - 2 \cdot 12 &= 1 \end{aligned}$$

   $x = (2 \cdot (-20) + 3 \cdot (-15) + 2 \cdot (-24)) \pmod{60} = 47$
2. Was ist $2^{1000} \pmod{1155}$? Primfaktorzerlegung: $1155 = 3 \cdot 5 \cdot 7 \cdot 11$
   1. Berechne $2^{1000} \pmod{3, 5, 7, 11}$:
      - $2^{1000} \pmod 3 = (-1)^{1000} \pmod 3 = 1$
      - $2^{1000} \pmod 5 = 4^{500} \pmod 5 = (-1)^{500} \pmod 5 = 1$
      - $2^{1000} \pmod 7 = (8^{333} \cdot 2) \pmod 7 = 2$
      - $2^{1000} \pmod{11} = (2^5)^{200} \pmod{11} = 1$
   2. Suche $0 \leq x < 1155$ mit

      $$x \equiv \begin{cases} 1 \pmod 3 \\ 1 \pmod 5 \\ 2 \pmod 7 \\ 1 \pmod{11} \end{cases}$$

      Chinesischer Restsatz liefert $x = 331$

Die Lösung x aus vorigem Beispiel ist eindeutig.

Beweis

Beweis. Betrachte die Abbildung $\psi : \mathbb{Z}_M \to (\mathbb{Z}_{m_1} \times ... \times \mathbb{Z}_{m_n})$, $x \mapsto (x \pmod{m_1}, ..., x \pmod{m_n})$. Der chinesische Restsatz besagt: Für jedes n-Tupel $(a_1, ..., a_n) \in \mathbb{Z}_{m_1} \times ... \times \mathbb{Z}_{m_n}$ gibt es ein $x \in \mathbb{Z}_M$ mit $\psi(x) = (a_1, ..., a_n)$.
$\implies$ ψ ist surjektiv.
Zu zeigen: ψ bijektiv, d.h. es gibt nur genau ein x, mit $\psi(x) = (a_1, , , ., a_n), \quad x \in \mathbb{Z}_M$.
Da $M = m_1 \cdot ... \cdot m_n$ ist $|\mathbb{Z}_M| = |\mathbb{Z}_{m_1} \times ... \times \mathbb{Z}_{m_n}|$
$\implies$ Jedes Element von $\mathbb{Z}_{m_1} \times ... \times \mathbb{Z}_{m_n}$ wird nur von genau einem x getroffen
$\implies$ ψ bijektiv Q.E.D.

Beispiel

Aus *Meister Suns Rechenhandbuch* von Sun Zi Suan Jing:
“Es gibt eine unbekannte Zahl von Dingen. Wenn mit drei gezählt wird, haben sie einen Rest von zwei; wird mit fünf gezählt, einen Rest von drei, mit sieben einen Rest von zwei. Rate die Zahl.”
Formal: Suche x mit

$$x \equiv \begin{cases} 2 \pmod 3 \\ 3 \pmod 5 \\ 2 \pmod 7 \end{cases}$$

TU DU!

1.14 Strukturgleichheit von Ringen

Seien $(R, +, \cdot)$ und $(R', \oplus, \odot)$ Ringe.

1. $\psi : R \to R'$ heißt (Ring-)Homomorphismus, falls $\forall x, y \in R$ gilt

$$\psi(x + y) = \psi(x) \oplus \psi(y)$$

$$\psi(x \cdot y) = \psi(x) \odot \psi(y)$$

2. Wenn ψ bijektiv, heißt ψ (Ring-)Isomorphismus. In diesem Fall heißen R, R' isomorph (d.h. sie sind strukturgleich). Man schreibt $R \cong R'$.

Beispiel

1. Boolesche Algebra:

$$(\{f, w\}, \texttt{XOR}, 1) \cong (0, 1, \oplus, \odot)$$

$\psi(f) = 0, \psi(w) = 1$. ψ Isomorphismus, falls Verknüpfungstafeln übereinstimmen

XOR	f	w
f	f	w
w	w	f

bzw.

$\oplus$	0	1
0	0	1
1	1	0

2. Homomorphismus:

$$\psi(\mathbb{Z}, +, \cdot) \to (\mathbb{Z}_n, \oplus, \odot), \quad x \mapsto x \pmod n$$

Bemerkung

Seien $(R, +, \cdot)$ und $(R', \oplus, \odot)$ Ringe und $\psi : R \to R'$ ein Isomorphismus.

1. $\psi(1)$ ist Eins in R': $\forall a \in R$, d.h. $\psi(a) \in R'$ gilt:

$$\psi(1) \odot \psi(a) = \psi(1 \cdot a) = \psi(a) = \psi(a \cdot 1) = \psi(a) \odot \psi(1).$$

2. $a \in R$ invertierbar $\iff$ $\psi(a) \in R'$ invertierbar.

$$\begin{aligned} a \in R \text{ invertierbar} &\iff \exists b \in R : ab = 1 \\ &\iff \psi(ab) = \psi(1) \\ &\iff \psi(a) \odot \psi(b) = \psi(1) \\ &\iff \psi(a) \text{ invertierbar} \end{aligned}$$

1.15 Berechnung der Eulerschen φ-Funktion

Über chinesischen Restsatz.

$M = m_1 \cdot ... \cdot m_n, \quad m_i \in \mathbb{N}$ paarweise teilerfremd.

$\implies \varphi(M) = \varphi(m_1) \cdot ... \cdot \varphi(m_n)$

Insbesondere durch Primfaktorzerlegung: $M = p_1^{a_1} \cdot ... \cdot p_k^{a_k}$

$\implies \varphi(M) = (p_1 - 1)p_1^{a_1 - 1} \cdot ... \cdot (p_k - 1)p_k^{a_k - 1}$

Beweis

Beweis. Es gilt $Z_M \cong Z_{m_1} \times ... \times Z_{m_n}$ mittels ψ aus voriger Bemerkung. Dann gilt

$$\begin{aligned} x \in \mathbb{Z}_M \text{ invertierbar} &\iff \psi(x) = (x \bmod m_1, ..., x \bmod m_n) \text{ invertierbar} \\ &\iff x \bmod m_i \text{ invertierbar}, \quad \forall i \in \{1, ..., n\} \end{aligned}$$

$\implies \varphi(M) = \varphi(m_1) \cdot ... \cdot \varphi(m_n)$
Angenommen $M = p_1^{a_1} \cdot ... \cdot p_k^{a_k}$ ist Primfaktorzerlegung. Es genügt zu zeigen, dass mit $p \in \mathbb{P}$ gilt $\varphi(p^a) = (p-1)p^{a-1} = p^a - p^{a-1}$. $\mathbb{Z}_{p^a}$ enthält p^a Elemente. Dabei sind die Elemente kp für $0 \le k \le p^{a-1} - 1$ nicht teilerfremd zu p^a. Davon gibt es p^{a-1} Stück. Q.E.D.

Beispiel

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

1.16 Euklidischer Algorithmus in Polynomringen über einem Körper K

1.16.1 ggT und kgV in $K[x]$

1. $f, g \in K[x], \ f \neq 0, \ f \mid g \iff \exists q \in K[x] : g = qf$
   Gradformel $\implies$ $\text{grad}(f) \le \text{grad}(g)$, falls $g \neq 0$
2. $f = \sum_{i=1}^n a_i x^i \in K[x]$ heißt *normiert*, falls der Leitkoeffizient $a_n = 1$.
3. $g, h \in K[x]$, beide $= 0$, $f = \text{ggT}(g, h)$ falls f *normiertes* Polynom von maximalem Grad, das g und h teilt.
4. $g, h \in K[x] \setminus \{0\}$, $f = \text{kgV}(g, h)$, falls f *normiertes* Polynom von minimalem Grad, das von g und h geteilt wird.

Bemerkung

Sei $f = \sum_{i=1}^{n} a_i x^i$, $a_n \neq 0$. Dann ist $a_n^{-1} \cdot f$ normiert, z.B. $f = 3x^2 + x + 7$
- $f \in \mathbb{R}[x] : \frac{1}{3} f = x^2 + \frac{x}{3} + \frac{7}{3}$
- $f \in \mathbb{Z}_{11}[x] : 4f = x^2 + 4x + 6$

In $K[x]$ kann der ggT zweier Polynome mit einer Rekursionsvorschrift analog zu ggT in $\mathbb{Z}$ berechnet werden. Man verwendet dazu Polynomdivision mit Rest (siehe Mathe 2).

1.16.2 Satz von Bézout

Analog zum Satz von Méziriac gilt: $g, h \in K[x]$, nicht beide $= 0 \implies \exists s, t \in K[x]$: $\text{ggT}(g, h) = sg + th$.

1.16.3 EEA in K[x]

Wie in $(\mathbb{Z}, +, \cdot)$ kann auch für $(K[x], +, \cdot)$ der EEA formuliert werden, um s, t im Satz des Bézout zu berechnen. Damit kann jener Satz auch für $K[x]$ bewiesen werden.

Beispiel

Seien $g = x^4 + x^3 + 2x^2 + 1$ und $k = x^3 + 2x^2 + 2$ in $\mathbb{Z}_3[x]$

x	y	s_1	s_2	s	t_1	t_2	t	q	r
g	h	1	0	/	0	1	/	/	/
h	$x^2 + x$	0	1	1	1	$2x + 2$	$2x + 1$	$x + 2$	$x^2 + x$
$x^2 + x$	$2x + 2$	/	/	$2x + 2$	/	/	x^2	$x + 1$	$2x + 2$

Normieren: $\text{ggT}(g, h) = 2^{-1}(2x + 2) = x + 1$

$$s = 2^{-1}(2x + 2) = x + 1$$
$$t = 2^{-1}(x^2) = 2x^2$$

Bemerkung

Sowohl in $\mathbb{Z}$ als auch in $K[x]$ müssen eigentlich Existenz und Eindeutigkeit der ggT und kgV gezeigt werden. Beweise trivial offensichtlich. W.T.F.

1.17 Primelemente in $K[x]$

Primelemente sind irreduzible Polynome.

$p \in K[x]$ mit grad ≥ 1 irreduzibel $\iff$ $f, g \in K[x]$ mit $p = f \cdot g \implies \text{grad}(f) = 0 \vee \text{grad}(g) = 0$

Beispiel

1. $ax + b,\ a \neq 0$ irreduzibel in $K[x]$
2. $x^2 - 2 \in \mathbb{Q}[x]$ irreduzibel, aber in $\mathbb{R}[x]$ reduzibel
3. $x^2 + 1 \in \mathbb{R}[x]$ irreduzibel, aber in $\mathbb{Z}_5[x]$ reduzibel

1.17.1 Lemma von Euklid in $K[x]$

$f \in K[x]$, $\text{grad}(f) \geq 1$. Dann sind folgende Aussagen äquivalent:

1. f irreduzibel
2. $g, h \in K[x]$, $f \mid g \cdot h \implies f \mid g \vee f \mid h$

Beweis

Beweis.

- (1) $\implies$ (2): Analog zu Lemma von Euklid in $\mathbb{Z}$.
- (2) $\implies$ (1): Angenommen es existiert Polynom g mit $g \mid f$.
  $\implies \exists g, h \in K[x] : f = gh$. Wir zeigen: $\text{grad}(h) = 0$ (d.h. f irreduzibel). $f = gh \implies f \mid g \vee f \mid h$. O.B.d.A. $f \mid g$. $\text{grad}(f) \leq \text{grad}(g) \leq \text{grad}(g) + \text{grad}(h) = \text{grad}(g \cdot h) = \text{grad}(f)$
  $\implies \text{grad}(h) = 0, \ \text{grad}(f) = \text{grad}(g)$

Q.E.D.

Bemerkung

Für $\mathbb{Z}$ gilt (2) $\implies$ (1) ebenfalls. Anstatt der Gradformel im vorigen Beweis schreibt man für $f, g, h \in \mathbb{Z}, \ f \geq 2 : 2 \leq f \leq |g| \leq gh = f \implies f = |g| \wedge |h| = 1 \implies f \in \mathbb{P}$.

1.18 Primfaktorzerlegung in $K[x]$

Sei $f \in K[x]$ mit Leitkoeffizient $a_n \neq 0, n \geq 1$. Dann: Es gibt eindeutige irreduzible Polynome $p_1, ..., p_e \in K[x]$ und $m_1, ..., m_l \in \mathbb{N}$ mit $f = a_n p_1^{m_1} \cdot ... \cdot p_e^{m_e}$.

1.19 Korollar

$f \in K[x]$, $\text{grad}(f) = n \geq 1$. Dann:

1. f hat max. n Nullstellen $a_1, ..., a_k \in K$.
2. $f = (x - a_1) \cdot ... \cdot (x - a_k) \cdot \bar{f}$ mit $\text{grad}(\bar{f}) = \text{grad}(f - k)$.

Beweis

Beweis.

- $n = 1$: $f = ax + b$ hat Nullstelle $-a^{-1}b$.
- $n > 1$: Hat f keine Nullstelle $\implies$ fertig.
  Sonst: Sei $a \in K$ Nullstelle $\implies f = (x - a) \cdot g, \ \text{grad}(g) = n - 1$.
  Sei $b \in K$ weitere Nullstelle, $b \neq a$: $\implies (x - b) \mid (x - a) \cdot g \implies (x - b) \mid g$, da $(x - b)$ irreduzibel.
  $\implies b$ Nullstelle von g. Per Induktion hat g maximal $n - 1$ Nullstellen.

Q.E.D.

Bemerkung

$(\mathbb{Z}_n, \oplus, \odot)$ Körper $\iff n \in \mathbb{P}$. Analog in $K[x]$: Sei $f \in K[x], \ \text{grad}(f) = n$. Dann ist $(K[x]_n, +, \odot_f)$ mit

- $K[x]_n = \{g \in K[x] \mid \text{grad}(g) < n\}$

- $g \odot_f h := g \cdot h \pmod{f}$

ein kommutativer Ring mit Eins.
Invertierbare Elemente bezüglich $\odot_f$: $K[x]_n^* := \{g \in K[x]_n \mid \mathrm{ggT}(g,f) = 1\}$ (Beweis wie für $\mathbb{Z}_n^*$). Es folgt $\exists s,t \in K[x] : sg + tf = 1 \implies s \cdot g \equiv 1 \pmod{f}$ und $g^{-1} \equiv s \pmod{f}$.
Damit erhält man $(K[x]_n, +, \odot_f)$ Körper $\iff f$ irreduzibel.
Für $K = \mathbb{Z}_p$ lässt sich zeigen:

1. $\mathbb{Z}_p[x]_n$ Körper der Ordnung $p^n \iff f$ irreduzibel, $p \in \mathbb{P}$
2. Jeder endliche Körper hat Primzahlpotenzordnung und ist durch seine Ordnung bis auf Isomorphie eindeutig festgelegt.

1.20 Anwendungsbeispiel aus der Kryptologie

Die ältesten Verfahren zur Verschlüsselung von Nachrichten sind symmetrisch, d.h. Sender und Empfänger verwenden denselben Schlüssel zur Ver- und Entschlüsselung einer Nachricht (z.B. Cäsar-Chiffre, ENIGMA, ...). Problem: Sender und Empfänger müssen Schlüssel auf sicherem Weg austauschen.

Zur Lösung des Problems wurden asymmetrische Verfahren entwickelt, bei denen kein Schlüssel getauscht werden muss (z.B. public-key-Verfahren, Diffie-Hellman, ...):

- Bob will Nachricht empfangen. Er erzeugt 2 Schlüssel:
  - public key, wird veröffentlicht
  - private key, geheim
- Alice verschlüsselt Nachricht an Bob mit public key
- Bob entschlüsselt mit private key

Eine der wichtigsten Realisationen: RSA-Verfahren. Verwende dazu Einwegfunktionen, d.h. Funktionen, die praktisch unmöglich umzukehren sind. Kanditaten dafür sind Potenzfunktionen in $\mathbb{Z}_n$, wobei $n = pq$, $p, q \in \mathbb{P}$: $x^e \pmod{n}$.

- Es ist praktisch unmöglich, n zu faktorisieren, wenn n sehr groß: Angenommen n ist 2000-Bit-Zahl und angenommen pro Sekunde kann man bei 10^9 Zahlen testen, ob sie teilerfremd zu n sind. Dazu bräuchte man
$$\frac{2^{1000}}{10^9}s = \frac{(2^{10})^{100}s}{(10^3)^3} \approx 10^{291}s \approx 3 \cdot 10^{285} \text{ Jahre.}$$
Faktorisierung von $n \approx 2^{1000}$ mit schnellsten Rechnern der Welt derzeit mehr als 10^{100} Jahre.
- Wurzelziehen in $\mathbb{Z}_n$ schwierig. Z.B. $x^3 \pmod{7} = 6 \implies x = 3$.
- Man kann zeigen: Wählt man e teilerfremd zu $\varphi(n) = (p-1)(q-1)$, so ist $x^e \pmod{n}$ bijektiv.
- Es gibt eine geheime Zahl d, mit der die Operation umgekehrt werden kann. Eine solche Einwegfaktorisierung heißt Trapdoorfunktion.

1.21 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

1.21.1 Korrektheit des Verfahrens:

Beweis

Zu zeigen: $c^d \pmod n = m$. Daraus folgt insbesondere, dass die Faktorisierung $m^e \pmod n$ bijektiv ist und Nachrichten korrekt entschlüsselt werden können.

$$c^d \equiv (m^e)^d \equiv m^{ed} \equiv m^{k\varphi(n)+1} \equiv m(m^{\varphi(n)})^k \pmod n$$

Beweis. Durch Fallunterscheidung:
1. Fall: $m = 0 \iff c = 0$, d.h. 0 wird durch 0 verschlüsselt.
2. Fall: $\mathrm{ggT}(m, n) = 1 \implies m^{\varphi(n)} \equiv 1 \pmod n \implies c^d \equiv m \pmod n$
3. Fall $p \mid m$ und $m \neq 0 \implies m = ap,\ a \in \{1, ..., q-1\} \implies \mathrm{ggT}(q, m^j) = 1 \forall j \in \mathbb{N}$, insbesondere für $j = \varphi(n) \implies m \pmod p = 0 \wedge m^{\varphi(n)} \pmod q = 1$. Chinesischer Restsatz: $m_1 = p, M_1 = q, m_2 = q, M_2 = p$. EEA: $\exists s, t \in \mathbb{Z} : sp + tq = 1 \implies c^d \equiv tqm + spm \equiv (tq + sp)m \pmod n$
4. Fall: $q \mid m$ und $m \neq 0$ analog zu Fall 3.

Q.E.D.

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 $c = 2$: $m = c^d \pmod n = 2^7 \pmod{33} = 2^5 \cdot 2^2 \pmod{33} = -4 \pmod{33} = 29$.

2 Funktionen und Stetigkeit im $\mathbb{R}^n$

2.1 Wiederholung

- Standardskalarprodukt auf $\mathbb{R}^n$:

$$x = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix},\ y = \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}$$

$$\implies (x|y) = x_1 y_1 + ... + x_n y_n$$

- Winkelberechnung: $\cos(\alpha) = \frac{(x|y)}{\|x\| \cdot \|y\|}$

- Längenberechnung: $\|x\| = \sqrt{(x|x)} = \sqrt{x_1^2 + ... + x_n^2}$
- Abstand: $d(x, y) = \|x - y\|$
- Norm: $\|\cdot\| : \mathbb{R}^n \to \mathbb{R}$

2.2 Konvergenz von Folgen

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

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

Bemerkung

$$x_k = \begin{pmatrix} x_1^{(k)} \\ \vdots \\ x_n^{(k)} \end{pmatrix} \to a \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix}$$

$$\iff x_i^{(k)} \to a_i \quad \forall i \in \{1, ..., n\}$$

Die Rechenregeln für Folgen in $\mathbb{R}$ gelten analog im $\mathbb{R}^n$.

Beispiel

- $\begin{pmatrix} x_k \\ y_k \end{pmatrix} = \frac{1}{\sqrt{k+1}} \begin{pmatrix} \cos(\frac{k\pi}{4}) \\ \sin(\frac{k\pi}{4}) \end{pmatrix}$
  $\left\| \begin{pmatrix} x_k \\ y_k \end{pmatrix} \right\| = \frac{1}{\sqrt{k+1}} \to 0$

2.3 Offene, abgeschlossene, kompakte 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
- $U \subseteq \mathbb{R}^n$ offen $:\iff \forall x \in U \exists \varepsilon > 0 : K_\varepsilon(x) \subseteq U$
- U heißt Umgebung von $x \in D \subseteq \mathbb{R}^n :\iff U$ offen und $x \in U$ und $U \subseteq D$
- $A \subseteq \mathbb{R}^n$ abgeschlossen $:\iff A^C = \mathbb{R}^n \setminus A$ offen

2.4 Rand

$x \in \mathbb{R}^n$ 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 Menge aller Randpunkte von D.

Beispiel

- $K_1\left(\begin{pmatrix} 0 \\ 2 \end{pmatrix}\right) \subseteq \mathbb{R}^2$ offen
- Allgemein: $K_\varepsilon(x_0) \subseteq \mathbb{R}^n$ offen
- $U = \left\{ \begin{pmatrix} x \\ y \end{pmatrix} \in \mathbb{R}^2 \mid x + y > 1 \right\}$ offen

2.5 Charakterisiserung abgeschlossener Mengen

Sei (x_k) Folge in $A \subseteq \mathbb{R}^n$ mit Grenzwert $a \in \mathbb{R}^n$.

A abgeschlossen $\iff a \in A$.

Beweis

Beweis. In beide Richtungen:

- „$\implies$" Sei A abgeschlossen und $x_k \to a \in \mathbb{R}^n$. Angenommen $a \notin A$:

$$\begin{aligned} &\implies a \in A^C \\ &\implies \exists \varepsilon > 0 : K_\varepsilon(a) \subseteq A^C \\ &\implies \exists N \in \mathbb{N} \forall k \geq N : \|x_k - a\| < \varepsilon \\ &\implies x_k \in K_\varepsilon(a) \quad \forall k \geq N \quad \lightning \end{aligned}$$

- „$\impliedby$" Durch Kontraposition: $A \subseteq \mathbb{R}^n$ nicht abgeschlossen $\implies$ Es gibt Folge (x_k) in A mit Grenzwert $a \in A^C$. A nicht abgeschlossen $\implies$ A^C nicht offen.

$$\begin{aligned} &\implies \exists a \in A^C : K_\varepsilon(a) \not\subseteq A^C \quad \forall \varepsilon > 0 \\ &\implies K_\varepsilon(a) \cap A \neq \emptyset \quad \forall \varepsilon > 0 \end{aligned}$$

  Wähle $x_k \in K_{1/k}(a) \cap A, \quad k \in \mathbb{N}$

$$\begin{aligned} &\implies \|x_k - a\| < \frac{1}{k} \\ &\implies x_k \to a \text{ für } k \to \infty \text{ und } x_k \in A \end{aligned}$$

Q.E.D.

Beispiel

$M = \left\{ \begin{pmatrix} x \\ y \end{pmatrix} \in \mathbb{R}^2 \mid 0 \leq x < 1 \right\}$ weder offen noch abgeschlossen:

- nicht offen, da z.B. $K_\varepsilon(0) \cap M^C \neq \emptyset \quad \forall \varepsilon > 0$
- nicht abgeschlossen, da z.B. $x_k = \begin{pmatrix} 1 - 1/k \\ 0 \end{pmatrix} \in M$, aber $x_k \to \begin{pmatrix} 1 \\ 0 \end{pmatrix} \notin M$

2.6 Vereinigung und Schnitt offener Mengen

Sei $\{U_i\}_{i \in \mathbb{N}}$ ein System offener Mengen. Dann:

- $\bigcup_{i=1}^\infty U_i$ offen
- $U_1 \cap U_2$ offen

Beweis

Beweis.

(a) Sei $x \in \bigcup_{i=1}^{\infty} U_i$

$$\begin{aligned}
&\implies \exists i \in \mathbb{N} : x \in U_i \\
&\implies \exists \varepsilon > 0 : K_\varepsilon(x) \subseteq U_i, \text{ da } U_i \text{ offen} \\
&\implies K_\varepsilon(x) \subseteq \bigcup_{i=1}^{\infty} U_i \\
&\implies \bigcup_{i=1}^{\infty} U_i \text{ offen}
\end{aligned}$$

(b) $x \in U_1 \cap U_2$

$$\begin{aligned}
&\implies \exists \varepsilon_1, \varepsilon_2 > 0 : K_{\varepsilon_1}(x) \subseteq U_1,\ K_{\varepsilon_2}(x) \subseteq U_2 \\
&\varepsilon := \min\{\varepsilon_1, \varepsilon_2\} \\
&\implies K_\varepsilon(x) \subseteq K_{\varepsilon_1}(x) \subseteq U_1 \wedge K_\varepsilon(x) \subseteq K_{\varepsilon_2}(x) \subseteq U_2 \\
&\implies K_\varepsilon(x) \subseteq U_1 \cap U_2
\end{aligned}$$

Q.E.D.

2.7 Folgerung

Sei $\{A_i\}_{i=1}^{\infty}$ ein System abgeschlossener Mengen. Dann:

- $\bigcap_{i=1}^{\infty} A_i$ abgeschlossen
- $A_1 \cup A_2$ abgeschlossen

Beweis

Beweis.

- $(\bigcap_{i=1}^{\infty} A_i)^C = \bigcup_{i=1}^{\infty} A_i^C$ offen
- $(A_1 \cup A_2)^C = A_1^C \cap A_2^C$ offen

Q.E.D.

2.8 Abschluss, Inneres

Sei $D \subseteq \mathbb{R}^n$.

- $\bar{D} := D \cup \partial D$ ist abgeschlossen und heißt Abschluss von D.
- $\mathring{D} := D \setminus \partial D$ ist offen und heißt Inneres von D.
- ∂D ist abgeschlossen

Beweis

Beweis.

- Sei (x_k) Folge in $\bar{D}$ mit Grenzwert $a \in \mathbb{R}^n$.
  Annahme: $a \notin \bar{D}$, d.h. insbesondere $a \notin \partial D$
  $\implies \exists \varepsilon > 0 : K_\varepsilon(a) \cap D = \emptyset$ und $K_\varepsilon(a) \cap \partial D = \emptyset$.
  Widerspruch, da $\exists N \in \mathbb{N} \forall n \geq N : x_n \in K\varepsilon(a)$.
- (i) Es ist $\partial D = \partial(D^C)$: $x \in \partial(D^C)$
  $\iff K_\varepsilon(x) \cap D^C \neq \emptyset$ und $K_\varepsilon \cap (D^C)^C \neq \emptyset \quad \forall \varepsilon > 0$

$\iff x \in \partial D$

(ii) $(D^C \cup \partial D)^C = D \cap (\partial D)^C = D \setminus \partial D \implies \mathring{D}$ offen

Q.E.D.

Beispiel

- $\bar{K}_\varepsilon(x_0) = \{x \in \mathbb{R}^n \mid \|x\| \leq \varepsilon\}$ abgeschlossene ε-Kugel um $x_0 \in \mathbb{R}^n$
- $$M = \left\{\begin{pmatrix} x \\ y \end{pmatrix} \in \mathbb{R}^2 \mid 0 \leq x < 1\right\}$$
$$\partial M = \left\{\begin{pmatrix} x \\ y \end{pmatrix} \in \mathbb{R}^2 \mid x = 0 \lor x = 1\right\}$$
$$\bar{M} = \left\{\begin{pmatrix} x \\ y \end{pmatrix} \in \mathbb{R}^2 \mid 0 \leq x \leq 1\right\}$$
$$\mathring{M} = \left\{\begin{pmatrix} x \\ y \end{pmatrix} \in \mathbb{R}^2 \mid 0 < x < 1\right\}$$

2.9 Beschränkte/kompakte Mengen

- $D \subseteq \mathbb{R}^n$ beschränkt $:\iff \exists K > 0 : \|x\| < K \quad \forall x \in D$
- $D \subseteq \mathbb{R}^n$ kompakt $:\iff$ Jede Folge in D besitzt eine in D konvergente Teilfolge.

2.10 Charakterisierung kompakter Mengen

$D \subseteq \mathbb{R}^n$ kompakt $\iff$ D beschränkt und abgeschlossen.

Beweis

Beweis. TODO. Q.E.D.

Beispiel

- $\bar{K}_\varepsilon(x_0)$ kompakt, da beschränkt und abgeschlossen
- $A = \left\{\begin{pmatrix} x \\ y \end{pmatrix} \in \mathbb{R}^2 \mid y = x^2,\ y \leq 1\right\}$ abgeschlossen und beschränkt, also kompakt

2.11 Mehrdimensionale reele Funktionen und Stetigkeit

- Eine reele Funktion von mehreren Veränderlichen ist eine Abbildung

$$f : D \subseteq \mathbb{R}^n \to \mathbb{R}^m$$
$$x = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \to f(x) = \begin{pmatrix} f_1(x) \\ \vdots \\ f_m(x) \end{pmatrix}$$

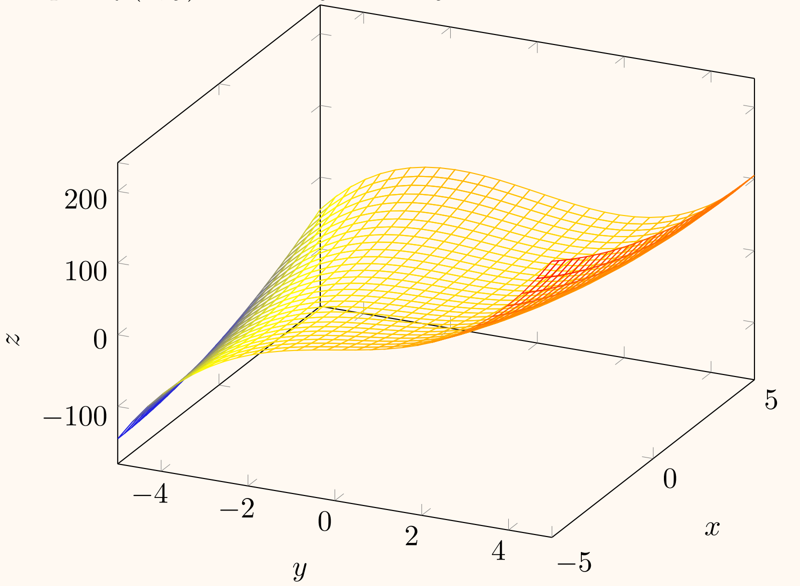
- Man unterscheidet folgende Fälle:

$$\begin{aligned} m = 1: &\quad f : D \subseteq \mathbb{R}^n \to \mathbb{R} &&\text{(skalare Funktion)}\\ m > 1: &\quad f : D \subseteq \mathbb{R}^n \to \mathbb{R}^m &&\text{(vektorwertige Funktion)}\\ n = 1: &\quad f : D \subseteq \mathbb{R} \to \mathbb{R}^m &&\text{(parameterisierte Kurve)} \end{aligned}$$

Beispiel

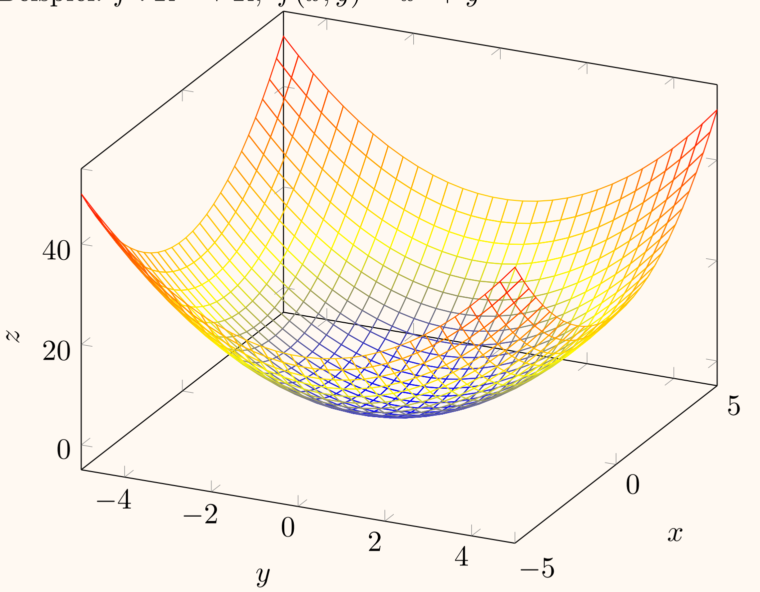
- Skalare Funktionen mit $D \subseteq \mathbb{R}^2$ lassen sich grafisch darstellen:
  - $\text{Graph}(f) := \left\{ \begin{pmatrix} x \\ y \\ z \end{pmatrix} \in \mathbb{R}^3 \mid \begin{pmatrix} x \\ y \\ z \end{pmatrix} \in D,\ z = f(x,y) \right\}$ ist eine Fläche im $\mathbb{R}^3$

    Beispiel: $f(x,y) = 5 - 2xy + x^3 + y^2$



  - Höhen-/Niveaulinien: $N_C(f) := \left\{ \begin{pmatrix} x \\ y \end{pmatrix} \in \mathbb{R}^2 \mid f(x,y) = c \right\}, \quad c \in \mathbb{R}.$

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



    TODO
- Parameterisierte Kurve

- $f : \mathbb{R} \to \mathbb{R}^2,\ x \to \begin{pmatrix} \cos(x) \\ \sin(x) \end{pmatrix}$ Einheitskreis
- Venusbahn geozentrisch: TODO: Graphen.

$$\begin{aligned} D(t) &= V(t) - E(t) \\ E(t) &\approx a_E(\cos(8 \cdot 2\pi t),\ \sin(8 \cdot 2\pi 2)) \\ V(t) &\approx a_V(\cos(13 \cdot 2\pi t),\ \sin(13 \cdot 2\pi t)) \end{aligned}$$

Innerhalb einer Zeiteinheit (0) dreht sich die Erde $8\times$ um die Sonne $\implies$ Umlaufzeit Erde: $T_E = \frac{1}{8} \implies$ Umlaufzeit Venus $T_V = \frac{1}{13}$. Aus dem 3. Keplerschen Gesetz folgt:

$$T_E^2 \sim a_E^3 \iff a_E \sim \sqrt[3]{T_E^2} = \sqrt[3]{\frac{1}{64}} = \frac{1}{4}$$

und

$$a_V \sim \sqrt[3]{\left(\frac{1}{13}\right)^2}.$$

Mit $a_E = \frac{1}{4}$ und $a_V = \sqrt[3]{\left(\frac{1}{13}\right)^2}$ erhält man für $D(t),\ 0 \le t \le 1$ eine Epitrochoide.
TODO: Graphen

2.12 Stetigkeit

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

- $c \in \mathbb{R}^m$ heißt Grenzwert von f in $a \in \mathbb{R}^n$, falls für jede Folge (x_k) mit $x_k \to a,\ x_k \neq a \quad \forall k \in \mathbb{N}$ gilt: $f(x_k) \to c$. Schreibweise: $\lim_{x\to a} f(x) = c$
- f stetig in $a \in D :\iff \lim_{x\to a} f(x) = f(a)$
- f stetig auf $D :\iff f$ stetig in $a \quad \forall a \in D$

Bemerkung

- $f : D \subset \mathbb{R}^n \to \mathbb{R}^m$ stetig in $a \in D \iff f_i : D \to \mathbb{R}$ stetig $\quad \forall i \in \{1, ..., m\}$
- Summen, Produkte, Quotienten, Kompositionen stetiger Funktionen sind stetig. Rechenregeln für Grenzwerte gelten analog.

Bemerkung

- Stetigkeit wurde anhand des Folgenkriteriums definiert. Analog dazu lässt sich dieses auch anhand des $\varepsilon - \delta$-Kriteriums formulieren:

$$\begin{aligned} f : D \subset \mathbb{R}^n \to \mathbb{R}^m \text{ stetig} \iff & \forall \varepsilon > 0 \exists \delta > 0 \forall x \in D : \|x - a\| < \varepsilon \\ \implies & \|f(x) - f(a)\| < \varepsilon \end{aligned}$$

- Anders formuliert:
$$\forall \varepsilon > 0 \exists \delta > 0 : f(K_\delta(a)) \subseteq K_\varepsilon(f(a))$$

Beispiel

- $f : \mathbb{R}^n \to \mathbb{R},\ f(x_1, ..., x_n) = x_i$ stetig in $a \in \mathbb{R}^n$:
  - Es sei $(a_k)_{k\in\mathbb{N}}$ Folge in $\mathbb{R}^n$ mit

$$a_k = \begin{pmatrix} a_1^{(k)} \\ \vdots \\ a_n^{(k)} \end{pmatrix} \to a = \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix}$$

$$\implies \lim_{k\to\infty} f(a_k) = \lim_{k\to\infty} a_i^{(k)} = a_i$$

  - $f(a) = a_i \implies f(a_k) \to f(a)$
- Es folgt, dass alle Polynome stetig sind
- Folgende Funktion ist stetig in $\mathbb{R}^2 \setminus \left\{\begin{pmatrix} 0 \\ 0 \end{pmatrix}\right\}$ (TODO: Graph)

$$f(x, y) = \begin{cases} 0 & (x, y) = (0, 0) \\ \frac{3x^2}{x^2+y^2} & \text{sonst} \end{cases}$$

  - Sei $a_k := \begin{pmatrix} 1/k \\ 1/k \end{pmatrix} \in \mathbb{R}^2 \setminus \left\{\begin{pmatrix} 0 \\ 0 \end{pmatrix}\right\}$. Es gilt

$$\begin{aligned} & a_k \to 0 \\ \implies & f(a_k) = \frac{3(1/k)^2}{(1/k)^2 + (1/k)^2} = \frac{3}{2} \\ \implies & f(a_k) \to \frac{3}{2} \end{aligned}$$

  - $f(0, 0) = 0 \implies f(a_k) \not\to f(0, 0)$ und f unstetig in $\begin{pmatrix} 0 \\ 0 \end{pmatrix}$
- Folgende Gleichung muss nicht notwendigerweise erfüllt sein (vorausgesetzt, die entsprechenden Grenzwerte existieren):

$$\lim_{x\to a}(\lim_{y\to b} f(x, y)) = \lim_{y\to b}(\lim_{x\to a} f(x, y))$$

Falls einer der Grenzwerte existiert oder sogar die Gleichung erfüllt ist, so folgt danach keineswegs, dass $\lim_{(x,y)\to(a,b)} f(x, y)$ existiert.

Beispiel

$$f : \mathbb{R}^2 \setminus \left\{\begin{pmatrix} 0 \\ 0 \end{pmatrix}\right\} \to \mathbb{R}$$

$$f(x, y) = \frac{xy^2}{x^2 + y^2}$$

Da $\lim_{x\to 0} f(x, y) = 0$ und $\lim_{y\to 0}(\lim_{x\to 0} f(x, y)) = 0$.
Analog $\lim_{x\to 0}(\lim_{y\to 0} f(x, y)) = 0$.

Aber: $\lim_{(x,y)\to(0,0)} f(x,y)$ existiert nicht, denn

$$f\left(\frac{1}{k},\frac{1}{k}\right) = \frac{k^2}{1/k^2 + 1/k^2} = \frac{k}{k^2+1} \to 0$$

$$f\left(\frac{1}{k^2},\frac{1}{k}\right) = \frac{1/k^2}{2/k^2} \to \frac{1}{2}$$

Insbesondere lässt sich f im Nullpunkt nicht stetig fortsetzen.

2.13 Stetigkeit und Offenheit

Sei $f : D \subseteq \mathbb{R}^n \to \mathbb{R}^n,\ V \subseteq f(0),\ V$ offen. Dann:

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

Beweis

Beweis. In beide Richtungen:

- „$\implies$“: Sei

$$\begin{aligned} y \in V &\implies \exists x \in D : f(x) = y \\ &\implies \exists \varepsilon > 0 : K_\varepsilon(y) \subseteq V \\ &\implies \exists \delta > 0 : f(K_\varepsilon(x)) \subseteq K_\varepsilon(y) \\ &\implies K_\varepsilon(x) \subseteq f^{-1}(K_\varepsilon(y)) \subseteq f^{-1}(V) \end{aligned}$$

- „$\impliedby$“: Trivial

Q.E.D.

2.14 Stetigkeit und Kompaktheit

$f : D \subseteq \mathbb{R}^n \to \mathbb{R}^m$ stetig, $A \subseteq D$ kompakt $\implies$ $f(A)$ kompakt.

Beweis

Beweis. Sei (y_k) Folge in $f(A)$. **Zu zeigen:** : (y_k) hat eine in $f(A)$ konvergente Teilfolge.
Sei (x_k) Folge in A mit $f(x_k) = y_k \quad \forall k \in \mathbb{N}$.
$\implies \exists (x_{k_j}) \subseteq A$ mit Grenzwert $a \in A$.
$\implies f(x_{k_j}) = y_{k_j}$ Teilfolge von (y_k) in $f(A)$ mit Grenzwert $f(a)$ Q.E.D.

2.15 Beschränktheit von Funktionen

Sei $D = \emptyset$, $f : D \subseteq \mathbb{R}^n \to \mathbb{R}^m$ beschränkt $:\iff f(D)$ beschränkt.

2.16 Minimax-Theorem von Weierstraß

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

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

Beweis

Beweis. Zu zeigen: $f(D)$ kompakt.

- $f(D)$ beschränkt $\implies \exists \inf f(D), \sup f(D)$

$$\implies \exists (a_k), (b_k) \subseteq f(D) : \begin{aligned} a_k &\to \inf f(D) \\ b_k &\to \sup f(D) \end{aligned}$$

- $f(D)$ abgeschlossen

$$\implies \begin{aligned} \inf f(D) &= \max f(D) = f(x_*) \\ \sup f(D) &= \max f(D) = f(x^*) \end{aligned}$$

Q.E.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

2.17 Kontraktion

Sei $A \subseteq \mathbb{R}^n$ abgeschlossen und sei $f : A \to \mathbb{R}^n$. f heißt Kontraktion auf $A :\iff$

- $f(A) \subseteq A$
- $\|f(x) - f(y)\| \leq q\|x - y\|,\ q \in [0,1) \quad \forall x, y \in A$

f ist eine stetige Abbildung.

Beispiel

- $f : \mathbb{R} \to \mathbb{R},\ f(x) = \frac{1}{2}x$
  $|f(x) - f(y)| = \frac{1}{2}|x = y|$, d.h. $q = \frac{1}{2}$
- f Kontraktion auf $A = [0,1]$: $f([0,1]) = [0, \frac{1}{2}] \subseteq [0,1]$
- f keine Kontraktion auf $A = [1,2]$, da $f([1,2]) = [\frac{1}{2}, 1] \not\subseteq [1,2]$

2.18 Banachscher Fixpunktsatz im $\mathbb{R}^n$

Sei $A \subseteq \mathbb{R}^n$ abgeschlossen und $f : A \to A$ eine Kontraktion auf A. Dann:

1. $\exists! \bar{x} \in A : A(\bar{x}) = \bar{x}$. $\bar{x}$ heißt Fixpunkt.
2. Für $x_0 \in A$ und $x_n := f(x_{x_n - 1}),\ n \in \mathbb{N}$, gilt: $x_n \to \bar{x}$ und $\|x_n - \bar{x}\| \leq \frac{qn}{1-q}\|x_1 - x_0\|$

Beweis

Beweis. TODO. Siehe Skript Q.E.D.

2.19 Matrixnorm

Sei $A \in \mathcal{M}_{m,n}(\mathbb{R})$. Die reele Zahl $\|A\| = \max\{\|Av\| \mid v \in \mathbb{R}^n,\ \|v\| = 1\}$ heißt Operatornorm von A.

3 Differenziation im $\mathbb{R}^n$

3.1 Partielle Ableitung

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

- f heißt an der Stelle a partiell nach x_j differenzierbar, falls für jede der Funktionen $f_i : \mathbb{R}^n \to \mathbb{R}$ gilt: Die skalare Funktion $f_i(a_1, ..., a_{j-1}, x_j, a_{j+1}, ..., a_n)$ einer Veränderlichen ist an der Stelle a_j differenzierbar, d.h.

$$\begin{aligned}&\lim_{k\to 0} \frac{f_i(a_1, ..., a_{j-1}, a_j + h, a_{j+1}, ..., a_n) - f_i(a_1, ..., a_n)}{h}\\ =&\lim_{h\to 0} \frac{f_i(a + h \cdot e_j) - f(a)}{h}\end{aligned}$$

  existiert für alle $1 \leq i \leq m$.
- Dieser Grenzwert heißt dann partielle Ableitung von f_i nach x_j an der Stelle a. Schreibweise: $\frac{\partial f_i}{\partial x_j}(a)$.
- Sind alle f_i nach allen x_j partiell differenzierbar in a, so heißt f partiell differenzierbar und man definiert die Jacobimatrix von f in a durch

$$f'(a) := \begin{pmatrix} \frac{\partial f_1}{\partial x_1}(a) & \dots & \frac{\partial f_1}{\partial x_n}(a) \\ \frac{\partial f_m}{\partial x_1}(a) & \dots & \frac{\partial f_m}{\partial x_n}(a) \end{pmatrix} \in \mathcal{M}_{m,n}(\mathbb{R})$$

- Für skalare Funktionen besteht $f'(a)$ aus nur einer Zeile. Man bezeichnet den Vektor

$$f'(a)^\top = \begin{pmatrix} \frac{\partial f}{\partial x_1}(a) \\ \vdots \\ \frac{\partial f}{\partial x_n}(a) \end{pmatrix} =: \nabla f(a) = \operatorname{grad}(f(a)) \in \mathbb{R}^n$$

  als Gradienten von f in a.

3.2 Geometriche Deutung der partiellen Ableitung

Sei $f : \mathbb{R}^2 \to \mathbb{R},\ a \in \mathbb{R}^2,\ a = \begin{pmatrix} a_1 \\ a_2 \end{pmatrix}$.

TODO: Graph

Beispiel

- $f : \mathbb{R}^2 \to \mathbb{R},\ f(x, y) = 3xy + 4y$

$$\begin{aligned}\frac{\partial f}{\partial x}(x, y) &= \lim_{h\to 0} \frac{f(x + h, y) - f(x, y)}{h}\\ &= \lim_{h\to 0} \frac{3(x + h)y + 4y - 3xy - 4y}{h}\\ &= \lim_{h\to 0} 3y\end{aligned}$$

  D.h.: y wird als Konstante behandelt und nach x wird abgeleitet.

- $f : \mathbb{R}^3 \to \mathbb{R},\ f(x,y,z) = y^2x + 3x^2z^2$

$$\begin{aligned} \frac{\partial f}{\partial x}(x,y,z) &= y^2 + 6xz^2 \\ \frac{\partial f}{\partial y}(x,y,z) &= 2xy \\ \frac{\partial f}{\partial z}(x,y,z) &= 6x^2z \end{aligned}$$

$$\begin{aligned} \implies f'(x,y,z) \quad &= (y^2 + 6xz^2, 2xy, 6x^2z) \\ f'(1,0,1) \quad &= (6,0,6) \\ \nabla f(x,y,z) &= \begin{pmatrix} y^2 + 6xz^2 \\ 2xy \\ 6x^2z \end{pmatrix} \end{aligned}$$

- $f : \mathbb{R}^3 \to \mathbb{R}^2,\ f(x,y,z) = \begin{pmatrix} x+y \\ xyz \end{pmatrix} \implies f'(x,y,z) = \begin{pmatrix} 1 & 1 & 0 \\ yz & xz & xy \end{pmatrix}$

Bemerkung

- Zeigen später: Der Gradient zeigt in Richtung des steilsten Anstiegs einer Funktion in einem gegebenen Punkt. Er steht senkrecht auf den Niveaulinien.
- Existieren für f in einem gegebenen Punkt alle partiellen Ableitungen, so muss f nicht automatisch stetig sein.

3.3 Totale Ableitung

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.

Bemerkung

- Für $m = n = 1$ erhält man die Differenzierbarkeit aus Mathe 1:

$$\begin{aligned} & f(x) = f(a) + A(x-a) + R(x) \\ \implies & \frac{f(x) - f(a)}{x-a} = A + \frac{R(x)}{x-a} \to A \\ \implies & f'(a) = A \end{aligned}$$

- $x \to a \iff x - a \to 0$. Sei $v = x - a \in \mathbb{R}^n$. Dann kann vorige Gleichung geschrieben werden als

$$f(a+v) = f(a) + Av + R(v) \quad \text{mit } \frac{R(v)}{\|v\|} \to 0$$

3.4 Differenzierbarkeit $\implies$ Stetigkeit

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

$\implies$ f stetig in a.

Beweis

Beweis.

$$\lim_{x\to a} f(x) = \lim_{x\to a}(f(a) + A(x-a) + R(x)) = f(a)$$

Q.E.D.

3.5 $A = f'(a)$

Sei $f : D \subseteq \mathbb{R}^n \to \mathbb{R}^m$ und differenzierbar in $a \in D$, D offen und sei $f(a+v) = f(a) + Av + R(v)$ wie zuvor. Dann ist f in a partiell differenzierbar und es gilt $A = f'(a)$. Insbesondere: A eindeutig.

Beweis

Beweis. Sei $A = (a_{i,j})_{i,j}$, $v = (v_1, ..., v_n)^\top \in \mathbb{R}^n$.
Für $i \in \{1, ..., m\}$ ist $f_i(a+v) = f_i(a) + \sum_{j=1}^n a_{ij} v_j + R_i(v)$.
Setzt man $v = \underbrace{h}_{\in\mathbb{R}} \cdot e_k$, so ist $\|v\| = |h| = \operatorname{sgn}(h) \cdot h$ und

$$\begin{aligned}
\frac{f_i(a+v) - f_i(a)}{\|v\|} &= \frac{a_{ik}\cdot h}{\|v\|} + \frac{R_i(v)}{\|v\|} \qquad | \cdot \operatorname{sgn}(h) \\
\iff \underbrace{\frac{f_i(a+v) - f_i(a)}{h}}_{\to \frac{\partial f}{\partial x_k}(a)} &= a_{ik}\cdot h + \underbrace{\frac{R_i(v)}{\|v\|}\cdot \operatorname{sgn}(h)}_{\to 0} \\
\implies a_{ik} &= \frac{\partial f_i}{\partial x_k}(a)
\end{aligned}$$

Q.E.D.

Beispiel

Tangentialebene berechnen:

- wir wissen, dass $\frac{R(x)}{\|x-a\|} \to 0$ gilt und demnach $f(x)$ in einer Umgebung von a angenähert werden kann durch

  $$g(x) = \underbrace{f(a)}_{\text{TODO?}} + \underbrace{f'(a)\cdot(x-a)}_{\text{lineare Abbildung}}$$

  vorausgesetzt f ist in a differenzierbar. g heißt lineare Approximation/Tangentialebene von f in a.

  Z.B.: $f(x_1, x_2) = x_1^2 + x_2^2$, $\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \in \mathbb{R}^2$ Tangentialebene in $(a_1, a_2, f(a_1, a_2))^\top \in \mathbb{R}^3$

für $a = \begin{pmatrix} a_1 \\ a_2 \end{pmatrix} = \begin{pmatrix} 1 \\ 2 \end{pmatrix}$.

$$\begin{aligned} g(x) &= f(a) + f'(a)(x-a) = 5 + \begin{pmatrix} 2 & 4 \end{pmatrix} \begin{pmatrix} x_1 - 1 \\ x_2 - 2 \end{pmatrix} \\ &= 5 + 2x_1 - 2 + 4x_2 - 8 \\ &= -5 + 2x_1 + 4x_2 \end{aligned}$$

- f differenzierbar in $a \in D \iff f_i$ differenzierbar in $a \in D \quad \forall i \in \{1, ..., n\}$.

Beweis

Beweis. Sei $f'(a) = (a_{ij})$ die Jacobimatrix von f in a.
Dann:

$$f(x) = f(a) + f'(a)(x-a) + R(x), \qquad \frac{R(x)}{\|x-a\|} \to 0$$

$$\iff f_i(x) = f_i(a) + \underbrace{\sum_{j=1}^{n} a_{ij}(x_j - a_j)}_{f_i'(a)(x-a)} + R_i(x), \quad \forall i \in \{1, ..., m\}; \; \frac{R(x)}{\|x-a\|} \to 0$$

Q.E.D.

3.6 Ableitungsregeln

3.6.1 Kettenregel

Seien $U \subseteq \mathbb{R}^n$, $V \subseteq \mathbb{R}^m$ offen, $a \in U$, $f : U \to \mathbb{R}^m$, $g : V \to \mathbb{R}^k$ mit $f(U) \subseteq V$.

Ist f differenzierbar in $a \in U$ und g differenzierbar in $f(a)$, so ist $g \circ f$ differenzierbar in a und es gilt:

$$(g \circ f)'(a) = g'(f(a)) \cdot f'(a)$$

Beweis

Beweis. Es seien $L := f'(a)$, $K := g'(f(a))$.
D.h.: $K \cdot L = g'(f(a)) \cdot f'(a)$.
Setze

- $R(v) = f(a+v) - f(a) - Lv$
- $S(w) = g(f(a) + w) - g(f(a)) - Kw$
- $T(v) = (g \circ f)(a+v) - (g \circ f)(a) - KLv$

f, g differenzierbar in a bzw. $f(a)$.
$\implies \lim_{v \to 0} \frac{R(v)}{\|v\|} = 0$, $\lim_{w \to 0} \frac{s(w)}{\|w\|} = 0$
$\lim_{v \to 0} \frac{T(v)}{\|v\|} = 0$ folgt durch simples Einsetzen und Umformen.
$\lim_{v \to 0} \frac{S(R(v)+Lv)}{\|v\|} = 0$ folgt ebenfalls (bisschen komplexer eigentlich).
Daraus folgt für $0 < \|v\| < \epsilon$:

$$\frac{\|R(v) + Lv\|}{\|v\|} \leq \frac{\|R(v)\|}{\|v\|} + \left\| L \cdot \frac{v}{\|v\|} \right\| \leq 1 + c$$

Damit ergibt sich:

$$\frac{S(R(v)+Lv)}{\|v\|} = \frac{S(R(v)+Lv)}{\|R(v)+Lv\|} \cdot \frac{\|R(v)+Lv\|}{\|v\|} \xrightarrow[v\to 0]{} 0$$

Q.E.D.

Beispiel

Sei $f : \mathbb{R} \to \mathbb{R}^2,\ f(t) = \begin{pmatrix} \cos t \\ t \end{pmatrix} \implies f'(t) = \begin{pmatrix} -\sin t \\ 1 \end{pmatrix}$

Sei außerdem $g : \mathbb{R}^2 \to \mathbb{R}^2,\ g(x,y) = \begin{pmatrix} x^2+3y \\ x-y \end{pmatrix} \implies g'(x,y) = \begin{pmatrix} 2x & 3 \\ 1 & -1 \end{pmatrix}$

Gesucht ist $(g \circ f)'$.

1. $(g\circ f)'(t) = g'(f(t)) \cdot f'(t) = \begin{pmatrix} 2\cos t & 3 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} -\sin t \\ 1 \end{pmatrix} = \begin{pmatrix} -2\cos t \cdot \sin t + 3 \\ -\sin t - 1 \end{pmatrix}$
2. $(g\circ f)(t) = g\begin{pmatrix} \cos t \\ t \end{pmatrix} = \begin{pmatrix} \cos^2 t + 3t \\ \cos t - t \end{pmatrix} \implies (g\circ f)'(t) = \begin{pmatrix} -2\cos t \cdot \sin t + 3 \\ -\sin t - 1 \end{pmatrix}$

3.6.2 Weitere Ableitungsregeln

Sei $D \subseteq \mathbb{R}^n$ offen, $f, g : D \to \mathbb{R}^m$ differenzierbar in $a \in D$, $\lambda \in \mathbb{R}$. Dann sind auch $f+g$, λf, $f^\top g$ in a differenzierbar und es gilt:

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

Beispiel

$f, g : \mathbb{R}^2 \to \mathbb{R}^2,\ f(x,y) = \begin{pmatrix} x-y \\ x \end{pmatrix},\ g(x,y) = \begin{pmatrix} x^2 \\ y \end{pmatrix},\ f'(x,y) = \begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix},\ g'(x,y) = \begin{pmatrix} 2x & 0 \\ 0 & 1 \end{pmatrix}$

$$\begin{aligned} \implies (f^\top g)'(x,y) &= (x-y, x)\begin{pmatrix} 2x & 0 \\ 0 & 1 \end{pmatrix} + (x^2, y)\begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix} \\ &= (2x^2 - 2xy, x) + (x^2 + y, -x^2) \\ &= (3x^2 - 2xy + y, x - x^2) \end{aligned}$$

3.7 Mittelwertsätze

3.7.1 Mittelwertsatz für skalare Funktionen

Sei $D \subseteq \mathbb{R}^n$ offen, $f : D \to \mathbb{R}$ differenzierbar und $a, b \in D$, sodass

$$S(a,b) := \{a + t(b-a) \mid t \in (0,1)\} \subseteq D$$

Dann existiert ein $\xi \in S(a,b)$, sodass

$$f(b) - f(a) = f'(\xi)(b-a)$$

Beweis

Beweis. Sei $\varphi : [0,1] \to D$ mit $\varphi(t) = a + t(b-a)$, $g := f \circ \varphi : [0,1] \to \mathbb{R}$. f differenzierbar, φ differenzierbar auf $(0,1)$ und stetig auf $[0,1]$.
$\implies g$ differenzierbar auf $(0,1)$ und stetig auf $[0,1] \implies \exists \vartheta \in (0,1)$ mit $\frac{g(1)-g(0)}{1-0} = g'(\vartheta)$.
Sei $\xi := \phi(\vartheta)$.

$$\begin{aligned}\implies f(b) - f(a) &= f(\varphi(1)) - f(\varphi(0)) = g(1) - g(0) \\ &= g'(\vartheta) = (f \circ \varphi)'(\vartheta) \\ &= f'(\varphi(\vartheta)) \cdot \varphi'(\vartheta) \qquad | \ \varphi'(t) = b - a \\ &= f'(\xi)(b-a)\end{aligned}$$

Q.E.D.

Bemerkung

Für vektorwertige Funktionen kann man den vorigen Satz nicht beweisen. Z.B.:
Sei $f : [0, 2\pi] \to \mathbb{R}^2,\ f(t) = \begin{pmatrix} \cos t \\ \sin t \end{pmatrix}$.
Gibt $\xi \in (0, 2\pi)$ mit $f(2\pi) - f(0) = f'(\xi)(2\pi - 0)$?
Nein, da

$$f(2\pi) - f(0) = \begin{pmatrix} 1 \\ 0 \end{pmatrix} - \begin{pmatrix} 1 \\ 0 \end{pmatrix} = 0 \neq f'(\xi) \cdot 2\pi \implies f'(\xi) = (0,0).$$

Aber: $f'(t) = (-\sin t, \cos t) \neq (0,0) \quad \forall t \in (0, 2\pi)$.
Es lässt sich jedoch eine Abschätzung mithilfe von Integralen zeigen.

3.8 Riemann-Integral

3.8.1 Zerlegung

Sei $[a,b] \subseteq \mathbb{R}$.

- $Z := \{x_0, x_1, ..., x_n\} \subseteq [a,b]$, $a = x_0 < x_1 < ... < x_n = b$ heißt Zerlegung von $[a,b]$
- $|Z| := \max_{i=1,...,n}(x_i - x_{i-1})$ heißt Feinheit von Z
- $\sum[a,b]$: Menge aller Zerlegungen von $\mathfrak{Z}[a,b]$

3.8.2 Riemannsche Summe

Sei $f : [a,b] \to \mathbb{R}$ und $Z = \{x_0, ..., x_n\} \in \mathfrak{Z}[a,b]$.

- $\xi := (\xi_1, ..., \xi_n)$, $\xi_i \in [x_{i-1}, x_i]$, heißt Zwischenvektor von Z
- $S(f, Z, \xi) := \sum_{i=1}^n f(\xi_i)(x_i - x_{i-1})$ heißt Riemannsche Summe

3.8.3 Riemann-Integral

$f : [a,b] \to \mathbb{R}$ heißt R-integrierbar auf $[a,b]$ $:\iff$ für jede Folge $Z_n \in \mathfrak{Z}[a,b]$ mit Zwischenvektor ξ_n und $|Z_n| \xrightarrow[n\to\infty]{} 0$ konvergiert $S(f, Z_n, \xi_n)$ gegen $A \in \mathbb{R}$.

Bezeichnung: $A = \int_a^b f(x) \mathrm{d}x$

Bemerkung

Die Definition ist äquivalent zu derjenigen aus Mathe 1.

3.8.4 Riemann-Integral für $f : [a, b] \to \mathbb{R}^m$

Sei $f : [a, b] \to \mathbb{R}^m$.

- Für Z, ξ wie zuvor ist $S(f, Z, \xi) := \sum_{i=1}^n f(\xi_i)(x_i - x_{i-1})$
- Für Z_n, ξ_n sei $A \in \mathbb{R}^m$ der Grenzwert von $S(f, Z_n, \xi_n)$, falls existent. Bezeichnung: $A = \int_a^b f(x)\mathrm{d}x$

Bemerkung

- Offensichtlich gilt:

$$f : [a, b] \to \mathbb{R}^m \text{ } R\text{-integrierbar} \iff f_i : [a, b] \to \mathbb{R} \text{ } R\text{-integrierbar} \quad \forall i = 1, ..., m.$$

  D.h.

$$\int_a^b f(x)\mathrm{d}x = \begin{pmatrix} \int_a^b f_1(x)\mathrm{d}x \\ \vdots \\ \int_a^b f_m(x)\mathrm{d}x \end{pmatrix}$$

- Eine Matrix $A(x) \in \mathcal{M}_{m,n}(\mathbb{R})$ kann man mit einem Vektor $v(x) \in \mathbb{R}^m \cdot n$ identifizieren, indem alle Matrixeingänge in eine Spalte geschrieben werden. Daher kann man definieren:
  $\int_a^b A(x)\mathrm{d}x := \left(\int_a^b a_{ij}(x)\mathrm{d}x\right)_{i,j}$ und es gilt

$$\int_a^b A(x) \cdot h\mathrm{d}x = \int_a^b A(x)\mathrm{d}x \cdot h \quad \forall h \in \mathbb{R}^n$$

3.8.5 Dreiecksungleichung

$$f : [a, b] \to \mathbb{R}^m \text{ stetig} \implies \left\| \int_a^b f(x)\mathrm{d}x \right\| \leq \int_a^b \|f(x)\| \, \mathrm{d}x$$

Beweis

Beweis.

$$\begin{aligned} \|S(f, Z, \xi)\| &= \|\sum_{i=1}^n f(\xi_i)(x_i - x_{i-1})\| \\ &\leq \sum_{i=1}^n \|f(\xi_i)\| \cdot \underbrace{(x_i - x_{i-1})}_{\geq 0} \\ &= S(\underbrace{\|f\|}_{\text{stetig, da } f \text{ stetig}}, Z, \xi) \end{aligned}$$

Q.E.D.

3.9 Mittelwertsätze für vektorwertige Funktionen

$f : D \subseteq \mathbb{R}^n \to \mathbb{R}^m$ (D offen) sei differenzierbar, sodass alle partiellen Ableitungen stetig sind (d.h. f stetig differenzierbar). Ferner seien $a, b \in D$, sodass

$$S = \{a + t(b-a) \mid t \in [0,1]\} \subseteq D.$$

Für $h := b - a$ folgt:

- $f(b) - f(a) = \underbrace{\int_0^1 f'(a+th)\mathrm{d}t}_{\in \mathcal{M}_{m,n}(\mathbb{R})} \cdot h \in \mathbb{R}^m$
- $\|f(b) - f(a)\| \leq M \cdot \|h\|$, wobei $M := \max_{x \in S} \underbrace{\|f'(x)\|}_{\text{stetig, da alle partiellen Ableitungen stetig}}$

Beweis

Beweis.

- $\varphi_j : [0,1] \to \mathbb{R}$, $\varphi_j(t) := f_j(a + t \cdot h)$, $h = b - a$.

$$\begin{aligned} \implies f_j(b) - f_j(a) &= \varphi_j(1) - \varphi_j(0) \\ &= \int_0^1 \varphi_j'(t)\mathrm{d}t \\ &= \int_0^1 \underbrace{f_j'(a+th)}_{\text{stetig, d.h. } R\text{-integrierbar}} \cdot h\mathrm{d}t \end{aligned}$$

$$\begin{aligned} \implies f(b) - f(a) &= \begin{pmatrix} \int_0^1 f_1'(a+th) \cdot h\mathrm{d}t \\ \vdots \\ \int_0^1 f_m'(a+th) \cdot h\mathrm{d}t \end{pmatrix} \\ &= \int_0^1 f'(a+th) \cdot h\mathrm{d}t \\ &= \int_0^1 f'(a+th)\mathrm{d}t \cdot h \end{aligned}$$

- $\|f(b) - f(a)\| = \left\| \int_0^1 f'(a+th)\mathrm{d}t \cdot h \right\| \leq \int_0^1 \underbrace{\|f'(a+th)\|}_{\leq M} \mathrm{d}t \cdot \|h\|$

Q.E.D.

Bemerkung

- Differenzierbarkeit $\implies$ partielle Differenzierbarkeit
- Umkehrung gilt nicht

3.10 Partielle und totale Differenzierbarkeit

Seien $D \subseteq \mathbb{R}^n$ offen, $a \in D$ und $f : D \to \mathbb{R}$ partiell differenzierbar in a. Sind alle partiellen Ableitungen $\frac{\partial f}{\partial x_i}$ $(i = 1, ..., n)$ stetig in a, so ist f total differenzierbar in a.

Beweis

TODO.

Bemerkung

- Partielle Differenzierbarkeit gilt auch für vektorwertige Funktionen $f : D \subseteq \mathbb{R}^n \to \mathbb{R}^m$ (D offen)
- Die Stetigkeit der partiellen Ableitung ist ein hinreichendes, aber kein notwendiges Kriterium für Differenzierbarkeit
- Alle Polynome sind differenzierbar, da die partiellen Ableitungen alle stetig sind

3.11 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, $\frac{\partial f}{\partial v}(a)$.

Beispiel

- $\frac{\partial f}{\partial e_i}(a) = \lim_{h\to 0} \frac{f(a+he_i)-f(a)}{h} = \frac{\partial f}{\partial x_i}(a)$
- $f : \mathbb{R}^2 \to \mathbb{R}$, $f(x,y) = \begin{cases} \frac{xy^2}{x^2+y^4} & (x,y) \neq (0,0) \\ 0 & (x,y) = (0,0) \end{cases}$
  - Wissen: f unstetig in $0 \in \mathbb{R}^2$
  - f ist in jede Richtung $v \in \mathbb{R}^2$, $\|v\| = 1$, ableitbar in 0: Sei $v = (v_1, v_2)^\top$

    $\implies \frac{f(hv)-f(0,0)}{h} = \frac{h^2 v_1 v_2^2}{h \cdot h^2(v_1^2 + h^2 v_2^4)} \implies \frac{\partial f}{\partial v}(0,0) = \begin{cases} v_2^2/v_1 & v_1 \neq 0 \\ 0 & v_1 = 0 \end{cases}$
- $f : \mathbb{R}^2 \to \mathbb{R}$, $f(x,y) = x^2 + y^2$, $h \to f(a+hv)$ ist eindimensionale Funktion. TODO: Graph

3.11.1 Satz

Sei $D \subseteq \mathbb{R}^n$ offen, $f : D \to \mathbb{R}$ differenzierbar. Dann existieren alle Richtungsableitungen von f in $a \in D$ und

$$\frac{\partial f}{\partial v}(a) = f'(a) \cdot v$$

Beweis

Beweis.

$$\begin{aligned} &\frac{f(a+hv)-f(a)}{h} - f'(a) \cdot v \\ =&\|v\| \frac{\overbrace{f(a+hv) - f(a) - f'(a) \cdot v \cdot h}^{R(hv)}}{\|hv\| \cdot \operatorname{sgn}(h)} \xrightarrow{h\to 0} 0 \\ \implies& \frac{\partial f}{\partial v}(a) = f'(a)v \end{aligned}$$

Q.E.D.

Beispiel

$$f(x,y) = e^{xy} + x^2 \implies f'(x,y) = (ye^{xy} + 2x, xe^{xy})$$

Sei $v = \frac{1}{\sqrt{2}}(1,1)^\top$

$\implies \frac{\partial f}{\partial v}(x,y) = (ye^{xy+2x,xe^{xy}}) \cdot \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \frac{1}{\sqrt{2}}(e^{xy}(x+y) + 2x)$

3.11.2 Satz

Sei $D \subseteq \mathbb{R}^n$ offen, $f : D \to \mathbb{R}$ differenzierbar in $a \in D$ mit $f'(a) \neq 0$. Dann gilt:

- $\nabla f(a) \in \mathbb{R}^n$ zeigt in Richtung des steilsten Anstiegs von f im Punkt a, d.h.: $\frac{\partial f}{\partial v}(a)$ wird für $v = \frac{\nabla f(a)}{\|\nabla f(a)\|}$ am größten.
- Ist $D \subseteq \mathbb{R}^2$, so steht $\nabla f(a)$ senkrecht auf der Niveaulinie $N_{f(a)}(f) = \{x \in D \mid f(x) = f(a)\}$

Beweis

Beweis. $\frac{\partial f}{\partial v}(a) = f'(a) \cdot v = (\nabla f(a) \mid v) = \cos\alpha \cdot \|\nabla f(a)\|$, $\alpha \in [0, 2\pi)$ der Winkel, der von $\nabla f(a)$ und v eingeschlossen wird.

(a) $\cos\alpha$ (und somit $\frac{\partial f}{\partial v}(a)$) maximal für $v = \frac{\nabla f(a)}{\|\nabla f(a)\|}$

(b) Sei $v \in \mathbb{R}^2$, $\|v\| = 1$, sodass $(\partial f(a) \mid v) = 0 \implies \frac{\partial f}{\partial v}(a) = 0$, d.h. in Richtung v weißt f keine Steigung auf im Punkt a. Somit zeigt v in Richtung der Niveaulinie $N_{f(a)}(f)$

Q.E.D.

3.12 Satz von Schwarz

3.12.1 Stetige Differenzierbarkeit

$D \subseteq \mathbb{R}$ offen, $f : D \to \mathbb{R}$.

- f heißt stetig differenzierbar ($f \in \mathcal{C}^1(D)$), wenn f in jedem Punkt von D partiell differenzierbar ist und alle $\frac{\partial f}{\partial x_i}$ $(i \in \{1, ..., n\})$ auf D stetig sind
- f heißt 2-mal stetig differezierbar ($f \in \mathcal{C}^2(D)$), wenn $f \in \mathcal{C}^1(D)$ und alle $\frac{\partial f}{\partial x_j}$ $(j \in \{1, ..., n\})$ $\in \mathcal{C}^1(D)$. Die partielle Ableitung von $\frac{\partial f}{\partial x_j}$ nach x_k wird mit $\frac{\partial^2 f}{\partial x_2 \partial x_j}$ bezeichnet (partielle Ableitung zweiter Ordnung). Für $k = j$ schreibt man kurz $\frac{\partial^2 f}{\partial x_j^2}$.
- Analog ist f s-mal stetig differenzierbar ($f \in \mathcal{C}^s(D)$), wenn alle partiellen Ableitungen der Ordnung s $\frac{\partial^s f}{\partial x_{j_s} \dots \partial x_{j_1}}$ existieren und stetig sind.

Gleiches gilt auch für vektorwertige Funktionen.

Beispiel

$f : \mathbb{R}^2 \to \mathbb{R}$, $f(x,y) = 3y + xy^2$
$\frac{\partial f}{\partial x}(x,y) = y^2$ und $\frac{\partial f}{\partial y}(x,y) = 3 + 2xy$.
Dann $\frac{\partial^2 f}{\partial x^2}(x,y) = 0$, $\frac{\partial^2 f}{\partial y \partial x}(x,y) = 2y = \frac{\partial^2 f}{\partial x \partial y}(x,y)$ sowie $\frac{\partial^2 f}{\partial y^2}(x,y) = 2x$.

3.12.2 Satz

$D \subseteq \mathbb{R}^n$ offen, $f : D \to \mathbb{R} \in \mathcal{C}^2(D)$

$\implies \frac{\partial^2 f}{\partial x_k \partial x_j} = \frac{\partial^2 f}{\partial x_j \partial x_k} \quad \forall j, k \in \{1, ..., n\}$

Beweis

Beweis. Es genügt, die Behauptung für $D \in \mathbb{R}^2$ zu beweisen.

Sei $a = \begin{pmatrix} a_1 \\ a_2 \end{pmatrix} \in D$.

Zu zeigen: $\frac{\partial^2 f}{\partial x \partial y}(a) = \frac{\partial^2 f}{\partial y \partial x}(a)$.

Sei $\delta > 0$ mit $K_\delta(a) \subseteq D$.

$\implies \exists \epsilon > 0, 0 < k, k < \epsilon$, sodass $(a_1 + k, a_2 + k)^\top \in K_\delta(a)$.

(a) Sei $\varphi : [a_1, a_1 + h] \to \mathbb{R}$, $\varphi(t) = f(t, a_2 + k) - f(t, a_2)$.

$\implies \exists \xi_1 \in (a_1, a_1 + h) : \varphi(a_1 + h) - \varphi(a_1) = h \cdot \varphi'(\xi_1)$

Setze

$$\begin{aligned} F(h,k) &:= \overbrace{f(a_1 + h, a_2 + k) - f(a_1 + h, a_2)}^{\varphi(a_1+h)} - \overbrace{f(a_1, a_2 + k) + f(a_1, a_2)}^{\varphi(a_1)} \\ &= h \cdot \varphi'(\xi_1) \\ &= h \Bigg[\underbrace{\frac{\partial f}{\partial x}(\xi_1, a_2 + k) - \frac{\partial f}{\partial x}(\xi_1, a_2)}_{= \frac{\partial^2 f}{\partial y \partial x}(\xi_1, \vartheta_1) \cdot k \text{ für ein } \vartheta_1 \in (a_2, a_2 + k)} \Bigg] \\ &\implies F(h,k) = h \cdot k \frac{\partial^2 f}{\partial y \partial x}(\xi_1, \vartheta_1) \end{aligned}$$

(b) Analog erhält man für $\psi(t) := f(a_1 + h, t) = f(a_1, t)$, dass $F(h,k) = \psi(a_2 + k) - \psi(a_2)$ und $F(h,k) = h \cdot k \frac{\partial^2 f}{\partial x \partial y}(\xi_2, \vartheta_2)$ für $\xi_2 \in (a_1, a_1 + h)$, $\vartheta \in (a_2, a_2 + k)$.

(c) Insgesamt folgt, da $h, k \neq 0$: $\frac{\partial^2 f}{\partial y \partial x}(\xi_1, \vartheta_1) = \frac{\partial^2 f}{\partial x \partial y}(\xi_2, \vartheta_2)$

$\xrightarrow{h,k \to 0} \frac{\partial^2 f}{\partial y \partial x}(a_1, a_2)$, da $f \in \mathcal{C}^2(D)$.

Q.E.D.

Beispiel

Ist für folgende Funktion nicht erfüllt:

$$f(x,y) = \begin{cases} 0 & (x,y) = (0,0) \\ \frac{x^3 y - x y^3}{x^2 + y^2} & \text{sonst} \end{cases}$$

3.13 Satz von Taylor

Sei $I \subseteq \mathbb{R}$ ein Intervall, $x_0 \in I$, $f : I \to \mathbb{R}$ $(k+1)$-mal stetig differenzierbar, $k \in \mathbb{N}_0$. Dann git die folgende Taylorentwicklung um x_0 für ein ξ zwischen x und x_0:

$f(x) = T_k(x) + R_k(x)$ mit $T_k(x) = \sum_{j=0}^{k} \frac{f^{(j)}(x_0)}{j!}(x - x_0)^j$ sowie $R_k(x) = \frac{f^{(k+1)}(\xi)}{(k+1)!}(x - x_0)^{x+1}$ (Restglied nach Lagrange)

Bemerkung

Die Taylorreihe $T(x) := \sum_{j=0}^{\infty} \frac{f^{(j)}(x_0)}{j!}(x - x_0)^j$ konvergiert gegen $f(x) \iff \lim_{k\to\infty} R_k(x) = 0$. (Vorausgesetzt f ist unendlich oft differenzierbar.)

Beispiel

Berechne $\sin(1)$ mit Fehlerdifferenz $< 10^{-3}$!.
Entwickle dazu $f(x) = \sin(x)$ um $x_0 = 0$. Suche $k \in \mathbb{N}$, sodass

$$|R_k(1)| = \frac{|f^{(k+1)}(\xi)|}{(k+1)!}|1-0|^{k+1} < \frac{1}{1000}, \quad \xi \text{ zwischen } 0 \text{ und } 1.$$

$f(x) = \sin x,\ f'(x) = \cos x,\ f''(x) = -\sin x, f'''(x) = -f'(x), f^{(4)}(x) = f(x)$
$\implies f^{(2n)}(x) = (-1)^n \sin(x)$ und $f^{(2n+1)}(x) = (-1)^n \cos(x)$ für $n \geq 0$
$\implies |R_k(1)| \leq \frac{1}{(k+1)!} < \frac{1}{1000}$
$\iff (k+1)! > 1000 \iff k \geq 6$

Für $k = 6$ ist

$$\begin{aligned}\sin(1) \approx T_6(1) &= \frac{\sin 0}{0!}(1-0)^0 + \frac{\cos 0}{1!}(1-0)^1 - \frac{\sin 0}{2!}(1-0)^2 \pm \dots \pm \frac{\sin 0}{6!}(1-0)^6 \\ &= 0 + 1 + 0 - \frac{1}{6} + 0 + \frac{1}{120} + 0 = \frac{101}{120} \\ &\approx 0.841\end{aligned}$$

3.13.1 Multiindex

$p := (p_1, \dots, p_m) \in \mathbb{N}_0^m$ heißt Multiindex.

$|p| := p_1 + \dots + p_m$ Ordnung von p.

$p! := (p_1!) \cdot \dots \cdot (p_m!)$

Für $x \in \mathbb{R}^m$, $x = (x_1, \dots, x_m)^\top$ sei $x^P := x_1^{P_1} \cdot \dots \cdot x_m^{P_m}$.

Ist f k-mal stetig differenzierbar, so sei $\partial^P f := \frac{\partial^{|P|} f}{\partial x_1^{P_1} \dots \partial x_m^{P_m}}$.

Beispiel

- $P = (0, \dots, 0) \implies \partial^P f = f$
- $P = (1, 0, \dots, 0) \implies \partial^P f = \frac{\partial f}{\partial x_1}$
- $P = (1, 2, 0, \dots, 0) \implies \partial^P f = \frac{\partial^3 f}{\partial x_1 \partial x_2^2}$

3.13.2 Taylorpolynome

Sei $D \subseteq \mathbb{R}^n$ offen, $a \in D$, $f : D \to \mathbb{R}$ k-mal stetig differenzierbar.

$T_k : \mathbb{R}^n \to \mathbb{R}$, $T_k(x) = \sum_{|P|\leq k} \frac{\partial^P f(a)}{P!}(x-a)^P$ heißt k-tes Taylorpolynom f in a. $R_k(x) = f(x) - T_k(x)$ heißt k-tes Restglied von f in a.

3.13.3 Hessematrix

Sei $D \subseteq \mathbb{R}^n$ offen, $f : D \to \mathbb{R}$ 2-mal stetig differenzierbar, $a \in D$. Dann ist

- $T_1(x) = \underbrace{f(a)}_{|p|=0} + \underbrace{\sum_{i=1}^{n} \frac{\partial f}{\partial x_i}(x_i - a_i)}_{|p|=1, p=(--\underbrace{1}_{i}--)} = f(a) + f'(a)(x-a)$ lineare Approximation in a
- $T_2(x) = f(a) + f'(a)(x-a) + \frac{1}{2!}\sum_{i,j=1}^{n} \frac{\partial^2 f}{\partial x_i \partial x_j}(a)(x_i - a_i)(x_j - a_j)$ und $H_f(a) := (a_{ij}) \in \mathcal{M}_n(\mathbb{R})$, $a_{ij} = \frac{\partial^2 f}{\partial x_i \partial x_j}(a)$ ist die sogenannte Hessematrix von f in a. Damit erhält man

$$T_2(x) f(a) + f'(a)(x-a) + \frac{1}{2}(x-a)^\top H_f(a)(x-a)$$

Beispiel

$f : \mathbb{R}^2 \to \mathbb{R}$, $f(x,y) = e^x = xy$
$f'(x,y) = (e^x + y, x)$.
$H_f(x,y) = \begin{pmatrix} \frac{\partial^2 f}{\partial x^2}(x,y) & \frac{\partial^2 f}{\partial x \partial y}(x,y) \\ \frac{\partial^2 f}{\partial y \partial x}(x,y) & \frac{\partial^2 f}{\partial y^2}(x,y) \end{pmatrix} = \begin{pmatrix} e^x & 1 \\ 1 & 0 \end{pmatrix}$.
Sei $a = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$.

$$\begin{aligned} \Longrightarrow T_2(x,y) &= f(0,1) + f'(0,1)\begin{pmatrix} x-0 \\ y-1 \end{pmatrix} + \frac{1}{2}(x-0, y-1) H_f(0,1)\begin{pmatrix} x-0 \\ y-1 \end{pmatrix} \\ &= 1 + (2,0)\begin{pmatrix} x \\ y-1 \end{pmatrix} + \frac{1}{2}(x, y-1)\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} x \\ y-1 \end{pmatrix} \\ &= 1 + 2x + \frac{12}{(}x^2 + 2(y-1)x) \\ &= 1 + x + \frac{1}{2}x^2 + xy \end{aligned}$$

3.14 Satz von Taylor für mehrdimensionale Funktionen

Sei $D \subseteq \mathbb{R}^n$ offen, $f \in \mathcal{C}^{k+1}(D, \mathbb{R})$ und seien $a, x \in D$, sodass $S(a,x) = \{a + t(x-a) \mid t \in (0,1)\} \subseteq D$. Dann existiert ein $\xi \in S(a,x)$ mit

$$R_k(x) = \sum_{|p|=k+1} \frac{\partial^P f(\xi)}{P!}(x-a)^P.$$

Lagrange-Form des Restgliedes

Beweis

Beweis. Sei $v = x - a$. Dann ist $S(a,x) = \{a + tv \mid t \in (0,1)\}$.

Setze $\varphi : [0,1] \to \mathbb{R}$, $\varphi(t) := f(a+tv)$.

$$\begin{aligned}
\implies \varphi'(t) &= f'(a+tv)\cdot v \\
&= \sum_{i=1}^{n} \frac{\partial f}{\partial x_i}(a+tv)v_i \\
&= \sum_{|P|=1} \partial^P f(a+tv)v^P. \\
\varphi''(t) &= \sum_{i,j=1}^{n} \frac{\partial^2 f}{\partial x_j \partial x_i}(a+tv)v_i v_j \\
&= 2\sum_{|p|=2} \frac{\partial^P f(a+tv)}{P!}v^P \\
&\vdots \\
\varphi^{(k+1)}(t) &= \sum_{i_1,\dots,i_{k+1}=1}^{n} \frac{\partial^{k+1} f}{\partial x_{i_1}\dots\partial x_{i_{k+1}}}(a+tv)v_{i_1}\dots v_{i_{k+1}} \\
&= (k+1)!\sum_{|P|=k+1} \frac{\partial^P f(a+tv)}{P!}v^P
\end{aligned}$$

$\implies \exists \vartheta \in (0,1)$ mit

$$\begin{aligned}
R_k^\varphi(1) &= \frac{\varphi^{(k+1)}(\vartheta)}{(k+1)!}(1-0)^{k+1} \\
&= \frac{\varphi^{(k+1)}(\vartheta)}{(k+1)!}
\end{aligned}$$

Sei $\xi := \varphi(\vartheta) = a + \vartheta v \in S(a,x)$

$$\begin{aligned}
\implies R_k^\varphi(1) &= \sum_{|p|=k+1} \frac{\partial^P f(\overbrace{a+\vartheta v}^{\xi})}{P!}\underbrace{v^P}_{=(x-a)^P} \\
&= R_k(x)
\end{aligned}$$

Es ist

$$\begin{aligned}
T_k^\varphi(1) &= \sum_{i=0}^{k} \frac{\varphi^{(i)}(0)}{i!}(1-0)^i \\
&= \sum_{i=0}^{k}\sum_{|P|=i} \frac{\partial^P f(a)}{P!}v^P \\
&= T_k(x)
\end{aligned}$$

$$\implies \varphi(1) = R_k^\varphi(1) + T_k^\varphi(1) \iff f(\underbrace{a+v}_{=x}) = R_k(x) + T_k(x)$$ Q.E.D.

3.15 Lokale Extrema

Sei $D \subseteq \mathbb{R}^n$ (nicht notwendigerweise offen), $f : D \to \mathbb{R}$, $a \in D$.

- a heißt Stelle eines lokalen Maximums/Minimums g.d.w.

$$\exists \varepsilon > 0 : f(a) \geq / \leq f(x) \quad \forall x \in K_\epsilon(a) \cup D.$$

- a heißt Stelle eines globalen Maximums/Minimums auf D g.d.w.

$$f(a) \geq / \leq f(x) \quad \forall x \in D.$$

3.16 Notwendige Bedingung für lokale Extrema

Sei $D \subseteq \mathbb{R}^n$ offen, $f : D \to \mathbb{R}$. Ist $a \in D$ Stelle eines lokalen Extremums und existiert in a die partielle Ableitung von f, so ist $\nabla f(a) = 0$.

Beweis

Beweis. Sei a lokale Extremstelle und $K_\epsilon(a) \subseteq D$.
$\Longrightarrow \varphi : (-\varepsilon, \varepsilon) \to \mathbb{R},\ \varphi(t) = f(a + tv),\ v = e_k$, besitzt in $t = 0$ Extremum.
$\underbrace{\Longrightarrow}_{\text{Mathe 1}} \varphi'(0) = 0$
$\Longleftrightarrow \lim_{k\to 0} \frac{\varphi(h)-\varphi(0)}{h} = \lim_{h\to 0} \frac{f(a+he_k)-f(a)}{h} = 0 = \frac{\partial f}{\partial x_k}(a)$ Q.E.D.

3.17 Hinreichende Bedingung für lokale Extrema

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

Dann:

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

Beweis

Beweis. (a) $\frac{\partial^2 f}{\partial x_i \partial x_j}$ sind alle stetig auf D, d.h. $H_f(x)$ stetig. Man kann aufgrund der Stetigkeit zeigen:

$$H_f(a) \text{ positiv definit} \Longrightarrow \exists \epsilon > 0 : H_f(x) \text{ positiv definit} \forall x \in K_\epsilon(a).$$

Für $x \in K_\epsilon(a)$ gilt:

$$\exists \xi \in S(a, x) = \{a + t(x - a) \mid t \in (0, 1)\} \subseteq K_\epsilon(a) :$$

$$\begin{aligned} f(x) &= T_1(x) + R_1(x) \\ &= f(a) + \underbrace{f'(a)(x-a)}_{=0} + \frac{1}{2} \underbrace{(x-a)^\top H_f(\xi)(x-a)}_{>0,\text{ falls } H_f(a) \text{ pos. def.}} \\ &\geq f(a) \end{aligned}$$

$\Longrightarrow$ a Stelle eines lokalen Minimums.

(b) Analog.
(c) Verwendet man als Definition für Sattelpunkte.

Q.E.D.

3.18 Kriterium von Sylvester

Zuvor wurde die Definitheit von $H_f(a)$ untersucht. Die Definitheit kann mit den Eigenwerten festgestellt werden (siehe Mathe 2).

Für positive/negative Definitheit gibt es auch das Kriterium von Sylvester (sehr einfach zu prüfen):

Sei $A \in \mathcal{M}_n(\mathbb{R})$, $A = (a_{ij})_{i,j=1}^n$. Dann heißt $A_k := (a_{ij})_{i,j=1}^k \in \mathcal{M}_k(\mathbb{R})$ k-te Haupminor von A, $k \leq n$.

Beispiel

$$A = \begin{pmatrix} 1 & 2 & -1 \\ 0 & 1 & 1 \\ 1 & -1 & 2 \end{pmatrix}$$

$\implies A_1 = (1),\ A_2 = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix},\ A_3 = A.$

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 $\iff \det(A_k) \begin{cases} < 0 & k \text{ ungerade} \\ > 0 & k \text{ gerade} \end{cases}$

Bemerkung

Über Semi-/Indefinitheit kann mit Sylvester keine Aussage gemacht werden! Speziell für 2×2-Matrizen gilt jedoch:

$$A \in \mathcal{M}_2(\mathbb{R}) \text{ indefinit } \iff \det(A) < 0.$$

Beispiel

- $f(x,y) = x^2 + y^2 + xy + 1, \quad f : \mathbb{R}^2 \to \mathbb{R}$. Es gilt:

  $$f'(x,y) = \big(2x + y, 2y + x\big) = (0,0) \iff \begin{cases} 2x + y = 0 \\ 2y + x = 0 \end{cases} \iff x = y = 0.$$

  Demnach gilt $H_f(x,y) = \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix} = H_f(0,0)$. Durch Sylvester folgt mit $\det(A_1) = 2$, $\det(A_2) = 3$ positive Definitheit. $\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$ ist damit lokale Minimalstelle und $f(0,0) = 1$ das lokale Minimum.
- TODO?
- TU DU!

3.19 Implizite Funktionen

Problemstellung:

- Niveaulinien einer Funktion $h : \mathbb{R}^2 \to \mathbb{R}$: TODO Graph. Frage: Kann $N_c(h)$ lokal um $\begin{pmatrix} a \\ b \end{pmatrix} \in N_c(h)$ als Funktion $y = f(x)$ dargestellt werden, d.h. $h(x, f(x)) - c = 0$?
  - ϵ, δ müssen klein genug gewählt werden, damit einem x-Wert nur ein y-Wert zugeordnet wird.
  - Für $\begin{pmatrix} a' \\ b' \end{pmatrix}$A gibt es keine ϵ,$\delta > 0$, sodass jedem $x \in K_\delta(a')$ genau ein $y \in K_\epsilon(b')$ zugeordnet werden kann. Daher Forderung: $\frac{\partial h}{\partial y}(a', b') \neq 0$.
- Anders formuliert: Ist $F(x, y) := h(x, y) - c = 0$ in einer Umgebung von x nach y auflösbar? Z.B.:
  - $F(x, y) = x^2 + y^2 + 1 = 0$ nicht lösbar, da $F(x, y) > 0$. Daher Forderung: $\exists a, b \in \mathbb{R} : F(a, b) = 0$.
  - $F(x, y) = x^2 + y^2 - 1 = 0, \quad x, y \in \mathbb{R}$
    $\iff y^2 = 1 - x^2$
    $\implies f_1(x) = \sqrt{1 - x^2} \wedge f_2(x) = -\sqrt{1 - x^2} \quad \text{für} x \in (-1, 1)$
    $f_1, f_2 \in \varphi^1(-1, 1)$ Lösungsfaktoren für $x \neq \pm 1$.
- Allgemein: Sei $x \in \mathbb{R}^P$, $y \in \mathbb{R}^a$ und $\begin{pmatrix} x \\ y \end{pmatrix} := (x_1, ..., x_p, y_1, ..., y_q)^\top$, $F : \mathbb{R}^p \times \mathbb{R}^q \to \mathbb{R}^q, \quad F = \begin{pmatrix} F_1 \\ \vdots \\ F_q \end{pmatrix}$, $F(x, y) := F(x_1, ..., x_p, y_1, ..., y_q)$.
  $F(x, y) = 0$ auf $G \subseteq \mathbb{R}^p$ nach y auflösen heißt, $f : G \subseteq \mathbb{R}^p \to \mathbb{R}^q$ zu finden, sodass $F(x, f(x)) = 0 \quad \forall x \in G$.
  D.h.:
  - $F_i(x_1, ..., x_p, y_1, ..., y_q) = 0 \quad \forall i \in \{1, ..., q\}$ auf G nach $y_q, ..., y_q$ auflösen, also $f_i : G \to \mathbb{R}$ best. mit $F_i(x_1, ..., x_p, f_1(x_1, ..., x_p), ..., f_q(x_1, ..., x_p)) = 0 \quad \forall i \in \{1, ..., q\}$.
- Falls F in c) partiell differenzierbar, so sei

$$\frac{\partial F}{\partial x} := \begin{pmatrix} \frac{\partial F_1}{\partial x_1} & \cdots & \frac{\partial F_1}{\partial x_p} \\ \vdots & & \vdots \\ \frac{\partial F_q}{\partial x_1} & \cdots & \frac{\partial F_q}{\partial x_p} \end{pmatrix} \in \mathcal{M}_{q,p}(\mathbb{R})$$

$$\frac{\partial F}{\partial x} := \begin{pmatrix} \frac{\partial F_1}{\partial y_1} & \cdots & \frac{\partial F_1}{\partial y_q} \\ \vdots & & \vdots \\ \frac{\partial F_q}{\partial y_1} & \cdots & \frac{\partial F_q}{\partial y_q} \end{pmatrix} \in \mathcal{M}_q(\mathbb{R})$$

3.20 Hauptsatz über implizite Funktionen

Seien $G \subseteq \mathbb{R}^P$, $H \subseteq \mathbb{R}^q$ nichtleer und offen, $F : G \times H \to \mathbb{R}^q$ stetig differenzierbar. Seien $a \in G$, $b \in H$ mit $F(a, b) = 0$ und $\frac{\partial F}{\partial y}(a, b)$ invertierbar.

Dann gibt es $\epsilon, \delta > 0$ und genau eine stetige Funktion $f : K_\delta(a) \to K_\epsilon(b)$ mit

1. $f(a) = b$ und $F(x, f(x)) = 0 \quad \forall x \in K_\delta(a)$
2. δ kann so gewählt werden, dass $f \in \varphi^1(K_\delta(a))$ und

$$f'(x) = -\left(\frac{\partial F}{\partial y}(x, f(x))\right)^{-1} \cdot \frac{\partial F}{\partial x}(x, f(x)) \forall x \in K_\delta(a).$$

Beweis

TODO. ODER NICHT. MIR DOCH EGAL.

Bemerkung

Da $h_x(y)$ im Beweis der Kontraktion, kann man $f : K_\delta(a) \to K_\epsilon(b)$ annähern durch $(f_n)_{n\geq 0},\ f_n : K_\delta(a) \to \mathbb{R}^d$
$f_0(x) := b \quad \forall x \in K_\delta(a)$
$f_{n+1}(x) := h_x(f_n(x)) = f_n(x) - A^{-1}F(x, f_n(x))$
Es gilt ausserdem $\forall x \in K_\delta(a)$:

$$\begin{aligned}\|f_n(x) - f(x)\| &\leq \frac{q^n}{1-q}\|f_1(x) - f_0(x)\| \\ &= \left(\frac{1}{2}\right)^{n-1}\|f_1(x) - b\|\end{aligned}$$

$\Longrightarrow f_n \to f$ gleichmäßig.

Beispiel

- $F(x,y) = x^3 + y^3 + x - y,\ \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$
  $A = \frac{\partial F}{\partial y}(0,0) = (3y^2 - 1)(0,0) = -1 \neq 0$
  $\Longrightarrow A^{-1} = -1$, d.h. A invertierbar
  $\Longrightarrow \exists \epsilon, \delta > 0$ und $f : K_\delta(0) \to K_\epsilon(0) : F(x, f(x)) = 0$
- Annäherung an f (siehe Bemerkung):

$$\begin{aligned}f_0(x) &= 0 = b \\ f_1(x) &= f_0(x) - A^{-1} \cdot F(x, f_0(x)) \\ &= 0 + 1 \cdot (x^3 + x) = x^3 + x \\ f_2(x) &= (x^3 + x) + 1 \cdot F(x, x^3 + x) \\ &= x^3 + x + x^3 + (x^3 + x)^3 + x - x^3 - x \\ &= x^9 + 3x^7 + 3x^5 + 2x^3 + x\end{aligned}$$

- Ableitung in $x = 0$:

$$f'(0) = -\left(\underbrace{\frac{\partial F}{\partial y}(0,0)}_{=-1}\right)^{-1} \cdot \underbrace{\frac{\partial F}{\partial x}(0,0)}_{=1} = 1$$

3.21 Lokale Umkehrbarkeit

3.21.1 Diffeomorphismus

$U, V \subseteq \mathbb{R}^n$ offen, $f : U \to V$.

- f heißt Diffeomorphismus $:\Longleftrightarrow$
  - f bijektiv und differenzierbar
  - $f^{-1} : V \to U$ differenzierbar
- f heißt φ^k-Diffeomorphismus $:\Longleftrightarrow$
  - f Diffeomorphismus
  - f, f^{-1} k-mal stetig differenzierbar

Bemerkung

$f : \mathbb{R} \to \mathbb{R}$ Diffeomorphismus.
$\implies (f^{-1}(y))' = \frac{1}{f'(x)}, \quad x = f^{-1}(y)$

Beispiel

$(\ln y)' = \frac{1}{(e^x)'} = \frac{1}{e^x} = \frac{1}{y}, \quad y > 0$

3.21.2 Ableitung der Umkehrfunktion

$f : U \subseteq \mathbb{R}^n \to V$ Diffeomorphismus $\implies$ $f'(x)$ invertierbar und

$$\forall y \in V : (f^{-1}(y))' = (f'(x))^{-1}, \quad x = f^{-1}(y)$$

Beweis

Beweis. $f^{-1} \circ f : U \to U,\ f^{-1} \circ f(x) = x$
$\implies E_n = (f^{-1} \circ f)'(x) = (f^{-1}(f(x))' \cdot f'(x)$
$\iff (f^{-1}(y))' = (f'(x))^{-1},\ x = f^{-1}(y)$ Q.E.D.

Bemerkung

Sei $f : D \subseteq \mathbb{R}^n \to \mathbb{R}^n$ differenzierbar, D offen.
Für $n = 1$: Falls $f'(x) > / < 0$ auf einem Intervall (a, b), so ist f injektiv und umkehrbar auf (a, b).
Für $n > 1$ gilt eine ähnliche Aussage nur eingeschränkt.

Beispiel

$f : \mathbb{R}^2 \to \mathbb{R}^2,\ f(x, y) = e^x \begin{pmatrix} \cos y \\ \sin y \end{pmatrix}$
$\implies f'(x, y) = e^x \begin{pmatrix} \cos y & -\sin y \\ \sin y & \cos y \end{pmatrix}$
$\implies \det f'(x, y) = e^x > 0 \quad \forall x, y \in \mathbb{R}$
Aber f ist nicht injektiv:

$$f(x, y + k \cdot 2\pi) = f(x, y) \quad \forall k \in \mathbb{Z}$$

Die Umkehrbarkeit gilt jedoch lokal - Überleitung!

3.21.3 Lokale Umkehrbarkeit

Sei $f \in \varphi^1(D, \mathbb{R}^n)$, $D \subseteq \mathbb{R}^n$ offen, $x_0 \in D$. Falls $f'(x_0)$ invertierbar, so gibt es offene Umgebungen U von x_0, V von $y_0 = f(x_0)$ mit $f(U) = V$, sodass $f : U \to V$ φ^1-Diffeomorphismus.

Beweis

TODO: Ojemine

3.21.4 Korollar

Sei $f \in \varphi^1(D, f(D))$ bijektiv und $D, f(D) \subseteq \mathbb{R}^n$ offen.

Dann sind äquivalent:

1. f ist φ^1-Diffeomorphismus
2. $f'(x)$ invertierbar $\forall x \in D$

Beweis

Beweis.

- $1 \implies 2$: wegen Ableitung der Umkehrfunktion
- $2 \implies 1$: f bijektiv $\implies \exists f^{-1} : f(D) \to D$.
  Zu zeigen ist: f^{-1} stetig differenzierbar.
  Sei $x_0 \in D \implies \exists g : V \to U : g = f^{-1}|_v$, wobei $U \subseteq D$, $V \subseteq f(D)$ Umgebungen von x_0 bzw. $y_0 = f(x_0)$. $\implies f^{-1}$ stetig differenzierbar in y_0.
  x_0 beliebig $\implies f^{-1}$ stetig differenzierbar auf $f(d)$.

Q.E.D.

3.21.5 Satz über offene Abbildungen

Sei $f \in \varphi^1(D, \mathbb{R}^n)$, $D \subseteq \mathbb{R}^n$ offen, sodass $f'(x)$ invertierbar $\forall x \in D$. $\implies W := f(D) \subseteq \mathbb{R}^n$ offen.

Insbesondere: f injektiv auf $D \implies f : D \to W$ φ^1-Diffeomorphismus.

Beweis

Beweis. Sei $y_0 \in W$.
$\implies \exists x_0 \in D : f(x_0) = y_0$
$\implies f'(x_0)$ invertierbar
$\implies \exists$ offene Umgebung U von x_0, V von y_0 mit $U \subseteq D$, $V \subseteq W$, sodass $f : U \to V$ φ^{-1}-Diffeomorphismus, d.h. bijektiv
$\implies \exists \epsilon > 0 : K_\epsilon(y_0) \subseteq V \subseteq W$
$\implies W$ offen.
Falls f injektiv, so ist $f : D \to W$ bijektiv. $\implies f$ φ^1-Diffeomorphismus. Q.E.D.

Beispiel

TODO. Wer braucht schon Beispiele? Alles trivial.

3.22 Extrema unter Nebenbedingungen

Beispiel

TODO.

Gegeben: $f : D \subseteq \mathbb{R}^n \to \mathbb{R}$ und $g : D \subseteq \mathbb{R}^n \to \mathbb{R}^q \quad q < n$.

f besitzt in $x_0 \in D$ ein lokales Maximum/Minimum unter der Nebenbedingung $g(x) = 0 :\iff$

- $x_0 \in N := \{x \in D \mid g(x) = 0\}$
- $\exists$ offene Umgebung U von x_0 mit $f(x) \leq / \geq f(x_0) \quad \forall x \in U \cap N$

3.23 Multiplikatorenregel v. Lagrange

Sei $D \subseteq \mathbb{R}^n$ offen, $f : D \to \mathbb{R}$, $g : D \to \mathbb{R}^q$ $(q < n)$ beide stetig differenzierbar. f besitze in $x_0 \in D$ ein lokales Extremum unter der Nebenbedingung $g(x) = 0$.

Dann: Falls $g(g'(x_0)) = q$, so gibt es q Zahlen $\lambda_1, ..., \lambda_q \in \mathbb{R}$ (Lagrange-Multiplikatoren), sodass

$$f'(x_0) + \sum_{j=1}^{q} \lambda_j q_j'(x_0) = 0$$