

1. NAIVE MENGENLEHRE

1.1 KARDINALZAHLEN:

DEF., SCHRÖDER BERNSTEIN, EINFACHE BEISPIELE

DEF: (•) Zwei Mengen A, B sind gleich groß, $|A| = |B|$, wenn
 $\exists f: A \rightarrow B$ bijektiv. $|A|$ wird Kardinalität oder
Kardinalzahl von A genannt.

(•) A ist kleiner (gleich) B , $|A| \leq |B|$, wenn $\exists f: A \rightarrow B$ inj.

Bsp: (•) $|\mathbb{N}| = |\mathbb{N} \setminus \{0\}|$ mit $f: n \mapsto n+1$

(•) $|\mathbb{N}| = |2\mathbb{N}|$ für $2\mathbb{N} = \{2 \cdot n : n \in \mathbb{N}\}$, Bew: \checkmark

(•) Allg.: Wenn $A \subseteq \mathbb{N}$ unendl., dann $|A| = |\mathbb{N}|$, Bew: \checkmark

Wir sehen: anders als bei endlichen Mg kann eine echte TM einer
unendlichen Menge gleich groß wie die ursprüngliche Menge sein.

Hilberts Hotel: unendlich viele Zimmer mit Nummer $0, 1, 2, \dots$

alle Zimmer belegt. Neuer Guest kommt in 0 , Guest aus n wird
nach $n+1$ verlegt.

Es gilt: \leq trans. und reflexiv

Bew: $|A| \leq |B|$ mit $f: A \rightarrow B$ inj., $|B| \leq |C|$ mit g , dann

$|A| \leq |C|$ mit $g \circ f: A \rightarrow C$ inj.

$|A| \leq |A|$ mit id .

Satz (Schröder Bernstein): $|A| \leq |B|$ & $|B| \leq |A| \rightarrow |A| = |B|$

Bew: \checkmark (Bem: Dazu braucht man kein AC)

Bem: Ähnliche Sätze gelten manchmal für zusätzliche Strukturen:

$\mathbb{Z} \rightarrow \mathbb{B}$: Wenn $f: A \rightarrow B$, $g: B \rightarrow A$ beide Borel, inj, dann

gibt es Borel isom. $h: A \rightarrow B$

aber es gilt $\mathbb{Z} \rightarrow \mathbb{B}$ nicht: wenn $f: A \rightarrow B$ und

$g: B \rightarrow A$ beide inj, stetig, dann A, B homöomorph

(-) $|2^{\mathbb{N}}| = |\mathbb{N}^{\mathbb{N}}|$ Mit S.B. $|2^{\mathbb{N}}| \leq |\mathbb{N}^{\mathbb{N}}|$ klar

Wissen schon: $\mathbb{N} \cong \mathbb{N} \times \mathbb{N}$

Dann gilt: $2^{\mathbb{N}} \cong 2^{\mathbb{N} \times \mathbb{N}} = (2^{\mathbb{N}})^{\mathbb{N}}$, und

$|2^{\mathbb{N}}| \geq |\mathbb{N}|$, daher $|2^{\mathbb{N}}| = |(2^{\mathbb{N}})^{\mathbb{N}}| \geq |\mathbb{N}^{\mathbb{N}}|$

In anderer Schreibweise: Sei $\varphi: \mathbb{N} \rightarrow \mathbb{N} \times \mathbb{N}$ bij.

Sei $a \in \mathbb{N}^{\mathbb{N}}$. Def $f(a) \in 2^{\mathbb{N}}$ durch $f(a)(\varphi(n,m)) = 1$ gdw $a(n) = m$.

(-) $|2^{\mathbb{N}}| = |10^{\mathbb{N}}|$ (weil $|2^{\mathbb{N}}| \leq |10^{\mathbb{N}}| \leq |\mathbb{N}^{\mathbb{N}}| = |2^{\mathbb{N}}|$)

(-) $|\mathbb{R}| = |(0,1)|$ \bar{U}

(-) $|\mathbb{R}| = |2^{\mathbb{N}}|$

(a) Def $f: 2^{\mathbb{N}} \rightarrow \mathbb{R}$ durch
 $(a(0), a(1), a(2), \dots) \in 2^{\mathbb{N}} \mapsto \sum_{n=0}^{\infty} \frac{a(n)}{2^n}$

(worum nicht $(2^n \cdot \frac{1}{2^n})$)

\bar{U} : f bij

(b) Def $g: (0,1) \rightarrow 10^{\mathbb{N}}$ inj. durch Dezimaldarst.

ZB $r \mapsto 0,8735\dots$ (oder Darst von $r \in (0,1)$,

entspricht Folge mit Einträgen aus $0, \dots, 9$)

Bem Abgesehen von Kardinalität (d.h. Bijektionen)

gibt es natürlich auch wichtige topolog. Äquivalenzen:

(i) $2^{\mathbb{N}}$ (mit der Produkttop.) ist homöomorph zur Cantormenge (die "kompakte 0-dimensionale Version" von \mathbb{R})

(ii) $\mathbb{N}^{\mathbb{N}}$ (mit der Prod. Top), auch Baire space genannt, ist homöomorph zu $\mathbb{R} \setminus \mathbb{Q}$, den irrationalen Zahlen. (Bem: Partialstrukturierung.)

($\mathbb{N}^{\mathbb{N}}$ ist eine "sehr nicht-lokal kompakte 0-dim Version" von \mathbb{R})

Weitere Bsp:

(.) $\mathbb{N}^{\omega} = \prod_p$ der endl. Folgen natürlicher Zahlen

$$|\mathbb{N}^{\omega}| = |\mathbb{N}| : f: (a_0, a_1, \dots, a_n) \mapsto 2^{a_0+1} \cdot \dots \cdot p_n^{a_n+1} \text{ inj.}$$

(.) $\mathbb{Q}[X]$ -- \prod_p der vet. Polynome.

$$|\mathbb{Q}[X]| = |\mathbb{N}| \quad \vec{v}$$

(.) Daraus folgt: Es gibt abzählbar viele algebraische Zahlen.



1.2 CANTORSCHER DIAGONALISIERUNG

Sind alle unendlichen \prod_p gleich groß?

Beh (Cantor): $|\mathbb{R}| \neq |\mathbb{N}|$

Wir schreiben $|A| < |B|$ für ($|A| \leq |B|$ und nicht $|B| \leq |A|$)

Es gilt also: $|\mathbb{N}| < |\mathbb{R}|$

Bew: Sonst $|\mathbb{R}| = |2^{\mathbb{N}}| = |\mathbb{N}|$, d.h. es gibt

surjektive $f: \mathbb{N} \rightarrow 2^{\mathbb{N}}$

$$f(0): (0, 1, 0, \dots, 0, \dots)$$

$$f(1): (1, 1, 1, \dots, 1, \dots)$$

\vdots

$$f(n): (0, 1, 1, \dots, 1, \dots)$$

Def $g(n) := 1 - f(n)(n) \quad g \in 2^{\mathbb{N}}$, d.h.

$g \neq f(n)$ für ein $n \in \mathbb{N}$. Dann $g(n) = 1 - f(n)(n)$

(Einfache Folgerung: Es gibt also nicht-algebraische reelle Zahlen)

Bem: Kontinuumshypothese (CH): Für jede

unendl TM A von \mathbb{R} gilt $|A| = |\mathbb{N}|$ oder $|A| = |\mathbb{R}|$

CH ist "unentscheidbar": Die üblichen Axiome der Mathematik (nämlich die ZFC Axiome) beweisen

weder CH noch \neg CH, Das ist das

"1. Hilbertsche Problem", gelöst von Gödel und Cohen.

$2^A \cong \Pi_{\mathcal{A}}$ die Fkt $A \rightarrow \{0,1\}$
 \cong \mathcal{A} Folgen indiziert mit A
 \cong Teilmengen von A ($\underline{\cup}$: char. Fkt.)

$\mathcal{P}(A)$... Potenzmenge von A , d.h. $\Pi_{\mathcal{A}}$ aller JM.
 $\mathcal{P}(A) \cong 2^A$ insbes. $|\mathcal{P}(A)| = |2^A|$

Satz (Cantor) : $|2^A| = |\mathcal{P}(A)| > |A|$

Bew: Wie vorher für $A = \mathbb{N}$: Sucht
 $f: A \rightarrow 2^A$ surj., $g(a) := 1 - f(a)(a) \notin$

Die Potenzmenge ist also immer größer als
 die Menge selbst. Insbesondere gibt es keine
 Allmenge $V = \{x: x=x\}$. Etwas genauer:
 Man kann nicht davon ausgehen dass
 sowohl die Allmenge V existiert und dass
 zugleich jede Menge eine Potenzmenge hat.
 Da die Allmenge keine mathematische
 Bedeutung hat, die Potenzmenge aber
 schon, wird das Potenzmengenaxiom in
 die axiomatische ZFC aufgenommen,
 das Allmengenaxiom aber nicht (es kann in
 ZFC widerlegt werden). Genauer klären
 kann man diese Fragen erst im Kapitel
 "axiomatische Mengenlehre".

Ein weiteres Bsp das "naive"
 Anwendung des Mengensilde-Operators
 $\{x: \varphi(x)\}$ zu Problemen führen kann:
 Russell Paradoxon $R = \{x: x \notin x\}$
 Denn $R \in R \Leftrightarrow R \notin R, \nexists$

1.3. ORDNUNGEN, AUSWAHLAXIOM

Naheliegende Frage: Ist $|\cdot| \leq |\cdot|$ eine lineare Ordnung? D.h.: gilt für alle Mengen A, B : $|A| \leq |B|$ oder $|B| \leq |A|$?

Antwort: Ja, verwendet AC:

Satz Auswahlaxiom, AC: Sei $I \neq \emptyset$ (Indexmenge) und $\forall i \in I$ X_i eine nichtleere Menge. Dann gibt es Fkt f mit $\text{Dom}(f) = I$ und $f(i) \in X_i$ für alle $i \in I$.

Äquivalent dazu (nur andere Formulierung):

Sei I, X_i wie oben. Dann $\prod_{i \in I} X_i \neq \emptyset$, d.h.: das kartesische Produkt nichtleerer M_j ist nichtleer.

"Bew": Wähle für jedes $i \in I$ ein $y_i \in X_i$, setze $f(i) := y_i$.

Das ist natürlich kein sehr überzeugender Bew. Woran werden sehen: In formaler Axiomatisierung der Mathematik ist AC ein Axiom, das nicht aus den anderen Axiomen folgt - ZF bezeichnet das Axiomensystem der Mathematik ohne AC; ZFC ist ZF mit dem zusätzlichen Axiom AC. Es gilt also: (-) Aus ZF kann man AC nicht ableiten
(-) Aus ZF kann man AC auch nicht widerlegen.

Bem: (.) Für endliches I "folgt" AC sehr wohl aus ZF (es gilt sogar ohne weitere Axiome, sondern ist Teil der Logik selbst).

(.) Dass alle X_i endlich sind nicht dagegen mit AC für endliche X_i (aber unendl. I) folgt nicht aus ZF.

(.) "countable choice", d.h. AC

eingeschränkt auf den Fall dass I abzählb. ist, folgt auch nicht aus ZF. Es hat viele der "allernotwendigsten" Folgerungen von AC (darunter Folgerungen die die meisten Mathematiker gar nicht als Anwendung von AC erkennen, wie z.B. König's-Lemma und "abz. Vererb. von abz. \mathcal{P}_f ist abz."); es hat aber keine der "allgemeineren" Folgerungen von AC und damit auch nicht die "pathologischen" Folgerungen von AC, wie: jeder VR hat Basis, nicht-messbare \mathcal{P}_f . etc.

(.) Solovay hat gezeigt dass AC für nicht-messbare Mengen nötig ist:
Aus ZF + countable choice folgt nicht dass es eine nicht-messbare TM von \mathbb{R} (oder \mathbb{R}^3 etc) gibt.

(Der Beweis setzt allerdings die Konsistenz einer großen Kardinalzahl voraus)

DAS ZORNISCHE LEMMA

Def: (A, \leq) heißt p.o. (partielle Ordnung), wenn
trans: $a \leq b \ \& \ b \leq c \rightarrow a \leq c$
refl.: $a \leq a$
antisym: $a \leq b \ \& \ b \leq a \rightarrow a = b$

Bem: (·) A ist die "Grundmenge", \leq die
Zustellige Relation. Üblicherweise lassen
wir \leq in der Notation weg und
sprechen nur von "der p.o. A "

(·) $a < b$ ist Abkürzung für: $a \leq b \ \& \ a \neq b$
Wenn umgekehrt die Ordnung $(A, <)$
gegeben ist wobei $<$ reflexiv ist,
definiert man mit $a \leq b \Leftrightarrow a = b \vee a < b$

(·) Genauso def man $a > b \Leftrightarrow b < a$ etc.

Es gilt: Wenn $B \subseteq A$, dann kann \leq
auf B eingeschränkt werden und ergibt
wieder p.o. (einfache $\bar{\cup}$)

Def (·) (A, \leq) p.o. heißt linear (l.o.), wenn
 $\forall a, b \in A \quad a \leq b \vee b \leq a$

(·) Sei A p.o. $B \subseteq A$ Kette, wenn B linear.
Äquiv: $\forall a, b \in B: a \leq b \vee b \leq a$

(·) $a \in A$ heißt minimales Element (Minimum),
wenn es kein $b \in A$ gibt mit $b < a$.
Analog Maximum.

(·) $a \in A$ ist größtes Element, wenn
 $a \geq b$ für alle $b \in A$
Analog kleinstes Element.

(·) $a \in A$ ist obere Schranke für $B \subseteq A$, wenn
 $a \geq b$ für alle $b \in B$. Analog untere Schranke.

(·) $a \in A$ ist kleinste obere Schranke von $B \subseteq A$,
wenn a kleinstes Element von $\{c: c \text{ o.S. von } B\}$

- Ü
- (*) Jede endl. Kette hat kleinste obere und größt. untere Schranke.
- (i) $(\mathcal{P}(X), \subseteq)$ ist p.o., jede TM hat kleinste obere und größt. untere Schranke
- (ii) Zeige: $(\mathbb{N} \setminus \{0\}, a|b)$ ist p.o., jede endl. TM hat kl. obere und gr. untere Schranke, aber keine unendl. TM hat obere Schranke.

Satz (Zornscher Lem.) Wenn A p.o. und wenn jede Kette eine obere Schranke hat, dann hat A max. El.

Anwendungen:

- (i) Jeder VR hat Basis
- Bew: Basis \Leftrightarrow max l.u. Menge.
- Sei A die M_g der l.u. TM von V , geordnet durch \subseteq (Teilmenge bez.).
- Wenn $B \subseteq A$ Kette, dann $\cup B$ l.u. und daher in A , d.h. obere Schranke.
- $\subset v_0, v_1, \dots, v_n \in B \rightarrow \exists a \in B$ s.d. $v_0, \dots, v_n \in a$
 $\rightarrow v_0, \dots, v_n$ l.u. (gilt nur weil B Kette!)
- Z.L. \rightarrow es gibt max El. in A , d.h. Basis.

- (ii) Jeder Ring mit 1 hat max. l.d. Ü
- (iii) Jeder Körper hat alg. Abschluss
- (iv) etc etc

^a "Beweis" von Z.C. mit AC:

Für "ordentlichem" Beweis braucht man axiomatische Mengenlehre (ZFC), die Beweis "idee" ist beliebig: Wähle als ersten Schritt die "eindelementige Kette" $\{a_0\}$ ($a_0 \in A$ beliebig). (im Schritt α sei Kette B_α schon gegeben. Fall 1: das nächste El von B_α ist max. El in A .

(dann sind wir fertig)

Fall 2: ansonsten wähle $a_\alpha \notin B_\alpha$ o. S. von B_α .

Behauptung: irgendwann (genauer: vor $|P(A)|$ vielen Schritten) muss Konstruktion abbrechen, d.h. Fall 1 eintreten: wir können keine beliebig langen Ketten in A konstruieren.



Def: (A, \leq) ist wohlgeordnet (w.o.), wenn A l.o. ist und jede nicht leere TM ein kleinstes Element hat.

Ü (AC): Sei A l.o. Dann $A \neq \emptyset \Leftrightarrow$ es gibt keine unendliche absteigende Folge in A .

Die wichtigste w.o. ist (\mathbb{N}, \leq) .

Die Bedeutung der w.o. = Erlaubt Induktion:

Induktion: Sei (A, \leq) w.p. Ang. für alle

$a \in A$ gilt:

$$\left[\forall b < a \quad P(b) \right] \rightarrow P(a)$$

Dann gilt $P(a)$ für alle a

Bew: Bei \mathbb{N} unterscheidet man üblicherweise Fälle $n=0$ und $n=m+1$. Bei trans-finiten Induktion braucht man auch einen Fall.

Def: Sei A, B p.o. (N) $A \cong B$, oder:

A und B sind isomorph, heißt:

$\exists f: A \rightarrow B$ bij. sol. $a \leq a' \Leftrightarrow f(a) \leq f(a')$

(1) A enthält sich in B einbetten, wenn

$\exists f: A \rightarrow B$ inj. sol. $a \leq a' \Leftrightarrow f(a) \leq f(a')$

(2) $A_a := \{b \in A : b < a\}$ "Aufangselement"

Lemma (1) Keine w.o. ist zu Aufangselement
isomorph, A w.o., $a \in A$, dann $A \not\cong A_a$

(2) Wenn A, B w.o. und isom., dann ist
Isomorphie eindeutig: wenn f, g beide
 $A \rightarrow B$ bij. und ordn. erh., dann $f = g$

(3) Seien A, B w.o. Dann tritt genau einer
der folgenden Fälle ein:

(a) $A \cong B$ (insbes: $|A| = |B|$)

(b) $\exists a \in A \quad A_a \cong B$ (insbes: $|A| \leq |B|$)

(c) $\exists b \in B \quad A \cong B_b$ (insbes: $|A| \geq |B|$)

Bem: $\bigcup \mathbb{R} \cong \mathbb{R}_a$ für alle $a \in \mathbb{R}$.
Dasselbe gilt für \mathbb{Q} .

Bew (Details in \bar{C})

1. Ang $f: A \rightarrow A_a$ isom. Sei b min sol $f(b) \neq b$.

Dann $f(b) > b$. Sei c sol $f(c) = b$. Dann
 $c > b$, aber $f(c) < f(b) \not\leq$

2. Ang $f \neq g$ beide isom. Sei a min sol $f(a) \neq g(a)$

oBdA $f(a) > g(a)$. Sei b sol $f(b) = g(a)$. Dann
 $b > a$, $f(b) = g(a) < f(a) \not\leq$

3. Setze $f(a) = b$ falls $A_a \cong B_b$.

Zeige: f part. Fkt $A \rightarrow B$, inj, ord-erh.,
und either $\text{dom}(f) = A_a$, dann $f: A_a \cong B$, oder
 $\text{dom}(f) = A$, dann $f: A \cong B_b$ oder $f: A \cong B$.

Der Wohlordnungsatz

Satz: Jede Menge A kann wohlgeordnet werden, d.h. es gibt Relation \leq sol. (A, \leq) w.o.

Bew: Mit Zorn: Sei X die Menge der (B, \leq) sol

$$(*) B \subseteq A$$

(*) \leq Relation auf B , (B, \leq) w.o.

geordnet durch: $(B_2, \leq_2) \geq (B_1, \leq_1)$ wenn (*) $B_2 \supseteq B_1$

(*) \leq_1 ist also durch \leq_2 induziert ordn. auf B_1 (d.h.: $b \leq_1 b' \Leftrightarrow b \leq_2 b'$ für alle $b, b' \in B_1$)

(*) $\forall b \in B_2 \setminus B_1, \forall b' \in B_1: b \leq_2 b'$
(d.h. B_2 ist "Erweiterung" von B_1)

Jede Kette $\mathcal{C} \in X$ hat o.S.:

$$B_\omega := \bigcup \{B : \exists (B, \leq) \in \mathcal{C}\}$$

$$b_1 \leq_\omega b_2 \Leftrightarrow \exists (B, \leq) \in \mathcal{C} : b_1, b_2 \in B, b_1 \leq b_2$$

oder äquivalent

$$\Leftrightarrow \forall (B, \leq) \in \mathcal{C}, b_1, b_2 \in B \rightarrow b_1 \leq b_2$$

(B_ω, \leq_ω) wieder w.o.: Wenn $C \subseteq B_\omega$ nicht leer, dann gibt es $(B, \leq) \in \mathcal{C}$ sol. $C \cap B \neq \emptyset$, d.h. $C \cap B$ hat min a . Das ist auch min von C .

Sei also (B, \leq) max in X . Beh: $B = A$, d.h. A ist wohlordenbar.

Sonst wähle $a \in A \setminus B$, def

$B_* := B \cup \{a\}$, und $b \leq_* b'$ durch:

$(b, b' \in B)$ und $b \leq b'$, oder $b' = a$.

Dann (B_*, \leq_*) größer als (B, \leq) , \nexists

Bem: AC, Z.C., Wohlordnungslehre sind alle äquivalent, d.h.:

$$ZF \text{ beweisbar } (AC \leftrightarrow Z.C.) \text{ etc}$$

Zusammen mit Lemma ergibt sich also:

Beh Je zwei Kardinalzahlen sind vergleichbar $\forall A, B \quad (|A| \leq |B| \vee |B| \leq |A|)$

Kardinalzahlen -- Äquivalenzklassen von beliebigen Mengen (ohne vorgegebene Struktur) unter der "gleich groß"

$|A|$ -- Kardinalzahl von A

Notation: $\aleph_0 = \aleph_0$

\aleph -- Aleph (erster Buchst. des Hebräischen Alphabets)

\aleph_1 : nächstgrößere Kardinalzahl (so etwas existiert)

$$2^{\aleph_0} = |\mathbb{R}|$$

$$CH: 2^{\aleph_0} = \aleph_1 \quad \text{Contour: } 2^{\aleph_0} > \aleph_0$$

Analog: Ordinalzahlen -- Äquivalenzkl. von Wohlordnungen unter "isomorph".

Notation: $\omega := \text{Äquiv.klasse von } (\mathbb{N}, \leq)$

$$\omega + 1, \quad \underbrace{\dots}_{\omega}, \quad \dots$$

$$\omega + 1 \neq \omega, \text{ aber } |\omega + 1| = |\omega| = \aleph_0$$

Beides, Ord. und Kard.zahlen, sind Verallgemeinerungen des endl. Zählens: ein, zwei, ... vs erster, zweites, ...