Vorlesung 1, 24. Sep. 2018

"Etwas Logik"

> Disclaimer: Wir machen keine mathematische Logik; das führt zu weit. Eigentlich muss man alles erst formalisieren.

Die (mathematische) Logik dreht sich um Aussagen, d.h. Sätze denen man einen Wahrheitswert "w = wahr" oder "f = falsch" zuordnen kann. (Und zwar eindeutig.)

Beispiel 1.1. $A =$ "Es regnet" ist eine Aussage.
$A =$ "Dieser Satz ist falsch" ist keine Aussage

Idee: Man will nun aus elementaren Aussagen zusammengesetzte Aussagen mittels Aussagenjunktoren kreieren ("Legomethode"). Die Junktoren sind Negation $\neg$, Konjunktion $\wedge$ ("und") und

Tippfehler: "nicht entweder-oder"

Disjunktion $\vee$ ("entweder-oder", gemeint "oder").
Diese sind durch Wahrheitstafeln definiert:

A	$\neg A$
w	f
f	w

A	B	$A \wedge B$	$A \vee B$
w	w	w	w
w	f	f	w
f	w	f	w
f	f	f	f

Eigenschaften E sind zusammengesetzte Ausdrücke, welche für Objekte x gelten können. Der Satz "x hat Eigenschaft E" wird dann als "$E(x)$ ist wahr" gelesen.
Gehört x zur Klasse X, dann schreiben wir $x \in X$; ansonsten $x \notin X$. Dann ist

$$\{x \in X \mid E(x)\}$$

die Klasse aller Objekte x, welche E erfüllen.

Beispiel 1.2 X = Klasse aller Menschen, $x \hat{=}$ Mensch
$E(x)$ = "Mensch x ist kleiner als 1,8m". Dann ist
$\{x \in X \mid E(x)\} \hat{=}$ Alle Menschen kleiner als 1,8m

---

Um Schreibweise zu vereinfachen führt man auch noch Quantoren ein:

$\exists$ = "es gilt" $\qquad \exists!$ = "es gilt genau ein" $\qquad \forall$ = "für alle"

$\exists x \in X \mid E(x)$ $\qquad \exists!\, x \in X \mid E(x)$ $\qquad \forall x \in X \mid E(x)$

"Es existiert ein x mit $E(x)$" $\qquad$ "Es gilt genau ein x mit $E(x)$" $\qquad$ "Alle x erfüllen $E(x)$"

Beispiel 1.3 Für X, x wie in Beispiel 1.2 ist $\exists x \in X \mid E(x)$ wahr, aber $\exists!\, x \in X \mid E(x)$ und $\forall x \in X \mid E(x)$ sind beide falsch.

Konvention 1.4

a) Wir lesen von links nach Rechts und z.B. "$\forall x \exists y \mid E(x,y)$" ist nicht dasselbe wie "$\exists y \forall x \mid E(x,y)$". Zur Deutlichkeit halber werden Klammern gesetzt.

b) Negationen werden häufig durch das Streichen von Symbolen angedeutet, e.g. "$\notin$" bedeutet "nicht in".

Beispiel 1.5

a) $\neg\neg A = \neg(\neg A) = A$

$\neg\neg A$	A
w	w
f	f

Wie in Beispiel 1.5 angedeutet sind zwei Aussagen (elementar oder zusammengesetzt) per Definition gleich, wenn sie dieselbe Wahrheitstafel haben.

Beispiel 1.6

a) $\neg(A \wedge B) = (\neg A) \vee (\neg B)$

A	B	$\neg(A \wedge B)$	$(\neg A) \vee (\neg B)$
w	w	f	f
w	f	w	w
f	w	w	w
f	f	w	w

b) $\neg(A \vee B) = (\neg A) \wedge (\neg B)$

c) $\neg(\forall x \in X \mid E(x)) = \exists x \in X \mid E(x)$

d) Mehr Beispiele in 1.1. [AE06]

Implikationen sind zusammengesetzte Aussage

$$(A \Rightarrow B) = (\neg A) \vee B$$

"aus A folgt B"

A	B	$A \Rightarrow B$
w	w	w
w	f	f
f	w	w
f	f	w

und eine Äquivalenz ist die Aussage

$$(A \Leftrightarrow B) = (A \Rightarrow B) \wedge (B \Rightarrow A)$$

"A gilt genau dann wenn B gilt"

A	B	$A \Leftrightarrow B$
w	w	w
w	f	f
f	w	f
f	f	w

<u>Beispiel 1.7</u>

A = "Es regnet", B = "Es stehen Wolken am Himmel"

dann ist $A \Rightarrow B$ wahr, aber $B \Rightarrow A$ nicht;

also $A \not\Leftrightarrow B$.

Die Kontraposition

$$(A \Rightarrow B) \Leftrightarrow (\neg B \Rightarrow \neg A)$$

"A impliziert B" gilt genau dann, wenn "nicht B, nicht A impliziert"

<u>Beispiel 1.8</u> Wie in Beispiel 1.7, es ist $\neg B \Rightarrow \neg A$ wahr "Wenn keine Wolken am Himmel stehen dann regnet es nicht", aber $\neg A \Rightarrow \neg B$ nicht, denn es kann auch bewölkt sein, ohne dass es regnet.

Konvention 1.9

Eine wahre Aussage wird als Proposition bezeichnet, wobei Theorem = "sehr wichtige Aussage" und Lemma = "Hilfsaussage" und Korollar = "direkte Folgerung" auch verwendet werden

---

Mathematik lebt von Beweisen, i.e. unter der Annahme "A = wahr" muss die Proposition "$A \Rightarrow B$" bewiesen werden, indem man zeigt, dass B wahr ist.

Dazu gibt es zwei Methoden:

- Direkter Beweis durch wiederholtes Anwenden von $(A \Rightarrow C) \land (C \Rightarrow B) \Rightarrow (A \Rightarrow B)$
- Indirekter Beweis durch Anwenden von
$$(A \Rightarrow B) \Leftrightarrow (\neg B \Rightarrow \neg A)$$

Beispiel 1.10

a) Proposition: $1+1+1=3$

Beweis: Wir wissen bereits, dass $1+1=2$ und $2+1=3$ gelten (Annahmen). Deswegen folgt

$$(1+1=2) \land (2+1=3) \Rightarrow (\underset{1+1}{\overset{\shortparallel}{2}}+1=3)$$

$\blacksquare$

(b) Proposition: A="Rabe" B="Schwarz"
(Also A => B bedeutet "Alle Raben sind schwarz")
Beweis: Durch Beobachtung von grünen Objekten, keine davon war ein Rabe, ~~was~~ bewiesen ☒
(Es gilt in diesem Fall nur zwei Farben "Schwarz" und "Grün". Aber Sie bemerken vielleicht, dass das ganze etwas absurd ist, aber Kontraposition in der Mathematik ist sehr nützlich.)

Zum Schluss sei nochmal betont, dass Sie Vorsicht walten lassen sollten, was Klammern angeht: x, y Menschen
$E(x,y)$ = " x und y sind Freunde"

Dann ist

$$\forall x \, (\exists y \mid E(x,y))$$

"Jeder Mensch hat einen Freund"

aber

$$\exists y \, (\forall x \mid E(x,y))$$

"Es gibt einen Mensch, welcher mit allen befreundet ist"

Vorlesung 2, 01. Okt. 2018

"Naive Mengenlehre I"

Disclaimer: Wir machen formale Mengenlehre später. Erstmal "naiv"

Die (mathematische) Mengelehre befasst sich mit Kollektionen von Objekten. Diese Kollektionen werden Mengen $X, Y, \ldots$ genannt. Ein Objekt x kann ~~enthalten~~ in einer Menge sein, geschrieben $x \in X$, oder nicht, geschrieben $x \notin X$. Objekte werden Elemente genannt.

Beispiel 2.1 X = Die Menge aller Menschen.
Objekte sind Menschen.

Sind X, Y Mengen so ist

$$X \subset Y \iff \forall x \in X \mid x \in Y$$

X ist Teilmenge von Y

Schreibe $Y \supset X$ für $X \subset Y$ und wir nennen Y eine Obermenge von X.

Ist X eine Menge dann ist $\{x \in X \mid E(x)\}$ die Teilmenge von X für die $E(x)$ wahr ist.

Die Menge $\emptyset_X = \{x \in X \mid x \neq x\}$ heißt leere Menge.

Mengen heißen gleich, geschrieben $X = Y$, wenn

$$X = Y \iff (X \subset Y) \wedge (Y \subset X)$$

Wir schreiben auch $X \subsetneq Y$ für $(X \subset Y) \wedge (X \neq Y)$ etc.

<u>Beispiel 2.2</u> X = Menge der Menschen, Y = Die Menge aller Lebewesen. Dann ist $X \subsetneq Y$

<u>Proposition 2.3</u> Seien X, Y, Z Mengen

a) Es gilt $X \subset X$ (Reflexivität)

b) Es gilt $(X \subset Y) \wedge (Y \subset Z) \Rightarrow (X \subset Z)$ (Transitivität)

c) Sei $E(x)$ eine Eigenschaft. Dann ist

$$x \in \emptyset_X \Rightarrow E(x)$$

wahr. ("Die leere Menge hat jede Eigenschaft".)

d) Es gilt $\emptyset_X = \emptyset_Y$ ("Es gibt nur eine leere Menge" und wir schreiben $\emptyset$.)

<u>Beweis</u> a+b) Ausgelassen.

c) Es gilt $(x \in \emptyset_X \Rightarrow E(x)) = \overbrace{\neg(x \in \emptyset_X) \vee E(x)}^{(*)}$

Aber $\neg(x \in \emptyset_X)$ ist für alle $x \in X$ wahr, also ist $(*)$ immer wahr.

d) Setze $E(x) = $ "$x \in \emptyset_Y$", dann folgt aus c), dass $\emptyset_X \subset \emptyset_Y$. Vertauschung von $X \leftrightarrow Y$ gibt die andere Richtung.

$\boxtimes$

Wir schreiben auch $\{x, y, \dots\}$ für die Menge, welche $x, y, \dots$ enthält

---

<u>Beispiel 2.4</u>: Die Menge $\{x\}$ besteht nur aus einem Element. Ist $x \neq y$, dann ist $\{x\} \neq \{y\}$

Sei X eine Menge, dann ist

$$P(X) = \{ A \mid A \subset X \}$$

die Potenzmenge von X. ("Die Menge aller Teilmengen.")

Beispiel 2.5 $P(\emptyset) = \{\emptyset\}$, $P(\{\emptyset\}) = \{\emptyset, \{\emptyset\}\}$

$P(\{x,y\}) = \{\emptyset, \{x\}, \{y\}, \{x,y\}\}$.

Seien $A, B \subset X$. Dann ist

$$A \cap B = \{ x \in X \mid (x \in A) \wedge (x \in B) \}$$

der Durchschnitt von A und B. Falls $A \cap B = \emptyset$, so heißen A und B disjunkt. Weiter

$$A \setminus B = \{ x \in X \mid (x \in A) \wedge (x \notin B) \}$$

heißt das Komplement (von B in A).

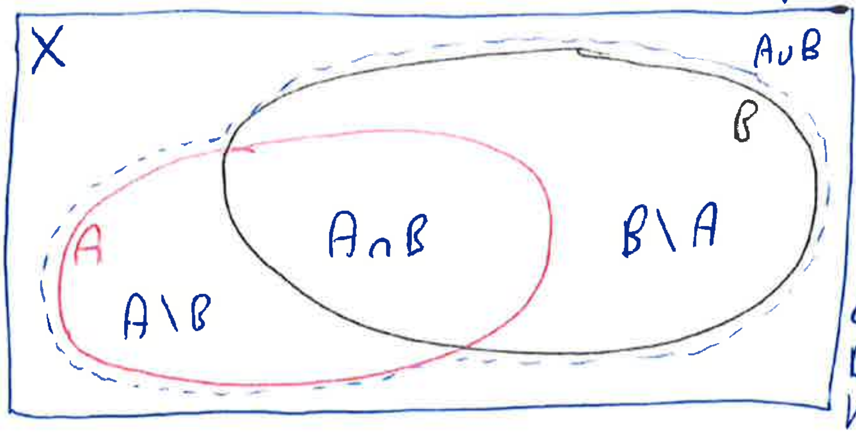
Die Menge

$$A \cup B = \{ x \in X \mid (x \in A) \vee (x \in B) \}$$

heißt Vereinigung.

Achtung: Häufig lässt man die Obermenge X weg und schreibt nur $A^c = X \setminus A$.

Beispiel 2.6 (Venn Diagramme – nur zur Veranschaulichung!)



X = Menschen
A = Brillenträger
B = Kontaktlinsenträger

dann z.B. $B \setminus A$ Menschen, welche Kontaktlinse benutzen

Proposition 2.7 Seien X, Y, Z Mengen. Dann gilt:

a) $X \cup Y = Y \cup X$, $X \cap Y = Y \cap X$ (Kommutativität)

b) $(X \cup Y) \cup Z = X \cup (Y \cup Z)$, $(X \cap Y) \cap Z = X \cap (Y \cap Z)$

(Assoziativität ⇝ Wir lassen Klammern weg)

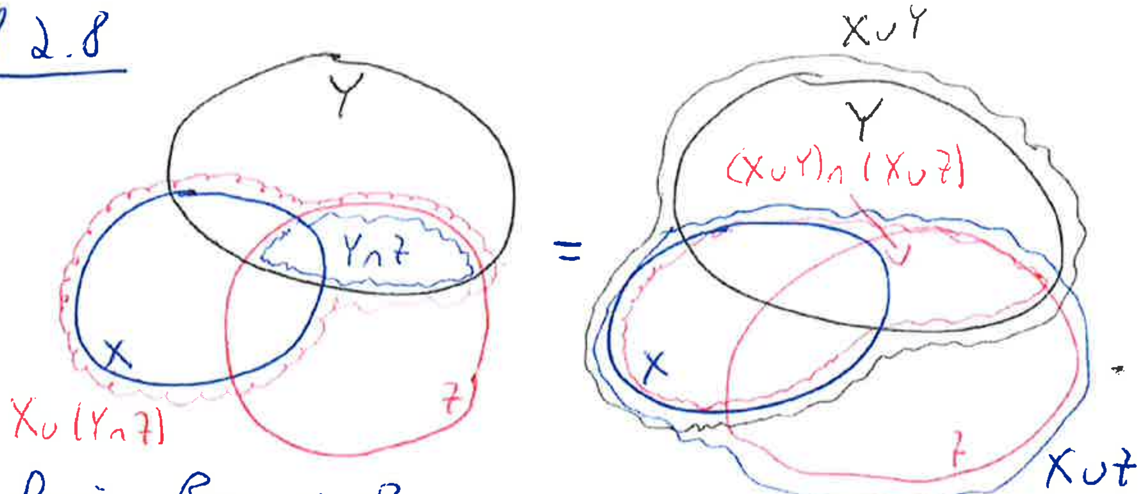
c) $X \cup (Y \cap Z) = (X \cup Y) \cap (X \cup Z)$ (Distributivität)

$X \cap (Y \cup Z) = (X \cap Y) \cup (X \cap Z)$

d) $X \subset Y \iff X \cup Y = Y \iff X \cap Y = X$

Beweis: Ausgelassen.

Beispiel 2.8



Das ist kein Beweis!

Seien X und Y Mengen. Dann ist

$$X \times Y = \{(x, y) \mid x \in X, y \in Y\}$$

"geordnete Paare" ⇜ $(x,y) = (x',y') \iff (x = x') \wedge (y = y')$

das Produkt.

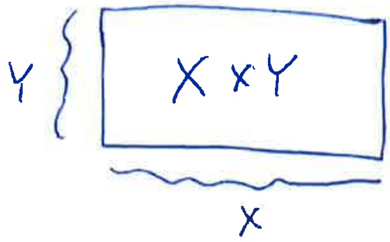
Analog, seien $X_1, \dots, X_n$ Mengen, dann ist

$$\bigtimes_{i=1}^{n} X_i = \{(x_1, \dots, x_n) \mid x_1 \in X_1, \dots, x_n \in X_n\}$$

Beispiel 2.9 Für $X = \{a,b\}$ und $Y = \{c,d,e\}$ ist

$$X \times Y = \{(a,c),(a,d),(a,e),(b,c),(b,d),(b,e)\}$$

Bildchen:



Proposition 2.10 Seien X, Y Mengen.

a) $X \times Y = \emptyset \Leftrightarrow (X = \emptyset) \vee (Y = \emptyset)$

b) $(X \times Y = Y \times X) \Leftrightarrow X = Y$ für $X, Y \neq \emptyset$

Beweis: b) Ausgelassen.

a) „$\Rightarrow$" Angenommen $X \times Y = \emptyset$, aber weder $X = \emptyset$ noch $Y = \emptyset$. Dann gibt es $x \in X$ und $y \in Y$. Dann ist aber $(x,y) \in X \times Y$. Widerspruch.

„$\Leftarrow$" Sei $X \times Y \neq \emptyset$ und wähle $(x,y) \in X \times Y$. Dann ist $x \in X$ und $y \in Y$, also $\neg((X = \emptyset) \vee (Y = \emptyset))$.

Sei $I \cancel{A} \neq \emptyset$. Weiter sei für $\alpha \in \cancel{A} I$ eine Menge A_α gegeben. Dann heißt die Menge

$$\{A_\alpha \mid \alpha \in I\}$$

Familie oder Mengensystem, und I heißt Indexmenge.

Vorsicht: Man verlangt nicht, dass $A_\alpha = A_\beta \Leftrightarrow \alpha = \beta$

Analog zu Produkte: $A_1 \cup \ldots \cup A_n = \{x \mid (x \in A_1) \vee \ldots \vee (x \in A_n)\}$

und $A_1 \cap \ldots \cap A_n = \{x \mid (x \in A_1) \wedge \ldots \wedge (x \in A_n)$

Das wollen wir verallgemeinern.
Es sei X eine Menge und $\{A_\alpha \mid \alpha \in I\}$ eine Familie von Teilmengen. Dann:

$$\bigcap_{\alpha \in I} A_\alpha = \{x \in X \mid \forall \alpha \in I \text{ gilt } x \in A_\alpha\} \subset X \quad \text{Durchschnitt}$$

$$\bigcup_{\alpha \in I} A_\alpha = \{x \in X \mid \exists \alpha \in I \text{ mit } x \in A_\alpha\} \subset X \quad \text{Vereinigung}$$

Proposition 2.11. Es seien $\{A_\alpha \mid \alpha \in I\}$ und $\{B_\beta \mid \beta \in J\}$ Familien von Teilmengen von X

a) $$\left(\bigcap_\alpha A_\alpha\right) \cap \left(\bigcap_\beta B_\beta\right) = \bigcap_{(\alpha,\beta) \in I \times J} A_\alpha \cap B_\beta$$

$$\left(\bigcup_\alpha A_\alpha\right) \cup \left(\bigcup_\beta B_\beta\right) = \bigcup_{(\alpha,\beta)} A_\alpha \cup B_\beta \qquad \text{(Assoziativität)}$$

b) $$\left(\bigcap_\alpha A_\alpha\right) \cup \left(\bigcap_\beta B_\beta\right) = \bigcap_{(\alpha,\beta)} A_\alpha \cup B_\beta$$

(Distributivität)

$$\left(\bigcup_\alpha A_\alpha\right) \cap \left(\bigcup_\beta B_\beta\right) = \bigcup_{(\alpha,\beta)} A_\alpha \cap B_\beta$$

Beweis: Ausgelassen

Theorem 2.12 (Regeln von De Morgan)

Es ~~seien~~ sei $\{A_\alpha \mid \alpha \in I\}$ eine ~~Fam~~ Familie von Teil-Menge von X. Dann gilt

$$\left(\bigcap_\alpha A_\alpha\right)^c = \bigcup_\alpha A_\alpha^c$$

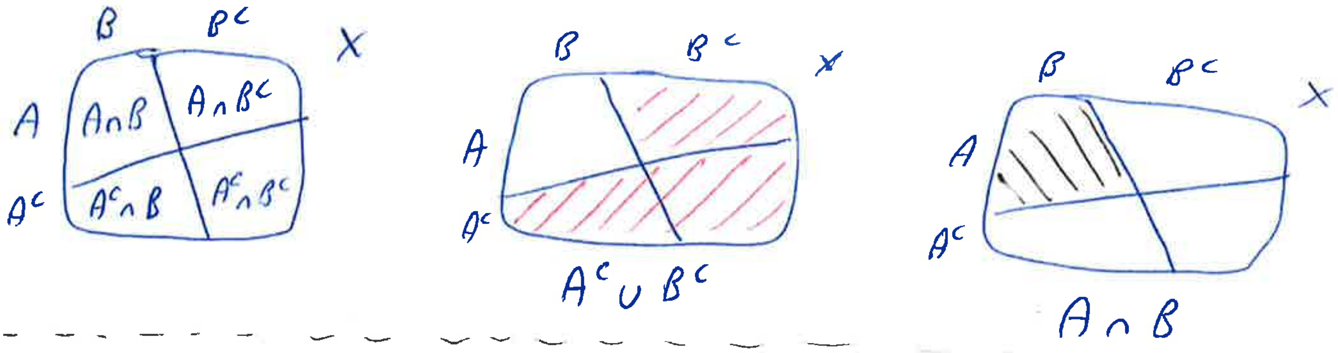
$$\left(\bigcup_\alpha A_\alpha\right)^c = \bigcap_\alpha A_\alpha^c$$

Beispiel 2.13

"Wenn Milch oder Zucker enthalten ist, dann trinke ich den Kaffee nicht"

$\Longleftrightarrow$

"Wenn ich den Kaffee trinke, dann ist weder Milch noch Zucker enthalten"



Beweis: Sei $x \in (\bigcap_\alpha A_\alpha)^c, x \in X \Rightarrow \exists \beta$ so, dass $x \notin A_\beta$ gilt.
Dann folgt, dass $x \in X \setminus A_\beta = A_\beta^c \Rightarrow$
$x \in \bigcup_\alpha A_\alpha^c$. Also $(\bigcap_\alpha A_\alpha)^c \subset \bigcup_\alpha A_\alpha^c$

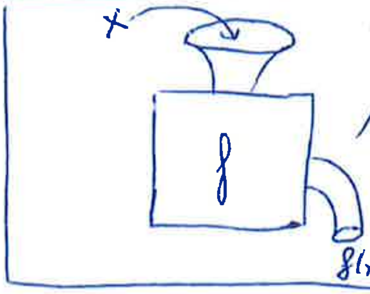
Sei $x \in \bigcup_\alpha A_\alpha^c, x \in X \Rightarrow \exists \beta$ so, dass $x \in A_\beta^c$.
Dann gilt aber $x \notin A_\beta \Rightarrow x \notin \bigcap_\alpha A_\alpha$. Da aber $x \in X \Rightarrow x \in (\bigcap_\alpha A_\alpha)^c$. Also
$(\bigcap_\alpha A_\alpha)^c \supset \bigcup_\alpha A_\alpha^c$.

$\Rightarrow$ Gleichheit.

Die Aussage, dass $(\bigcup_\alpha A_\alpha)^c = \bigcap_\alpha A_\alpha^c$ folgt durch analoge Überlegungen. $\square$

Vorlesung 3, 08. Okt. 2018

"Naive Mengenlehre II"



Wie eine Maschine

Wichtiger als Mengen selbst ist, wie diese in Verbindung/Relation stehen. Dies wird durch den Begriff der Abbildung/Funktion geklärt: Eine Abbildung $f: X \to Y,\ x \mapsto f(x)$ ist eine Vorschrift, welche jedem $x \in X$ genau ein $f(x) \in Y$ zuordnet. $f(x)$ heißt Wert, X Definitionsbereich/source und Y Wertebereich/target. Die Menge

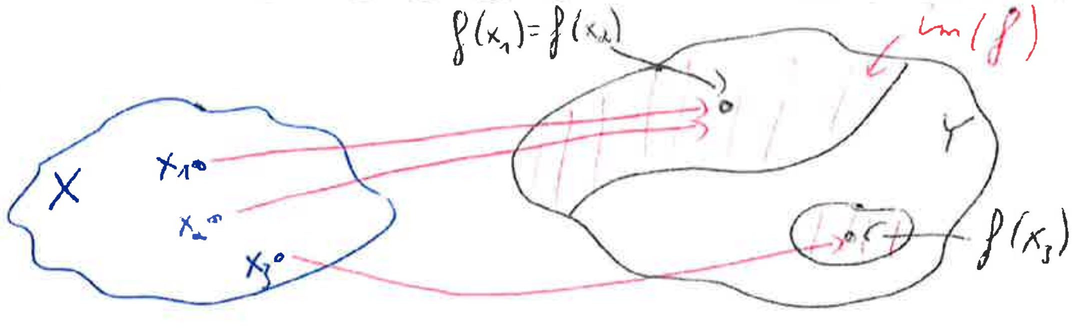
$$\operatorname{im}(f) = \{ y \in Y \mid \exists x \in X \text{ mit } f(x) = y \}$$

heißt Bild und die Menge

$$G(f) = \operatorname{graph}(f) = \{ (x, f(x)) \in X \times Y \mid x \in X \}$$

heißt Graph von f.

Beispiel 3.1



Bemerkung 3.2 Formal sollte man Funktionen auch als Mengen definieren, vgl. [AE06, Bemerkung 3.1]

Beispiel 3.3 X = Menge aller Hüte, Y = Menge der Menschen

$f: X \to Y$, Hut $\mapsto$ Besitzer

Zwei Abbildungen $f: X \to Y$, $g: X' \to Y'$ heißen **gleich**, falls

$$X = X', \quad Y = Y' \quad \text{und} \quad f(x) = g(x) \quad \forall x \in X$$

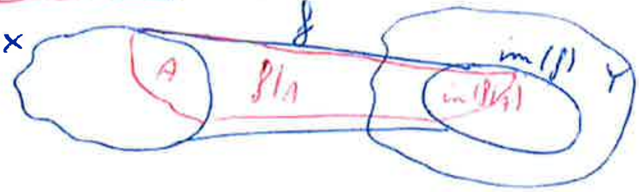
Beispiele 3.4

a) Die leere Abbildung $f: \emptyset \to Y$. Achtung: $\emptyset$ kann nie die Zielmenge sein, falls der Definitionsbereich leer ist.

b) Die **Identität** $id_X : X \to X$, $x \mapsto x$

c) **Inklusionen**: Ist $X \subset Y$, dann $i: X \to Y$, $x \mapsto x$

d) **Einschränkung**: $f: X \to Y$ and $A \subset X$, dann $f|_A : A \to Y$, $a \mapsto f(a)$



e) Weitere Beispiele [AE06, Beispiele 3.2]

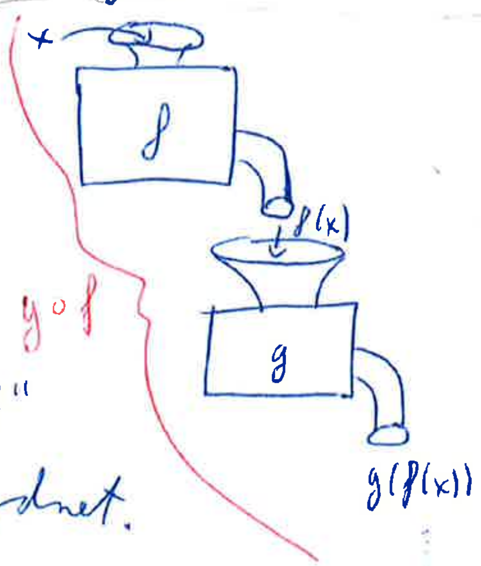
Seien $f: X \to Y$, $g: Y \to Z$ Abbildungen. Dann ist die **Komposition** $g \circ f$ die Abbildung

$$g \circ f : X \to Z, \quad x \mapsto g(f(x))$$

Beispiel 3.5 Wie in Beispiel 3.3

und sei $g: X \to Z$ (Menge der Städte), $y \mapsto$ Wohnort

Dann ist $g \circ f$ die Abbildung welche jedem Hut seinen "Wohnort" oder seinen "Aufenthaltsort" zuordnet.



Proposition 3.6

Es seien $f: X \to Y$, $g: Y \to Z$, $h: Z \to A$ Abbildungen. Dann gilt $(h \circ g) \circ f = h \circ (g \circ f)$.

(Assoziativität, Wir lassen also Klammern weg)

Beweis: Ausgelassen.

Schreibweise $f: X \to Y \rightsquigarrow X \xrightarrow{f} Y$. Dann heißt ein Diagramm kommutativ, falls

$$\begin{tikzcd} X \arrow[rr, "f"] \arrow[dr, "h"'] & & Y \arrow[dl, "g"] \\ & Z & \end{tikzcd} \qquad \begin{tikzcd} X \arrow[r, "f"] \arrow[d, "g'"'] & Y \arrow[d, "g"] \\ Z' \arrow[r, "f'"'] & Z \end{tikzcd}$$

$h = g \circ f$ $\qquad$ $f' \circ g' = g \circ f$ $\qquad$ rot = schwarz

Analog für kompliziertere Diagramme. Dabei ist wie folgt zu lesen:

$$\begin{tikzcd} X_1 \arrow[r, "f_1"] \arrow[rr, bend right, dashed, "f_2 \circ f_1"'] & X_2 \arrow[r, "f_2"] \arrow[rrr, bend right=40, dashed, "f_n \circ f_{n-1} \circ \dots \circ f_3 \circ f_2"'] & X_3 \arrow[r, "f_3"] & \dots \arrow[r, "f_n"] & X_{n+1} \end{tikzcd}$$

Beispiel 3.7

Die Kommutativität von

$$\begin{tikzcd} X \arrow[rr, "f"] & & Y & \\ Z \arrow[rr, "h"'] \arrow[urr, "i"] & & A \arrow[u, "g"] \arrow[ull, "j"] & B \arrow[l, "k"] \arrow[ul, "l"'] \end{tikzcd}$$

bedeutet:

$g = f \circ j$, $l = g \circ k$

$i = g \circ h$, $l = \underbrace{f \circ j}_{g} \circ k$

Man braucht $l = g \circ k$ nicht

Eine Abbildung $f: X \to Y$ heißt

Injektiv, falls $(f(x) = f(x')) \Rightarrow x = x'$

Surjektiv, falls $\operatorname{im}(f) = Y$

Bijektiv, falls injektiv und surjektiv

Man spricht auch von Injektion, Surjektion, Bijektion

Beispiel 3.8

a) Wie in Beispiel 3.3 f ist nicht injektiv, da ein Mensch mehrere Hüte haben kann und f ist nicht surjektiv, da es Menschen gibt, die keinen Hut besitzen.

b) Die Identität ist bijektiv.

c) Siehe [AE06, Beispiele 3.4]

Beispiel 3.9 $X = \{1,2,3\}$ $Y = \{4,5,6\}$ $f: \begin{array}{l} 1 \mapsto 4 \\ 2 \mapsto 5 \\ 3 \mapsto 6 \end{array}$ ist eine Bijektion. "Bijektion $\hat{=}$ X und Y sind effektiv gleich".

Proposition 3.10 Eine Abbildung $f: X \to Y$ ist genau dann bijektiv, wenn $\exists g: Y \to X$ so, dass $g \circ f = id_X$ und $f \circ g = id_Y$ gilt. In diesem Fall ist g eindeutig.

Beweis: „$\Rightarrow$" Ist f bijektiv, dann $\underline{\exists} y \in Y \ \exists! \ x \in X$ mit $y = f(x)$. Definiere also $g(y) = x$. Tippfehler: Für alle

„$\Leftarrow$" Aus $f \circ g = id_Y$ folgt, dass f surjektiv ist.

Seien also $x, x' \in X$ mit $f(x) = f(x')$. Dann gilt aber $x = id_X(x) = g(f(x)) = g(f(x')) = id_X(x') = x'$. Also ist f injektiv.

Sei $h : Y \to X$ eine weitere Abbildung mit $h \circ f = id_X$ und $f \circ h = id_Y$. Dann

$$g = g \circ id_Y = g \circ \underbrace{f \circ h}_{id_Y} = \underbrace{g \circ f}_{id_X} \circ h = id_X \circ h = h \qquad \square$$

Die Funktion g aus Proposition 3.10 wird Umkehrabbildung genannt und f^{-1} geschrieben. (Auch Inverse genannt)

Proposition 3.11 Seien $f : X \to Y$, $g : Y \to Z$ bijektiv. Dann ist $g \circ f : X \to Z$ bijektiv und

$$(g \circ f)^{-1} = f^{-1} \circ g^{-1}$$

Beweis: $g \circ f$ ist surjektiv, weil f und g surjektiv sind. Seien $x, x' \in X$ mit $\cancel{g \circ f}$ $g(f(x)) = g(f(x'))$ $\Rightarrow$ $f(x) = f(x')$, da g injektiv ist $\Rightarrow$ $x = x'$ da f injektiv ist. Es gilt weiter, dass

$$(f^{-1} \circ \underbrace{g^{-1}) \circ (g}_{id_Y} \circ f) = f^{-1} \circ id_Y \circ f = \underbrace{f^{-1} \circ f}_{id_X} = id_X$$

$\Rightarrow$ Behauptung, da Inverse eindeutig sind $\square$

Seien $f : X \to Y$, $A \subset X$, $C \subset Y$. Dann

$f(A) = \{ f(a) \in Y \mid a \in A \}$ Bild

$f^{-1}(C) = \{ x \in X \mid f(x) \in C \}$ Urbild

Sei $f: X \to Y$ eine Abbildung und sei $P(X)$ die Potenzmenge von X und $P(Y)$ die von Y. Bezeichne mit

$$\mathrm{Abb}(X,Y) = Y^X = \{ f: X \to Y \mid f \text{ Abbildung} \}$$

die Menge aller Abbildungen von $X \to Y$.

<u>Beispiel 3.12</u> Ist $X = \{1,2\} = Y$, dann gilt es

$$f_1: \begin{matrix} 1 \mapsto 1 \\ 2 \mapsto 1 \end{matrix} \qquad f_2: \begin{matrix} 1 \mapsto 1 \\ 2 \mapsto 2 \end{matrix} \qquad f_3: \begin{matrix} 1 \mapsto 2 \\ 2 \mapsto 1 \end{matrix} \qquad f_4: \begin{matrix} 1 \mapsto 2 \\ 2 \mapsto 2 \end{matrix}$$

und $Y^X = \{f_1, f_2, f_3, f_4\}$ welche 2^2 Elemente hat.

Es gilt auch die folgenden Mengenabbildungen:

$$\tilde{f}: P(X) \to P(Y), \quad A \subset X \mapsto f(A)$$

$$\tilde{f}^{-1}: P(Y) \to P(X), \quad B \subset Y \mapsto f^{-1}(B)$$

Vorsicht: f^{-1} steht für das Urbild und die Inverse. Ersteres gilt es immer, zweiteres nur für f bijektiv

---

Man schreibt $\tilde{f}^{-1} = f^{-1}$ und z.B. $f^{-1}(y) = \tilde{f}^{-1}(\{y\})$

Man nennt $f^{-1}(y) \subset X$ die Faser von f an y.

<u>Beispiel 3.13</u>

Die Faser $f^{-1}(y) = \{x \in X \mid f(x) = y\}$ kann leer sein. Zum Beispiel, zurück nach 3.3.: $f^{-1}(\text{Mensch}) =$ Alle Hüte, die den Mensch besitzt.

Proposition 3.14

Sei $f: X \to Y$ eine Abbildung. Dann:

a) $A \subset B \subset X \Rightarrow f(A) \subset f(B)$

b) $A_\alpha \subset X \ \forall \alpha \in I \Rightarrow f(\bigcup_\alpha A_\alpha) = \bigcup_\alpha f(A_\alpha)$

c) $A_\alpha \subset X \ \forall \alpha \in I \Rightarrow f(\bigcap_\alpha A_\alpha) \subset \bigcap_\alpha f(A_\alpha)$

d) $A \subset X \Rightarrow f(A^c) \supset f(X) \setminus f(A)$

e) $A' \subset B' \subset Y \Rightarrow f^{-1}(A') \subset f^{-1}(B')$

f) $A'_\beta \subset Y \ \forall \beta \in J \Rightarrow f^{-1}(\bigcup_\beta A'_\beta) = \bigcup_\beta f^{-1}(A'_\beta)$

g) $A'_\beta \subset Y \ \forall \beta \in J \Rightarrow f^{-1}(\bigcap_\beta A'_\beta) = \bigcap_\beta f^{-1}(A'_\beta)$

i) $A' \subset Y \Rightarrow f^{-1}(A'^c) = f^{-1}(A')^c$

Beweis: Ausgelassen

Proposition 3.15

$f: X \to Y$, $g: Y \to Z$.

Dann gilt $(g \circ f)^{-1}(B) = f^{-1} \circ g^{-1}(B) \ \forall B \subset Z$

Beweis:

Vergleich von den Fasern:

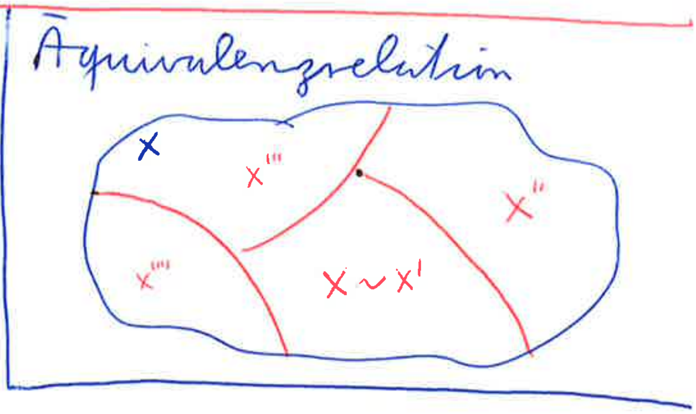
$(g \circ f)^{-1}(z) = \{x \in X \mid g(f(x)) = z\}$

$g^{-1}(z) = \{y \in Y \mid g(y) = z\}$

$f^{-1}(g^{-1}(z)) = \{x \in X \mid f(x) = g^{-1}(z)\}$ $\{y \in Y \mid g(y) = z\}$

Gleichheit folgt, da $g(g^{-1}(z)) = z$

Vorlesung 4, 15. Okt. 2018

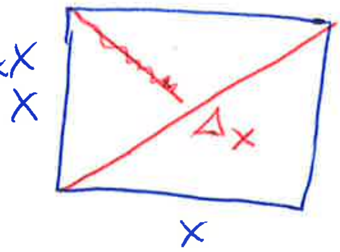


"Naive Mengenlehre III"

Relationen setzen Elemente einer Menge in Verbindung.

Eine (binäre) Relation R auf X ist eine Teilmenge $R \subset X \times X$. Für $(x,y) \in R$ schreibt man $x R y$ oder $x \sim_R y$ oder ...

Die Diagonale $\Delta_X = \{(x,x) \mid x \in X\} \subset X \times X$ bestimmt die reflexiven Relationen R.



Eine Relation R heißt

- reflexiv, falls $\Delta_X \subset R$, also $x R x$
- transitiv, falls $(x R y) \wedge (y R z) \Rightarrow (x R z)$
- symmetrisch, falls $(x R y) \Rightarrow (y R x)$
- äquivalent, falls R reflexiv, transitiv und symmetrisch ist

---

Beispiel 4.1 a) $X = \{1,2,3\}$ $R = \{(1,2),(2,3),(1,3)\}$ geschrieben $<$. Denn $1<2$ und $2<3 \Rightarrow 1<3$, also ist $<$ transitiv. Aber $<$ ist weder reflexiv noch symmetrisch.

b) Wie in a) nur mit $\leq$ $\rightsquigarrow$ transitiv + reflexiv.

c) $R = \Delta_X$ heißt Identitätsrelation, denn $(x R x') \Leftrightarrow (x = x')$. Diese ist eine Äquivalenzrelation.

d) X = Menschenmenge, R = Gleiche Hutgröße
R ist Äquivalenzrelation.

~~Theorem~~ Eine (disjunkte) Zerlegung von X ist eine Teilmenge $\mathfrak{Z} \subset P(X) \setminus \{\emptyset\}$ so, dass

$$\forall x \in X \quad \exists!\, Z \in \mathfrak{Z} \text{ mit } x \in Z$$

oder $\bigcup_{Z \in \mathfrak{Z}} Z = X$ und $Z \cap Z' = \emptyset$ für $Z, Z' \in \mathfrak{Z}$

Theorem 4.2 Sei $\sim$ eine Äquivalenzrelation auf X. Dann induziert $\sim$ eine Zerlegung von X.
(Die Teilmengen der Zerlegung nennt man Äquivalenzklasse und schreibt $[x]$.)

Beweis: Für $x \in X$ sei $[x] = \{x' \in X \mid x' \sim x\} \subset X$

Wegen $x \sim x$ ist $[x] \neq \emptyset$ und jedes $x \in X$ ist in einer solchen Klasse, nämlich $x \in [x]$.
Sei $[x] \cap [y] \neq \emptyset$ und sei $z \in [x] \cap [y]$. Dann folgt $z \sim x$ und $z \sim y \overset{\text{Symmetrie}}{\Longrightarrow} (x \sim z) \wedge (z \sim y) \overset{\text{Transitiv}}{\Longrightarrow} (x \sim y)$
Analog $y \sim x$. Deswegen folgt $[x] = [y]$, denn $\forall a \in [x]$ gilt $(a \sim x) \wedge (x \sim y) \Rightarrow (a \sim y)$, also $a \in [y]$ und umgekehrt.

Die Restklassenmenge

$$X/\!\sim \; = \{[x] \mid x \in X\} \subset P(X)$$

in der Zerlegung von X in Theorem 4.2 definiert eine Surjektion

$$p_x : X \longrightarrow X/\!\sim \;, \quad x \longmapsto [x]$$

welche als Projektion bezeichnet wird.

Beispiel 4.3 Wie in Beispiel 4.1 d), dann ist $[x]$ = Menge der Menschen mit Hutgröße k, falls x Hutgröße k hat.
Jeder Mensch mit Hutgröße k ist ein Repräsentant der Menge $[x]$ und $X/\sim$ teilt die Menschen in Hutgrößenklassen. (wird allgemein verwendet)

Eine Relation R heißt

- antisymmetrisch $(xRy) \land (yRx) \Rightarrow x = y$
- total, falls $(xRy) \lor (yRx)$

Eine Relation $R = \leq$ heißt Ordnung auf X, falls $\leq$ reflexiv, transitiv und antisymmetrisch ist.
$\leq$ heißt totale Ordnung, falls sie zusätzlich total ist.
$(X, \leq)$ heißt (total) geordnete Menge.

Beispiel 4.4 a) Wie in 4.1 b) $\leq$ auf $\{1,2,3\}$ ist totale Ordnung.
b) X = Menschen, $\leq$: Hat kleinere Hutgröße ist eine totale Ordnung c) Siehe [AE06, Beispiele 4.4]

Man schreibt auch

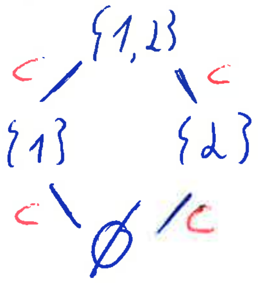
$x \geq y$ für $y \leq x$; $x < y$ für $(x \leq y) \land x \neq y$; $x > y$ für $y < x$

Proposition 4.5 $(X, \leq)$ total geordnet. Dann gilt für alle $x, y \in X$:
$(x < y) \lor (x = y) \lor (x > y)$ und nicht gleichzeitig.

Beweis: Wegen Totalität gilt mind. eins davon, wegen Antisymmetrie nicht zwei.

Beispiel 4.6 Proposition 4.5 gilt nur für total geordnete Mengen. Zum Beispiel ist $(P(X), \subset)$ eine geordnete Menge (genannt natürliche Ordnung auf $P(X)$) aber für $X = \{1,2\} \Rightarrow P(X) = \{\emptyset, \{1\}, \{2\}, \{1,2\}\}$

und

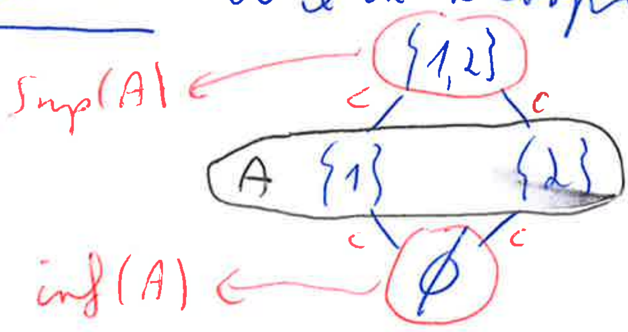


also nicht total und $\{1\}, \{2\}$ stehen in keine Relation.

Sei $(X, \leq)$ geordnet und $A \subset X$, $A \neq \emptyset$. Dann heißt A

- nach oben beschränkt, wenn $\exists\, t \in X$ mit $t \geq a \;\forall a \in A$ $(*)$
- nach unten beschränkt, wenn $\exists\, b \in X$ mit $b \leq a \;\forall a \in A$ $(\square)$
- beschränkt, wenn A nach oben und unten beschränkt ist
- ein t wie in $(*)$ heißt obere Schranke von A
- ein b wie in $(\square)$ heißt untere Schranke von A
- t wie in $(*)$ heißt Maximum von A, falls $t \in A$
- b wie in $(\square)$ heißt Minimum von A, falls $b \in A$
- $\sup(A) = \min\{t \in X \mid t \text{ ist obere Schranke}\}$
  Supremum ↳ ein Minimum dieser Menge
- $\inf(A) = \max\{b \in X \mid b \text{ ist untere Schranke}\}$
  Infimum ↳ ein Maximum dieser Menge

Beispiel 4.7 Wie in Beispiel 4.6



A ist beschränkt

$\min(A) = 1$ oder 2

$\max(A) = 1$ oder 2

Weitere Beispiele siehe [AE06, Bemerkung 4.5, Beispiel 4.6]

$(X, \leq_X)$, $(Y, \leq_Y)$ geordnet und $f: X \to Y$ Abbildung
$\qquad\;\; \overset{\shortparallel}{\leq} \qquad\quad \overset{\shortparallel}{\leq}$

- f heißt wachsend, falls $(x \leq y) \Rightarrow (f(x) \leq f(y))$
- f heißt fallend, falls $(x \leq y) \Rightarrow (f(x) \geq f(y))$
- strikt wachsend, falls $(x < y) \Rightarrow (f(x) < f(y))$
- strikt fallend, falls $(x < y) \Rightarrow (f(x) > f(y))$
- beschränkt (nach oben/unten), falls $\mathrm{im}(f)$ beschränkt (nach oben/unten)
- beschränkt auf beschränkten Teilmengen, falls $f(A)$ beschränkt ist für $A \subset X$ beschränkt

Beispiele siehe [AE06, Beispiele 4.7]

Eine Verknüpfung $\circledast: X \times X \to X$ ist eine Abbildung. Man schreibt $x \circledast y$ für $\circledast(x, y)$. Für $A, B \subset X$, $\neq \emptyset$

$$A \circledast B = \{a \circledast b \mid a \in A, b \in B\}$$

$$A \circledast b = A \circledast \{b\} \; ; \quad a \circledast B = \{a\} \circledast B$$

$A \subset X$, $A \neq \emptyset$ heißt abgeschlossen bzgl. $\circledast$, falls $A \circledast A \subset A$ gilt.

Beispiel 4.8 a) $\circ: \mathrm{Abb}(X,X) \times \mathrm{Abb}(X,X) \to \mathrm{Abb}(X,X)$
$$g \,,\, f \mapsto g \circ f$$
ist eine Verknüpfung.

b) Addition, Multiplikation etc. sind Verknüpfungen ("Blaupausenbeispiele")

c) $\cup : P(X) \times P(X) \longrightarrow P(X)$
$\quad A, B \longmapsto A \cup B$

$\cap : P(X) \times P(X) \longrightarrow P(X)$
$\quad A, B \longmapsto A \cap B$

sind Verknüpfungen

Eine Verknüpfung $\circledast$ heißt

- assoziativ, falls $(a \circledast b) \circledast c = a \circledast (b \circledast c)$ $\forall a, b, c \in X$
- kommutativ, falls $(a \circledast b) = (b \circledast a)$

Beispiel 4.9 Alle Verknüpfungen aus 4.8 sind assoziativ, aber $\circ$ ist im Allgemeinen nicht kommutativ.

$e \in X$ heißt Einheit oder neutrales Element, falls

$$e \circledast x = x = x \circledast e \quad \forall x \in X$$ bzgl. $(*)$

Beispiel 4.10 Wie in Beispiel 4.8

a) Die Einheit ist id_X.

b) Die Einheit bzgl $+$ ist 0, die bzgl. $\cdot$ ist die 1

c) $\emptyset$ ist Einheit bzgl. $\cup$, X ist Einheit bzgl. $\cap$

Proposition 4.11 Es gibt nur eine Einheit bzgl. $\circledast$.

Beweis: Seien $e, e' \in X$ Einheiten. Dann

$$e = e \circledast e' = e'$$

$\boxed{\text{Z}}$

Beispiel 4.12 Zurück zu Beispiel 4.6.

$$P(\{1,2\}) = \begin{tikzcd}[column sep=small] & \{1,2\} & \\ \{1\} \arrow[ur, phantom, "\subset"] & & \{2\} \arrow[ul, phantom, "\subset"] \\ & \emptyset \arrow[ul, phantom, "\subset"] \arrow[ur, phantom, "\subset"] & \end{tikzcd}$$

Nehme $\circledast = \cup$

Diese ist symmetrisch also kommutativ.

$\emptyset$ → Einheit, denn

$\emptyset \cup \emptyset = \emptyset$, $\emptyset \cup \{1\} = \{1\}$, $\emptyset \cup \{2\} = \{2\}$

$\emptyset \cup \{1,2\} = \{1,2\}$

$$A \subset P(\{1,2\}) = \begin{tikzcd}[column sep=small] & \{1,2\} & \\ \{1\} \arrow[ur, dash] & A & \{2\} \arrow[ul, dash] \\ & \emptyset \arrow[ul, dash] \arrow[ur, dash] & \end{tikzcd}$$

A ist $\cup$-abgeschlossen:

$\{1\} \cup \{1\} = \{1\} \in A$

$\{1\} \cup \{2\} = \{1,2\} \in A$

$\{2\} \cup \{1\} = \{1,2\} \in A$

usw.

"Multiplikationstabelle":

$* \cup \square$

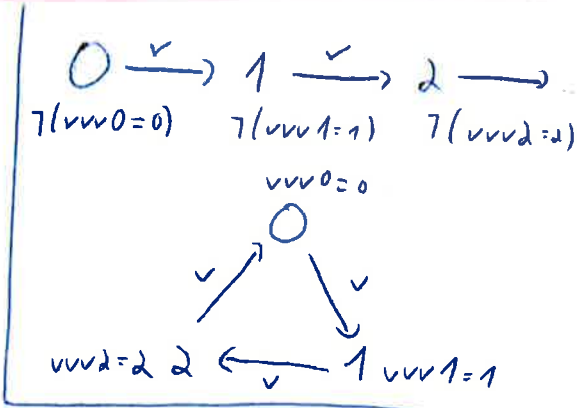
Symmetrisch = kommutativ

$\cup$	$\emptyset$	$\{1\}$	$\{2\}$	$\{1,2\}$
$\emptyset$	$\emptyset$	$\{1\}$	$\{2\}$	$\{1,2\}$
$\{1\}$	$\{1\}$	$\{1\}$	$\{1,2\}$	$\{1,2\}$
$\{2\}$	$\{2\}$	$\{1,2\}$	$\{2\}$	$\{1,2\}$
$\{1,2\}$	$\{1,2\}$	$\{1,2\}$	$\{1,2\}$	$\{1,2\}$

A

Vorlesung 5, 22. Okt. 2018

"Die natürlichen Zahlen I"



Peano (1888): "Was sind und was sollen die Zahlen?"
Idee: Auch die natürlichen Zahlen, und alle ihre Eigenschaften, sollen über die Mengenlehre definiert werden.

Vorsicht: Obwohl Sie alle schon wissen, was die natürlichen Zahlen sind, wollen wir diese rein axiomatisch einführen.

Definition (Peano Axiome)

Die natürlichen Zahlen (mit Null) bilden eine Menge $\mathbb{N}_0$ für die es ein Element $\boxed{0 \in \mathbb{N}_0}$ und eine Funktion

$$\boxed{v : \mathbb{N}_0 \longrightarrow \mathbb{N} = \mathbb{N}_0 \setminus \{0\}}$$

so gilt, dass

Nachfolgerfunktion
$v(n)$ = Nachfolger von n

PA 1: v ist injektiv

PA 2: $N \subset \mathbb{N}_0$ so, dass $0 \in N$ und $(\forall n \in N) \Rightarrow (v(n) \in N)$ gilt. Dann ist $N = \mathbb{N}_0$

Das ist das Induktionsaxiom.

Proposition 5.1 ν ist bijektiv

Tippfehler: bijective auf N (nicht N_0)

Beweis: Es sei $N = \{ n \in \mathbb{N}_0 \mid \exists n' \in \mathbb{N}_0 \text{ mit } \nu(n') = n \} \cup \{0\}$

Dann ist $N = \mathrm{im}(\nu) \cup \{0\}$ und wegen PA2 folgt $N = \mathbb{N}_0$. $\Rightarrow \mathrm{im}(\nu) = \mathbb{N}$, also ist ν surjektiv.

ν ist injektiv per Definition. $\boxtimes$

Bemerkung 5.2 Wir kommen in der letzten Vorlesung darauf zurück, aber man muss eigentlich zeigen, dass $\mathbb{N}$ existiert. Siehe aus [AE06, Bemerkungen 5.2]

Beispiel 5.3 Schreibe $0 = \emptyset$ und setze $\underset{\nu(n)}{n+1} = \{0, \dots, n\}$ ~~$1 = \{\emptyset\}$~~ ~~$n+1 = \{n, \{n\}\}$~~. Dann ist für alle n

$$\mathbb{N}_0 = \{ \underset{\emptyset}{0},\ 1 = \underset{\{\emptyset\}}{\{0\}},\ 2 = \underset{\{\emptyset, \{\emptyset\}\}}{\{0,1\}},\ 3 = \underset{\{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}}{\{0,1,2\}},\ 4 = \dots \}$$

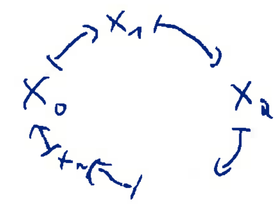
Wir schreiben $1 = \nu(0)$, $2 = \nu(\nu(0))$, $3 = \nu(\nu(\nu(0)))$ etc.

Proposition 5.4 $\mathbb{N}_0$ ist nicht endlich

Beweis: Angenommen $\mathbb{N}_0 = \{ \underset{0}{x_0}, \dots, x_n \}$ und

$$x_0 \overset{\nu}{\longmapsto} x_1 \longmapsto \dots \overset{\nu}{\longmapsto} x_n$$

Dann muss $\nu(x_n) = x_0$ sein, da ν injektiv ist.

$\rightsquigarrow$ 

Aber das ist ein Widerspruch dazu, dass $\nu : \mathbb{N}_0 \longrightarrow \mathbb{N}$ gilt. $\boxtimes$

Theorem 5.5 (Peano)

Auf $\mathbb{N}$ gibt es zwei eindeutige Verknüpfungen $+$ (Addition), $\cdot$ (Multiplikation) und eine Ordnung $\leq$ (natürliche oder Zählordnung) so, dass:

a) $+$ ist assoziativ, kommutativ und 0 ist Einheit

b) $\cdot$ ist assoziativ, kommutativ und 1 ist Einheit

c) Es gilt $\forall\, l, m, n \in \mathbb{N}_0 \quad (l+m)\cdot n = l \cdot n + m \cdot n$ "Distributiv"

d) $0 \cdot n = 0$

e) $(\mathbb{N}_0, \leq)$ ist total geordnet mit $0 = \min(\mathbb{N}_0)$

f) Für $n \in \mathbb{N}_0 \not\exists\, k \in \mathbb{N}_0$ so, dass $n < k < n+1$.

g) $\forall\, m, n \in \mathbb{N}_0$: $\quad m \leq n \iff \exists\, d \in \mathbb{N}_0$ mit $m + d = n$
$\quad m < n \iff \exists\, d \in \mathbb{N}$ mit $m + d = n$

d ist eindeutig und heißt Differenz.

h) $\forall\, m, n \in \mathbb{N}_0$: $\quad m \leq n \iff m + l \leq n + l$
$\quad m < n \iff m + l < n + l \quad \forall\, l \in \mathbb{N}_0$

i) Für $m, n \in \mathbb{N}$ ist $m \cdot n \in \mathbb{N}$ $\quad (m \cdot n = 0 \iff (m = 0) \vee (n = 0))$

j) $\forall\, m, n \in \mathbb{N}_0$: $\quad m \leq n \iff m \cdot l \leq n \cdot l$
$\quad m < n \iff m \cdot l < n \cdot l \quad \forall\, l \in \mathbb{N}$

Beweis: Wir beweisen nur a), für alle anderen siehe z.B. die Referenz in [AE06, Theorem 5.3].

Der Punkt ist alles herzuleiten, ohne die vertrauten Regeln zu verwenden ☺

i) Angenommen $\circledast : \mathbb{N}_0 \times \mathbb{N}_0 \longrightarrow \mathbb{N}_0$ ist eine kommutative Verknüpfung, welche

$0 \otimes 0 = 0 \quad , \quad n \otimes 1 = \nu(n) \; ; m \otimes \nu(m) = \nu(m \otimes m)$

$\forall m, n \in \mathbb{N}_0$ erfüllt. Betrachte (*)

$$N = \{ n \in \mathbb{N}_0 \mid 0 \otimes n = n \}$$

Dann gilt $0 \in N$, und $n \in N \Rightarrow 0 \otimes \nu(n) = \nu(0 \otimes n) = \nu(n)$

Also ist $\nu(n) \in N \overset{PA2}{\Longrightarrow} N = \mathbb{N}_0$, d.h. $0 \otimes n = n \quad \forall n \in \mathbb{N}_0$

ii) Sei $\boxed{*}$ eine weitere kommutative Verknüpfung, welche (*) erfüllt. Setze für $n \in \mathbb{N}_0$ fest

$$M_n = \{ m \in \mathbb{N}_0 \mid m \otimes n = m \boxed{*} n \}$$

Es folgt $0 \in M_n$, und sei $m \in M_n$. Dann

$$\nu(n \otimes m) = \nu(m \boxed{*} n) = \nu(n \boxed{*} m)$$

also

$$\nu(m) \otimes n = n \otimes \nu(m) = n \boxed{*} \nu(m) = \nu(m) \boxed{*} n$$

$\Rightarrow \nu(m) \in M_n \overset{PA2}{\Longrightarrow} M_n = \mathbb{N}_0 \quad \forall n \in \mathbb{N}_0$ ~~also~~

Also $\otimes = \boxed{*}$, da $n \in \mathbb{N}_0$ beliebig war.

Es gilt nur eine kommutative Verknüpfung mit (*) (☆)

iii) Konstruiere $+ : \mathbb{N}_0 \times \mathbb{N}_0 \to \mathbb{N}_0$ mit (*) welche kommutativ ist. Dazu setze

$$N = \{ n \in \mathbb{N}_0 \mid \exists \varphi_n : \mathbb{N}_0 \to \mathbb{N}_0 \text{ mit } \varphi_n(0) = \nu(n) \text{ und } \varphi_n(\nu(m)) = \nu(\varphi_n(m)) \; \forall m \in \mathbb{N}_0 \}$$

Mit $\varphi_0 = \nu$ folgt $0 \in N$. Sei nun $n \in N$, dann setze

$$\psi : \mathbb{N}_0 \to \mathbb{N}_0 \quad , \quad m \longmapsto \nu(\varphi_n(m))$$

Dann gilt $\psi(0) = \nu(\varphi_n(0)) = \nu(\nu(n))$ und

$\psi(v(m)) = v(\varphi_n(v(m))) = v(v(\varphi_n(m))) = v(\psi(m))\ \forall_{m\in\mathbb{N}_0}$

Also $(n\in N) \Rightarrow (v(n)\in N) \overset{PA2}{\Rightarrow} N = \mathbb{N}_0$.

φ_n ist eindeutig: Sei ψ_n eine weitere Abbildung mit denselben Eigenschaften. Dann kann man ~~nicht~~ für $M_n = \{m\in\mathbb{N}_0 \mid \varphi_n(m) = \psi_n(m)\}$ und PA2, dass $M_n = \mathbb{N}_0$ gilt. Das bedeutet $\varphi_n = \psi_n$

Tippfehler: "mittels PA2 zeigen"

Also: Für alle $n\in\mathbb{N}_0$ $\exists!$

$\varphi_n : \mathbb{N}_0 \to \mathbb{N}_0$ mit $\varphi_n(0) = v(n)$ und $\varphi_n(v(m)) = v(\varphi_n(m))$ $\forall_{m\in\mathbb{N}_0}$

Definiere

$$+ : \mathbb{N}_0\times\mathbb{N}_0 \to \mathbb{N}_0,\quad n+m = \begin{cases} n, & \text{falls } m = 0, \ (\square) \\ \varphi_n(m'), & \text{falls } m = v(m'). \end{cases}$$

Dann erfüllt $+$ $(*)$, denn

$$n+0 = n, \quad n+1 = n+v(0) = \varphi_n(0) = v(n) = v(n+0)$$

$$n+v(m) = \varphi_n(m) = \varphi_n(v(m')) = v(\varphi_n(m')) = v(n+m)$$

für $n\in\mathbb{N}_0$, $m\in\mathbb{N}$ und $m = v(m')$. Dann ist auch 0 die Einheit bezüglich $(+)$, weil $(\square)$ gilt.

iv) Sei $N_{l,m} = \{n\in\mathbb{N}_0 \mid (l+m)+n = l+(m+n)\}$ für $l,m\in\mathbb{N}_0$ fest. Dann $0\in N_{l,m}$ und für $n\in N$

$$(l+m)+v(n) = v((l+m)+n) = v(l+(m+n)) = l+v(m+n)$$

$= l+(m+v(n))$. Also folgt $v(n)\in N \overset{PA2}{\Rightarrow} N = \mathbb{N}_0$

$\Rightarrow$ Assoziativität, da l,m beliebig waren.

v) Kommutativität: Betrachte

$$N = \{ n \in \mathbb{N}_0 \mid n+1 = 1+n \}$$

Wie vorher folgt $0 \in N$ und für $n \in N$

$$v(n)+1 = v(v(n)) = v(n+1) = v(1+n) = 1+v(n)$$

Also $v(n) \in N \overset{PA2}{\Rightarrow} N = \mathbb{N}_0$.

Dasselbe Argument funktioniert für

$$M_n = \{ m \in \mathbb{N}_0 \mid m+n = n+m \}$$

für alle $n \in \mathbb{N}_0$. Daraus folgt dann Kommutativität.

Zusammengefasst: $\exists$ die Addition durch (iii), welche Assoziativ ist bei (iv) und kommutativ bei (v). 0 ist Einheit, durch Konstruktion und + ist eindeutig durch (☆). $\boxtimes$

<u>Beispiel 5.6</u>

+ = die vertraute Addition

$\cdot$ = die vertraute Multiplikation

(schreibe auch $mn = m \cdot n$)

$\leq$ = die vertraute Ordnung, bestimmt durch $\quad n < n+1 = v(n) \; \forall n \in \mathbb{N}_0$

$$0 < 1 < v(1) = 2 < v(2) = 3 < \dots$$

Proposition 5.7 Für $m, n \in \mathbb{N}_0$, $k \in \mathbb{N}$ mit $mk = nk$ gilt $m = n$
"Kürzen"

Beweis: Wegen (j) von Theorem 5.5 ▭

$m \in \mathbb{N}$ heißt Teiler von n, falls es $k \in \mathbb{N}$ gibt so, dass $mk = n$. Schreibe in diesem Fall $m | n$.
k heißt in diesem Fall Quotient und wird mit n/m bezeichnet.

Theorem 5.8 (Division mit Rest, a.k.a. Euklids Algorithmus)
Zu $m \in \mathbb{N}$ und $n \in \mathbb{N}_0$ $\exists!$ $k \in \mathbb{N}$ und $l \in \mathbb{N}$ mit
$$n = km + l \quad \text{für } l < m$$

Tippfehler: Beide, k und l, sind aus N_0

Beweis i) Existenz. Setze
$$N = \{n \in \mathbb{N}_0 \mid \exists k, l \text{ mit } n = km + l,\ l < m\}$$
Wegen $0 = 0 \cdot m + 0$ ist $0 \in N$. Also sei $n \in N$, und wähle k, l mit $n = km + l$, $l < m$. Also $n + 1 = km + (l+1)$. Ist $l + 1 < m$, so folgt $n+1 \in N$. Ist $l + 1 = m$, dann ist $n + 1 = (k+1)m$ und $n + 1 \in N$. Wegen PAα folgt $N = \mathbb{N}_0$.

ii) Eindeutigkeit. Seien k, k', l, l' gegeben so, dass
$$km + l = k'm + l' \qquad l, l' < m.$$
Angenommen $l \le l'$, dann $k'm + l' = km + l \le km + l'$, also $k'm \le km$, also $k' \le k$. Aber wegen $l' < m$ folgt
$$km \le k'm + l < k'm + m = (k'+1)m \Rightarrow k < k' + 1$$
Tippfehler: l' nicht l

$\Rightarrow$ Wegen $k' \le k$ folgt also $k = k'$ und damit $l = l'$ ▭

Vorlesung 6, 29. Okt. 2018

"Die natürlichen Zahlen II"

Wir haben schon gesehen, dass PA2 sehr wichtig ist. Dies führt uns zum Begriff der mathematischen Induktion (später).

$3^{k+1}-1$ ist durch 2 teilbar:

$$3^{k+1}-1 = 3\cdot 3^k - 1 = \underbrace{2\cdot 3^k}_{\checkmark} + \underbrace{(3^k-1)}_{\text{per Induktion}}$$

Proposition 6.1

$\mathbb{N}_0$ ist wohlgeordnet, d.h. $A\subset\mathbb{N}_0$, $A\neq\emptyset$ besitzt ein Minimum.

nach unten wohlgeordnet

Beweis: Sei $A\subset\mathbb{N}_0$ nicht leer. Setze

$$B=\{n\in\mathbb{N}_0 \mid n \text{ ist eine } \text{untere Schranke} \text{ von } A\}$$

Es ist $0\in B$. Angenommen A besitzt kein Minimum und sei $n\in B$. Dann $n\notin A$, und

$\left.\begin{array}{l} a\geq n \\ a\neq n \end{array}\right\} a>n \quad \forall a\in A$ zeigt $a\geq n+1 \quad \forall a\in A$.

Also ist $n+1\in B \overset{PA2}{\Longrightarrow} B=\mathbb{N}_0$. Also muss A leer sein, da $A\cap B=\emptyset$ ist unter der Annahme, dass A kein Minimum hat. Widerspruch. $\boxed{\text{☺}}$

Beispiel 6.2 Endliche Teilmengen von $\mathbb{N}_0$ haben klarerweise ein Minimum, aber auch $\{n\in\mathbb{N}_0 \mid 2\nmid n\}$ (die ungeraden Zahlen) hat 1 als Minimum.

Eine Zahl $p \in \mathbb{N}$ heißt Primzahl, falls $p \geq 2$ und $n | p \Rightarrow (n=1) \vee (n=p)$.

<u>Proposition 6.3</u> Jedes $n \in \mathbb{N}_0$ mit $n \neq 0,1$ besitzt eine Primfaktorzerlegung (PFZ), d.h. $n = p_1 \cdot \ldots \cdot p_k$ mit Primzahlen $p_1, \ldots, p_k$. Diese ist eindeutig bis auf Reihenfolge.

<u>Beweis</u>: i) Angenommen die Menge

$$A = \{ n \in \mathbb{N}_0 \mid n \neq 0,1 \,,\, n \text{ besitzt keine PFZ} \}$$

ist nicht leer. Dann $\exists\, a \in A$ minimal, nach Proposition 5.1. Insbesondere ist a selbst keine Primzahl, also $\exists\, b, c \in \mathbb{N}$ mit $b, c \neq 1$ und $a = bc$. Aber dann gilt $b < a$ und $c < a$

$\Rightarrow \exists\, p_1, \ldots, p_k \,,\, p'_1, \ldots, p'_{k'}$ mit $b = \underbrace{p_1 \cdots p_k}_{\boxed{PFZ}}$ und $c = \underbrace{p'_1 \cdots p'_{k'}}_{\boxed{PFZ}} \Rightarrow a = p_1 \cdots p_k p'_1 \cdots p'_{k'}$ ist eine PFZ von a. Widerspruch, also ist $A = \emptyset$.

---

ii) Angenommen die Menge

$$B = \{ n \in \mathbb{N}_0 \mid n \neq 0,1 \,,\, n \text{ besitzt mehrere PFZ} \}$$

ist nicht leer. Dann $\exists\, b \in B$ minimal mit

$$b = \underbrace{p_1 \cdots p_k}_{\boxed{PFZ}} = \underbrace{p'_1 \cdots p'_{k'}}_{\boxed{PFZ}}$$

Angenommen $p_i = p_j'$ für irgendwelche i,j.
Dann kann man kürzen und erhält b' mit $b' < b$ und $b' \in B$. Widerspruch zur Minimalität.
Also können wir annehmen, dass $p_1 \leq \ldots \leq p_k$, $p_1' \leq \ldots \leq p_l'$ und $p_1 < p_1'$ gilt. Setze

$$q = p_1 p_2' \cdots p_l'$$

Dann gilt $p_1 | q$ und $p_1 | b \Rightarrow p_1 | (b-q)$ und $b-q \in \mathbb{N}$
Also existiert eine eindeutige PFZ

$$b - q = \underbrace{p_1 r_1 \cdots r_e}_{\boxed{PFZ}} = (p_1' - p_1) p_2' \cdots p_k'$$

Wenn man jetzt als eine PFZ von $p_1' - p_1$ wählt, dann erhält man eine weitere PFZ von $b-q$. Also ~~trotz~~ $b - q \in B$; Widerspruch zur Minimalität.

Das führt uns zum Begriff der Induktion:
Um eine Aussage $E(n)$ für alle $n \in \mathbb{N}_0$ zu beweisen geht man wie folgt vor:

a) Induktionsanfang (IA) Prüfe $E(0)$ ist wahr.
b) Induktionsschluss (IS)
   α) Nehme an $E(n)$ ist wahr.
   β) Zeige dass daraus $E(n+1)$ folgt.

Proposition (Induktionsprinzip) 6.4
Induktion liefert, dass $E(n)$ wahr ist für $\forall n \in \mathbb{N}_0$

Beweis: Das folgt aus PA2 ☒

Proposition 6.5 (Induktionsprinzip)
Sei $n_0 \in \mathbb{N}_0$ und sei für alle $n \geq n_0$ eine Aussage $E(n)$ so gegeben, dass:
a) $E(n_0)$ ist wahr.
b) $\forall n \geq n_0$ gilt: $E(n)$ wahr $\Rightarrow$ $E(n+1)$ wahr.
Dann ist $E(n)$ für alle ~~$n \in \mathbb{N}$~~ $n \geq n_0$ wahr.

Beweis: Setze $N = \{ n \in \mathbb{N}_0 \mid E(n+n_0) \text{ ist wahr} \}$.
Dann gilt $0 \in N$ wegen a) und $n \in N \Rightarrow n+1 \in N$ wegen b). Also $N = \mathbb{N}_0$ wegen PA2 ☒

Schreibweise: $m^n = \underbrace{m \cdot m \cdot \ldots \cdot m}_{n}$ für $m \in \mathbb{N}_0, n \in \mathbb{N}$

Beispiel 6.6 **Behauptung:** $3^k - 1$ ist für alle $k \in \mathbb{N}$ durch 2 teilbar.
Beweis: Durch Induktion.
(IA): $k = 1$, dann ist $3^1 - 1 = 2$ durch 2 teilbar.

(IS) Sei die Behauptung wahr für ein $n \in \mathbb{N}$ (*)

Dann ist $3^{n+1}-1 = 3(3^n)-1$

$$= (2+1)3^n - 1 = \underbrace{(2\cdot 3^n)}_{\text{durch 2 teilbar}} + \underbrace{(3^n-1)}_{\text{durch 2 teilbar wegen } (*)}$$

$\Rightarrow 3^{n+1}-1$ ist durch 2 teilbar $\boxed{}$

Beispiel 6.7 **Behauptung**: Für $n \in \mathbb{N}$ gilt $1+3+\dots+(2n-1) = n^2$.

Beweis: Durch Induktion.

(IA): $n=1$, dann $1 = 1^2 = 1$.

(IS): Sei die Behauptung wahr für ein $n \in \mathbb{N}$. (*)

Dann ist $\underbrace{1+3+\dots+(2n-1)}_{= n^2 \text{ wegen } (*)} + (2n+1)$

$$= n^2 + (2n+1) = (n+1)^2$$ $\boxed{}$

Beispiel 6.8 **Behauptung**: $2^n > n^2$ für alle $n \geq 5$.

Beweis: Durch Induktion.

(IA): $n=5$, dann ist $36 = 2^5 > 5^2 = 25$.

(IS): Sei die Behauptung wahr für ein $n \geq 5$. (*)

Dann ist

$$2^{n+1} = 2\cdot 2^n \underset{\text{wegen }(*)}{>} 2\cdot n^2 = n^2 + n\cdot n$$

Weiter ist $n\cdot n \geq 5n > 2n+1$, da $n \geq 5$ ist.

Also folgt:

$$2^{n+1} > n^2 + n\cdot n > n^2 + 2n + 1 = (n+1)^2 \quad \boxed{2}$$

<u>Proposition 6.9</u> Sei $n_0 \in \mathbb{N}_0$ so, dass für alle $n \geq n_0$ $E(n)$ eine Aussage ~~und~~ ist so, dass

a) $E(n_0)$ ist wahr.

b) Für alle $n \geq n_0$: $E(k)$ ist wahr für $n_0 \leq k \leq n$ $\Rightarrow$ $E(n+1)$ ist wahr.

Dann ist $E(n)$ für alle $n \geq n_0$ wahr.

<u>Beweis:</u> Betrachte die Menge

$$N = \{ n \in \mathbb{N}_0 \mid n \geq n_0 \text{ und } E(n) \text{ falsch} \}.$$

Angenommen $N \neq \emptyset$. Dann existiert nach dem Wohlordnungsprinzip ein Minimum von N, nennen wir es m. Wegen a) gilt $m \neq n$ (Tippfehler: m not = n_0), also $m > n_0$. Es folgt aus der Definition von m, dass $E(k)$ wahr ist für alle $n_0 \leq k \leq n$ wobei $n+1 = m$. Aus (b) folgt dann aber, dass $E(n+1)$ wahr ist. Widerspruch. $\boxed{}$

Diese Version des Induktionsprinzips stellt sicher, dass wir alle Schritte zwischen n_0 und n benutzen können, um $E(n+1)$ zu zeigen.

Beispiel 6.10 (a) "Behauptung": Alle ungeraden Zahlen sind durch 2 teilbar.

"Beweis": Sei n die n^{te} ungerade Zahl. Durch Induktion sehen wir, dass n durch 2 teilbar ist. Dann ist also auch die $(n+1)^{te}$ ungerade Zahl $n+2$ durch 2 teilbar. $\boxed{\not}$

Wo liegt der Fehler?

Der Induktionsanfang wurde vergessen: In der Tat ist $n=1$ nicht durch 2 teilbar, genauso ~~wied~~ jeder andere mögliche Startpunkt.

Vorlesung 7, 05. Nov. 2018

"Die natürliche Zahlen III"

```
def fact(n)
  ...
  ...
  return n·fact(n-1)
```

Zur Erinnerung: Die natürliche Zahlen (mit Null) $\mathbb{N}_0$ sind induktiv definiert. Und das Hauptwerkzeug ist das Prinzip der Induktion.

Proposition 7.1 Es sei $\otimes : X \times X \to X$ eine assoziative Verknüpfung auf einer Menge. Dann kommt es auch bei mehr als drei Faktoren nicht auf die Klammerung an.

Wichtig: Assoziativität fordert nur Gleichheit für Ausdrücke der Länge 3, z.B. $(x \otimes y) \otimes z = x \otimes (y \otimes z)$. Daraus folgt aber schon Gleichheit für alle Längen.

Beweis: Es sei K_n eine "Klammerung der Länge n" für $n \geq 3$, d.h. für $a_1, \dots, a_n \in X$ eine beliebige Klammerung der Form $K_7 = ((a_1 \otimes a_2) \otimes (a_3 \otimes a_4)) \otimes ((a_5 \otimes (a_6 \otimes a_7)))$.
Nennen wir die Klammerung der Form

$$\overline{K}_n = (\cdots(a_1 \otimes a_2) \otimes a_3) \otimes \dots) \otimes a_n \qquad n \geq 3$$

kanonisch.

Behauptung: Jede Klammerung K_n ist gleich der kanonischen, i.e. $\overline{K}_n = K_n$.

Beweis: Durch Induktion.

(IA): Der Fall $n=3$ ist genau die Assoziativität.

(IS): Es sei $K_k = \overline{K}_k$ für $\forall\, 3 \le k \le n$, und sei K_{n+1} ein Klammerausdruck der Länge $n+1$. Dann gibt es $l, m \in \mathbb{N}$ so, dass $K_{n+1} = K_l \circledast K_m$.

Fall 1: $m=1$, also $K_m = a_{n+1}$. Dann ist nach Induktion $K_l = \overline{K}_l$ und somit $K_{n+1} = K_l \circledast a_{n+1} = \overline{K}_{n+1}$

Fall 2: $m>1$. Dann ist nach Induktion $K_m = \overline{K}_{m-1} \circledast a_{n+1}$

Also
$$K_{n+1} = K_l \circledast (\overline{K}_{m-1} \circledast a_{n+1})$$
$$\overset{\text{Asso.}}{=} (K_l \circledast \overline{K}_{m-1}) \circledast a_{n+1}$$

Nach Induktion
$$= (\cdots(a_1 \circledast a_2) \circledast a_3) \cdots) \circledast a_{n+1}$$
$$= \overline{K}_{n+1}$$

$\square$

Bevor wir nun das Prinzip der Rekursion einführen ein motivierendes Beispiel.

Beispiel 7.2

Die Fakultät ist die ~~Abbildung~~ Abbildung

Schreibe $n! = !(n)$ für diese Abbildung

$$!: \mathbb{N}_0 \to \mathbb{N}_0, \quad \begin{array}{l} 0 \mapsto 1 \\ n \mapsto 1 \cdot \ldots \cdot n \text{ für } n>0 \end{array}$$

Diese Abbildung wächst sehr schnell:

$0! = 1$; $1! = 1$; $2! = 1 \cdot 2 = 2$; $3! = 1 \cdot 2 \cdot 3 = 6$; ...

$10! = 1 \cdot 2 \cdot \ldots \cdot 9 \cdot 10 > 3628000$, ..., $1000! > 4 \cdot 10^{2567}$...

Rekursive Definition: $3! = 3 \cdot 2! = 3 \cdot 2 \cdot 1! = 3 \cdot 2 \cdot 1 \cdot 0!$ Rekursion

Startbedingung $0! = 1$ und $(n+1)! = (n+1) \cdot n!$ für $n>0$

Theorem 7.3 (Rekursionsprinzip)

Es sei $X \neq \emptyset$ und $a \in X$, genannt Startwert. Sei für $\forall n \in \mathbb{N}$ eine Abbildung $V_n : \underbrace{X \times .. \times X}_{n} = X^n \longrightarrow X$ gegeben.

Dann $\exists!\ f : \mathbb{N}_0 \longrightarrow X$ so, dass

a) $f(0) = a$ Startbedingung

b) $f(n+1) = V_{n+1}(f(0), f(1), \ldots, f(n))$ $n \in \mathbb{N}$ Rekursion

---

Beweis: i) ~~Existenzbeweis~~ Eindeutigkeit durch Induktion.

Seien also $f, g : \mathbb{N}_0 \longrightarrow X$ zwei solche Abbildungen.

Behauptung: $f(n) = g(n)$ $\forall n \in \mathbb{N}_0$

Beweis: Durch Induktion.

(IA): $n = 0$ ist wegen a) wahr.

(IS): Sei also $f(k) = g(k)$ $\forall\ 0 \leq k \leq n$. Dann folgt wegen b), dass

$$f(n+1) = V_{n+1}(f(0), \ldots, f(n)) = V_{n+1}(g(0), \ldots, g(n)) = g(n+1).$$

ii) Existenzbeweis durch Induktion.

Behauptung(*): Für jedes $n \in \mathbb{N}_0$ gibt es eine Abbildung $f_n : \{0, \ldots, n\} \rightarrow X$ mit

$$f_n(0) = a$$
$$f_n(k) = f_k(k) \qquad 0 \leq k < n$$
$$f_n(k+1) = V_{k+1}(f_n(0), \ldots, f_n(k)).$$

Beweis: (IA): $n = 0$ ist wahr, da es kein $0 \leq k < 0$ gibt also $f_0 : \{0\} \rightarrow X$ keine Bedingung erfüllen muss.

(IS): Existiere nun eine solche Funktion für alle $0 \le k \le n$. Setze

$$f_{n+1} = \begin{cases} f_n(k), & 0 \le k \le n, \\ V_{n+1}(f_n(0), \dots, f_n(n)), & k = n+1. \end{cases}$$

Per Induktion folgt

$$f_{n+1}(k) = f_n(k) = f_k(k) \quad 0 \le k \le n$$

und, zusammen mit folgt dann

$$f_{n+1}(k+1) = f_n(k+1) = V_{k+1}(f_n(0), \dots, f_n(k))$$
$$= V_{k+1}(f_{n+1}(0), \dots, f_{n+1}(k))$$

für $0 < k+1 \le n$ und

$$f_{n+1}(n+1) = V_{n+1}(f_n(0), \dots, f_n(n))$$
$$= V_{n+1}(f_{n+1}(0), \dots, f_{n+1}(n)).$$

Das beweist die Behauptung (*).

Definiere nun $f: \mathbb{N}_0 \longrightarrow X$ durch

$$f(n) = \begin{cases} a, & n = 0, \\ f_n(n), & n \in \mathbb{N}. \end{cases}$$

Wegen Behauptung (*) gilt nun aber

$$f(n+1) = f_{n+1}(n+1) = V_{n+1}(f_{n+1}(0), \dots, f_{n+1}(n))$$
$$= V_{n+1}(f_0(0), \dots, f_n(n))$$
$$= V_{n+1}(f(0), \dots, f(n))$$

Dies beweist die Existenz der Abbildung f. ☐

Beispiel 7.4

Was man eigentlich will ist die Bedeutung von "..." in der Definition von $n! = 1 \cdot \ldots \cdot n$ zu klären.

Das geht wie folgt:

Setze $V_n : \mathbb{N}_0 \times .. \times \mathbb{N}_0 \longrightarrow \mathbb{N}_0 \, , \, (y_0, .., y_{n-1}) \longmapsto y_{n-1} \cdot n$

Dann $\exists!$ $f : \mathbb{N}_0 \to \mathbb{N}_0$ so, dass $f(0) = 1$ und

$$f(n) = V_n(f(0), .., f(n-1)) = f(n-1) \cdot n$$

$\Rightarrow$ Das gilt die Fakultät.

Beispiel 7.5

Allgemeiner als Beispiel 7.4. Sei $\circledast$ eine assoziative Verknüpfung auf einer Menge $X \neq \emptyset$. Und seien $x_k \in X$ für $k \in \mathbb{N}_0$ gegeben. Um

$$\bigcircledast_{k=0}^{n} x_k = x_0 \circledast \ldots \circledast x_n$$

zu definieren benutze die Abbildung

$$V_n : X^n \longrightarrow X \, , \quad (y_0, .., y_{n-1}) \longmapsto y_{n-1} \circledast x_n$$

Dann $\exists!$ $f : \mathbb{N}_0 \longrightarrow X$ so, dass $f(0) = x_0$ und

$$f(n) = V_n(f(0), .., f(n-1)) = f(n-1) \circledast x_n = \bigcircledast_{k=0}^{n} x_k$$

$\Rightarrow$ Wir erhalten

Rekursion

$$\bigcircledast_{k=0}^{0} x_k = x_0 \quad \text{und} \quad \bigcircledast_{k=0}^{n+1} x_k = \bigcircledast_{\ell=0}^{n} x_\ell \circledast x_{n+1}$$

Startbedingung

Beispiel 7.6

Wie in Beispiel 7.5 können wir ⊛ auch als

$+ : \mathbb{N}_0 \times \mathbb{N}_0 \longrightarrow \mathbb{N}_0$ oder $\cdot : \mathbb{N}_0 \times \mathbb{N}_0 \longrightarrow \mathbb{N}_0$

wählen und erhalten rekursiv

$$\sum_{k=0}^{n} x_k = x_0 + \ldots + x_n \quad \text{und} \quad \prod_{k=0}^{n} x_k = x_0 \cdot \ldots \cdot x_n$$

Proposition 7.7 Sei ⊛ wie in Beispiel 7.5, aber zusätzlich kommutativ. Und sei $\sigma : \{0,\ldots,n\} \to \{0,\ldots,n\}$ eine Bijektion (Permutation $\hat{=}$ Umnummerierung).

Dann ist $\circledast_{k=0}^{n} x_k = \circledast_{k=0}^{n} x_{\sigma(k)}$

Beweis: Ausgelassen. (Induktion)

Proposition 7.8 Seien $+, \cdot$ wie in Beispiel 7.6.

Dann gelten folgende Rechenregeln.

a) $\sum_{k=0}^{n} a_k + \sum_{k=0}^{n} b_k = \sum_{k=0}^{n} (a_k + b_k)$

b) $\prod_{k=0}^{n} a_k \cdot \prod_{k=0}^{n} b_k = \prod_{k=0}^{n} (a_k b_k)$

c) $\sum_{j=0}^{m} a_j \cdot \sum_{k=0}^{n} b_k = \sum_{j=0}^{m} \left(\sum_{k=0}^{n} a_j b_k \right) = \sum_{k=0}^{n} \left(\sum_{j=0}^{m} a_j b_k \right)$

Beweis: Ausgelassen (Induktion)

7.6 + 7.8 gelten allgemeiner für Verknüpfungen welche kommutativ +assoziativ und distributiv sind.

$\boxed{\text{Aber Vorsicht: Alles ist endlich!}}$

Beispiel 7.9

Sei $\circledast$ wie in Beispiel 7.5 und sei e eine Einheit für $\circledast$ $\boxed{(\text{Denke: } \circledast = \cdot \quad e = 1)}$

Für $a \in X$ definiere rekursive die n-te Potenz

Start $a^0 = e$ und $a^{n+1} = a^n \circledast a$ Rekursion

Dann kann man folgende $\boxed{\text{Rechenregeln}}$ zeigen:

$$a^1 = a \quad , \quad e^n = e \quad ; \quad a^n \circledast a^m = a^{n+m} \quad , \quad (a^n)^m = a^{nm}$$

Für $a, b \in X$ mit $a \circledast b = b \circledast a$ folgt sogar

$$(a \circledast b)^n = a^n \circledast b^n$$

Beispiel 7.10

Sei $+$ wie in Beispiel 7.6. und $a \in \mathbb{N}_0$.

Dann kann man rekursiv

Start $0 \cdot a = 0$ und $(n+1) \cdot a = (n \cdot a) + a$ Rekursion

definiere, genannt n-fache von a.

Es gilt dann:

$$n \cdot 0 = 0 \quad , \quad n \cdot a + m \cdot a = (n+m) \cdot a$$

$$m \cdot (n \cdot a) = (mn) \cdot a$$

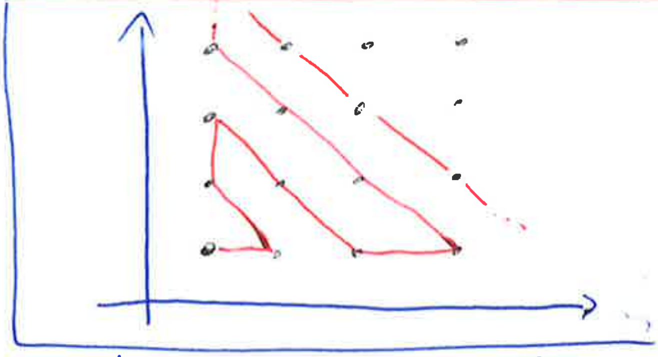
$$n \cdot a + n \cdot \underset{\mathbb{N}_0}{\underset{\cap}{b}} = n \cdot (a + b)$$

$\boxed{\text{Rechenregeln}}$

Vorlesung 8, 12. Nov. 2018

"Naive Mengenlehre IV"

Was wir noch nicht wirklich behandelt haben ist Unendlichkeit von Mengen. Das ist das Ziel der Vorlesung.



Lemma 8.1 Es sei $\varphi : \{1, \dots, n\} \xrightarrow{1:1} \{1, \dots, m\}$ eine Bijektion. Dann ist $m = n$.

Schreibweise für bijektiv

Beweis: Wegen Surjektivität folgt, dass $m \leq n$ gilt, und wegen Injektivität folgt, dass $n \leq m$ gilt. $\square$

Eine Menge $X \neq \emptyset$ heißt endlich, falls $\exists \varphi : X \xrightarrow{1:1} \{1, \dots, n\}$ bijektiv, ansonsten heißt X unendlich. $\emptyset$ ist auch endlich.

Die (naive) Anzahl der Elemente von X ist

$$~~\text{Anz}(X)~~ \; |X| = \begin{cases} 0, & \text{falls } X = \emptyset \\ n \in \mathbb{N}, & \text{falls } \exists \varphi : X \xrightarrow{1:1} \{1, \dots, n\} \\ \infty, & \text{sonst.} \end{cases}$$

Wegen Lemma 8.1 ist $|X|$ wohldefiniert.

X heißt n-elementig, falls $|X| = n \in \mathbb{N}$ oder $X = \emptyset$

0-elementig

Beispiel 8.2 Die Menge $\{1, 2, 3\}$ ist 3-elementig, genauso wie die Menge $\{a, b, c\}$.

Eine Permutation einer endlichen Menge X ist eine Bijektion $\sigma : X \xrightarrow{1:1} X$, deren Menge ist $S(X)$.

Proposition 8.3

Für eine n-elementige Menge X gilt $|S(X)| = n!$

Beweis Durch Induktion.

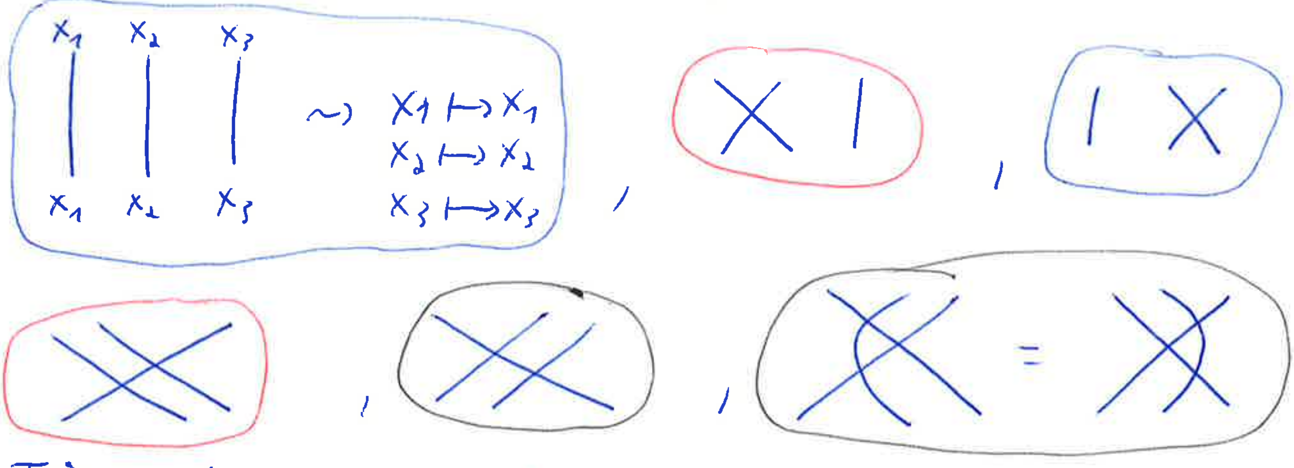
(IA): $n=0$ ist klar, da es genau eine Abbildung $\emptyset \to \emptyset$ gibt.

(IS): Sei die Behauptung also wahr für n.

Sei $X = \{x_1, \dots, x_{n+1}\}$ $n+1$-elementig. Dann gibt es nach Induktion genau $n!$ Bijektionen $\sigma : X \xrightarrow{1:1} X$ mit $\sigma(x_{n+1}) = x_{n+1}$.

Anfang für jedes andere x_ℓ $(1 \le \ell < n+1)$, also gibt es $n!(n+1)$ Permutationen. $\boxtimes$

Beispiel 8.4 Bildchen für $n=3$



Fixiere $x_1 \mapsto x_1$, $x_2 \mapsto x_1$, $x_3 \mapsto x_1$

Zwei Mengen X, Y heißen gleichmächtig, falls $\exists \varphi : X \xrightarrow{1:1} Y$, und X heißt abzählbar unendlich, wenn $\exists \varphi : X \xrightarrow{1:1} \mathbb{N}_0$

Beispiel 8.5 $\mathbb{N}_0$ und $\mathbb{N}$ sind gleichmächtig

(und beide abzählbar unendlich). Hier ist eine Bijektion:

$$\nu : \mathbb{N}_0 \longrightarrow \mathbb{N}, \quad n \longmapsto n+1$$

Eine Menge X heißt abzählbar, wenn X endlich ist oder unendlich abzählbar, sonst heißt X überabzählbar. Frage: Gibt es überabzählbare Mengen?

abzählbar unendlich (Wortdreher)

Theorem (Cantor) 8.6

Es gibt keine Surjektion $X \longrightarrow P(X)$.
(Und damit sind X und $P(X)$ niemals gleichmächtig.)

Beweis: Wegen $P(\emptyset) = \{\emptyset\}$ ist dies klar für $X = \emptyset$.
Sei also $X \neq \emptyset$ und betrachte für eine beliebige Abbildung $\varphi : X \longrightarrow P(X)$ die Teilmenge

$$A = \{x \in X \mid x \notin \varphi(x)\} \subset X.$$

Angenommen $\exists\, y \in X$ mit $\varphi(y) = A$. Dann:
$y \in A \Rightarrow y \notin \varphi(y) = A$ (Widerspruch) oder
$y \notin A \Rightarrow y \in \varphi(y) = A$ (Widerspruch). Somit hat A kein Urbild. ☒

Beispiel 8.7 Cantors Theorem liefert sofort eine überabzählbare Menge, nämlich $P(\mathbb{N}_0)$.

Proposition 8.8

Jede Teilmenge einer abzählbaren Menge ist selbst abzählbar.

Beispiel 8.9 Alle Teilmengen von $\mathbb{N}_0$, z.B. die geraden Zahlen, sind abzählbar.

Beweis: Die Aussage ist klar für X endlich, also können wir annehmen, dass X abzählbar unendlich ist. Dann können wir aber sogar annehmen, dass $X = \mathbb{N}_0$ gilt, wo die Aussage für A endlich klar ist.
Sei also $A \subset \mathbb{N}_0$ ~~abzählbar~~ nicht endlich.

Definiere rekursiv $\alpha : \mathbb{N}_0 \longrightarrow A$ durch

$$\alpha(0) = \min(A) \quad , \quad \alpha(n+1) = \min\{m \in A \mid m > \alpha(n)\}$$

Existiert nach dem Wohlordnungsprinzip

Es gilt nun $\alpha(n+1) > \alpha(n)$ und $\alpha(n+1) \geq \alpha(n) + 1 \ \forall n \in \mathbb{N}_0$.
Deswegen $\boxed{\text{liefert Induktion}}$, dass sogar $\alpha(n+k) > \alpha(n)$ für $k \in \mathbb{N}$ gilt. Also ist α $\boxed{\text{injektiv.}}$

Per Induktion zeige ich:

Dem Leser überlassen.

Behauptung $\alpha(m) \geq m \quad \forall m \in \mathbb{N}_0$

Beweis: (IA) $m = 0$ ist klar. (IS) ~~Es~~ $\boxed{\text{Ausgelassen}}$

(OD) Angenommen $\alpha(m + \cancel{1}) \geq m$ und fixiere $n_0 \in A$.
Sei $B = \{m \in \mathbb{N}_0 \mid \alpha(m) \geq n_0\}$ welche wegen $\alpha(m) \geq m$ nicht leer ist. Setze $m_0 = \min(B)$. Gilt $m_0 = 0$, so folgt

$$\min(A) = \alpha(0) \geq n_0 \geq \min(A)$$

injektiv

also $n_0 = \alpha(0)$. Für $n_0 > \min(A)$ gilt

$$\alpha(m_0 - 1) < n_0 \leq \alpha(m_0) \Rightarrow \alpha(m_0) = n_0$$

$\boxed{2}$

~~Beispiel 18.9 (Cantor-Schröder-Bernstein)~~

Tippfehler: "Wie in" nicht "Wegen".

Wegen Proposition 8.8 kann man bei Aussage über abzählbar unendliche Mengen immer annehmen, dass sie $\mathbb{N}_0$ sind.

Beispiel 8.10 Cantors Schema

$\mathbb{N}_0 \times \mathbb{N}_0$ ist abzählbar:

$$
\begin{array}{c|cccccc}
 & \vdots & \vdots & \vdots & \vdots & \\
 & (0,3) & (1,3) & (2,3) & (3,3) & \cdots \\
\mathbb{N}_0 & (0,2) & (1,2) & (2,2) & (3,2) & \cdots \\
 & (0,1) & (1,1) & (2,1) & (3,1) & \cdots \\
 & (0,0) & (1,0) & (2,0) & (3,0) & \cdots \\
\hline
 & & & \mathbb{N}_0 & &
\end{array}
$$

Dasselbe gilt für $\mathbb{N}_0^n$!

Proposition 8.11

Jede abzählbare Vereinigung abzählbarer Mengen ist selbst abzählbar.

Beweis: ~~Benutze~~ Ausgelassen. (Benutze Cantors Schema)

Proposition 8.12

Jedes endliche Produkt abzählbarer Mengen ist abzählbar.

Beweis: Ausgelassen. (Benutze Cantors Schema)

Beispiel 8.13 Endliche Produkte endlicher Mengen

sind nicht gleichmächtig. Zum Beispiel für $X = \{1,2\}$ hat $X \times X$ die Elemente

$$
\begin{array}{c|cc}
X & (1,2) & (2,2) \\
 & (1,1) & (2,1) \\
\hline
 & & X
\end{array}
$$

, also

~~Anz~~ $|X| = 2$

$|X \times X| = \cancel{2}\ 4 = 2^2$

Allgemeiner: Sei $|X_k| = x_k \in \mathbb{N}_0$. Dann ist

$$\left|\prod_{k=0}^{n} X_k\right| = |X_0| \cdot \ldots \cdot |X_k| = \prod_{k=0}^{n} |X_k| \geq |X_k| \;\forall k$$

Aber $\prod_{k=0}^{n} \mathbb{N}_0$ ist gleichmächtig ("gleich groß") zu $\mathbb{N}_0$, wie Cantors Schema zeigt.

Zur Erinnerung: $X^Y = Abb(Y, X)$

Im allgemeinen sind "unendliche Produkte" endlicher Mengen nicht abzählbar.

"Unendliches Produkt" ist per Definition X^Y für unendliches Y wie folgendes Lemma sicherstellt:

Lemma 8.14 Es gilt für jedes ~~Menge~~ $n \in \mathbb{N}_0$ eine Bijektion $\varphi: X^n \xrightarrow{1:1} X^n$.

$\boxed{X \neq \emptyset}$

$$X^n = \underbrace{X \times \ldots \times X}_{n}, \qquad X^n = \begin{cases} Abb(\{1, \ldots, n\}, X), & n \neq 0 \\ \emptyset, & n = 0 \end{cases}$$

Beweis: Der Fall $n = 0$ ist klar. Betrachte nun folgende Abbildungen:

$$\varphi: \underbrace{X \times \ldots \times X}_{n} \longrightarrow Abb(\{1, \ldots, n\}, X)$$
$$(x_1, \ldots, x_n) \longmapsto \begin{cases} \psi \in Abb(\{1, \ldots, n\}, X) \\ \psi(k) = x_k \end{cases}$$

$$\psi: Abb(\{1, \ldots, n\}, X) \longrightarrow X \times \ldots \times X$$
$$\psi \longmapsto (\psi(1), \ldots, \psi(n))$$

Dann gilt $\psi \circ \varphi = id_{X \times \ldots \times X}$ und $\varphi \circ \psi = id_{Abb(\{1, \ldots, n\}, X)}$.

Zur Erinnerung: $f \circ g = id$ und $g \circ f = id$ $\Rightarrow$ beide bijektiv

(3)

Proposition 8.15 Es gilt eine Bijektion $\{0,1\}^{\mathbb{N}_0} \xrightarrow{1:1} P(\mathbb{N}_0)$. Insbesondere ist $\{0,1\}^{\mathbb{N}_0}$ nicht abzählbar.

Beweis: Definiere

$$\varphi: \{0,1\}^{\mathbb{N}_0} \longrightarrow P(\mathbb{N}_0)$$
$$\psi \longmapsto A = \{n \in \mathbb{N}_0 \mid \psi(n) = 1\}$$

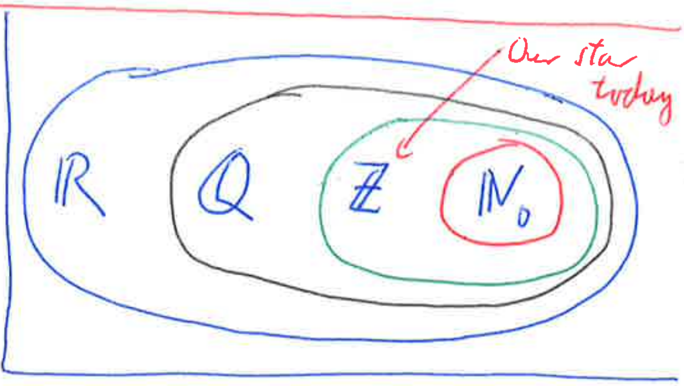
und

$$\psi: P(\mathbb{N}_0) \longrightarrow \{0,1\}^{\mathbb{N}_0}$$
$$A \longmapsto \left(\psi: \mathbb{N}_0 \to \{0,1\},\ \psi(n) = \begin{cases} 0, & \text{falls } n \notin A, \\ 1, & \text{falls } n \in A. \end{cases}\right.$$

Dann gilt $\psi \circ \varphi = id_{\{0,1\}^{\mathbb{N}_0}}$ und $\varphi \circ \psi = id_{P(\mathbb{N}_0)}$, also ist φ eine Bijektion. $\boxed{}$

Vorlesung 9, 15. Nov. 2018

"Die rationalen Zahlen I"



Sei $\otimes : X \times X \longrightarrow X$ eine Verknüpfung mit Einheit e. Dann heißt $x \in X$ <u>invertierbar</u> (bzgl. $\otimes$) mit <u>Inverse</u> x^{-1} falls $x^{-1} \in X$ existiert und $x \otimes x^{-1} = e = x^{-1} \otimes x$ gilt.

Wie immer sind Inverse eindeutig, falls existent:

$$x^{-1} = x^{-1} \otimes x \otimes \tilde{x}^{-1} = \tilde{x}^{-1}$$

<u>Beispiel 9.1</u> $\mathbb{N}_0$ hat zwei Verknüpfungen, $+$ und $\cdot$, mit Einheiten 0 und 1. Aber kein Element $n \in \mathbb{N}$ $(n \neq 1)$ ist invertierbar, weder bzgl. $+$ noch $\cdot$, denn

$$m + n = 0 \Rightarrow m = n = 0 \quad \text{bzw.} \quad m \cdot n = 1 \Rightarrow m = n = 1$$

Genau das wollen wir "beheben" und führen dazu $\mathbb{Z}$ (heute) bzw. $\mathbb{Q}$ ein (nächstes Mal)

<u>Konvention 9.2</u>: Im Folgenden bezeichnet $+$ eine assoziative und kommutative Verknüpfung mit Einheit 0 ← genannt <u>Null</u>, und $\cdot$ eine assoziative und kommutative Verknüpfung mit Einheit 1. ← genannt <u>Eins</u>

Vorsicht: Diese müssen nicht auf $\mathbb{N}_0$ sein, ~~[illegible]~~

Außerdem, falls $+, \cdot$ auf einer Menge sind, bindet $\cdot$ stärker, d.h. $a \cdot b + c = (a \cdot b) + c$ etc.

Ein kommutativer Ring R mit Eins, kurz: Ring, ist eine Menge R mit $\boxed{\text{zwei Verknüpfungen}}$

$+ : R \times R \longrightarrow R \qquad \cdot : R \times R \longrightarrow R$

welche $\boxed{\text{distributiv}}$ sind

$$(a+b)c = ac + bc \quad \forall\, a,b,c \in R$$

und jedes Element $a \in R$ ist $\boxed{\text{bzgl. } + \text{ invertierbar}}$

Vorsicht: Im allgemeinen fordert man nicht, dass $\cdot$ kommutativ ist und eine Einheit besitzt.

Das Inverse von a wird mit $-a$ bezeichnet, also

$a + (-a) = a - a = 0 = (-a) + a$

Für folgende Tatsache sei auf [AE06, Bemerkungen 8.1] verwiesen:

- Für alle $a, b \in R$ hat $a + x = b$ eine Lösung, nämlich $x = b + (-a) = b - a$, genannt Differenz. (Man kann + kürzen)
- Für $\forall\, a \in R$ gilt $a0 = 0a = 0$
- Es kann $a, b \neq 0$ geben mit $ab = 0$. Deswegen besitzt $ab = x$ im Allgemeinen keine Lösung. (Man kann $\cdot$ nicht kürzen.)
- Es gilt $a(-b) = (-a)b = -(ab) = -ab$ und $(-a)(-b) = ab$
- Es gilt $(-1)a = -a$.
- Rekursiv kann man $n \cdot a = $ "na" $= a + \dots + a$ und $a^n = a \cdots a$ definieren.

Analog für endl. Produkte und Summen

Beispiel 9.3 Ist R ein Ring, so ist $R \times R$ auch ein Ring, wobei die Multiplikation und Addition komponentenweise definiert sind: ↪ Null ist $(0,0)$

$$(a_1,a_2)+(b_1,b_2)=(a_1+b_1,\ a_2+b_2)$$

$$(a_1,a_2)\cdot(b_1,b_2)=(a_1b_1,\ a_2b_2)$$ Eins ist $(1,1)$

Damit gilt insbesondere $(1,0)\cdot(0,1)=(1\cdot 0,\ 0\cdot 1)=(0,0)$

Analog für alle endliche Produkte.

<u>Beispiel 9.4</u> Für unendliche Produkte R^X kann man durch

$$(f+g)(x)=f(x)+g(x) \qquad x\in X$$
$$(fg)(x)=f(x)\,g(x) \qquad f,g\in R^X=\mathrm{Abb}(X,R)$$

eine Ringstruktur definieren. Null ist die Abbildung $f(x)=0$, Eins die Abbildung $f(x)=1$.

<u>Theorem 9.5 (Binomische Satz)</u>

Sei R ein Ring. Dann gilt $\forall a,b\in R\ \ \forall n\in\mathbb{N}_0$:

$$(*)\qquad (a+b)^n=\sum_{k=0}^{n}\binom{n}{k}a^k b^{n-k},$$

wobei $\binom{n}{k}=\begin{cases}\frac{n!}{k!(n-k)!} & \\ 0, & \text{falls } k>n\end{cases}$ ← $\in\mathbb{N}_0$ wegen Übungsaufgabe 7.1

$n,k\in\mathbb{N}_0$

<u>Beweis</u>: Bemerke zuerst, dass beide Seiten von $(*)$ wohldefiniert sind.

Weiter: <u>Behauptung</u>: Es gilt $\binom{n}{k-1}+\binom{n}{k}=\binom{n+1}{k}$ für $1\le k\le n$.

<u>Beweis</u>: Ausgelassen. (Induktion nach n)

Nun ~~...~~ Induktion nach n.

(IA): $n=0$ ist wahr, denn $(a+b)^0 = 1 = \sum_{k=0}^{0} \binom{0}{k} a^k b^{n-k}$.

(IS): Gelte $(*)$ nun also für n.

Dann $(a+b)^{n+1} = (a+b)^n (a+b)$

$$\overset{\text{Induktion}}{=} \left(\sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k} \right)(a+b)$$

$$= \sum_{k=0}^{n} \binom{n}{k} a^{k+1} b^{n-k} + \sum_{k=0}^{n} \binom{n}{k} a^k b^{n+1-k}$$

$$= a^{n+1} + \left(\sum_{k=0}^{n-1} \binom{n}{k} a^{k+1} b^{n-k} \right) + \left(\sum_{k=1}^{n} \binom{n}{k} a^k b^{n+1-k} \right) + b^{n+1}$$

$$= a^{n+1} + \left(\sum_{k=1}^{n} \left[\binom{n}{k-1} + \binom{n}{k} \right] a^k b^{n+1-k} \right) + b^{n+1}$$

$$\overset{(\boxtimes)}{=} a^{n+1} + \sum_{k=1}^{n} \binom{n+1}{k} a^k b^{n+1-k} + b^{n+1} \qquad \boxtimes$$

Beispiel 9.6 Es gilt $(a+b)^0 = 1$,
$(a+b)^2 = a^2 + 2ab + b^2$, $(a+b)^3 = a^3 + 3a^2b + 3ab^2 + b^3$
etc. und das gilt in jedem Ring.

Zurück zu $\mathbb{N}_0$: Dies ist beinahe ein Ring, es fehlen die Inversen, also "$-n$".

Idee: Nehmen wir an $\mathbb{Z}$ sei ein Ring mit $\mathbb{Z} \supset \mathbb{N}_0$ so, dass $+, \cdot$ von $\mathbb{Z}$ mit den von $\mathbb{N}_0$ übereinstimmt.

Dann ist aber $m - n \in \mathbb{Z}$ für $(m,n) \in \mathbb{N}_0^2$

definiert. Allgemeiner:

$$\underbrace{m-n = m'-n'}_{\text{in } \mathbb{Z}} \iff \underbrace{m+n' = m'+n}_{\text{in } \mathbb{N}_0}$$

Diese Betrachtung legt nahe $\mathbb{Z}$ aus Zahlenpaaren $(m,n) \in \mathbb{N}_0^2$ zu konstruieren. In der Tat:

Theorem 9.7 Es gibt einen kleinsten, nullteilerfreien Ring $\boxed{\mathbb{Z}} \supset \mathbb{N}_0$, der auf $\mathbb{N}_0$ die ursprüngliche $+$ und $\cdot$ induziert. Dieser Ring ist bis auf Isomorphie eindeutig und wird Ring der ganzen Zahlen genannt.

Bemerkung 9.8 – "kleinste" bedeutet, dass jeder andere Ring R mit diesen Eigenschaften $R \supset \mathbb{Z}$ erfüllt (mit induzierten $+, \cdot$)

– "nullteilerfrei" heißt $a \cdot b = 0 \iff (a = 0 \vee b = 0)$

– "Ein Isomorphismus von Ringen $(R, +, \cdot)$ und $(Q, \tilde{+}, \tilde{\cdot})$ ist eine Bijektion $\varphi: R \to Q$ so, dass "die Ringstruktur erhalten wird", d.h.

$$\varphi(a+b) = \varphi(a) \tilde{+} \varphi(b), \quad \varphi(a \cdot b) = \varphi(a) \tilde{\cdot} \varphi(b)$$
$$\varphi(0_R) = 0_Q \quad ; \quad \varphi(1_R) = 1_Q$$

Das ist der technische Ausdruck für "als Ringe gleich bis auf Umbenennung" (Details [AE06, Sektion I.8].).

Beweis (Skizze, denn der echte Beweis ist lang)

Schritt 1: Definiere auf $\mathbb{N}_0 \times \mathbb{N}_0$ eine Relation ~ durch

$$(m,n) \sim (m',n') \Leftrightarrow m+n' = m'+n.$$

Dies ist eine Äquivalenzrelation, denn

Reflexiv $(m,n)\sim(m,n)$, da $m+n = m+n$

Symmetrisch $(m,n)\sim(m',n')$, da $m+n = n+m$
$\Rightarrow (m',n')\sim(m,n)$

Transitiv $\underbrace{(m,n)\sim(m',n')}_{m+n'=m'+n} \wedge \underbrace{(m',n')\sim(m'',n'')}_{m'+n''=m''+n'}$, wegen Kürzungsregel
$\Rightarrow (m,n)\sim(m'',n'') \rightarrow m+n'' = m''+n$

$m+n'+n'' = m'+n+n''$
$m+n''+n'$ $\quad m''+n+n'$

Schritt 2:
Setze $\mathbb{Z} = \mathbb{N}_0^2/\sim$ und notiere $\underset{[(n,0)]}{\overset{}{n}} \in \mathbb{Z}$, $-\underset{[(0,n)]}{n} \in \mathbb{Z}$ für $n \in \mathbb{N}_0$

Definiere:

$$[(m,n)] + [(m',n')] = [(m+m', n+n')]$$
$$[(m,n)]\cdot[(m',n')] = [(mm'+nn', mn'+n'n)]$$

Man überlege sich, warum das wohldefiniert ist...

Dann ist $[(0,0)] + [(m,n)] = [(m,n)]$
und $+_{\mathbb{Z}}$ ist kommutativ und assoziativ, da $+_{\mathbb{N}_0}$ beides ist.

Null in $\mathbb{Z}$

Analog, man sieht durch ausrechnen, dass $\cdot_{\mathbb{Z}}$ kommutativ und assoziativ ist, da $+_{\mathbb{N}_0}, \circ_{\mathbb{N}_0}$ dies sind und ~~be~~ zusammen distributiv sind. Auch ist

$$\underbrace{[(1,0)]}_{\text{Eins in } \mathbb{Z}} \cdot [(m,n)] = [(m,n)]$$

Schritt 3:

Und weiter gilt es einen ~~Ringisomorphismus~~ Abbildung: $\varphi: \mathbb{N}_0 \longrightarrow \mathbb{Z}$

$$n \longmapsto [(n,0)] = n$$

welche injektiv ist und $\varphi(0) = 0_{\mathbb{Z}}$, $\varphi(1) = 1_{\mathbb{Z}}$

$\varphi(m+n) = \varphi(m) +_{\mathbb{Z}} \varphi(n)$ und $\varphi(mn) = \varphi(m) \cdot_{\mathbb{Z}} \varphi(n)$

Schritt 4: Es gilt $n + (-n) = 0$, denn

$$[(n,0)] + [(0,n)] = [(n,n)], \text{ aber}$$

$$(n,n) \sim (0,0), \text{ denn } n + 0 = \cancel{n+0}\ 0 + n$$

Also gilt es Inverse.

Zusammen: Schritte 1–4 zeigen, das $\mathbb{Z}$ ein Ring ist, welcher $\mathbb{N}_0$ enthält.

Schritt 5: $\underbrace{[(m,n)]}_{a} \cdot \underbrace{[(m',n')]}_{b} = [(mm' + nn'), (mn' + m'n)] = 0_{\mathbb{Z}}$

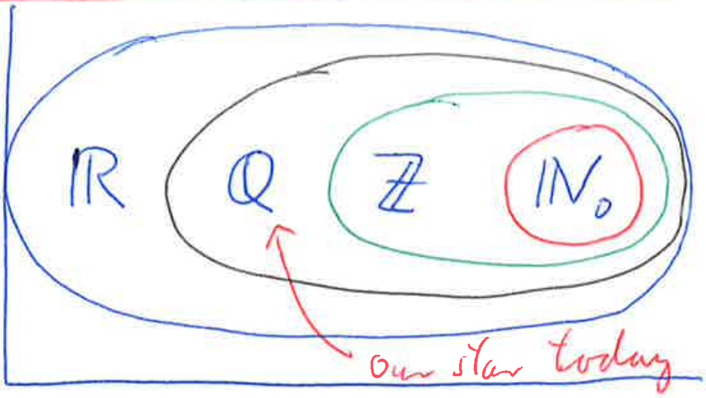
$\Leftrightarrow$ $m = n$ oder $m' = n'$ $\Leftrightarrow$ $a = 0 \vee b = 0$

Schritt 6: $\mathbb{Z}$ ist minimal, da exakt die $+$-Inversen hinzugefügt werden "$\mathbb{Z} = -\mathbb{N} \cup \underbrace{\{0\} \cup \mathbb{N}}_{\mathbb{N}_0}$"

Schritt 7: Man baut induktiv einen Ringisomorphismus zu anderen minimalen Konstruktionen.

Vorlesung 10, 19. Nov. 2018

$\boxed{\text{"Die rationalen Zahlen II"}}$



Letztes Mal haben wir additive Inverse zu $\mathbb{N}_0$ hinzugefügt, damit wir subtrahieren können: Wir haben den Ring $\mathbb{Z} \supset \mathbb{N}_0$ ~~als~~ rein algebraisch aus $\mathbb{N}_0$ konstruiert. Aber wir können noch nicht teilen. Deswegen:

Ein Körper K ist ein $\boxed{\text{Ring}}$, so, dass
- $\boxed{0 \neq 1}$ gilt.
- Jedes Element $a \in K^\times = K - \{0\}$ $\boxed{\text{invertierbar bzgl. } \cdot}$ ist.

__Beispiel 10.1__ Jeder Körper hat wegen $0 \neq 1$ mindestens zwei Elemente. In der Tat gibt es einen Körper $\mathbb{F}_2$ mit zwei Elementen: Es ist $\mathbb{F}_2 = \{0, 1\}$ mit

+	0	1
0	0	1
1	1	0

$1+1=0$

·	0	1
0	0	0
1	0	1

Man prüft nach, dass dies die Körperaxiome erfüllt.

Für $a \in K^\times$ schreibt man a^{-1} für das Inverse. Wie immer sind diese eindeutig

$$a'^{-1} = a'^{-1} \cdot a \cdot a^{-1} = a^{-1}.$$

Also gilt $(a^{-1})^{-1} = a$.

__Lemma ($\boxed{\cdot\text{-Kürzen}}$) 10.2__

Jeder Körper ist nullteilerfrei, d.h.

$$a \cdot b = 0 \iff a = 0 \lor b = 0$$

Beweis: Sei $ab=0$ ~~und~~ wobei $a\neq 0$. Dann ist $b = a^{-1}\{ab\} = a^{-1}\cdot 0 = 0$ $\boxed{\checkmark}$

Es folgt also, dass $ax=b$ für alle $a\in K^{\times}$, $x,b\in K$ eine Lösung besitzt, nämlich $x=ba^{-1}$. Diese nennt man Quotienten und schreibt $\frac{b}{a}$.

Vorsicht: Null 0 besitzt kein Inverses. Also "darf nicht durch Null geteilt werden".

Lemma 10.3 (Rechenregeln)

Für $a,c\in K$, $b,d\in K^{\times}$ gilt:

a) $\frac{a}{b}=\frac{c}{d} \Leftrightarrow ad=bc$

b) $\frac{a}{b}\pm\frac{c}{d}=\frac{ad\pm cb}{bd}$, $\frac{a}{b}-\frac{c}{d}=\frac{ad-cb}{bd}$

c) $\frac{a}{b}\cdot\frac{c}{d}=\frac{ac}{bd}$

d) $\frac{a}{b}/\frac{c}{d}=\frac{ad}{bc}$, falls $c\neq 0$.

Beweis: Ausgelassen.

Lemma 10.3 a) legt nahe einen Körper $K\supset\mathbb{Z}$ durch paare ganze Zahlen zu konstruieren. Dabei soll dieser Körper wieder minimal sein, mit der Eigenschaft, das $+,\cdot$ auf $\mathbb{Z}$ übertragen werden. Dieser Körper, welcher bis auf Ringisomorphismen = Körperisomorphismen, eindeutig ist wird mit $\mathbb{Q}$ bezeichnet.

Man kann zeigen, dass $\varphi(a^{-1})=\varphi(a)^{-1}$ automatisch für einen Ringisomorphismus zwischen $K\to K'$ gilt.

Theorem 10.4 Es gibt einen kleinsten Körper $\mathbb{Q} \supset \boxed{\mathbb{Z}} \supset \boxed{\mathbb{N}_0}$, der auf $\mathbb{Z}$ und $\mathbb{N}_0$ die ursprüngliche $+$ und $\cdot$ induziert. Dieser Körper ist bis auf Isomorphie eindeutig und wird Körper der rationalen Zahlen genannt.

Beweis (Skizze). Sei $\mathbb{Z}^\times = \mathbb{Z} - \{0\}$.

Schritt 1: Definiere auf $\mathbb{Z} \times \mathbb{Z}^\times$ eine Relation $\sim$ durch

$$(a,b) \sim (a',b') \iff ab' = a'b.$$

Dies ist eine Äquivalenzrelation, denn

Reflexiv $\quad (a,b) \sim (a,b)$, da $ab = ab$

Symmetrisch $\quad (a,b) \sim (a',b') \Rightarrow (a',b') \sim (a,b)$, da $ab = ba$

Transitiv $\quad \underbrace{(a,b) \sim (a',b')}_{ab' = a'b} \wedge \underbrace{(a',b') \sim (a'',b'')}_{a'b'' = a''b'} \Rightarrow \underbrace{(a,b) \sim (a'',b'')}_{ab'' = a''b}$, wegen Kürzen

$$ab'b'' = a'bb'' = a''b'b$$

Kürze

Schritt 2: Setze $\mathbb{Q} = (\mathbb{Z} \times \mathbb{Z}^\times)/\sim$ und notiere

$$[(a,b)] = \frac{a}{b} \quad \text{und} \quad [(a,1)] = a.$$

Definiere:

$$[(a,b)] + [(a',b')] = [(ab' + a'b, bb')]$$

$$[(a,b)] \cdot [(a',b')] = [(aa', bb')]$$

Man überlege sich, dass das wohldefiniert ist

$+_{\mathbb{Q}}$ ist kommutativ

$$[(a,b)] + [(a',b')] = [(ab' + a'b, bb')]$$

$$\shortparallel$$

$$[(a',b')] + [(a,b)] = [(a'b + ab', b'b)]$$

da $+_{\mathbb{Z}}, \cdot_{\mathbb{Z}}$ kommutativ sind.

Analog $+_{\mathbb{Q}}$ ist assoziativ, $\cdot_{\mathbb{Q}}$ ist assoziativ

$\cdot_{\mathbb{Q}}$ ist kommutativ und zusammen distributiv

Weiter ist $[(0,b)] = [(0,1)]$, da

$$(0,b) \sim (0,1) \text{ wegen } 0 \cdot 1 = 0 = 0 \cdot b$$

Also ist $[(0,1)] + [(a,b)] = [(a,b)]$ das Nullelement.

Weiter ist $[(1,1)] \cdot [(a,b)] = [(a,b)]$, also ist $[(1,1)]$ das Einselement.

<u>Schritt 3:</u> Es gilt eine Abbildung

$$\varphi : \mathbb{Z} \longrightarrow \mathbb{Q}$$
$$a \longmapsto [(a,1)] = a$$

welche injektiv ist und $\varphi(0) = 0_{\mathbb{Q}}$, $\varphi(1) = 1_{\mathbb{Q}}$

$\varphi(a+b) = \varphi(a) +_{\mathbb{Q}} \varphi(b)$ und $\varphi(ab) = \varphi(a) \cdot_{\mathbb{Q}} \varphi(b)$ erfüllt.

Man könnte sagen $\mathbb{Z}$ ist ein Unterring von $\mathbb{Q}$.

Schritt 4: Es gilt $a \cdot a^{-1} = 1$ für $a \in \mathbb{Q}^\times$, denn

$$[(a,1)] \cdot [(\underbrace{1,a}_{a^{-1}})] = [(a,a)], \text{ aber}$$

$$(a,a) \sim (1,1), \text{ denn } a \cdot 1 = 1 \cdot a$$

Also gilt es Inverse.

Zusammen: Schritte 1–4 zeigen, dass $\mathbb{Q}$ ein Körper ist, welcher $\mathbb{Z}$ enthält.

Schritt 5: Entfällt, da Körper immer Nullteilerfrei sind

Schritt 6: $\mathbb{Q}$ ist Minimal, da exakt die Inverse hinzugefügt werden "$\mathbb{Q} = (\mathbb{Z}^\times)^{-1} \cup \underbrace{\{0\} \cup \mathbb{Z}^\times}_{\mathbb{Z}}$"

Schritt 7: Man baut auch wieder einen Ringisomorphismus zu anderen minimalen Konstruktionen $\boxed{\mathbb{Z}}$

Proposition 10.5 $\mathbb{Z}$ und $\mathbb{Q}$ sind abzählbar unendlich.

Beweis: Wegen $\mathbb{N}_0 \subset \mathbb{Z} \subset \mathbb{Q}$ sind $\mathbb{Z}$ und $\mathbb{Q}$ unendlich. Sei $\varphi: \mathbb{N}_0 \longrightarrow \mathbb{Z}$

$$\varphi(n) = \begin{cases} n/2, & \text{falls } n \text{ gerade} \\ -(n+1)/2, & \text{falls } n \text{ ungerade} \end{cases}$$

Dann ist φ ein Isomorphismus.

Behauptung: $r \in \mathbb{Q} \iff \exists (p,q) \in \mathbb{Z} \times \mathbb{N}$ mit $r = p/q$. ~~und~~ Weiter kann q minimal gewählt werden.

Beweis: „$\Leftarrow$" Ist klar, da $\mathbb{Q}$ ~~so~~ durch $\mathbb{Z} \times \mathbb{Z}^\times$ konstruiert wurde.

„$\Rightarrow$" Setze

$$N = \{ n \in \mathbb{N} \mid \exists m \in \mathbb{Z} \text{ mit } \tfrac{m}{n} = r \}$$

Da $N \subset \mathbb{N}_0$ ist besitzt N ~~so~~ wegen dem Wohlordnungsprinzip ein Minimum $q = \text{Min}(N)$.

Setze $p = r \cdot q$, dann ist $r = \frac{p}{q}$ mit $q \in \mathbb{N}$.

Beachte das q minimal ist, da $q = \text{Min}(N)$

Diese Behauptung liefert eine Abbildung

$$\varphi : \mathbb{Q} \longrightarrow \mathbb{Z} \times \mathbb{N}$$
$$r = \tfrac{p}{q} \longmapsto (p,q)$$

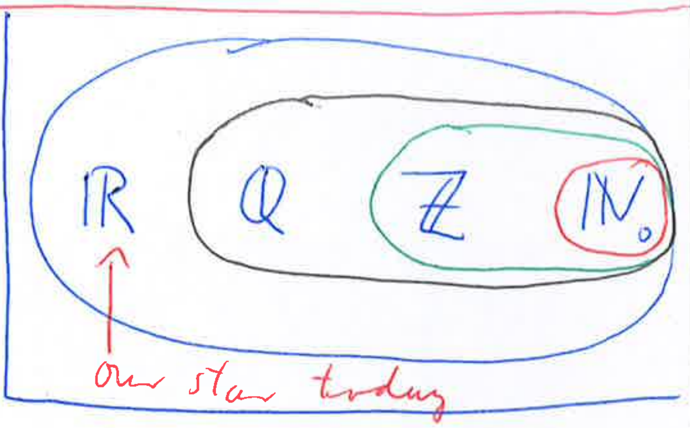
φ ist eine Bijektion auf eine Teilmenge von $\mathbb{Z} \times \mathbb{N}$:

- Die Darstellung $r = \frac{p}{q}$ ist eindeutig, da $q = \text{Min}(N)$. Also ist φ injektiv.
- Die Teilmenge auf welche φ surjektiv geht ist $(p,q) \in \mathbb{Z} \times \mathbb{N}$ mit p, q teilerfremd.

$\Rightarrow$ Behauptung, da Teilmengen abzählbarer Mengen abzählbar sind

Vorlesung 11, 03. Dez. 2018

"Die reellen Zahlen I"



Bisher war alles rein algebraisch $\mathbb{N}_0 \rightsquigarrow \mathbb{Z} \rightsquigarrow \mathbb{Q}$. Um weiter zu gehen, braucht man ein extra "Axiom" wie wir sehen werden.

Dazu: Ein Körper K heißt angeordnet, falls:

- $(K, \leq)$ ist total geordnet
- $\boxed{x < y \Rightarrow x + z < y + z}$ $\quad \forall x, y, z \in K$ (✓)
- $\boxed{x, y > 0 \Rightarrow xy > 0}$ $\quad \forall x, y \in K, x, y > 0$

Tippfehler:

Beispiel 11.1 Später sehen wir, dass $\mathbb{Q}$ ~~total~~ angeordnet ist. Dabei ist $\frac{a}{b} < \frac{a'}{b'} \Leftrightarrow ab' < a'b$
$\Leftrightarrow a'b - ab' \in \mathbb{N}_0$

Proposition 11.2 (Rechenregeln)

Seien $x, y, a, b \in K$. Dann gilt für K angeordnet:

a) $x > y \Leftrightarrow x - y > 0$.

b) $x + a > y + b$ falls $x > y$ und $a > b$.

c) $ax > ay$, falls $a > 0$ und $x > y$.

d) Aus $x > 0$ (bzw. $x < 0$) folgt $-x < 0$ (bzw. $-x > 0$)

e) Sei $x > 0$. Dann ist $xy < 0$ (bzw. $xy > 0$) falls $y < 0$ (bzw. falls $y > 0$).

f) $ax < ay$ falls $a < 0$ und $x > y$

g) $x^2 = x \cdot x > 0$ für $x \in K^\times$. Insbesondere $1 > 0$.

h) Aus $x > 0$ folgt $x^{-1} > 0$.

i) Aus $x > y > 0$ folgen $0 < x^{-1} < y^{-1}$ und $xy^{-1} > 1$.

Beweis: Nur i), alle andere sind ausgelassen.

Sei $x > y > 0$. Dann folgt $x - y > 0$ aus a) und $x^{-1} > 0$ und $y^{-1} > 0$ aus h). Deswegen gilt wegen (e)

$$0 < (x-y)x^{-1}y^{-1} = y^{-1} - x^{-1},$$

also $x^{-1} < y^{-1}$ sowie $0 < (x-y)y^{-1} = xy^{-1} - 1$, also $xy^{-1} > 1$

$\square$

Beispiel 11.3 $\mathbb{F}_2$ aus Beispiel 10.1 kann nicht angeordnet werden, denn $1 > 0$ (11.2 g) und 11.2 b) gilt $0 = 1 + 1 > 0$, also $0 \neq 0$.

Sei K angeordnet. Definiere Betrag $|\cdot|$ und Signum $\operatorname{sign}(\cdot)$

$$|\cdot| : K \to K \quad |x| = \begin{cases} x, & x > 0, \\ 0, & x = 0, \\ -x, & x < 0, \end{cases} ; \quad \operatorname{sign}(\cdot) : K \to K \quad \operatorname{sign}(x) = \begin{cases} 1, & x > 0, \\ 0, & x = 0, \\ -1, & x < 0. \end{cases}$$

Proposition 11.4 (Rechenregeln)

Sei K ein angeordneter Körper, $x, y, a \in K$ und $\varepsilon \in K$, $\varepsilon > 0$.

a) $x = |x| \operatorname{sign}(x)$, $|x| = x \cdot \operatorname{sign}(x)$

b) $|x| = |-x|$, $x \leq |x|$

c) $|xy| = |x||y|$

d) $|x| \geq 0$ und ($|x| = 0 \Leftrightarrow x = 0$)

e) $|x - a| < \varepsilon \Leftrightarrow a - \varepsilon < x < a + \varepsilon$

f) Dreiecksungleichung $|x+y| \leq |x|+|y|$ $\boxed{\Delta\text{-Ungl.}}$

Beweis: Exemplarisch f), die anderen sind ausgelassen.

Für $x+y \geq 0$ folgt aus b), dass
$$\left.\begin{array}{l} |x+y| = x+y \leq |x|+|y|. \end{array}\right\}(\boxed{z})$$

Für $x+y<0$ ist $-(x+y)>0$ und
$$|x+y| \overset{b)}{=} |-(x+y)| = |(-x)+(-y)| \overset{(\square)}{\leq} |-x|+|-y| \overset{b)}{=} |x|+|y|. \quad \boxed{z}$$

Proposition 11.5 (Reversed Δ-Ungleichung)

In jedem angeordneten Körper gilt
$$|x-y| \geq \big||x|-|y|\big| \quad x,y \in K$$

Beweis: Aus $x=(x-y)+y$ und Δ-Ungl. folgt
$|x| \leq |x-y|+|y|$, d.h. $|x|-|y| \leq |x-y|$.
Nun erhalten wir $|y|-|x| \leq |y-x| = |x-y|$
durch Vertauschen von $x \Leftrightarrow y$ $\boxed{z}$

Zur Erinnerung: $(\mathbb{Q}, \leq)$ mit $\frac{a}{b} \leq \frac{a'}{b'} \Leftrightarrow ab'-a'b \in \mathbb{N}_0$

Theorem 11.6: $(\mathbb{Q}, \leq)$ ist ein angeordneter Körper.

Die Ordnung $\leq$ induziert die Ordnung $\leq$ auf $\mathbb{N}_0$

Beweis: Ausgelassen.

Vorsicht: Teilmengen von $\mathbb{Q}$ besitzen i.A. kein Minimum

Das $\boxed{\text{Vollständigkeitsaxiom}}$: (VSA)

Sei $(X, \leq)$ eine total geordnete Menge. X erfüllt (VSA) wenn jede nach oben beschränkte Teilmenge $A \neq \emptyset$ ein Supremum besitzt.

<u>Proposition 11.7</u> Sei $(X, \leq)$ total geordnet. Dann sind a), b), c) wie folgt äquivalent.

a) X erfüllt (VSA)

b) Jede nach unten beschränkte nicht leere Teilmenge besitzt ein Infimum.

c) Für $A, B \subset X$, $A, B \neq \emptyset$ mit $a \leq b$ für $(a,b) \in A \times B$ $\exists\, c \in X$ mit $a \leq c \leq b$. (<u>Sandwichprinzip</u>)

<u>Beweis</u>: [AE06, Satz 10.1] $\square$

<u>Beispiel 11.8</u> $\mathbb{Q}$ erfüllt nicht das (VSA).

Betrachte dazu $A = \{x \in \mathbb{Q} \mid x^2 < 2,\ x > 0\}$ und $B = \{x \in \mathbb{Q} \mid x^2 > 2 \text{ und } x > 0\}$.

Es gilt $1 \in A$ und $2 \in B$. Aus $b - a = (b^2 - a^2)/(b+a) > 0$ folgt $(a,b) \in A \times B \Rightarrow a < b$.

Es gibt aber kein c mit $c \in \mathbb{Q}$ und $a \leq c \leq b$ $\forall (a,b) \in A \times B$, denn $\sqrt{2} \notin \mathbb{Q}$.

Siehe auch [AE06, Beispiel 10.3] für ein formales Argument.

Theorem 11.9 (Dedekind)

Es gibt einen kleinsten Körper $\mathbb{R} \supset \boxed{\mathbb{Q}} \supset \boxed{\mathbb{Z}} \supset \boxed{\mathbb{N}_0}$, welcher angeordnet ist und (VSA) erfüllt, der auf $\mathbb{Q}$, $\mathbb{Z}$, $\mathbb{N}$ die ursprüngliche Ordnung induziert. Dieser Körper ist bis auf ordnungserhaltende Isomorphie eindeutig und wird Körper der reellen Zahlen genannt.

Ordnungserhaltende Isomorphie: Ein Ringisomorphismus $\varphi : (K, \leq) \to (K', \leq')$ mit

$$\varphi(x) \leq' \varphi(y), \text{ falls } x \leq y$$

Beweis (Skizze): Schritt 1:

Definiere eine Teilmenge $\mathbb{R} \subset P(\mathbb{Q})$ durch

$$\mathbb{R} = \{ R \subset \mathbb{Q} \mid R \text{ erfüllt i), ii), iii)} \}$$

i) $R \neq \emptyset$, $R^c = \mathbb{Q} \setminus R \neq \emptyset$.

ii) $R^c = \{ x \in \mathbb{Q} \mid x < r \ \forall r \in R \}$.

iii) R besitzt kein Minimum.

Schritt 2:

Die Abbildung

$$\mathbb{Q} \to \mathbb{R}, \quad r \mapsto \{ x \in \mathbb{Q} \mid x > r \} \ (\boxed{\text{Z}})$$

ist injektiv.

Schritt 3: Definiere Addition

$$+ : \mathbb{R} \times \mathbb{R} \to \mathbb{R}, \quad (R, S) \mapsto R + S = \{ r + s \mid r \in R, s \in S \}$$

Diese ist assoziativ und kommutativ und

$0 := \{x \in \mathbb{Q} \mid x > 0\}$ ist Nullelement.

Das +-Inverse ist $-R = \{x \in \mathbb{Q} \mid x + r > 0 \ \forall r \in R\}$.

Analog: $R \cdot R' = \{rr' \in \mathbb{Q} \mid r \in R, r' \in R'\}$ definiert eine Multiplikation, welche zusammen mit + $\mathbb{R}$ die Struktur eines Körpers gibt.

Schritt 4: Für $R, R' \in \mathbb{R}$ setze

$$R \le R' \iff R \supset R'.$$

Dies induziert eine Ordnung auf $\mathbb{R}$, welche ~~wegen~~ total ist: Ist $R \neq R'$, dann gibt es ein $r \in R$ mit $r \in (R')^c$ oder ein $r' \in R'$ mit $r' \in R^c$. Im ersten Fall folgt $R' \subset R$ also $R' \geq R$, im zweiten $R' \supset R$, also $R' \leq R$.

Schritt 5: $$R \cdot R' = \begin{cases} -((-R) \cdot R'), & R < 0,\ R' \geq 0, \\ -(R \cdot (-R')), & R \geq 0,\ R' < 0, \\ (-R) \cdot (-R'), & R < 0,\ R' < 0. \end{cases}$$

Damit zeigt man das $\mathbb{R}$ angeordnet ist.

Schritt 6: Man checkt, dass alles mit den Strukturen auf $\mathbb{Q}$ unter ( ) verträglich ist.

Schritt 7: Man zeigt, dass $\mathbb{R}$ das (VSA) erfüllt.

Sup ist S=\bigcup R für R\subset\mathbb{R}

Schritt 8: Man kann nachprüfen, dass $\mathbb{R}$ minimal ist und bis auf Isomorphie eindeutig.

Für $M \subset \mathbb{R}$, $M \neq \emptyset$ und nicht nach oben beschränkt setze $\sup(M) = \infty$. Analog $\inf(M) = -\infty$, falls $M \neq \emptyset$ nicht nach unten beschränkt ist. (*)

(Zur Erinnerung: Alle anderen Suprema und Infima existieren, da $\mathbb{R}$ das (VSA) erfüllt.)

Proposition 11.10

a) Für $A \subset \mathbb{R}$ und $x \in \mathbb{R}$ gilt:

α) $x < \sup(A) \Leftrightarrow \exists\, a \in A$ mit $x < a$.

β) $x > \inf(A) \Leftrightarrow \exists\, a \in A$ mit $x > a$.

b) Jede Teilmenge $A \subset \mathbb{R}$ hat ein Supremum und ein Infimum in $\mathbb{R} \cup \{\infty\} \cup \{-\infty\}$.

Beweis: b) folgt aus Theorem 11.8 und der Definition (*).

a) α) Für $A = \emptyset$ ist nichts zu zeigen. Sei $A \neq \emptyset$.

~~Für~~ „$\Rightarrow$" Für $x < \sup(A)$ sei $a \leq x$ für $\forall a \in A$. Dann ist x eine Schranke von A, was nach ~~und~~ Definition von $\sup(A)$ unmöglich ist.

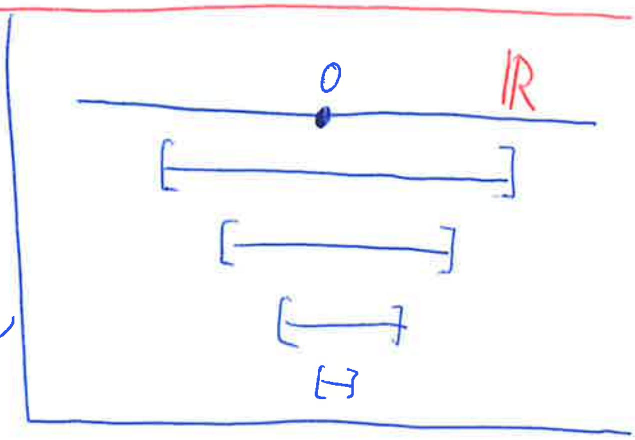
„$\Leftarrow$" Es sei $a \in A$ mit $x < a$. Dann gilt $x < a \leq \sup(A)$.

β) geht analog. $\boxed{}$

Vorlesung 12, 10. Dez. 2018

$\boxed{\text{Die reellen Zahlen II}}$

Der Punkt ist, dass die reellen Zahlen keine "Lücke" haben, wie wir unten sehen werden.



Proposition 12.1 (Satz von Archimedes)

$\mathbb{N}_0 \subset \mathbb{R}$ ist nicht nach oben beschränkt, d. h. für jedes $x \in \mathbb{R}$ $\exists n \in \mathbb{N}_0$ mit $n > x$.

Beweis: Für $x < 0$ oder $x = 0$ ist die Aussage gültig. Sei also $x > 0$ und betrachte $A = \{n \in \mathbb{N} \mid n \leq x\}$. Dann ist $0 \in A$, also $A \neq \emptyset$. Weiter ist A nach oben beschränkt (durch x). Tippfehler: Für...existiert...
Sei $s = \sup(A) \in \mathbb{R}$ und es existiert $a \in A$ mit $s - 1/2 < a$. Dann folgt für $n = a + 1$ dass $n > s$. Weiter ist $n \notin A$ wegen $n > s$, also $n > x$. $\square$

Proposition 12.2

a) Gilt $0 \leq a \leq 1/n$ $\forall n \in \mathbb{N}$, so folgt $a = 0$.

b) Zu jedem $a \in \mathbb{R}$ mit $a > 0$ $\exists n \in \mathbb{N}$ mit $1/n < a$.

b) ist nur eine Umformulierung von a). a) Wäre $0 < a < 1/n$ für $\forall n \in \mathbb{N}$ dann folgt $n \leq 1/a$. Widerspruch zu Satz von Archimedes. $\square$

für alle n in N

Die rationalen Zahlen $\mathbb{Q}$ approximieren die reelle beliebig gut. Formal nennt man das Dichtheit von $\mathbb{Q}$ in $\mathbb{R}$ und ist wie folgt:

Proposition 12.3

Zu $a < b \in \mathbb{R}$ gilt es $r \in \mathbb{Q}$ mit $a < r < b$.

Beweis: Schritt 1: Wegen $a < b$ gilt $b - a > 0$. Also $\exists\, n$ mit $n > 1/(b-a) > 0$ und somit $nb > na + 1$. ($\boxed{S}$)

Schritt 2: Es gilt nun aber $m_1, m_2 \in \mathbb{N}$ mit $m_1 > na$ und $m_2 > -na$, d.h. $-m_2 < na < m_1$.

Somit gilt es $m \in \mathbb{Z}$ mit $m - 1 \leq na < m$.

Zusammen mit ($\boxed{S}$) folgt

$$na < m \leq 1 + na < nb.$$

Setze $r = m/n \in \mathbb{Q}$ und es folgt $a < r < b$. $\boxed{S}$

Das heißt $\mathbb{Q}$ liegt dicht in $\mathbb{R}$. ("Zwischen zwei reellen Zahlen liegt immer eine rationale").

Die irrationalen Zahlen $\mathbb{R} \setminus \mathbb{Q}$ liegen auch dicht:

Proposition 12.4

Zu $a < b \in \mathbb{R}$ gilt es $\xi \in \mathbb{R} \setminus \mathbb{Q}$ mit $a < \xi < b$.

Beweis: Schritt 1: Wir behaupten, dass es eine reelle Zahl $x \in \mathbb{R}$ mit $x > 0$ so gilt, dass $x^2 = 2$. Wir notieren $x = \sqrt{2}$.

In der Tat ist $R = \{x \in \mathbb{Q} \mid x^2 < 2 \text{ und } x > 0\}$ eine Teilmenge von $P(\mathbb{Q})$ welche die Axiome einer reellen Zahl erfüllt.

p/q reduziert

<u>Schritt 2:</u> $\sqrt{2} \notin \mathbb{Q}$. Angenommen $\sqrt{2} = p/q \in \mathbb{Q}$, dann gilt $2q^2 = p^2$. Daraus folgt aber, dass $p = 2\ell$ für ein $\ell \in \mathbb{Z}$, was wiederum $q = 2\ell'$ impliziert. Widerspruch.

<u>Schritt 3:</u> Finde rationale Zahlen $r_1, r_2 \in \mathbb{Q}$ mit $a < r_1 < b$ und $r_1 < r_2 < b$. Setze $\xi = r_1 + (r_2 - r_1)/\sqrt{2}$ folgt dann $a < \xi < b$.
Wegen $\boxed{\text{Schritt 2}}$ ist ξ irrational.

2

Ein Intervall I ist eine Teilmenge von $\mathbb{R}$ mit:

Tippfehler: es existiert z in I mit ....

$$(x, y \in I,\ x < y) \Rightarrow (z \in I \text{ für } x < z < y)$$

<u>Beispiel 12.5</u> Seien $a < b \in \mathbb{R}$. "Intervalle haben keine Löcher"

$[\text{———}] = [a,b] = \{z \mid a \leq z \leq b\}$ genannt abgeschlossen

$(\text{———}] = (a,b] = \{z \mid a < z \leq b\}$ weder offen noch geschlossen

$[\text{———}) = [a,b) = \{z \mid a \leq z < b\}$

$(\text{———}) = (a,b) = \{z \mid a < z < b\}$ genannt offen

Aber auch $\emptyset$, $\mathbb{R}$, $\mathbb{R}_{\geq 0}$, $-\mathbb{R}_{\geq 0}$ sind Intervalle. Kein Intervall:

$\mathbb{R} - \{0\}$

Ein Intervall $I \subset \mathbb{R}$ heißt **offen**, falls $\inf(I) \notin I$ und $\sup(I) \notin I$, und **abgeschlossen**, falls $\inf(I) \in I$ und $\sup(I) \in I$. I heißt **beschränkt**, wenn $\inf(I) \in \mathbb{R}$ und $\sup(I) \in \mathbb{R}$; in diesem Fall ist $|I| = \sup(I) - \inf(I) \in \mathbb{R}$ die **Länge** von I.

Beispiel 12.6 $I = \underbrace{\{a\}}_{=[a,a]}$ ist ein abgeschlossenes Intervall der Länge 0, genauso wie $(a,a) = \emptyset$. $\emptyset$ ist aber auch offen.

Für jedes $n \in \mathbb{N}$ sei $I_n \neq \emptyset$ ein beschränktes Intervall, welches abgeschlossen ist.

Die Familie $\{I_n \mid n \in \mathbb{N}\}$ heißt **Intervallschachtelung** (IVS) falls:

i) $I_{n+1} \subset I_n$

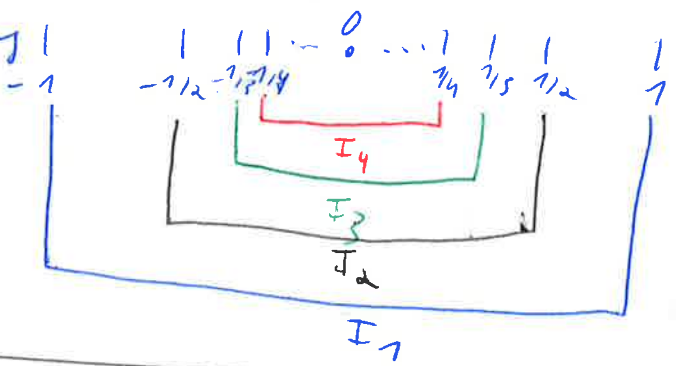
ii) Für alle $\varepsilon > 0$ $\exists I_n$ mit $|I_n| < \varepsilon$.

Eine IVS heißt rational, falls $\sup(I_n), \inf(I_n) \in \mathbb{Q}$ für alle n

---

Beispiel 12.7 Die Familie $\{[-1/n, 1/n] = I_n \mid n \in \mathbb{N}\}$ ist eine Intervallschachtelung.

Im Schnitt liegt exakt die Null.



Theorem 12.8 (Intervallschachtelung)

a) Zu jeder IVS $\{I_n\}$ gibt es genau ein $x \in \mathbb{R}$ mit $x \in \bigcap_n I_n$.

b) Zu jedem $x \in \mathbb{R}$ gibt es genau eine rationale IVS mit $\{x\} = \bigcap_n I_n$

Theorem 12.8 sagt, dass rationale IVS und reelle Zahlen "dasselbe sind". Das gibt eine alternative Konstruktion der reellen Zahlen.

Beweis: a) Schritt 1: Eindeutigkeit

Seien $x, x' \in \bigcap_n I_n$ und sei $I_n = [a_n, b_n]$.

Dann gilt $a_n \leq x \leq b_n$ und $a_n \leq x' \leq b_n \quad \forall n \in \mathbb{N}_0$

Angenommen $x < x' \rightsquigarrow$ ~~Finde ε mit x ε x' und~~

setze $\varepsilon = x' - x$. Dann ist $\varepsilon < |I_n| \quad \forall n \in \mathbb{N}_0$,

denn $\underbrace{a_n \leq \underbrace{x < x'}_{\varepsilon} \leq b_n}_{|I_n|}$. Widerspruch.

Schritt 2: Existenz

Wegen $I_{n+1} \subset I_n$ folgt, dass $A = \{a_n \mid n \in \mathbb{N}_0\}$ nach oben beschränkt ist. Also ist $\sup(A) \in A$.

Da jedes b_n wegen $I_{n+1} \subset I_n$ eine obere Schranke von A ist folgt $\sup(A) \leq b_n \; \forall n \Rightarrow \sup(A) \geq a_n \wedge \sup(A) \leq b_n \quad \forall n \Rightarrow \sup(A) \in I_n \quad \forall n$.

$$a_0 \leq a_1 \leq a_2 \leq \ldots \leq \sup(A) \leq \ldots \leq b_2 \leq b_1 \leq b_0$$

---

b) Schritt 1: ~~Wähle ein~~ betrachte für $n \in \mathbb{N}$ das Intervall $\tilde{I}_n := [x - 1/n, x + 1/n]$.

Das hat noch keine rationalen Endpunkte falls $x \in \mathbb{R} \setminus \mathbb{Q}$ ist.

Deswegen finde $p_n \in \mathbb{Q}$ und $q_n \in \mathbb{Q}_{>0}$, dass $x - 1/n \leq p_n \leq x - 1/{n+1}$ und $x + 1/{n+1} \leq q_n \leq x + 1/n$ gilt. Setze $I_n = [p_n, q_n] \neq \emptyset$, welches ein Intervall gilt, denn $p_n < x < q_n$.

Schritt 2: Per Konstruktion ist $x \in I_n$ für alle $n \in \mathbb{N}$. Also ist $x \in \bigcap_n I_n$.

Schritt 3: $\{I_n \mid n \in \mathbb{N}\}$ ist eine Intervallschachtelung, denn $I_{n+1} \subset I_n$, per Konstruktion.

Weiter gilt $|I_n| = \cancel{p_n}\, q_n - p_n \leq 2/n$.

Schritt 4: Es gilt $\{x\} = \bigcap_n I_n$, denn ~~das~~ wir können wegen Schritt 2 den Schritt 1 in a) verwenden. $\boxed{\text{E}}$

Zum Abschluss noch Wurzeln:

Proposition 12.9

a) Zu $a \in \mathbb{R}_{>0}$ und $n \in \mathbb{N}$ gibt es genau ein $x \in \mathbb{R}_{>0}$ mit $x^n = a$. (Genannt n-te Wurzel)

b) Ist n ungerade, so hat $x^n = a$ genau eine Lösung in $\mathbb{R}$.

Beweis: a) Schritt 1: Eindeutigkeit

Für $x^n = y^n$ und $y < x$ folgt $x^n - y^n = 0$ und $x - y > 0$. Aber nach Binomialer Formel:

$$0 = (x^n - y^n) = \underbrace{(x-y)}_{>0} \underbrace{\sum_{j=0}^{n-1} x^j y^{n-j}}_{>0} > 0$$

Widerspruch

Schritt 2: Existenz folgt durch Betrachte von $A = \{x \in \mathbb{R}_{\geq 0} \mid x^n \leq a\}$. Nehme sup(A) als n-te Wurzel

Details siehe [AE06, Satz 10.9]

b) Wegen a) und $x<0 \Rightarrow x^n<0$ für n reicht es ~~die Eindeutigkeit zu~~ ungerade ~~beweisen~~ den Fall $a < 0$ zu betrachten.

Ist $a < 0$, dann $\exists\, y \in \mathbb{R}_{>0}$ mit $y^n = -a$ durch a).

Setze $x = -y$ und die Behauptung folgt. $\boxed{\text{Z}}$

Vorlesung 13, 17. Dec. 2018

$\boxed{\text{„Nicht ganz so naive Mengenlehre"}}$

Warum das Ganze? Betrachte das folgende Axiom:

$$\begin{tikzcd} & \mathrm{LoZ} \arrow[dr, Rightarrow] & \\ \mathrm{AOC} \arrow[ur, Rightarrow] & & \mathrm{WOT} \arrow[ll, Rightarrow] \end{tikzcd}$$

Axiom (Problematisch)

Sei E eine Eigenschaft. Dann gibt es eine Menge $X = \{x \mid E(x)\}$

„Beweis warum Problematisch" (Russell)

Betrachte die Menge $R = \{X \mid X \notin X\}$.
Ist $R \in R$ oder $R \notin R$?

$R \in R \Rightarrow R \notin R$ $\qquad$ $R \notin R \Rightarrow R \in R$

Also kann R keine Menge sein?

Das ist das Lügnerparadoxon „Dieser Satz ist falsch" in Mengenschreibweise?

Um solche Sachen zu vermeiden baut man alles, was „Menge" ist, axiomatisch.

Dabei gilt das „Legoprinzip": Wenn man bereits Mengen hat, so kann man daraus neue Mengen bauen.

Axiome von Zermelo-Fraenkel

A.1 "Mengen sind genau dann gleich, wenn sie dieselben Elemente haben"

$$\forall A, B : (A = B \Leftrightarrow \forall C : (C \in A \Leftrightarrow C \in B))$$

A.2 "Es gilt Paarmengen $\{A, C\}$"

$$\forall A, C \boxed{\exists B} : \forall D : (D \in B \Leftrightarrow (D = A) \vee (D = C))$$

A.3 "Teilmengenschema"

$$\forall A : \boxed{\exists B} : \forall C : (C \in B \Leftrightarrow C \in A \wedge E(C))$$

A.4 "Es gilt Vereinigungen"

B enthält die Elemente der Elemente von A

$$\forall A : \boxed{\exists B} : \forall C : (C \in B \Leftrightarrow \exists D : (D \in A \wedge C \in D))$$

Schreibweise $B = \bigcup A$

A.5 "Es gilt Potenzmengen"

B enthält die Teilmengen von A

$$\forall A \boxed{\exists B} : \forall C : (C \in B \Leftrightarrow \forall D : (D \in C \Rightarrow D \in A))$$

A.6 "Es gilt eine (unendliche) Menge"

A.7 "Wenn man Elemente einer Menge gegen Mengen austauscht erhält man eine Menge"

$$\forall X, Y, Z : (E(X,Y) \wedge E(X,Z) \Rightarrow Y = Z)$$

$$\Rightarrow \forall A : \boxed{\exists B} : \forall C : (C \in B \Leftrightarrow \exists D : (D \in A \wedge E(D,C))$$

B enthält für jedes Element von A eine Menge

A.8 „Jede nicht leere Menge A enthält ein Element B so, dass $A \cap B = \emptyset$“

$$\forall A : (A \neq \emptyset \Rightarrow \boxed{\exists B} : (B \in A \wedge \neg \exists C : (C \in A \wedge C \in B)))$$

Beispiel 13.1

Alles setzt die Existenz von Menge voraus, außer A.6!

A.1 ⇝ sollte klar sein

A.2 ⇝ Sind A, B Mengen so ist $\{A, B\}$ eine Menge

A.3 ⇝ Ist A eine Menge so kann man Teilmengen von A auch als Menge betrachten.

A.4 → Ist z.B. $A = \{C, D\}$ so ist $B = \bigcup A$ $= C \cup D$

↳ Existiert wegen A.2

A.5 ⇝ Die Potenzmenge im üblichen Sinne.

$\boxed{\text{Creatio ex nihilo}}$

A.6 ⇝ $\boxed{\text{Deus ex machina}}$ (A.6 + A.3 ⇝ leere Menge)

A.7 → Ist z.B. $A = \{1, 2\}$ dann ist auch $B = \{C, D\}$ eine Menge durch $1 \longmapsto C$, $2 \longmapsto D$

A.8 → Verhindert unendliche Zykel wie $A = \{x_1, x_2, \ldots\}$ mit $x_1 \ni x_2 \ni x_3 \ni \ldots$

Beispiel 13.2

Wo ist der Schnitt? Wo ist das Komplement? Als $\boxed{\text{Teilmengen}}$, also via A.3

$$X \cap Y = \{u \in X \mid u \in Y\} \quad \text{und} \quad X \setminus Y = \{u \in X \mid u \notin Y\}$$

Beispiel 13.3.

Die einelementige Mengen sind $\{a\} = \{a, a\}$.

Die Paare sind $(a,b) = \{\{a\}, \{a,b\}\}$

$(a,b,c) = \{\{a\}, \{a,b\}, \{a,b,c\}\}$ etc.

geordnet!

Beispiel 13.4 Wo sind Produktmenge?

Via $\boxed{\text{Potenzmengen}}$ A.5 und $\boxed{\text{Teilmengen}}$ A.3

$$X \times Y \subset P(P(X \cup Y))$$

$$(a,b) = \{\{a\}, \{a,b\}\} \in P(X \cup Y)$$

$\boxed{\text{Analog: Höhere Produkte}}$

"Theorem" (Zermelo - Fraenkel)

So kann man alle mathematische Begriffe als Menge auffassen.

Axiom (Auswahlaxiom) $\boxed{\text{"Liest sich eher wie ein Theorem"}}$

A.9. ~~...~~ "Jede Familie von nicht leeren Teilmenge hat eine Auswahlfunktion"

$$\forall A : (((\emptyset \notin A) \wedge \forall X, Y, Z : ((X \in A \wedge Y \in A \wedge Z \in X \wedge Z \in Y) \Rightarrow (X = Y)))$$

$$\Rightarrow \boxed{\exists B} : \forall X : (X \in A \Rightarrow \exists! Y : (Y \in X \wedge Y \in B))$$

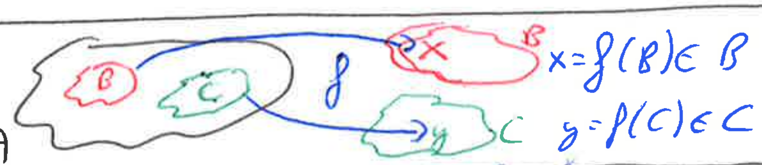
Sei A eine Menge nicht leeren Mengen. Dann $\exists f : A \to \bigcup A$, die jedem Element C von A ein Element $D \in C$ zuordnet.

Beispiel 13.4

Erstmal kann man Funktion als Menge auffassen. Ist $f: X \longrightarrow Y$ eine Abbildung, so kann man sagen $f \subset X \times Y$ mit $(x, f(x)) \subset X \times Y$

Beispiel 13.5

Bild:



Das Auswahlaxiom postuliert die Existenz eine Abbildung auf S = Familie nicht leere Teilmengen so, dass $f(X) \in X$ für $X \in S$ gilt.

z.B.

i) $S = \{\{x\}, \{y\}, \{z\}, \dots\}$, $\{x\} \xrightarrow{f} x$, $\{y\} \xrightarrow{f} y$, $\{z\} \xrightarrow{f} z$

In diesem Fall explizit konstruiert.

ii) $S = \{1, \dots, n\}$ Existenz auch klar bei Induktion nach $|S|$.

iii) $S \subset \mathbb{R}$, S endlich. $f(X) = \inf(X)$ tut den Job.

Aber: Im Allgemeinen ist f nicht konstruiert und wird axiomatisch vorausgesetzt.

Eine Konsequenz des Auswahlaxioms ist:

Theorem 13.6 Jede Menge $\boxed{\text{besitzt}}$ eine Wohlordnung.

(Zur Erinnerung: Der Begriff "Wohlordnung" kam auf den Übungszetteln vor).

Beispiel 13.7

Diese Aussage ist hochgradig nicht trivial, außer in den Fällen, wo man es explizit machen kann:

i) Endliche Mengen

ii) $\mathbb{N}_0$, $\mathbb{Z}$, $\mathbb{Q}$

Nicht explizit: $\mathbb{R}$ kann wohlgeordnet werden.

In der Tat sind das Auswahlaxiom und Theorem 13.6 (Wohlordnungssatz) äquivalent.

Eine weitere ~~Appi~~ äquivalente und häufig verwendete Version des Auswahlaxioms ist das Lemma von Zorn:

Theorem 13.8 (Lemma von Zorn)

Sei $(X, \leq)$ eine partiell geordnete Menge. Angenommen jede Kette $\subseteq X$ hat eine obere Schranke.
Dann $\boxed{\text{besitzt}}$ X ein maximales Element.

Partielle Ordnung: – reflexiv
– transitiv
– antisymmetrisch

Kette: Nicht leere Teilmenge, welche bzgl. $\leq$ total geordnet ist.

Obere Schranke: Muss nicht in der Kette liegen.

Folgerungen / Äquivalente Aussagen (*)

- Jeder Vektorraum besitzt eine Basis (*)
- Existenz algebraischer Abschlüsse von Körpern
- Hahn-Banach Theorem
- Tikhonov's Theorem (*)
- Maximale Ideale in Ringen (*)
- nicht meßbare Mengen
- Spannbaum Theorem (*)
- etc.