Logische Grundlagen – Vorlesungsnotizen

Achtung: Dies ist kein richtiges Vorlesungsskript, sondern nur stichpunktartige Notizen, die ich für mich selbst gemacht habe. Insbesondere kann unvollständig sein, und außerdem ist es vermutlich manchmal zu knapp, um verständlich zu sein, und sicher voll von Tippfehlern.

Einleitung

10.4.2013

0.1 Ziele

Haupt-Ziel: präzise Definition davon, was ein Beweis ist.

Plan der Vorlesung:

- 1. Teil (groß): Mengenlehre: Einführung (präzise Definitionen) und wie man die restliche Mathematik nur aus Mengen konstruiert. Unterwegs auch andere Nützlichkeiten: Kardinalitäten...
- 2. Teil: Logisches Schlussfolgern präzise machen; unterwegs: Strukturen

0.2 Literatur

- Deiser: Einführung in die Mengenlehre (beginnt mit naiver Mengenlehre; hat auch ein übersichtliches Kapitel mit den Axiomen von ZFC)
- Cameron: Sets, Logic and Categories (beginnt mit naiver Mengenlehre; hat auch ein axiomatisches Kapitel)
- Halmos: Naive Set Theory (fängt etwas axiomatischer an, listet aber ZFC-Axiome nicht so genau auf)
- Rautenberg: Einführung in die mathematische Logik (Logik und insbes. Hilbert-Kalkül; keine Mengenlehre)
- Ziegler: Mathematische Logik (Logik und Axiome der Mengenlehre; sehr kompakt)
- Doxiadis, Papadimitriou: Logicomix (Geschichte der Logik als Comic)

0.3 Erst mal ein bisschen naive Mengenlehre

Anschauliche Def. einer Menge, erster Versuch (Cantor, Ende 19. Jahrhundert): Eine Menge M ist *irgend eine Ansammlung von „mathematischen Objekten“*; diese Objekte werden als die „Elemente“ von M bezeichnet. Notation: $a \in M$.

Beispiele:

M_1 = die Menge der natürlichen Zahlen (also: $a \in M_1 \iff a$ ist natürliche Zahl)
M_2 = die Menge, die nur die Zahl 4 enthält; Notation: $M_2 = \{4\}$ (nützliche Konvention: M_2 ist nicht das selbe wie 4)
M_3 = die Menge aller konvergenten Folgen in $\mathbb{R}$ (Folgen sind auch mathematische Objekte)
M_4 = die Menge aller Vektorräume...

Mengen selbst sind auch mathematische Objekte, Also:
$M_5 = \{M_1, M_2\}$. Also: M_5 hat zwei Elemente, nämlich 1. die Menge der natürlichen Zahlen und 2. die Menge $\{4\}$.

Vorsicht: Wenn $a \in M$ und $M \in M'$, dann muss nicht $a \in M'$ sein. Beispiel: $M_1 \in M_5$ und $12 \in M_1$ aber $12 \notin M_5$.

Vorsicht: uneindeutige Sprechweise: Manchmal sagt man „M enthält M'“. Wenn M und M' beides Mengen sind, könnte das zwei verschiedene Bedeutungen haben: 1. M' ist ein Element von M (Beispiel: $M_1 \in M_5$) oder 2. M' ist eine Teilmenge von M (d.h. jedes Element von M' liegt auch in M; Beispiel: $M_2 \subseteq M_1$).

M_5 = die Menge aller Mengen.

So weit, so gut. Aber:

Russel-Paradox: M_6 = die Menge aller Mengen, die sich nicht selbst enthalten.

Frage: Ist M_6 Element von M_6?

Annahme ja. Dann dürfte es nach Def. von M_6 nicht Element von M_6 sein. Also folgt $M_6 \notin M_6$

Andererseits: Annahme nein. Dann müsste es nach Def. von M_6 Element von M_6 sein. Also folgt $M_6 \in M_6$

$\rightsquigarrow$ Mengenlehre von Cantor funktioniert nicht.

Das zeigt:

- Was intuitiv richtig klingt, muss kein richtiger Beweis sein. Es wäre gut, wenn man präzise beschreiben könnte, was ein Beweis ist.

  $\rightsquigarrow$ Entwicklung von präziser Definition von Beweis $\rightsquigarrow$ „formales System“ (oder „Kalkül“)
- „Alle Mengen, die sich nicht selbst enthalten“ ist einerseits etwas vernünftiges, über das man reden kann, aber es kann selbst keine Menge sein. Brauche also eine eingeschränktere Definition davon, was eine Menge ist. (Verwende den Begriff **Klasse** für Dinge, die (möglicherweise) keine Menge sind.)

  $\rightsquigarrow$ Entwicklung der Mengenlehre

0.4 Formale Beweise

Idee:

- Führe eine präzise Notation für mathematische **Aussagen** ein.
  Beispiel: „$\forall n \in \mathbb{N} : n + 0 = n$“ (wahre Aussage), „$3 \cdot 3 = 10$“ (falsche Aussage)
  Nicht-Beispiel: „$\exists bananen$“ (hat keinen Sinn…zumindest nicht mathematisch)
- Nimm die Wahrheit von einigen Aussagen als gegeben an (**Axiome**).
  Beispiel: $\forall x \colon x = x$
- Wähle einen Satz von **Ableitungsregeln**, die besagen, wie man aus wahren Aussagen neue wahre Aussagen gewinnen kann.
  Z.B.: Ist ϕ eine wahre Aussage und ist „$\phi \Rightarrow \psi$“ eine wahre Aussage, dann ist auch ψ eine wahre Aussage.
- Dann definiere: Ein **formaler Beweis** einer Aussage ϕ ist eine endliche Liste von Aussagen $\phi_1, \ldots, \phi_n$ mit $\phi_n = \phi$, so dass jedes ϕ_i entweder ein Axiom ist oder sich mit Hilfe von Ableitungsregeln aus den Aussagen $\phi_1, \ldots, \phi_{i-1}$ ergibt.

(Ein **formales System** besteht aus Aussagen, Axiomen, Ableitungsregeln…)

Aussagen sind Zeichenketten aus einem festen Satz von Symbolen. Die Beschreibung, welche Zeichenketten wirklich Aussagen sind und die Beschreibung der Ableitungsregeln sind einfach Manipulationen von Zeichenketten, d. h. in einem formalen System könnte ein Computer überprüfen, ob etwas wirklich ein Beweis ist.

Ein paar Haken an der Sache:

- Können wir auf diese Art wirklich nur wahre Aussagen beweisen? (Stimmen die Axiome? Funktionieren die Ableitungsregeln?)

  Antwort: Wir wissen es nicht. (Mit irgend was muss man anfangen zu beweisen. Das beste, was wir tun können, ist, uns auf möglichst wenig, möglichst plausible Axiome und Ableitungsregeln zu beschränken.)

  Besonders ärgerlich wäre es, wenn es eine Aussage ϕ gibt, so dass sowohl ϕ als auch ihr Gegenteil bewiesen werden können. (**Inkonsistenz**)
- Können wir alle wahren Aussagen beweisen?

  Wenn man davon ausgeht, dass jede Aussage ϕ entweder richtig oder falsch ist, dann sollte man entweder ϕ oder das Gegenteil von ϕ beweisen können. (**Vollständigkeit**)

Gödel hat gezeigt: Unter gewissen (vernünftigen) Nebenbedingungen gibt es keinen formales System, dass sowohl konsistent als auch vollständig ist.

Also müssen wir uns damit abfinden, ein formales System zu verwenden, das „hinreichend vollständig“ ist für alles, was man üblicherweise so in der Mathematik macht, und von dem wir hinreichend überzeugt sind, dass es konsistent ist.

Das funktioniert bis heute ganz gut.

Ausblick:

- Beweis vom Satz von Gödel kommt in Logik-Vorlesung.
- Mengenlehre befasst sich (u.a.) damit, welche Aussagen mit den üblichen Axiomen weder beweisbar noch widerlegbar sind.

1 Mengenlehre

1.1 Formeln und Aussagen

defn.fml-me

Definition 1.1 *Eine **Formel** (genauer: eine **Formel in der Sprache der Mengenlehre**) ist eine Zeichenkette bestehend aus $\wedge$, $\vee$, $\Rightarrow$, $\neg$, $\forall$, $\exists$, $=$, $\in$, (,) und (Symbolen für) Variablen, die nach folgenden Regeln gebildet werden kann:*

- *Sind x und y Variablen, so sind „$x = y$“ und „$x \in y$“ Formeln.*
- *Sind ϕ und ψ Formeln und ist x eine Variable, so sind „$(\phi \wedge \psi)$“, „$(\phi \vee \psi)$“, „$(\phi \Rightarrow \psi)$“, „$\neg\phi$“, „$\forall x\, \phi$“, „$\exists x\, \phi$“ Formeln.*

Beispiele:

1. „$\forall x \forall y\, (x \in y \wedge \neg x \in y)$“
2. "$\exists x\, \neg x = x$“
3. „$\neg \exists x\, x \in y$“

Die Variablen werden für Mengen stehen.

Anschauliche Bedeutung:
1. Für jedes x und jedes y gilt: entweder x ist ein Element von y oder x ist kein Element von y. Also: wahr (im intuitiven Sinn).
2. . . . falsch
3. Ob das wahr ist, hängt von y ab. (Es ist wahr, wenn y die leere Menge ist.)

Die Variablen einer Formel, die „zu einem Quantor gehören“, heißen gebundene Variablen; die anderen heißen „freie Variablen“. (Ob eine Formel wahr ist, hängt also davon ab, was die Werte der freien Variablen sind – oder kann zumindest davon abhängen.)

Definition 1.2 *Eine Variable x ist **frei** in einer Formel ϕ wenn:*

- *$\phi =$ „$x = x$“ oder „$x = y$“ oder „$y = x$“ oder „$x \in x$“ oder „$x \in y$“ oder „$y \in x$“ und y ist eine weitere Variable.*

- $\phi = (\psi_1 \wedge \psi_2)$ *oder* $(\psi_1 \vee \psi_2)$, $(\psi_1 \Rightarrow \psi_2)$ *und* x *kommt frei in* ψ_1 *oder in* ψ_2 *vor.*
- $\phi = \neg\psi$ *und* x *kommt frei in* ψ *vor.*
- $\phi = \forall y\, \psi$ *oder* $\phi = \exists y\, \psi$, x *kommt frei in* ψ *vor und* x *ist* nicht *die selbe Variable wie* y.

Sind $x_1, \ldots, x_n$ *die freien Variablen einer Formel* ϕ, *so schreibt man oft* $\phi(x_1, \ldots, x_n)$. *(Das macht deutlich, dass man für* $x_1, \ldots, x_n$ *etwas einsetzen muss.)*

Variablen, die in einer Formel vorkommen aber nicht frei sind, heißen ***gebunden****.*

defn.aussage

Definition 1.3 *Eine* ***Aussage*** *(genauer: eine* ***Aussage in der Sprache der Mengenlehre****) ist eine Formel ohne freie Variablen.*

Zur Erinnerung: Das formale System wird uns erlauben, Aussagen zu beweisen. (Formeln mit freien Variablen werden aber anderweitig nützlich sein.)

Wir werden oft abkürzende Schreibweisen für Formeln und Aussagen verweden, z. B.:

- Klammern weglassen
- $\phi \Leftrightarrow \psi$ statt $(\phi \Rightarrow \psi) \wedge (\psi \Rightarrow \phi)$
- $x \neq y$ statt $\neg x = y$; entsprechend $x \notin y$.
- $\forall x, y\, \phi(x, y)$ statt $\forall x \forall y\, \phi(x, y)$, etc. (Manchmal zur Verdeutlichung auch $\forall x, y \colon \phi(x, y)$)
- $\forall x \in A \colon \phi(x)$ statt $\forall x\, (x \in A \Rightarrow \phi(x))$
- Entsprechend: $\exists x \in A \colon \phi(x)$ statt $\exists x\, (x \in A \wedge \phi(x))$
- später noch mehr (z.B. $\subseteq$, $\cap$, $\cup$, $\ldots$)

Vorsicht: Man muss eigentlich unterscheiden zwischen der Aussage „$\phi \Rightarrow \psi$“ und der Behauptung, dass die Aussage ψ aus der Aussage ϕ folgt.

Wenn man mit einem formalen System arbeitet, kann „aus ϕ folgt ψ“ mehrere Bedeutungen haben:

1. Es kann bedeuten, dass die Aussage „$\phi \Rightarrow \psi$“ wahr ist
2. Es kann bedeuten, dass man die Aussage ψ mit Hilfe des formalen Systems aus ϕ ableiten kann.
3. (Und es könnte auch bedeuten, dass ψ in einem intuitiven Sinn aus ϕ folgt.)

Wenn das formale System gut gewählt ist, sollten 1. und 2. äquivalent sein; das wird in der Tat der Fall sein. Deshalb werden wir vorerst nicht präzise sein bei der Unterscheidung zwischen 1. und 2.

`logwahr`

Das formale System, das wir betrachten werden, besteht aus zwei Ebenen:

- Axiome und Ableitungsregeln, die es erlauben, alle „rein logischen“ Aussagen zu beweisen. Genauer: alle Aussagen, für die man nicht wissen muss, was „$\in$“ bedeutet.

  Beispiele:

  Für beliebige Aussagen ϕ kann man „$\phi \vee \neg\phi$“ beweisen.

  „$\forall x, y, z\colon (x \in z \wedge x = y) \Rightarrow y \in z$“ (Was auch immer „$\in z$“ bedeutet: Wenn es auf x zutrifft und $x = y$ ist, dann trifft es auch auf y zu.)
- Dann kommen die „Axiome der Mengenlehre“ hinzu, die beschreiben, was $\in$ bedeutet (und damit indirekt, was Mengen sind).

In den Aussagen kommen viele in der Mathematik üblichen Symbole nicht vor (0, 1, 2, $+$, $-$, $\mathbb{N}$, $\mathbb{R}$, etc.). Wir werden plausibel machen, dass man trotzdem die gesamte (übliche) Mathematik mit solchen Aussagen formulieren (und formal beweisen) kann. Die fehlenden Zeichen werden abkürzende Schreibweisen sein.

In dieser Vorlesung fangen wir mit den Axiomen der Mengenlehre an. Dabei werden wir logische Schlussfolgerungen erst mal weiterhin intuitiv machen (wie im 1. Semester).

Erst später werden wir auch Axiome und Schlussfolgerungsregeln für logische Schlussfolgerungen kennenlernen.

1.2 Die Axiome von ZFC

17.4.2013

Das heute gängigste Axiomensystem ist „ZFC“: entwickelt anfang des 20. Jahrhunderts von Zermelo (Z) und Fraenkel (F); (C) = Choice = Auswahlaxiom = ein Axiom, das etwas später hinzugekommen ist.

Erinnerung: Alle mathematischen Aussagen, die wir zeigen werden, werden Aussagen im Sinne von Def. 1.3 sein. Um von der informellen Verwendung von „Aussage“ zu unterscheiden sagen wir auch „Aussage in der Sprache der Mengenlehre“.

Anmerkung zu Klammerung: Quantoren binden stärker als $\wedge, \vee, \Rightarrow, \ldots$, also bedeutet $\exists x\, \phi \wedge \psi$ z. B. $(\exists x\, \phi) \wedge \psi$.

Idee: Die einzigen mathematischen Objekte, die wir betrachten, sind Mengen. Die Bedeutung von „$\forall x$“ ist: „Für alle Mengen x“; entprechend „$\exists x$“: „Es gibt eine Menge x“. Insbesondere sind die Elemente von Mengen auch wieder Mengen. Alle anderen mathematischen Objekte (Zahlen, Funktionen, etc.) werden wir später geeignet durch Mengen kodieren.

Erinnerung: Wir hatten gesehen, dass nicht für jede „Ansammlung“ von Mengen wieder eine Menge sein kann. Die Axiome werden sagen, was Mengen sind. Wenn wir noch nicht wissen, ob etwas eine Menge ist, nennen wir es eine **Klasse** (also z.B. die „Klasse der Mengen, die sich nicht selbst enthalten“).

Axiom (EXT) = Extensionalität. *Zwei Mengen sind gleich, wenn sie die gleichen Elemente enthalten; also formal:*

$$\forall a \forall b\, (a = b \iff \forall x\, (x \in a \iff x \in b))$$

(Anders ausgedrückt: Mengen haben keine weitere Eigenschaften außer, welche Elemente sie enthalten.)

Definition 1.4 *a ist Teilmenge von b, wenn jedes Element von a auch Element von b ist:*

$$a \subseteq b :\iff \forall x\, (x \in a \Rightarrow x \in b)$$

Naive Mengenlehre würde sagen: zu jeder „Eigenschaft“ gibt es eine Menge der Elemente mit dieser Eigenschaft. Dies lässt sich präzise formulieren, indem man „Eigenschaft“ durch „Formel“. Also: Ist $\phi(x)$ eine Formel (mit

einer freien Variable x), so gibt es eine Menge a so dass für alle x gilt: $x \in a \iff \phi(x)$. Aber wenn wir dies als Axiom nehmen würden, würden wir Russel's Paradox erhalten. Deshalb erlaubt man diese Konstruktion nur, um Teilmengen von gegebenen Mengen zu definieren: Ist b eine Menge und ist $\phi(x)$ eine Formel, so ist gibt es eine Teilmenge a von b so dass für alle $x \in b$ gilt: $x \in a \iff \phi(x)$. Oder, kürzer ausgedrückt: Für alle Mengen b und alle Formeln $\phi(x)$ ist $\{x \in b \mid \phi(x)\}$ eine Menge.

Das ist aber keine Aussage in der Sprache der Mengenlehre, da „Für alle Formeln ϕ" nicht in einer Aussage vorkommen kann. Statt dessen nehmen wir ein Axiom für jedes mögliche ϕ. Wir müssen übrigens außerdem noch weitere Variablen für für Mengen erlauben; Beispiel folgt...

Axiom (AUSS) = Aussonderung. *Für jede Formel $\phi(x, y_1, \ldots, y_n)$ gilt:*

$\forall y_1, \ldots, y_n : \forall b \exists a : \forall x : (x \in a \iff (x \in b \wedge \phi(x, y_1, \ldots, y_n)))$.

Jetzt können wir schon die Existenz von Schnittmengen zeigen:

prop.cap **Proposition 1.5** *Sind c und c' zwei Mengen, so existiert auch die Schnittmenge. Genauer: Es existiert genau eine Menge a so dass $x \in a \iff (x \in c \wedge x \in c')$.*

Formal als Aussage: $\forall a, b \exists^{=1} c : \ldots$. Hierbei ist „$\exists^{=1} x \phi(x, \ldots)$" eine Abkürzung für „$\exists x \phi(x, \ldots) \wedge \forall x, x' : ((\phi(x, \ldots) \wedge \phi(x', \ldots)) \Rightarrow x = x')$

Bew. von prop.cap 1.5: Eindeutigkeit: Wir wollen zeigen: sind a_1 und a_2 beides Mengen mit
(*) $\forall x(x \in a_i \iff (x \in c \wedge x \in c'))$,
so ist $a_1 = a_2$. Aus (*) folgt: $\forall x(x \in a_1 \iff x \in a_2)$. Jetzt besagt (EXT), dass daraus schon $a_1 = a_2$ folgt.

Existenz: Idee: Wende (AUSS) an um die Teilmenge von c zu erhalten bestehend aus denjenigen x, für die „$x \in c'$" gilt. Wir wählen also „$x \in c'$" als Formel ϕ. Beachte: Nicht nur x, sondern auch c' ist eine freie Variable von „$x \in c'$". Formal benutzen wir also das folgende Axiom:

$\forall y_1 \forall b \exists a : \forall x : (x \in a \iff (x \in b \wedge x \in y_1))$.

Jetzt setzen wir c' für y_1 ein und c für b und erhalten:

$\exists a : \forall x : (x \in a \iff (x \in c \wedge x \in c'))$.

Also ist a die gesuchte Schnittmenge. $\square$

Wir führen die üblichen Notationen „$a \cap b$“ für den Schnitt der Mengen a und b ein, und „$a \cup b$“ für die Vereinigung. (Bei der Vereinigung wissen wir aber noch nicht, ob sie existiert.) Das sind natürlich auch abkürzende Schreibweisen für Aussagen (oder Formeln).

Übung: Wie formuliert man „$(a \cap a') \in b$“ als Formel?

Wir können auch schon beweisen, dass die Klasse aller Mengen keine Menge ist. Formal:

Proposition 1.6 $\neg\exists a \forall x\, x \in a$.

Idee: Wende (AUSS) an, um daraus die Menge aller Mengen, die sich nicht selbst enthalten, zu konstruieren...

(AUSS) liefert viel Freiheit, um Teilmengen gegebener Mengen zu konstruieren, aber dazu brauchen wir erst mal gegebene Mengen. Die nächsten Axiome erlauben uns, Mengen zu konstruieren. (Die Schwierigkeit in der Wahl der Axiome besteht darin, zu ermöglichen, hinreichend große Mengen zu konstruieren, ohne dabei zu große Mengen (wie die Menge aller Mengen) zu erlauben.)

Axiom (LEER) = Existenz der leeren Menge. $\exists a \forall y\, y \notin a$.

Aus (EXT) folgt, dass es höchstens ein solches a geben kann. Notation: $\emptyset$.

Übung: Mit (AUSS) zeigen: Wenn es eine Menge gibt, dann gibt es auch die leere Menge.

(Wir werden später sehen, dass man (LEER) auch aus anderen Axiomen folgt.)

Axiom (PAAR) Paarmengen. *Sind a, b Mengen, so ist auch $\{a, b\}$ eine Menge. Formal:* $\forall a, b \exists c \forall x\, (x \in c \iff x = a \vee x = b)$.

Notation: Wir schreiben $\{a_1, \ldots, a_n\}$ für eine Menge, die genau die Elemente $a_1, \ldots, a_n$ enthält. ($a_1, \ldots, a_n$ müssen nicht verschieden sein.)

Eindeutigkeit folgt aus Extensionalität. Das Paarmengen-Axiom sagt Existenz für $n = 2$ (also $\{a_1, a_2\}$). Außerdem erlaubt das Paarmengen-Axiom $a = b$, also auch Existenz von $\{a\}$.

Man könnte ein n-Element-Mengen-Axiom einführen, aber statt dessen lieber:

Axiom (VER) Vereinigung. *Ist a eine Menge, so ist auch $\bigcup_{y\in a} y$ eine Menge. Formal:*
$\forall a \exists b \forall x\, (x \in b \iff \exists y \in a : x \in y)$.

Anmerkung: In Mengenlehre-Büchern wird oft „$\cup a$“ als Kurzschreibweise für $\bigcup_{y\in a} y$ verwendet. Wir verwenden diese Schreibweise nicht.

Damit können wir jetzt zeigen:

prop.cup **Proposition 1.7** *$a \cup b$ ist eine Menge.*

Bew: (PAAR) liefert, dass $\{a, b\}$ eine Menge ist. Darauf (VER) anwenden liefert die gewünschte Vereinigung. □

Jetzt könenn n-Element-Mengen bauen:

prop.n-menge **Proposition 1.8** *$\{a_1, \ldots, a_n\}$ für eine Menge.*

Bew: Übung.

Bevor wir weitere Axiome einführen, geben wir eine erste Konstruktion von Objekten an, die keine Mengen sind: **geordnete Paare**: (a, b).

Wir wollen: (*) $(a, b) = (a', b') \iff (a = a' \wedge b = b')$.

Idee: Definiere (a, b) als eine aus a, b konstruierte Menge, so dass (*) gilt.

Lösung: $(a, b) := \{\{a\}, \{a, b\}\}$.

Aus bisherigem folgt: Sind a, b Mengen, so ist auch (a, b) eine Menge.

Bew. von (*): $\Leftarrow$ ist klar; $\Rightarrow$: Aus $(a, b) = (a', b')$ folgt entweder
(1) $\{a\} = \{a'\}$ und $\{a, b\} = \{a', b'\}$ oder
(2) $\{a\} = \{a', b'\}$ und $\{a'\} = \{a, b\}$
(oder beides, falls alle vier Mengen gleich).

Aus (1) folgt zuerst $a = a'$ und dann $b = b'$.

Aus (2) folgt $a' = b' = a$ und $a' = a = b$, also insbesondere $a = a'$ und $b = b'$. □

Mit den bisherigen Axiomen haben wir schon die gesamte „endliche Mengenlehre“. Wie drückt man aus, dass es eine unendliche Menge a gibt? 24.4.2013

Wähle eine Menge b_0, von der wir verlangen, dass sie Element von a ist; gib eine Konstruktionsvorschrift $b_i \mapsto b_{i+1}$ an, die sicher stellt, dass alle b_i verschieden sind (z.B. weil sie verschieden viel Elemente enthalten); schreibe in das Axiom, dass $b_0 \in a$ sein soll, und dass aus $b_i \in a$ folgen soll, dass $b_{i+1} \in a$ ist.

Die genaue Wahl von b_0 und $b_i \mapsto b_{i+1}$ ist unwichtig, aber üblich ist:

$b_0 = \emptyset$ und $b_{i+1} = b_i \cup \{b_i\}$. Also:

Axiom (INF) = Unendlichkeit. *Es gibt eine Menge a mit $\emptyset \in a$ und so dass für jedes $x \in a$ gilt: $x \cup \{x\} \in a$.*

In der Tat sind alle b_i verschieden. Genauer gesagt kann für jedes i zeigen, dass b_i genau i Elemente enthält, nämlich $b_0, \ldots, b_{i-1}$. (Später genauer.)

Achtung: „Für alle i gilt: b_i enthält i Elemente.“ ist keine Aussage in der Sprache der Mengenlehre.

Anmerkung: Aus (INF) folgt (LEER).

Wir brauchen noch zwei weitere Axiome, um andere unendliche Mengen zu konstruieren.

Axiom (POT) = Potenzmenge. *Ist a eine Menge, so ist $\mathcal{P}(a) := \{b \mid b \subseteq a\}$ auch eine Menge.*

Anmerkung: Wir werden später sehen, dass $\mathcal{P}(a)$ „echt größer“ ist als a. In diesem Sinne ist (POT) nötig, um große Mengen zu konstruieren.

Eine Anwendung:

prop.x **Proposition 1.9** *Sind a und b Mengen, so ist auch das kartesische Produkt $a \times b = \{(x, y) \mid x \in a, y \in b\}$ eine Menge.*

Beweis:

Erinnerung: $(x, y) = \{\{x\}, \{x, y\}\}$.

Habe $\{x\}, \{x, y\} \subseteq a \cup b$, also $\{x\}, \{x, y\} \in \mathcal{P}(a \cup b)$.

Also $(x, y) \subseteq \mathcal{P}(a \cup b)$; also $(x, y) \in \mathcal{P}(\mathcal{P}(a \cup b))$.

Also $a \times b \subseteq \mathcal{P}(\mathcal{P}(a \cup b))$.
Nach 1.7 ist $a \cup b$ eine Menge, und zweimal (POT) anwenden liefert, dass $\mathcal{P}(\mathcal{P}(a \cup b))$ eine Menge ist. Jetzt kann man $a \times b$ mit (AUSS) aus $\mathcal{P}(\mathcal{P}(a \cup b))$ erhalten:

$$a \times b = \{z \in \mathcal{P}(\mathcal{P}(a \cup b)) \mid \exists x \in a, y \in b : z = \{\{x\}, \{x, y\}\}\}$$

□

(Allgemein ist das häufigste Beweisprinzip um zu zeigen, dass eine Klasse c schon eine Menge ist: Konstruiere zunächst mit (VER) und (POT) eine Obermenge von c; wende dann (AUSS) an.)

Eine andere wichtige Methode, um aus einer (unendlichen) Menge a eine neue Menge b zu erhalten, besteht darin, eine „Funktion“ f auf a anzuwenden, also $b = \{f(x) \mid x \in a\}$. „Funktion“ steht hier in Anführungszeichen, weil wir später eine andere Definition von Funktion geben werden, als das, was wir hier meinen. Was wir hier meinen, ist, dass f durch eine Formel $\phi(x, y)$ beschrieben wird: Für jedes x soll es genau ein y geben, so dass $\phi(x, y)$ wahr ist; dieses y soll der Wert $f(x)$ sein. Also haben wir formaler (für eine solche Formel $\phi(x, y)$): $b = \{y \mid \exists x \in a : \phi(x, y)\}$

Wie bei (AUSS) müssen wir auch hier zusätzliche freie Variablen in ϕ zulassen, und wie bei (AUSS) ist das nicht ein einzelnes Axiom, sondern ein Axiom für jedes mögliche ϕ.

Axiom (ERS) = Ersetzung. *Für jede Formel $\phi(x, y, z_1, \ldots, z_n)$ gilt:*

$\forall z_1, \ldots, z_n, a :$
$(\forall x \in a \exists^{=1} y \, \phi(x, y, z_1, \ldots, z_n)$
$\Rightarrow$
$\exists b : \forall y : (y \in b \iff \exists x \in a : \phi(x, y, z_1, \ldots, z_n))).$

Beispiel: Ist a eine Menge, so ist auch $b := \{\mathcal{P}(x) \mid x \in a\}$ eine Menge. Dies folgt aus (ERS) mit $\phi(x, y) =$„$y = \mathcal{P}(x)$“.

(In diesem Beispiel hätte man auch b mit (AUSS) aus $a \times a$ erhalten können. Ein Beispiel, wo man wirklich (ERS) braucht (und die anderen Axiome nicht ausreichen), ist nicht so einfach anzugeben.)

Das waren die Axiome, um (große) Mengen zu konstruieren. Es kommen noch zwei weitere Axiome (die am Anfang noch nicht im Axiomensystem dabei waren):

Wir haben nicht verboten, dass $x \in x$ sein kann. Tatsächlich könnte es eine Menge x geben mit $x = \{x\}$. Theoretisch könnte man das erlauben, aber es ist unschön, da solche Mengen schwierig zu unterscheiden sind: Wenn $x' = \{x'\}$ aber $x \neq x'$, dann ist das schwierig zu zeigen: Um $x \neq x'$ zu zeigen, müsste man zeigen, dass das Element von x ungleich dem Element von x' ist; aber dann ist man wieder beim selben Problem wie vorher. Generell stößt man auf solche Probleme, wenn es unendliche Ketten $x_0 \ni x_1 \ni x_2 \ni \ldots$ gibt. Wir wollen ein Axiom einführen, das solche Ketten verbietet. Das lässt sich nicht so leicht direkt formulieren. Wir werden später sehen, dass das folgende Axiom solche Ketten verbietet.

Axiom (FUND) = Fundierung. *Ist $a \neq \emptyset$ so gibt es $b \in a$ mit $a \cap b = \emptyset$.*

Was wir aber jetzt schon damit zeigen können, ist:

Proposition 1.10 *Für alle x gilt: $x \notin x$.*

Bew: Ann. $x \in x$. Wende (FUND) auf $a = \{x\}$ an. Also $b = x$. Aber $a \cap b = \{x\} \cap x \ni x$. □

Jetzt fehlt noch ein weiteres Axiom für Teilmengen. (AUSS) erlaubt uns nur, Teilmengen zu wählen, die wir durch eine Formel beschreiben können. Manchmal braucht man auch die Existenz von Mengen, die sich nicht durch Formeln beschreiben lassen.

Axiom (AC) = Auswahlaxiom (axiom of choice). *Ist a eine Menge von nicht-leeren, paarweise disjunkten Mengen, so gibt es eine Menge b, so dass für jedes $x \in a$ der Schnitt $x \cap b$ genau ein Element enthält.*

Falls $a = \{x_1, \ldots, x_n\}$ folgt die Existenz von b auch aus den bisherigen Axiomen: N.V. sind alle $x_i \neq \emptyset$. Also gibt es $y_i \in x_i$. Aus 1.8 folgt, dass $b := \{y_1, \ldots, y_n\}$ eine Menge ist.

1.3 Funktionen und Relationen

Wir kodieren weitere Objekte durch Mengen.

Eine Funktion $f\colon a \to b$ wird kodiert durch ihren Graph, als Teilmenge von $a \times b$. Also genauer durch die Menge $\{(x, f(x)) \mid x \in a\}$.

Formal:

Definition 1.11 *Seien a, b Mengen. Eine **Funktion** (oder **Abbildung**) von a nach b ist eine Teilmenge f von $a \times b$, so dass es für jedes $x \in a$ genau ein $y \in b$ gibt mit $(x, y) \in f$.*
Notation „$f : a \to b$“ für: „f ist Fkt von a nach b“.
Notation: Falls $x \in a$ schreibe $f(x)$ für das Element $y \in b$ mit $(x, y) \in f$.
Notation: $\mathrm{dom}(f) = a$ *(*$= \{x \mid \exists y : (x, y) \in f\}$*) (Domain; Definitionsbereich)*
Notation: $\mathrm{im}(f) = \{y \mid \exists x : (x, y) \in f\}$*) (image; Bildbereich)*

*Wie üblich heißt $f : a \to b$ **injektiv/surjektiv/bijektiv** wenn es zu jedem $y \in b$ höchstens/mindetens/genau ein $x \in a$ gibt mit $f(x) = y$.*

Übung: $\mathrm{im}(f)$ ist eine Menge.

Vorsicht: Ist $f : a \to b$ und $b \subseteq b'$, so ist f auch eine Funktion von a nach b'; ob f surjektiv (oder bijektiv) ist, hängt aber davon ab, ob wir es als Funktion nach b oder nach b' betrachten.

Weitere Definitionen wie üblich:

Definition 1.12 *Für $f : a \to b$ und $g : b \to c$ sei $g \circ f$ die Verknüpfung. Also formal: $g \circ f = \{(x, g(f(x))) \mid x \in a\}$.*
Für $f : a \to b$ und $y \in b$ schreibe $f^{-1}(y)$ für das Urbild von y, also formal: $f^{-1}(y) = \{x \in a \mid f(x) = y\}$.

Übung: $g \circ f$ und $f^{-1}(y))$ sind Mengen (und nicht nur Klassen).

defn.rel2

Definition 1.13 *Sei a eine Menge. Eine **Relation** R auf a ist eine Teilmenge von $a \times a$. Wir schreiben xRy falls $(x, y) \in R$.*

Definiere reflexiv, symmetrisch, transitiv, Äquivalenzrelation wie üblich.

*R heißt **Ordnungsrelation** (oder einfach nur Ordnung), wenn gilt:*

1. *R ist reflexiv, d.h. xRx für alle x*
2. *R ist transitiv, d.h. aus xRy und yRz folgt xRz.*
3. *R ist antisymmetrisch, d.h. aus xRy und yRx folgt $x = y$.*
4. *Für beliebige x, y gilt xRy oder yRx.*

Ist R Ordnungsrelation, so schreibe üblicherweise $x \leq y$ statt xRy (und sage „x ist kleiner oder gleich y“). Schreibe außerdem: $x < y$ als Abkürzung für $x \leq y$ und $x \neq y$, und manchmal $y \geq x$ statt $x \leq y$, etc.

Anmerkung: Sind a, b Mengen, so ist auch die Klasse der Funktionen von a nach b wieder eine Menge, und die Klasse der Relationen auf a auch. (Beweis analog zu 1.9, mit 1.7, (POT) und (AUSS).) Mit einer weiteren Anwendung von (AUSS) erhält man daraus die Menge der injektiven/surjektiven/bijektiven Funktionen, die Menge der Äquivalenz-Relationen, der Ordnungsrelationen, etc.

prop.x prop^cup

8.5.2013

Definition 1.14 *Ist $\leq$ eine Ordnungsrelation auf einer Menge a und ist $b \subseteq a$ eine Teilmenge, so ist ein **Minimum** von b ein Element $x \in b$ mit $x \leq y$ für alle $y \in b$. Notation: $x = \min b$. Entsprechend: **Maximum**, falls $x \geq y$ für alle $y \in b$; Notation $x = \max b$.*

*$\leq$ heißt **Wohlordnung**, wenn jede nicht-leere Teilmenge ein Minimum hat.*

Bem: Ein Minimum oder Maximum muss nicht immer existieren, aber wenn sie existieren, sind sie eindeutig (Übung).

Beispiel $a = \mathbb{N}$, $b = 2\mathbb{N}$: hat Minimum aber kein Maximum. Wir werden zeigen: $\leq$ auf $\mathbb{N}$ ist Wohlordnung.

Bespiel $a = \mathbb{R}$, $b = \{x \in a \mid x > 0\}$: hat weder Minimum noch Maximum; $\leq$ auf $\mathbb{R}$ ist keine Wohlordnung.

1.4 Natürliche Zahlen: Definition

Es gibt verschiedene Möglichkeiten, die natürlichen Zahlen als Mengen zu kodieren. Praktisch ist, jede natürliche Zahl durch die Menge ihrer Vorgränger zu kodieren, also: $0 = \emptyset$, $1 = \{0\}$, $2 = \{0, 1\}$, $3 = \{0, 1, 2\}$. Wir definieren also:

Definition 1.15 *$0 := \emptyset$, und der Nachfolger von n ist $s(n) := n \cup \{n\}$. Außerdem haben wir die Notationen $1 := s(0)$, $2 := s(s(0))$, etc.*

Ausgeschrieben ergibt das:

Also: $1 = s(0) = 0 \cup \{0\} = \{\emptyset\}$,
$2 = s(1) = 1 \cup \{1\} = \{0, 1\} = \{\emptyset, \{\emptyset\}\}$,
$3 = s(2) = 2 \cup \{2\} = \{0, 1, 2\} = \{\emptyset, \{\emptyset\}, \dots\}$,
$\dots$

Um mit den natürlichen Zahlen arbeiten zu können, brauchen wir, dass die Klasse der natürlichen Zahlen eine Menge ist. (Erst dann können wir Aussagen formulieren der Art „$\forall n \in \mathbb{N} \ldots$“.) Dazu wollen wir zunächst eine Formel $\phi(x)$ (in der Spr. d. ML) angeben, die ausdrückt: „x ist natürliche Zahl“.

Das folgende sind *keine* geeigneten Definitionen:

- $\mathbb{N} = \{0, s(0), s(s(0)), \ldots\}$; das lässt sich nicht als Formel ohne Pünktchen schreiben.
- $x \in \mathbb{N} \iff x = s(\ldots(s(0))\ldots)$. Die Pünktchen stehen für endlich viele Anwendungen von $s()$. Wenn man fest legt, wie viele Anwendungen von $s()$ man meint, hat man in der Tat eine gültige Formel in der Sprache der Mengenlehre, aber die würde besagen, dass x nur eine bestimmte natürliche Zahl sein kann. Mit den Pünktchen ist also eine variable Anzahl von Anwendungen von $s()$ gemeint, und das lässt sich wieder nicht als eine einzige Formel ausdrücken.

Feststellungen:

- Ist n eine natürliche Zahl, so ist $\leq$ eine Ordnungsrelation auf n.
- Diese Ordungsrelation kann definiert werden durch: $k \leq m$ gdw. $k = m$ oder $k \in m$.

Definition 1.16 *Eine Menge a heißt **transitiv**, wenn für alle $x \in a$ gilt: $x \subseteq a$. Oder anders ausgedrückt: $y \in x$ und $x \in a \Rightarrow y \in a$.*

(Vorsicht: Diese Bedeutung von transitiv ist nicht die selbe wie bei Relationen.)

defn.N **Definition 1.17** *Eine Menge n heißt **natürliche Zahl** wenn gilt:*

1. *n ist transitiv.*
2. *Die Relation $x \leq y :\iff (x \in y \vee x = y)$ auf n ist eine Ordnungsrelation.*
3. *Ist $b \subseteq n$ nicht leer, so hat b ein Minimum und ein Maximum.*

Es sollte klar sein, dass sich „n ist nat. Zahl“ (in diesem Sinne) durch eine Formel (in der Sprache der Mengenlehre) ausdrücken lässt.

Ist ist nicht schwer zu sehen, dass $0, 1, 2, 3, \ldots$ natürliche Zahlen im Sinne dieser Definition sind. Allerdings ist „$0, 1, 2, \ldots$ sind natürliche Zahlen“ keine Aussage in der Sprache der Mengenlehre. Eine formale Aussage ist hingegen das folgende:

prop.Nrek **Proposition 1.18** *1.* 0 *ist eine natürliche Zahl.*

2. Ist n *eine natürliche Zahl, so ist auch* $s(n)$ *eine natürliche Zahl.*

Beweis: Übung

Jetzt müssen wir noch zeigen, dass es keine weiteren Mengen gibt, die natürliche Zahlen sind. Genauer gesagt zeigen wir:

prop.Nstrukt **Proposition 1.19** *Ist* n *eine natürliche Zahl mit* $n \neq 0$*, so gibt es genau eine natürliche Zahl* m *mit* $s(m) = n$*. Außerdem gilt:* $x \in n \iff x$ *ist natürliche Zahl und* $x \leq m$*.*

Beweis:

Wir zeigen als erstes, dass jedes Element $m \in n$ eine natürliche Zahl ist. 1.: Sei $y \in x \in m$. Aus Transitivität von n erhält man zunächst $x \in n$ und dann auch $y \in n$. Da $\leq$ eine Ordnungs-Rel auf n ist (und $y \in x \in m$ bedeutet: $y < x < m$), folgt $y \in m$.
2.+3.: Es reicht z.z., dass $m \subseteq n$ ist. Das folgt aus der Transitivität von n.

Existenz von m: Wähle für m das maximale Element der Menge n (existiert nach defn.N 1.17 3.; und wir haben gerade gezeigt, dass m dann eine natürliche Zahl ist).
Behauptung: $m \cup \{m\} = n$
„$\supseteq$“ $x \in n \Rightarrow x < m \vee x = m \Rightarrow x \in m \vee x = m$.
„$\subseteq$“ $m \in n$ ist klar. $m \subseteq n$ folgt aus Transitivität von n.

Eindeutigkeit von m: Aus $m \cup \{m\} = n$ folgt (1) $m \in n$ und (2) $\forall x \in n : x = m \vee x \in m$, also $x \leq m$. Diese beiden Aussagen zusammen sagen gerade: m ist maximales Element der Menge n.

Beweis von „Ausserdem“:

"⇒": ist bereits gezeigt.

"⇐": Aus $x \leq m$ folgt $x = m$ ($\Rightarrow x \in n$) oder $x \in m$ ($\Rightarrow x \in n$ mit Transitivität von n). □

Eine der wichtigsten Eigenschaften der natürlichen Zahlen ist, dass man Induktionsargumente machen kann. Das werden wir auch verwenden, um die Existenz der Menge der natürlichen Zahlen zu zeigen.

satz.ind **Satz 1.20** *(Prinzip der vollständigen Induktion) Ist a eine Menge mit: $0 \in a$, und so dass für jedes $x \in a$ gilt $s(x) \in a$, so enthält a alle natürlichen Zahlen. (Formal: $\forall x : x$ natürliche Zahl $\Rightarrow x \in a$.)*

Beweis: Annahme, a enthält nicht alle natürlichen Zahlen. Es gibt also eine Menge n mit: n ist natürliche Zahl und $n \notin a$.

Betrachte $b := s(n) \setminus a$. Das ist nicht-leer (da es n enthält), also hat b ein Minimum $m = \min b$.

Da $0 \in a$ ist $0 \notin b$, also $m \neq 0$, also gibt es m' mit $m = s(m')$.
Da $m' < m$ (und m Minimum von b) folgt $m' \notin b$, also $m' \in a$. Daraus folgt aber nach Voraussetzung $m \in a$. Widerspruch. □

Jetzt können wir zeigen: 15.5.2013

satz.N **Satz 1.21** *Die Klasse der natürlichen Zahlen (also der Mengen, die* defn.N *1.17 erfüllen), ist eine Menge. Diese Menge wird mit $\mathbb{N}$ oder ω bezeichnet.*

Beweis: Erinnerung an (INF): Es gibt eine Menge a mit $0 \in a$ und für alle $x \in a$ gilt: $s(x) \in a$.
Nach Satz satz.ind 1.20 gilt für alle x: x ist natürliche Zahl $\Rightarrow x \in a$.

Jetzt erhalten wir $\mathbb{N}$ mit (AUSS):
$\mathbb{N} = \{x \in a \mid x \text{ ist natürliche Zahl}\}$ □

1.5 Natürliche Zahlen: Grundlegende Operationen

Ab jetzt können wir eigentlich wieder vergessen, wie wir die natürlichen Zahlen durch Mengen kodiert haben; das einzige, was wir brauchen, sind Prop.

prop.Nrek 1.18 und Satz satz.ind 1.20. Manchmal ist es aber praktischer, trotzdem noch die Kodierung zu verwenden.

Bisher hat $\leq$ eine Ordnungsrelation auf jeder einzelnen natürlichen Zahl definiert. Jetzt erhalten wir eine Ordnungsrelation auf ganz $\mathbb{N}$:

Definition 1.22 *Für $m, n \in \mathbb{N}$ definiere $m \leq n \iff m \in n \vee m = n$.*

Bem: Es folgt:
$m < n \iff m \in n$
$m \leq n \iff m \in s(n)$

satz.Nle **Satz 1.23** *1. $\leq$ definiert eine Ordnungsrelation auf $\mathbb{N}$.*

2. $0 \leq n$ für alle $n \in \mathbb{N}$, und $s(n)$ ist der direkte Nachfolger von n, d.h. aus $n \leq m \leq s(n)$ folgt $m = n$ oder $m = s(n)$.

3. $\leq$ definiert eine Wohlordnung auf $\mathbb{N}$.

Beweis:
Wir fangen mit 2. an:

2., 1. Teil: Wir benutzen Induktion satz.ind 1.20 über n.
Formal: Sei $a = \{n \in \mathbb{N} \mid 0 \leq n\}$. Wir müssen zeigen: $0 \in a$ und wenn $m \in a$, dann $s(m) \in a$. Danach folgt aus satz.ind 1.20: $a = \mathbb{N}$
$0 \leq 0$ ist klar
$0 \leq n$
$\Rightarrow (0 = n \vee 0 \in n) \Rightarrow 0 \in s(n) \Rightarrow 0 \leq s(n)$

2., 2. Teil: Übung.

1.
Für jede natürliche Zahl n wissen wir, dass $\leq$ eine Ordnungsrel. auf der Menge n definiert; die Frage ist nur, ob es auch eine Ord-Rel auf ganz $\mathbb{N}$ definiert. Für Reflexivität, Anti-Symmetrie und Transitivität lässt sich das direkt übertragen. Genauer:

Reflexivität ist klar nach Def..

Anti-Symmetrie: Sei $m \leq n$ und $n \leq m$. Insbesondere sind $m, n \in s(n)$. Dann folgt Anti-Symmetrie aus der Antisymmetrie von $\leq$ auf $s(n)$.

Transitivität: Sei $k \leq m$ und $m \leq n$. Dann sind $k, m, n \in s(n)$, und transitivität folgt aus der Transitivität von $\leq$ auf $s(n)$.

Die einzige Schwierigkeit ist zu zeigen, dass je zwei Zahlen verlgeichbar sind, also dass für beliebige $m, n \in \mathbb{N}$ gilt: $m \leq n$ oder $n \leq m$. Wir benutzen Induktion über n. Sei also
$a = \{n \in \mathbb{N} \mid \forall m \in \mathbb{N} : (m \leq n \vee n \leq m)\}$.
Wir müssen wieder zeigen:
(a) $0 \in a$
und
(b) $n \in a \Rightarrow s(n) \in a$.

(a) haben wir bereits gezeigt.

Bew. von (b): Seien m, n gegeben. Z.Z: m, $s(n)$ vergleichbar.
Nach I.V. sind m und n vergleichbar.
Fall $m \leq n$: Dann ist $m \in s(n)$, also $m < n$.
Fall $n < m$:
Setze $n' := \min\{k \in s(m) \mid n < k\}$. (Die Menge ist nicht leer, da sie m enthält.)
Da $n' \in s(m)$ ist $n' \leq m$. Bleibt zu zeigen: $n' = s(n)$.
In der Tat gilt für alle x: $x \in n' \iff x < n' \iff^* x \leq n \iff x \in s(n)$
Bzgl. $\iff^*$:
„$\Leftarrow$“: Aus $x \leq n < n'$ folgt $x < n'$
„$\Rightarrow$“: Aus $x < n'$ folgt $x \not> n$, da n' minimal ist. Da $x, n \in s(m)$, sind sie aber vergleichbar, also $x \leq n$.

3.
Sei $a \subseteq \mathbb{N}$ nicht-leer. Wähle $n \in a$ und betrachte $a' := a \cap s(n)$. Das ist eine nicht-leere TM von $s(n)$ (da $n \in a'$), also hat sie ein Minimum $m \in a'$.
Behauptung: m ist auch Minimum von a.
Zu zeigen ist: $k \in a \Rightarrow k \geq m$.
Falls $k \leq n$ ist, folgt das aus $k \in a'$. Ansonsten folgt es aus $m \leq n \leq k$. $\square$

Jetzt wollen wir Addition und Multiplikation auf $\mathbb{N}$ definieren. Idee: $m+n := s(...s(m))$ (n mal); und danach $m \cdot n = m + \cdots + m$ (n mal). Solche Pünktchen-Definitionen kann man als **rekursive Definitionen** formalisieren:

Addition: (1) $m + 0 := m$ und (2) $m + s(n) := s(m + n)$.

Zu zeigen ist: (*) Es gibt genau eine Funktion $+\colon \mathbb{N} \times \mathbb{N} \to \mathbb{N}$, die (1) und (2) erfüllt.

Multiplikation entsprechend: $m \cdot 0 := 0$ und $m \cdot s(n) := m \cdot n + n$.

Um (*) zu zeigen, benutzen wir den folgenden Satz:

satz.rek

Satz 1.24 *(Rekursionssatz) Seien a, b Mengen und $f\colon a \to b$ und $g\colon a \times \mathbb{N} \times b \to b$ Funktionen. Dann gibt es genau eine Funktion $h\colon a \times \mathbb{N} \to b$ mit folgenden Eigenschaften:*
(1) $h(x, 0) = f(x)$
(2) $h(x, s(n)) = g(x, n, h(x, n))$

Zur Veranschaulichung von diesem Satz hier erst mal eine vereinfachte Version: Sei b eine Menge, $e \in b$ und $g\colon b \to b$. Dann gibt es genau eine Funktion $h\colon \mathbb{N} \to b$ mit folgenden Eigenschaften:
(1) $h(0) = e$
(2) $h(s(n)) = g(h(n))$

Beispiel-Anwendung der vereinfachten Version: Definition der Verdopplungsfunktion $d\colon \mathbb{N} \to \mathbb{N}, n \mapsto 2n$. Dies lässt sich rekursiv definieren durch: $d(0) = 0$ und $d(s(n)) = s(s(d(n)))$. Setze in diesem Fall also $e = 0$ und $g(k) = s(s(k))$.

Bei der vereinfachten Version kann die definierte Funktion h nur von einer Variablen $n \in \mathbb{N}$ abhängen; bei der vollständigen Version ist noch eine weitere Variable $x \in a$ erlaubt. (Dies wird für die Def. von Add. und Mult. benötigt.)

Anwendung von satz.rek 1.24, um Addition zu definieren: $a = b = \mathbb{N}$, $f(m) = m$, $g(m, n, k) = s(k)$.
Dann erfüllt h folgendes: $h(m, 0) = f(m) = m$; $h(m, s(n)) = g(m, n, h(m, n)) = s(h(m, n))$. (Nachdem wir so die Exitenz von h gezeigt haben, schreiben wir $m + n$ statt $h(m, n)$.)
Anwendung von satz.rek 1.24, um (danach) Mult. zu definieren: $f(m) = 0$, $g(m, n, k) := k + m$.

Beweis vom Rekursionssatz:

Wir werden per Induktion zeigen: Für jedes $m \in \mathbb{N}$ gibt es genau eine Funktion $h_m\colon a \times \{0, \ldots, m\} \to b$, die (1) erfüllt und die (2) für $n < m$ erfüllt. Danach folgt daraus die Existenz und Eindeutigkeit von h:

Existenz von h: Definiere $h(x,n) := h_n(x,n)$. Das erfüllt (1), da h_0 (1) erfüllt. Damit h (2) erfüllt, ist zu zeigen: $h_{s(n)}(x,s(n)) = g(x,n,h_n(x,n))$.
Da $h_{s(n)}$ (2) erfüllt, haben wir $h_{s(n)}(x,s(n)) = g(x,n,h_{s(n)}(x,n))$; bleibt also zu zeigen: $h_n(x,n) = h_{s(n)}(x,n)$. Aus der Eindeutigkeit von h_n folgt, dass die Einschränkung von $h_{s(n)}$ auf die Menge $a \times \{0,\dots,n\}$ gleich h_n ist; also insbesondere $h_n(x,n) = h_{s(n)}(x,n)$.

Eindeutigkeit von h. Annahme, h' erfüllt auch (1), (2), aber es gibt x,m mit $h(x,m) \neq h'(x,m)$. Dann erfüllen die Einschränkungen dieser Funktionen auf $a \times \{0,\dots,m\}$ die Bedingungen (1), (2), sind aber verschieden; Widerspruch zur Eindeutigkeit von h_m.

Beweis von der Existenz und Eindeutigkeit der h_m per Induktion über m; sei also a die Menge der m, für die genau ein solches h_m existiert. 29.5.2013

Ind. Anfang: $0 \in a$:
Klar. (h_0 wird eindeutig durch (1) definiert, und (2) macht keine Aussage über h_0.)

Ind. Schritt: $m \in a \Rightarrow s(m) \in a$:
Existenz: Definiere $h_{s(m)}(x,n) := \begin{cases} h_m(x,n) & \text{falls } n \leq m \\ g(x,m,h_m(x,m)) & \text{falls } n = s(m) \end{cases}$.

Daraus, dass h_m (1) und (2) erfüllt, folgt, dass $h_{s(m)}$ diese Bedingungen für $n < m$ auch erfüllt. Bleibt Bedingung (2) im Fall $n = m$ zu zeigen; dies gilt nach Def. von $h_{s(m)}$.

Eindeutigkeit: Annahme, $h'_{s(m)}$ ist eine weitere Funktion, die (1), (2) für $n \leq m$ erfüllt.
Die Einschränkung von $h'_{s(m)}$ auf die Menge $a \times \{0,\dots m\}$ erfüllt (1), (2) für $n < m$, ist also nach I.V. gleich h_m. D.h. $h'_{s(m)}(x,n) = h'_{s(m)}(x,n)$ für alle x und alle $n \leq m$. Aus (2) für $m = n$ folgt dann $h'_{s(m)}(x,s(m)) = g(x,m,h'_m(x,m))) = g(x,m,h_m(x,m)) = h_{s(m)}(x,s(m))$ □

Eine weitere Beispiel-Anwendung des Rekursionssatzes: Für eine Funktion $\rho\colon \mathbb{N} \to \mathbb{N}$ wollen wir $\sum_{i=0}^{n} \rho(i) = \rho(0) + \dots + \rho(n)$ definieren.
Rekursive Definition:
$\sum_{i=0}^{0} = \rho(0) \rightsquigarrow f(x) := \rho(0)$
$\sum_{i=0}^{s(n)} = (\sum_{i=0}^{n} \rho(i)) + \rho(s(n)) \rightsquigarrow g(x,n,k) := k + \rho(s(n))$.
Wende Rek.-Satz auf f, g (und $b = \mathbb{N}, a = \{\emptyset\}$) an; erhalte genau ein $h\colon \{\emptyset\} \times$

$\mathbb{N} \to \mathbb{N}$; dies ist die gesuchte Funktion.

Wir haben jetzt Addition und Multiplikation definiert, aber haben sie auch die erwarteten Eigenschaften?

prop.Nop **Proposition 1.25** *Für alle $k, m, n \in \mathbb{N}$ gilt:*

1. $0 + k = k + 0 = k$ *(0 ist neutrales Element bzgl. +)*
2. $k + m = m + k$ *(+ ist kommutativ)*
3. $(k + m) + n = k + (m + n)$ *(+ ist assoziativ)*
4. *Aus $m + k = n + k$ folgt $m = n$*

5. $1 \cdot k = k \cdot 1 = k$ *(1 ist neutrales Element bzgl. ·)*
6. $k \cdot m = m \cdot k$ *(· ist kommutativ)*
7. $(k \cdot m) \cdot n = k \cdot (m \cdot n)$ *(· ist assoziativ)*
8. $k \cdot (m + n) = k \cdot m + k \cdot n$ *(Distributivität)*
9. $0 \cdot k = k \cdot 0 = 0$
10. *Aus $m \cdot k = n \cdot k$ und $k \neq 0$ folgt $m = n$*

11. $m \leq n \iff \exists \ell \in \mathbb{N}\colon m + \ell = n$
12. $m \leq n \Rightarrow k + m \leq k + n$
13. $m \leq n \Rightarrow k \cdot m \leq k \cdot n$

Ein paar dieser Aussagen sind direkt klar, der Beweis der restlichen geht per Induktion. Hier nur ein paar Beispiele:

Bew. von 1.:

Nach Definition von + ist $k + 0 = k$. Bleibt also zu zeigen: $0 + k = k$; wir machen eine Induktion über k:
Ind. Anf: $0 + 0 = 0$ gilt per Def. von +.
Ind. Schluss: $0 + s(k) = s(0 + k) = s(k)$. □

Bew. von 2.:

Wir zeigen $k + m = m + k$ per Induktion über m. (Formal betrachten wir die Menge $a = \{m \in \mathbb{N} \mid \forall k \in \mathbb{N} : k + m = m + k\} \dots$)

Ind. Anfang ($m = 0$): Z.z. ist $k + 0 = 0 + k$. Das haben wir bereits gezeigt.

Ind Schluss ($m \to s(m)$): Zu zeigen ist: $k + s(m) = s(m) + k$. Die l.S. ist nach Def. gleich $s(k + m)$. Mit einer weiteren Induktion über k zeigen wir, dass für alle m, k gilt: $s(m) + k = s(m + k)$.
Ind. Anf: $s(m) + 0 = s(m) = s(m + 0)$.
Ind. Schluss: $s(m) + s(k) = s(s(m) + k) \stackrel{I.V.}{=} s(s(m + k)) = s(m + s(k))$ □

Weitere Teilaussagen: Übung.

(Weitere „Grundaussagen“ über $\mathbb{N}$: Zusammenhang zwischen $+$, $\cdot$ und $\leq$, z.B. $m \leq n \Rightarrow k + m \leq k + n \dots$)

1.6 Ganze Zahlen, rationale Zahlen und der ganze Rest

Die anschaulichste Art, $\mathbb{Z}$ (mit Hilfe von $\mathbb{N}$) zu definieren wäre, indem man $\mathbb{N}$ nimmt und die „disjunkte Vereinigung“ mit $\mathbb{N} \setminus \{0\}$ bildet; die Elemente der disjunkten Kopie stehen dann für die entsprechenden negativen Zahlen. Nachteil: Das macht die Definition von $+$ und $-$ und $\cdot$ auf $\mathbb{Z}$ fallunterscheidungslastig. (und die Beweise von Kommutativität, etc. auch).

Praktischer: Jede ganze Zahl n lässt sich als Differenz zweier natürlicher Zahlen $m - k$ schreiben. Stelle die Zahl n durch das Paar (m, k) dar. Dabei werden Paare identifiziert, wenn sie die gleiche Differenz haben. Dass $m - k = m' - k'$ können wir zwar noch nicht ausdrücken (dazu bräuchten wir ja die negativen Zahlen schon), aber das ist äquivalent zu $m + k' = m' + k$.

prop.Zaeq

Proposition 1.26 *Auf $\mathbb{N} \times \mathbb{N}$ wird durch $(m, k) \sim (m', k') :\iff m + k' = m' + k$ eine Äquivalenzrelation definiert.*

Bew: Reflexivität und Symmetrie sind klar. Transitivität ist auch nicht schwer: Sei $(m, k) \sim (m', k')$ und $(m', k') \sim (m'', k'')$, also $m + k' = m' + k$ und $m' + k'' = m'' + k'$. Zu zeigen: $m + k'' = m'' + k$.
Addiere dazu die beiden anderen Gleichungen. Das liefert: $m + k' + m' + k'' = m' + k + m'' + k'$. Mit prop.Nop 1.25 folgt das Gewünschte. □

Jetzt können wir definieren:

Definition 1.27 $\mathbb{Z} := (\mathbb{N}\times\mathbb{N})/\sim$, *wobei* $\sim$ *die Äquivalenzrelation aus Prop. 1.26 ist.*

prop.Zaeq

(Erklärung der Notation: Ist a eine Menge und $\sim$ eineAus $m + k = n + k$ folgt $m = n$ Äquivalenzrelation auf a, so schreiben wir $a/\sim$ für die Menge der Äquivalenzklassen.)

Um $+$, $-$, $\cdot$ auf $\mathbb{Z}$ zu definieren, stellen wir uns (m, k) als „$m - k$“ vor. Zunächst liefert das eine Definition auf $\mathbb{N} \times \mathbb{N}$:

Definition 1.28 *Definiere* $+$, $-$, $\cdot$, $\leq$ *auf* $\mathbb{N} \times \mathbb{N}$ *durch:*
$(m_1, k_1) + (m_2, k_2) := (m_1 + m_2, k_1 + k_2)$.
(da $(m_1 - k_1) + (m_2 - k_2) := (m_1 + m_2) - (k_1 + k_2)$*)*
$(m_1, k_1) - (m_2, k_2) := (m_1 + k_2, k_1 + m_2)$.
(da $(m_1 - k_1) - (m_2 - k_2) := (m_1 + k_2) - (k_1 + m_2)$*)*
$(m_1, k_1) \cdot (m_2, k_2) := (m_1m_2 + k_1k_2, m_1k_2 + k_1m_2)$.
(da $(m_1 - k_1) \cdot (m_2 - k_2) := (m_1m_2 + k_1k_2) - (m_1k_2 + k_1m_2)$*)*

Jetzt müssen zeigen, dass das mit $\sim$ kompatibel ist, also:

Proposition 1.29 *Wenn* $(m_1, k_1) \sim (m'_1, k'_1)$ *und* $(m_2, k_2) \sim (m'_2, k'_2)$*, dann auch:*
(a) $(m_1, k_1) + (m_2, k_2) \sim (m'_1, k'_1) + (m'_2, k'_2)$
(b) $(m_1, k_1) - (m_2, k_2) \sim (m'_1, k'_1) - (m'_2, k'_2)$
(c) $(m_1, k_1) \cdot (m_2, k_2) \sim (m'_1, k'_1) \cdot (m'_2, k'_2)$.

Beweis: Leichte Rechnungen in $\mathbb{N}$ (die Prop. 1.25 verwenden). Beispiel: Aus $m_1 + k'_1 = m'_1 + k_1$ und $m_2 + k'_2 = m'_2 + k_2$ folgt $m_1 + m_2 + k'_1 + k'_2 = m'_1 + m'_2 + k_1 + k_2$, also (a). □

prop.Nop

Eine Unschönheit an dieser Definition von $\mathbb{Z}$ ist: Streng formal gilt *nicht* $\mathbb{N} \subseteq \mathbb{Z}$. Das ist allerdings nicht weiter schlimm: Wir können $\mathbb{N}$ mit der entsprechenden Teilmenge von $\mathbb{Z}$ „identifizieren“: Identifiziere $n \in \mathbb{N}$ mit $(n, 0) \in \mathbb{Z}$.

„Identifizieren“ bedeutet, dass man eine unpräzise Notation verwendet: Wenn $n \in \mathbb{N}$ eine natürliche Zahl ist und z die „gleiche“ Zahl als Element von $\mathbb{Z}$, dann schreiben wir $n = z$, obwohl das nach unserer formalen Definition nicht stimmt. Entsprechend schreiben wir auch $\mathbb{N} \subseteq \mathbb{Z}$. In der Praxis ist das kein Problem, da wir uns normalerweise nicht dafür

interessieren, wie die Zahlen durch Mengen kodiert wurden, sondern nur, wie man mit ihnen rechnet.

Damit diese Indentifikation keine Probleme bereitet, ist zu zeigen:

Proposition 1.30 *(1) Die Abbildung* $\mathbb{N} \to \mathbb{Z}, n \mapsto (n, 0)$ *ist injektiv.*
Für alle $m, n \in \mathbb{N}$ *gilt:*
(2.1) $(m + n, 0) = (m, 0) + (n, 0)$ *und*
(2.2) $(m \cdot n, 0) = (m, 0) \cdot (n, 0)$.

Bew: Für (1) zu zeigen: Aus $(n, 0) \sim (n', 0)$ folgt $n = n'$. Das folgt direkt aus der Def. von $\sim$.

(2.1) Leicht.

(2.2) Auch leicht: $(m, 0) \cdot (n, 0) = (mn + 0 \cdot 0, m \cdot 0 + 0 \cdot n) = (mn, 0)$. □

Bisher war „$(m, k) = m - k$“ nur die Anschaung hinter (m, k). Jetzt können wir formal nachrechnen: $m - k$ „=“ $(m, 0) - (k, 0) = (m + 0, k + 0) = (m, k)$.

Und jetzt können wir auch prüfen, dass $+, -, \cdot$ die gewünschten Eigenschaften auf $\mathbb{Z}$ haben:

prop.Zop

Proposition 1.31 *Prop.* prop.Nop *1.25 1.– 10. gelten auch für* $k, m, n \in \mathbb{Z}$.
Außerdem gilt $k + m - m = k$*; insbesondere ist* $(\mathbb{Z}, +, 0)$ *ist abelsche Gruppe, wobei* $-m := 0 - m$ *das additive Inverse von* k *ist.*

Beweis: Nicht schwer. Beispiel: Kommutativität von $\cdot$:
Zu zeigen ist: $(m_1, k_1) \cdot (m_2, k_2) = (m_2, k_2) \cdot (m_1, k_1)$.

L.S. $= (m_1 m_2 + k_1 k_2, m_1 k_2 + k_1 m_2)$
R.S. $= (m_2 m_1 + k_2 k_1, m_2 k_1 + k_2 m_1)$
Verwende Kommuatativität von $+$ und $\cdot$ in $\mathbb{N}$. □

Die Definition der rationalen Zahlen aus den ganzen Zahlen geht analog zur Definition der ganzen Zahlen aus den natürlichen Zahlen: Jede ganze Zahl ist *Differenz* zweier natürlicher Zahlen; jede rationale Zahl ist *Quotient* zweier ganzer Zahlen. Genauer: 5.6.2013

Definition 1.32 $\mathbb{Q} := (\mathbb{Z} \times (\mathbb{N} \setminus \{0\}))/\sim$, *wobei* $(m, k) \sim (m', k') :\iff m \cdot k' = m' \cdot k$.

Wie bei den ganzen Zahlen, ist dann zu tun:

- Zeige, dass $\sim$ eine Äquiv-Rel. ist
- Definiere $+, -, \cdot, /$ so wie man es erwarten würde, wenn man sich (m, k) als $\frac{m}{k}$ vorstellt. Zum Beispiel: $(m_1, k_1)+(m_2, k_2) := (m_1k_2+m_2k_1, k_1k_2)$ und $(m_1, k_1)/(m_2, k_2) := (m_1k_2, m_2k_1)$
- Zeige, dass diese Def. mit $\sim$ kompatibel sind.
- Identifiziere $\mathbb{Z}$ mit der entsprechenden Teilmenge von $\mathbb{Q}$, d.h. zeige, dass die Abbildung $\mathbb{Z} \to \mathbb{Q}$, $n \mapsto (n, 1)$ injektiv und kompatibel mit $+$, $-$, $\cdot$ ist.
- Zeige prop.Zop 1.31 für $k, m, n \in \mathbb{Q}$. Insbesondere: $\mathbb{Q}$ ist Körper.

Wie man aus den rationalen Zahlen die reellen konstruiert, sollte in einer Vorlesung im 1. Semester dran gewesen sein: reelle Zahlen sind als Suprema von Mengen von rationalen Zahlen gegeben. (Formal wird $\mathbb{R}$ definiert als eine geeignete Teilmenge von $\mathcal{P}(\mathbb{Q})$, modulo einer geeigneten Äquivalenzrelation.)

Wie man aus den reellen Zahlen die komplexen Zahlen erhält, kam auch schon dran: $\mathbb{C} = \mathbb{R} \times \mathbb{R}$...

Jetzt sollte einigermaßen klar sein, dass man sämtliche mathematischen Objekte durch Mengen kodieren kann und alle Sätze als Aussagen in der Sprache der Mengenlehre formulieren kann.

Ein paar weitere Beispiele:

- Den Vektorraum $\mathbb{R}^n$ kann man z.B. definieren als $\underbrace{\mathbb{R} \times \mathbb{R} \times \cdots \times \mathbb{R}}_{n \text{ mal}}$.

  Wenn man dann Aussagen über $\mathbb{R}^n$ für alle $n \in \mathbb{N}$ beweisen will, muss man das ohne Pünktchen schreiben. Das geht z.B. wieder mit dem Rekursionssatz. (Es ist aber technisch etwas aufwändig zu zeigen, dass das g aus dem Rekursionssatz dann wirklich eine Funktion ist.)

  Einfache Alternative: $\mathbb{R}^n$ = Fkt von $\{1, \ldots, n\}$ nach $\mathbb{R}$.
- Eine Zahlenfolge $(a_n)_{n\in\mathbb{N}}$ (z.B. mit $a_n \in \mathbb{R}$) kann man kodieren als eine Funktion $a\colon \mathbb{N} \to \mathbb{R}$ (mit $a(n) = a_n$).

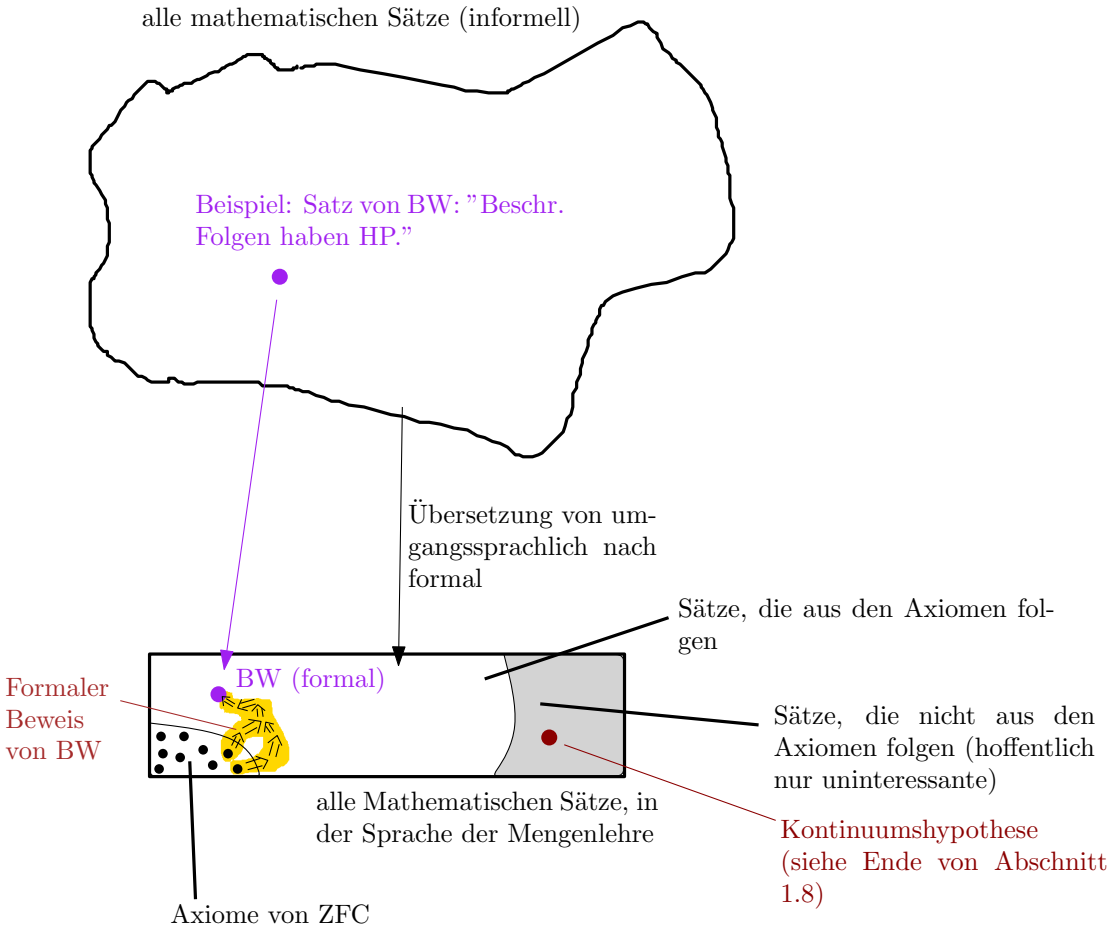
Und nochmal ein „echtes Beispiel aus der Analysis“: Der Satz von Bolzano-Weierstrass: Jede beschränkte Folge hat einen Häufungspunkt.
Wie man diesen Satz komplett in die Sprache der Mengenlehre übersetzen würde:

- Mathematischere Formulierung: „$\forall (a_i)_i : (a_i)_i$ ist beschränkte Folge von reellen Zahlen $\Rightarrow \exists b : b$ ist Häufungspunkt von $(a_i)_i$“
- Definition von beschränkter Folge einsetzen: $\exists N \in \mathbb{N} : \forall i \in \mathbb{N} : |a_i| \leq N$.
- Definition von Häufungspunkt einsetzen (siehe Ana I)
- Kodiere die Zahlenfolge $(a_i)_i$ durch eine Funktion $a\colon \mathbb{N} \to \mathbb{R}$. Also: „$\forall a\colon \mathbb{N} \to \mathbb{R} : ((\exists N \in \mathbb{N} : \forall i \in \mathbb{N} : |a(i)| \leq N) \Rightarrow \dots)$“
- Definition von $\mathbb{R}$ einsetzen; das geht auf verschiedene Arten. Zum Beispiel: Führe eine Variable R für $\mathbb{R}$ ein und schreibe dazu, dass R die Definition von $\mathbb{R}$ erfüllt: (Dann muss man nicht für jedes auftauchende $\mathbb{R}$ separat die Def. von $\mathbb{R}$ einsetzen.)

  $\exists R : (R = \{r \in \mathcal{P}(\mathbb{Q}) \mid \dots\}/\sim \quad \wedge \quad \forall a\colon \mathbb{N} \to R : \dots)$

  Statt $\exists R$ kann man auch $\forall R$ schreiben, da R sowieso eindeutig definiert wird.
- Entsprechend: Def. von $\mathbb{Q}$, von $\mathbb{Z}$, von $\mathbb{N}$ einsetzen.
- Ersetze $|a(i)| \leq N$ durch $a(i) \leq N \wedge a(i) \geq -N$. Setze die Def. von $-N$ ein (nämlich $(0, N) \in \mathbb{Z}$).
  Setze die Def. von $\leq$ ein. Dazu müssen aber vorher N und $-N$ als reelle Zahlen interpretiert werden.
  etc.
- noch viel mehr etc.

Zusammenfassung des bisherigen Vorlesungs-Inhalts:



Das wichtigste, was man gelernt haben sollte: Man sollte – zumindest theoretisch – in der Lage sein:

1. einen beliebigen mathematischen Satz komplett in der Sprache der Mengenlehre zu formulieren.
2. zu einem Beweis so viele Details hinzuzufügen, bis jeder Schritt auf den Axiomen beruht.

Natürlich wäre sowohl 1. als auch 2. viel zu aufwändig, um es komplett durchzuführen.

1.7 Das Auswahlaxiom und Zorns Lemma

Erinnerung: (AC) Ist a eine Menge von nicht-leeren, paarweise disjunkten Mengen, so gibt es eine Menge b, so dass für jedes $x \in a$ der Schnitt $x \cap b$ genau ein Element enthält.

Bisher haben wir es noch kaum gebraucht. Hier ein paar Dinge, wo es benötigt wird.

prop.inj-surj

Proposition 1.33 *Seien a, b nicht-leere Mengen und $f\colon a \to b$. Dann gilt:*

1. *f ist injektiv gdw. ex. $g\colon b \to a$ mit $g \circ f = \mathrm{id}_a$.*
2. *f ist surjektiv gdw. ex. $g\colon b \to a$ mit $f \circ g = \mathrm{id}_b$.*

Bew: „$\Leftarrow$“ ist jeweils leicht.

1. „$\Rightarrow$“: Wähle irgend ein $x_0 \in a$ und setze $g(y) := x$ falls $y = f(x)$ und $g(y) := x_0$ falls $y \notin \operatorname{im} f$.

Zur Sicherheit überlegen wir uns nochmal, ob die Klasse, die dieses g codiert, wirklich eine Menge ist. In der Tat ist

$$\{(y, x) \in b \times a \mid y = f(x) \vee (y \notin \operatorname{im} f \wedge x = z)\}$$

eine Menge nach (AUSS).

2. „$\Rightarrow$“: Idee: Wähle für jedes $y \in b$ irgend ein Urbild $x_y \in f^{-1}(y)$ und setze $g(y) := x_y$. Die Schwierigkeit besteht darin zu zeigen, dass die Klasse, die g codiert, eine Menge ist:

$$\{(y, x) \in b \times a \mid x = \text{ ein (fest gewähltes) Element mit } f(x) = y\}???$$

„Aus jeder der Mengen $f^{-1}(y)$ ein Element auswählen“ lässt sich nicht als Formel ausdrücken. Das Auswahlaxiom erlaubt uns aber, Wahlen zu treffen: Wende (AC) auf $a' := \{f^{-1}(y) \mid y \in b\}$ an. Jede Menge $f^{-1}(y)$ ist nicht-leer (da f surjektiv), also gibt es eine Menge b', so dass $f^{-1}(y) \cap b'$ aus genau einem Element besteht. Jetzt können wir schreiben:

$$\{(y, x) \in b \times a \mid f^{-1}(y) \cap b' = \{x\}\}.$$

□

Definition 1.34 *Sei $(A_i)_{i\in I}$ eine Familie von Mengen. (Also formal: I Menge, und $a\colon I \to Z$ mit $A(i) = A_i$ für eine geeignete Menge von Mengen Z). Dann definieren wir das* ***kartesische Produkt***

$$\prod_{i\in I} A_i$$

als die Menge der Folgen $(a_i)_{i\in I}$ mit $a_i \in A_i$. (Formal: $a_i = a(i)$ für eine Funktion $a\colon I \to \bigcup_{i\in I} A_i \ldots$)

Beispiel: Falls $I = \{1, 2\}$ Habe $\prod_{i\in I} A_i$ „=“ $A_1 \times A_2$. (Diese Mengen sind formal nicht gleich, aber es gibt eine „kanonische“ Bijektion...)

Proposition 1.35 *Sei $(A_i)_{i\in I}$ eine Familie von Mengen. Ist $A_i \neq \emptyset$ für alle $i \in I$, so ist auch $\prod_{i\in I} A_i \neq \emptyset$.*

Bew: Die Idee ist wieder: Wähle für jedes i irgend ein $a_i \in A_i \ldots$
Formal wieder mit (AC): Erst mal machen wir alle A_i künstlich disjunkt: $A_i' := \{i\} \times A_i$. Wende das Auswahlaxiom auf $\{A_i' \mid i \in I\}$ an. (Prüfe, dass das eine Menge ist.) Erhalte eine Menge b, so dass $A_i' \cap b$ für jedes i genau ein Element enthält. Diese Elemente haben die Form (i, a_i) mit $a_i \in A_i$... □

So eine Funktion $a\colon I \to \bigcup_{i\in I} A_i$ mit $a(i) \in A_i$ heißt auch **Auswahlfunktion**. (Sie wählt aus jeder Menge A_i ein Element aus.)

Bem: Auf ähnliche Art kann man auch zeigen, dass $\prod_{i\in I} A_i$ „groß“ ist (z.B. mindestens so viele Elemente enthält wie jedes einzelne A_i).

In der LA I Vorlesung wurde bisher nur behauptet (aber nicht bewiesen):

satz.basis **Satz 1.36** *Jeder Vektorraum hat eine Basis.*

Das holen wir jetzt nach.

Im Folgenden sei V immer ein Vektorraum über einem Körper K.

Sei $S \subseteq V$. Erinnerung:

- S heißt **linear unabhängig**, falls für alle $v_1, \ldots, v_n \in S$ mit $v_i \neq v_j$ und alle $\lambda_1, \ldots, \lambda_n \in K$ gilt:

$$\sum_i \lambda_i v_i = 0 \Rightarrow \lambda_1 = \cdots = \lambda_n = 0.$$

- S ist eine **Basis** von V wenn S eine maximale linear unabhängige Teilmenge von V ist (d.h. S ist lin.unabh aber jede Obermenge von S ist lin.abh.)

(Die Def. aus LA I waren ein bisschen anders, aber man kann zeigen, dass das äquivalent ist.)

satz.basis

Unvollständige Beweis-Idee von 1.36: Fange mit irgend einer linear unabhängigen Menge S an (z.B. $S = \emptyset$) und mache sie so lange größer, bis sie eine Basis ist. Genauer: Wenn S maximal ist, sind wir fertig. Ansonsten ersetzen wir S durch irgend eine linear unabhängige Obermenge. Das machen wir so lange, bis S maximal ist.

Aber wie machen wir das formal? Ein Versuch per Induktion: Wir fangen mit S_0 an und konstruieren daraus S_1, S_2, ... durch Hinzufügen von Elementen. Wenn eine der Mengen S_i maximal ist, sind wir fertig. Ansonsten setze $S'_0 := \bigcup_{i\in\mathbb{N}} S_i$. Man kann leicht zeigen: S'_0 ist wieder linear unabhängig. Wenn S'_0 maximal ist, sind wir fertig; wenn nicht, machen wir wieder weiter: $S'_0 \subsetneq S'_1 \subsetneq \ldots$. Wenn wir wieder nicht fertig werden, erhalten wir $S''_0 := \bigcup_{i\in\mathbb{N}} S'_i$. Und dann S'''_0, S''''_0, ... Dann bilde die Vereinigung über all diese Mengen. etc. etc.

Das Problem dabei ist: Es ist nicht klar, dass wir so je fertig werden. Um so eine „unendlich verschachtelte Induktion“ zu machen, braucht man das Zornsche Lemma.

12.6.2013

Definition 1.37 *Eine **Halbordnung** auf einer Menge a ist eine Relation $\leq$ auf a, die reflexiv, transitiv und antisymmetrisch ist (also wie Ordnung, aber ohne die Bedingung, dass beliebige Elemente vergleichbar sind).*

Notation: $x < y :\iff x \leq y \wedge x \neq y$. (Bei Halbordnungen ist das nicht *äquivalent zu $x \not\geq y$.)*

*Ein **Maximum** einer Halbordnung a ist ein Element $m \in a$, so dass es kein $x \in a$ gibt mit $x > a$. (**Minimum** entsprechend.)*

*Eine Teilmenge $b \subseteq a$ heißt **Kette**, wenn b durch $\leq$ total geordnet wird, d.h. wenn die Einschränkung von $\leq$ auf b eine Ordnungsrelation ist (d.h. je zwei Elem. von b vergleichbar sind).*

Beispiel: [Bild: endlicher Graph... mit mehreren Maxima.]

Beispiel: Sei a eine Menge von Mengen, und $x \leq y :\iff x \subseteq y$ für $x, y \in a$.

Satz 1.38 *(**Zorns Lemma**) Sei $\leq$ eine Halbordnung auf a, so dass folgendes gilt: Für jede Kette $b \subseteq a$ existiert ein $x \in a$ mit $x \geq y$ für alle $y \in b$. Dann hat a ein Maximum.*

Beweis von satz.basis 1.36 mit dem Zornschen Lemma: Was wir suchen ist eine maximale (bzgl. $\subseteq$) linear unabhängige Teilmenge von V. Sei also a die Menge der lin.unah. TM von V, mit der durch $\subseteq$ gegebenen Halbordnung. Das Zornsche Lemma sagt, dass es ein Maximum gibt... wenn wir die Bedingung mit den Ketten zeigen.

Also zu zeigen: Ist b eine total geordnete Menge von lin. unabh. TM von V, so gibt es eine lin. unabh. TM $S \subseteq V$ mit $S' \subseteq S$ für alle $S \in b$. Wir wählen einfach $S := \bigcup_{S' \in b} S'$. Dann ist klar, dass $S \supseteq S'$ ist für alle $S' \in b$, und wir müssen nur zeigen, dass S lin. unabh. ist.

Seien also $v_1, \ldots, v_n \in S$ und $\lambda_1, \ldots, \lambda_n \in K$ gegeben mit $\sum \lambda_i v_i = 0$. Nach Def. von S ist $v_i \in S_i$ für ein $S_i \in b$. Da b total geordnet ist, ist nach Umnummerierung oBdA $S_1 \subseteq \ldots \subseteq S_n$, also insbesondere $v_1, \ldots, v_n \in S_n$. Da S_n lin.unabh. folgt aus $\sum \lambda_i v_i = 0$, dass alle $\lambda_i = 0$ sind, was zu zeigen war. □

Bem: Die meisten Anwendungen des Zornschen Lemmas gehen so oder so ähnlich: a ist eine Menge von Mengen, die Halbordnung ist $\subseteq$, und um zu einer Kette b ein $x \in a$ zu finden mit $x \supseteq y$ für alle $y \in b$, wähle einfach $x := \bigcup_{y \in b} y$. (Zu zeigen ist dann nur, dass ein solches x auch wieder in a liegt.)

Beweis des Zornschen Lemmas:

Beweis-Plan:

1. Wir zeigen, dass es ausreicht, den Fall wie im Beweis von satz.basis 1.36 zu behandeln; insbes. ist a eine Menge von Mengen und $\leq$ ist die Mengen-Inklusion.
2. Die Idee ist die, die bei satz.basis 1.36 erwähnt wurde. Um aus einer Menge S_i die Menge S_{i+1} zu konstruieren, verwenden wir (AC) (um das neue Element zu wählen).
3. Jetzt brauchen wir eine Möglichkeit, formal die Menger aller Mengen S_i, S_i', etc. zu definieren, die in unserer Konstruktion auftauchen (egal wie lang und verschachtelt die Induktion ist). Idee dazu: Wir definieren einen *Turm* als eine Menge von Mengen, die enthält und die abgeschlossen ist unter $S_i \mapsto S_{i+1}$ und unter Vereinigung von Ketten. Dann ist der Schnitt aller Türme genau das, was wir suchen. (Das zu zeigen ist aber noch etwas Arbeit.)

Teil 1:

Wir wollen uns auf die folgende Situation reduzieren:

1. a ist eine Menge von Mengen.
2. $x \leq y \iff x \subseteq y$ für $x, y \in a$.
3. Ist $x \in a$, so ist auch jede Teilmenge von x in a.
4. Ist $b \subseteq a$ eine Kette, so ist auch $\bigcup_{x \in b} x \in a$.

Um den allgemeinen Fall darauf zu reduzieren, sei $a' :=$ die Menge der Ketten in a (bzgl. $\leq$). (Auf a' verwenden wir dann $\subseteq$ als Halbordnung.) Dann sind 1., 2., 3. klar, und 4. ist auch leicht zu prüfen: Ist $b' \subseteq a'$ eine $\subseteq$-Kette, so ist zu zeigen, dass $y' := \bigcup_{x' \in b'} x'$ in a' liegt, also eine $\leq$-Kette in a ist. Also zu zeigen: je zwei Elemente von y' sind vergleichbar bzgl. $\leq$. Seien also $y_1, y_2 \in y'$, d.h. $y_1 \in x_1'$, $y_2 \in x_2'$ mit $x_1', x_2' \in b'$. Da b' $\subseteq$-Kette ist oBdA $x_1' \subseteq x_2'$, also insbes $y_1 \in x_2'$. Da x_2' eine $\leq$-Kette ist, sind y_1, y_2 vergleichbar.

Wenn wir das Zornsche Lemma für a' bewiesen haben, wissen wir, dass es $m \in a'$ gibt, das bezüglich $\subseteq$ maximal ist. (m ist also eine $\leq$-Kette in a.) Nach Voraussetzung für a gibt es ein $x \in a$ mit $x \geq y$ für alle $y \in m$. Behauptung: y ist Maximum von a. Wenn nicht, d.h. wenn es $z > y$ gäbe, dann wäre $m \cup \{z\}$ eine Kette, die der Maximalität von m widerspricht.

Teil 2:

Für jede Menge $x \in a$, die nicht maximal ist, wollen wir ein Element z wählen mit $n(x) := x \cup \{u\} \in a$ („n“ = „Nachfolger“). Benutze dazu (AC), bzw. genauer: die Existenz von Auswahlfunktionen:

Setze $V := \bigcup_{x \in a} x$ und wähle eine Auswahlfunktion f auf $\mathcal{P}(V) \setminus \emptyset$: Für jedes $x \subseteq V, x \neq \emptyset$ ist $f(x) \in x$.
Definiere damit, für $x \in a$ nicht maximal, $n(x) := f(\{u \in V \mid x \cup \{u\} \in a\})$. Wir müssen prüfen, dass $\{u \in V \mid x \cup \{u\} \in a\}$ nicht leer ist. In der Tat: Da x nicht maximal ist, gibt es $y \supsetneq x$, $y \in a$. Wähle irgend ein $u \in y$. Nach 3. ist auch $x \cup \{u\} \in a$.

Falls $x \in a$ maximal ist, definieren wir $n(x) := x$.

Teil 3:

Ein *Turm* ist eine Teilmenge $t \subseteq a$ mit folgenden Eigenschaften:
(a) $\emptyset \in t$.

(b) Falls $x \in t$, dann auch $n(x) \in t$.
(c) Falls $b \subseteq t$ eine Kette ist, dann ist auch $\bigcup_{x \in b} x \in t$.

Erste Feststellung: a selbst ist ein Turm. Insbesondere gibt es Türme, und es macht Sinn zu definieren: $t_0 :=$ der Schnitt aller Türme.

Man sieht leicht: Der Schnitt von Türmen ist wieder ein Turm; insbesondere ist t_0 ein Turm.

Wir werden zeigen, dass t_0 eine Kette ist. Daraus folgt:
(c) $\Rightarrow m := \bigcup_{y \in t_0} y \in t_0$
(b) $\Rightarrow n(m) \in t_0$
Also ist m Maximum von a (sonst wäre $n(m)$ echt größer als m).

Sei $s = \{x \in t_0 \mid \forall y \in t_0 : (x \subseteq y \wedge y \subseteq x)\}$ die Teilmenge der Elemente von t_0, die mit allen anderen Elementen verleichbar sind. Zu zeigen ist $s = t_0$. Dazu reicht es zu zeigen, dass s auch ein Turm ist. 19.6.2013

(a) für s: Klar.

(c) für s:
Sei also $b \subseteq s$ eine Kette und $m := \bigcup_{x \in b} x$. Zu zeigen ist, dass jedes $y \in t_0$ mit m vergleichbar ist. Falls es ein $x \in b$ gibt mit $y \subseteq x$, dann ist $y \subseteq m$. Ansonsten ist $y \supseteq x$ für alle $x \in b$, und damit auch $y \supseteq m$.

(b) für s:
Zu zeigen ist: Falls jedes Element von t_0 mit x vergleichbar ist, dann ist auch jedes Element von t_0 mit $n(x)$ vergleichbar.
Definiere $t_1 := \{y \in a \mid y \supseteq n(x)\} \cup \{y \in t_0 \mid y \subseteq x\}$. Jedes Element von t_1 ist mit $n(x)$ vergleichbar, d.h. es reicht zu zeigen, dass t_1 ein Turm ist (da daraus folgt: $t_0 \subseteq t_1$).

(a) für t_1: Klar.

(b) für t_1: Z.z: $y \in t_1 \Rightarrow n(y) \in t_1$
1. Fall: $y \supseteq n(x)$: Dann ist auch $n(y) \supseteq n(x)$.
2. Fall: $y \in t_0, y \subseteq x$: Der Fall $y = x$ ist ok (da $n(x) \in t_1$); sei also $y \subsetneq x$. Aus $y \in t_0$ folgt $n(y) \in t_0$. Nach Annahme sind $n(y)$ und x vergleichbar. $n(y)$ kann keine echte Obermenge von x sein, also $n(y) \subseteq x$.

(c) für t_1: Sei $b \subseteq t_1$ eine Kette.
1. Fall: In b kommt eine Obermenge von $n(x)$ vor. Dann ist die Vereinigung auch eine Obermenge von $n(x)$.
2. Fall: Jedes Element von b ist eine Teilmenge von x, die in t_0 liegt. Dann

gilt dies auch für die Vereinigung über b.

Jetzt sind wir mit dem Beweis fertig: t_1 ist Turm, also ist $t_0 \subseteq t_1$, also ist jedes Element von t_0 mit $n(x)$ vergleichbar. Damit ist der Beweis fertig, dass s ein Turm ist, also $t_0 \subseteq s$, also ist jedes Element von t_0 mit jedem Element von t_0 vergleichbar, d.h. t_0 ist eine Kette, d.h. die Vereinigung aller Mengen in t_0 ist ein Element von a, und das ist dann auch ein Maximum von a. $\square$

sect.kard

1.8 Kardinalitäten

Frage: Wie kann man formal ausdrücken, wie groß eine Menge ist?
Antwort: Eine Menge a hat n Elemente $\iff$ Es gibt eine Bijektion zwischen a und $\{1, \ldots, n\}$.

Notation: $|a| = n$.

Allgemeiner:

Definition 1.39 *Seien a, b Mengen.*

1. *Schreibe $|a| = |b|$, falls es eine Bijektion $a \to b$ gibt. In diesem Fall heißen a und b **gleichmächtig**. (Schreibe $|a| \neq |b|$ falls dies nicht der Fall ist.)*
2. *Schreibe $|a| \leq |b|$, falls es eine Injektion $a \to b$ gibt. („b ist mindestens so mächtig wie a“)*
3. *Schreibe $|a| < |b|$ falls $|a| \leq |b| \wedge |a| \neq |b|$, etc.*

$|a|$ nennt man die **Kardinalität** oder **Mächtigkeit** von a. Wenn a nicht endlich ist, haben wir gar nicht definiert, was $|a|$ sein soll. Das kommt in weiterführenden Logik- (oder Mengenlehre-) Vorlesungen dran. (Dort wird dann $|a|$ durch eine geeignete Menge m kodiert, für die es eine Bijektion $a \to m$ gibt.) In dieser Vorlesung verwenden wir $|a|$ nur als Notation.

Es ist nicht schwer zu zeigen: $|a| \leq |b|$ gdw. es eine Surjektion $b \to a$ gibt (Übung).

Jetzt stellen sich einige Fragen:

1. Gilt $a \subseteq b \Rightarrow |a| \leq |b| \rightsquigarrow$ Ja
2. Gilt $a \subsetneq b \Rightarrow |a| < |b| \rightsquigarrow$ Nein

3. Gibt es unendliche Mengen a, b mit $|a| \neq |b|$? $\rightsquigarrow$ Ja
4. Folgt aus $|a| \leq |b|$ und $|b| \leq |c|$ auch $|a| \leq |c|$? $\rightsquigarrow$ Ja
5. Aus $|a| = |b|$ folgt $|a| \leq |b|$ und $|b| \leq |a|$; aber folgt aus $|a| \leq |b|$ und $|b| \leq |a|$ auch $|a| = |b|$? $\rightsquigarrow$ Ja (Satz satz.CB 1.43)
6. Gibt es Mengen a, b so dass weder $|a| \leq |b|$ noch $|b| \leq |a|$ gilt? $\rightsquigarrow$ Nein (Satz satz.kard-ord 1.44)

Zu 1.: Leicht.

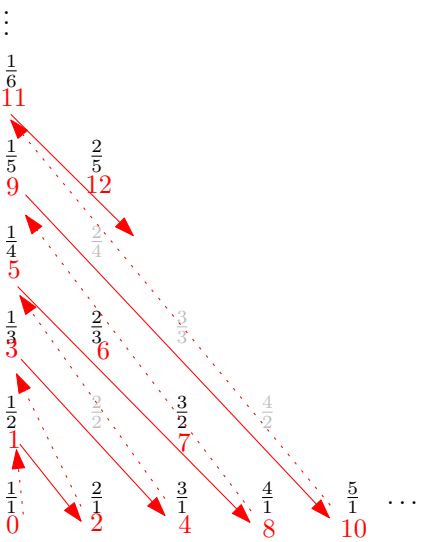
Zu 2.: Beispiel: $b = \mathbb{N}$, $a = \mathbb{N} \setminus \{0\}$. Bijektion $a \to b$, $n \mapsto n + 1$.

Zu 4: Leicht.

Zu 3.:
Erster Versuch: $a = \mathbb{N}$, $b = \mathbb{Z}$.... Habe Bijektion $a \to b$, $2n \mapsto n$, $2n + 1 \mapsto -n - 1$. Also $|\mathbb{N}| = |\mathbb{Z}|$.

Nächster Versuch: $a = \mathbb{N}$, $b = \mathbb{Q}$:
Ich behaupte: Es gilt auch $|\mathbb{Q}| = |\mathbb{N}|$.

Das folgende Bild beschreibt eine Bijektion zwischen den positiven rationalen Zahlen und $\mathbb{N}$: Schreibe alle Brüche wie angegeben auf; radiere alle ungekürzten Brüche wieder weg. Nummeriere die restlichen „diagonalenweise“ durch (in rot). (Die Bijektion ist dann: bilde jeden Bruch auf seine rote Nummer ab.)



Um auch 0 und die negativen rationalen Zahlen zu erhalten, wende Methoden wie bei „zu 2.“ und $|\mathbb{N}| = |\mathbb{Z}|$ an.

Trotzdem ist die Antwort auf Frage 3 ja:

Proposition 1.40 *Für jede Menge a gilt: $|\mathcal{P}(a)| > |a|$. Insbesondere ist $|\mathcal{P}(\mathbb{N})| > |\mathbb{N}|$.*

Bew: Dass $|a| \leq |\mathcal{P}(a)|$ ist, ist leicht: Wähle als Injektion $a \to \mathcal{P}(a), x \mapsto \{x\}$.

Annahme, es gäbe eine Bijektion $f\colon a \to \mathcal{P}(a)$. Definiere $b \subseteq a$ wie folgt: $x \in b \iff x \notin f(x)$. Behauptung: $b \notin \operatorname{im} f$. Annahme: $b = f(y)$. Dann ist $y \in b \iff y \notin f(y) = b$. Widerspruch. □

Notation 1.41 *Wir setzen $\aleph_0 := |\mathbb{N}|$ und $2^{\aleph_0} := |\mathcal{P}(\mathbb{N})|$. (Das Zeichen $\aleph$ ist ein Aleph; hebräischer Buchstabe.) Mengen mit $|a| = \aleph_0$ heißen **abzählbar**, Mengen mit $|a| > \aleph_0$ heißen **überabzählbar**.*

Proposition 1.42 *$|\mathbb{Z}| = |\mathbb{Q}| = \aleph_0$; $|\mathbb{R}| = 2^{\aleph_0}$.*

Bew: Das erste haben wir bereits gezeigt. Was $\mathbb{R}$ angeht: Wir verwenden Satz satz.CB 1.43.

$|\mathbb{R}| \leq |\mathcal{P}(\mathbb{N})|$: Da $|\mathbb{N}| = |\mathbb{Q}|$ gilt $|\mathcal{P}(\mathbb{N})| = |\mathcal{P}(\mathbb{Q})|$ (Übung); es reicht also, eine Injektion $\mathbb{R} \to \mathcal{P}(\mathbb{Q})$ anzugeben. Eine mögliche Injektion ist $r \mapsto \{q \in \mathbb{Q} \mid q \leq r\}$.

$|\mathbb{R}| \geq |\mathcal{P}(\mathbb{N})|$: Bilde die Teilmenge $a \subseteq \mathbb{N}$ ab auf die reelle Zahl mit Dezimalschreibweise $0, x_0x_1x_2\ldots$ ab, wobei $x_i = 1$ falls $i \in a$ und $x_i = 0$ falls $i \notin a$. □

satz.CB **Satz 1.43** *(Cantor-Bernstein-Schröder) Sind a und b zwei Mengen mit $|a| \leq |b|$ und $|b| \leq |a|$, so ist $|a| = |b|$.*

Bew: (Bild)

Seien $f\colon a \to b$ und $g\colon b \to a$ die Injektionen.

Seien $c_0 := b \setminus \operatorname{im} f$, $d_i := g(c_i)$, $c_{i+1} := f(d_i)$
und $c := \bigcup_{i\in\mathbb{N}} c_i$ und $d := \bigcup_{i\in\mathbb{N}} d_i$.

Definiere $h\colon a \to b$ durch

$$h(x) := \begin{cases} f(x) & \text{falls } x \notin d \\ g^{-1}(x) & \text{falls } x \in d \end{cases}$$

Behauptung: h ist eine Bijektion. In der Tat prüft man leicht, dass h Bijektionen definiert von $a \setminus d$ nach $b \setminus c$ und von d_i nach c_i für jedes i. □

26.6.2013

satz.kard-ord **Satz 1.44** *Sind a und b zwei Mengen, so gilt $|a| \leq |b|$ oder $|b| \leq |a|$.*

Beweis: Gesucht ist eine Bijektion $f\colon a' \to b'$ für Teilmengen $a' \subseteq a$, $b' \subseteq b$, wobei entweder $a' = a$ ist (dann habe eine Injektion $a \to b$) oder $b' = b$ (dann habe eine Injektion $b \to a$).

Idee dafür: Wir fangen mit leeren a', b' an und vergrößern sie Stück für Stück: Wenn wir schon $f\colon a' \to b'$ haben aber weder $a' = a$ noch $b' = b$, können wir $x \in a \setminus a'$ wählen und $y \in b \setminus b'$ und f fortsetzen zu $a' \cup \{x\} \to b' \cup \{y\}$, indem wir $f(x) := y$ setzen.

Um das formal zu machen, wenden wir Zorns Lemma an auf die Menge m der Bijektionen $f\colon a' \to b'$ von einer Teilmenge $a' \subseteq a$ zu einer Teilmenge $b' \subseteq b$. Darauf definieren wir eine Halbordnung durch: $f_1 \leq f_2 \iff \operatorname{dom}(f_1) \subseteq \operatorname{dom}(f_2) \wedge \forall x \in \operatorname{dom}(f_1) : f_1(x) = f_2(x)$.

Erste Feststellung: Ist $f\colon a' \to b'$ ein maximales Element bzgl. $\leq$, dann muss schon $a' = a$ oder $b' = b$ sein, da man sonst f wie oben beschrieben fortsetzen könnte. Also: Wenn wir Zorns Lemma anwenden können, sind wir in der Tat fertig mit dem Beweis.

Bleibt also zu zeigen: Ist k eine Kette, so gibt es ein f_0 so dass für alle $f \in k$ gilt: $f_0 \geq f$. Idee: Setze $\operatorname{dom}(f_0) := \bigcup_{f \in k} \operatorname{dom} f$, und für $x \in \operatorname{dom}(f_0)$ wähle irgend ein $f \in k$ mit $x \in \operatorname{dom} f$ und setze $f_0(x) := f(x)$. Dieses $f_0(x)$ hängt nicht von der Wahl von f ab, da für $f, f' \in k$ auf dem Schnitt ihrer Definitionsbereiche übereinstimmen. Dass $f_0 \geq f$ ist (für jedes $f \in k$), ist dann klar.

Bleibt zu zeigen, dass f_0 eine Bijektion (von $\operatorname{dom} f_0$ nach $\operatorname{im} f_0$) ist, d.h. dass für $x, x' \in \operatorname{dom} f_0$ gilt: $f_0(x) \neq f_0(x')$. In der Tat ist $x \in \operatorname{dom} f$ und $x' \in \operatorname{dom} f'$ für geeignete $f, f' \in k$. Da k total geordnet, ist oBdA $f \leq f'$, also insbesondere auch $x \in \operatorname{dom} f'$. Also $f_0(x) = f'(x) \neq f'(x') = f_0(x')$. □

Ausblick:

prop.card-arith

Proposition 1.45 *Sind a, b unendliche Mengen, so ist $|a \cup b| = |a \times b| = \max\{|a|, |b|\}$.*

Falls a, b abzählbar: Beweis ähnlich wie $|\mathbb{N}| = |\mathbb{Z}| = |\mathbb{Q}|$. Für beliebige Mengen: aufwändiger; siehe Mengenlehre-Vorlesung.

Proposition 1.46 *$\aleph_0$ ist die kleinste unendliche Kardinalität, d.h. man kann zeigen (nicht sehr schwer): a unendlich $\iff |a| \geq \aleph_0$.*

Beweis-Idee: Ist a unendlich, so gibt es für jedes n eine Injektion $\{1, \ldots, n\} \hookrightarrow a$. Diese kann man (mit etwas basteln und dem Auswahlaxiom) zusammensetzen zu einer Injektion $\mathbb{N} \hookrightarrow a$.

Die nächst-größeren unendlichen Kardinalitäten werden mit $\aleph_1, \aleph_2, \ldots$ bezeichnet. Tatsächlich kann man zeigen, dass „nächst-größere“ Kardinalitäten existieren: Ist a eine Menge, so gibt es eine Menge b mit $|b| > |a|$, so dass es keine Menge c gibt mit $|a| < |c| < |b|$. (Es gibt aber auch noch größere Kardinalitäten als alle $\aleph_n$ ...)

Eine natürliche Frage ist: Ist $2^{\aleph_0} = \aleph_1$? (Das ist die **Kontinuumshypothese**.)

Es stellt sich heraus: Weder die Kontinuumshypothese noch ihr Gegenteil lassen sich aus den Axiomen von ZFC beweisen!

2 Der Gödelsche Volständigkeitssatz

Wir haben die Axiome von ZFC eingeführt und gesehen, wie daraus die komplette Mathematik ableiten kann. (Naja, fast...) Dabei haben wir logische Schlussfolgerungen trotzdem noch intuitiv gemacht.

Behauptung: Auch die logischen Schlussfolgerungen kann man präzise axiomatisch formulieren.

Genauer: Der **Hilbertkalkül** ist eine Liste von Axiomen und eine (einzige) Ableitungsregel. Es gilt:

satz.hvi

Informeller Satz 2.1 *(Gödelscher Vollständigkeitssatz) Ist T eine Menge von Aussagen (in der Sprache der Mengenlehre) und ist ϕ eine Aussage, die*

„aus rein logischen Gründen“ aus den Aussagen von T folgt, so lässt sich ϕ mit dem Hilbertkalkül herleiten.

Die Ableitungsregel vom Hilbertkalkül ist übrigens der **Modus Ponens**: „Sind ϕ und $\phi \Rightarrow \psi$ wahre Aussagen, so ist auch ψ eine wahre Aussage.“

satz.hvi

Um Satz 2.1 präzise zu formulieren, ist etwas Vorarbeit notwendig. Insbesondere müssen wir definieren, was es heißt, aus rein logischen Gründen zu folgen. (Außerdem müssen wir uns überlegen, wie es überhaupt möglich ist, Aussagen über Aussagen zu beweisen.)

Wir werden den Vollständigkeitssatz in einem allgemeineren Kontext betrachten, weil er dann auch andere, ganz praktische Anwendungen hat.

2.1 Sprachen und Strukturen

Gruppen, Ringe, Körper, Vektorräume, etc. sind alles Mengen zusammen mit irgend welchen Funktionen darauf (und evtl. auch Relationen). Eine „Struktur“ soll was sein, was alles unter einen Hut bringt. Die verschiedenen Arten von Strukturen haben verschieden viele (und verschiedenartige) Funktionen. Die Liste der Symbole für diese Funktionen nennt man „Sprache“.

defn.spst

Definition 2.2 *Eine **Sprache** L besteht aus **Funktionssymbolen**, **Relationssymbolen** und **Konstantensymbolen**. Jedem Funktionssymbol f und jedem Relationssymbol R ist eine **Stelligkeit** $st(f), st(R) \in \mathbb{N}_{\geq 1}$ zugeordnet. (Ist $st(f) = m$, so sagt man, f ist ein Symbol für eine m-stellige Funktion. Entsprechend für R.)*

Beispiel: Die **Gruppensprache** ist $L_{Grp} = \{\circ, ^{-1}, e\}$. Hierbei ist $\circ$ ein zweistelliges Funktionssymbol, $^{-1}$ ein einstelliges Funktionssymbol und e ein Konstantensymbol.

Definition 2.3 *Ist L eine Sprache, so ist eine L-**Struktur** eine Menge M zusammen mit:*

- *für jedes Funktionssymbol f eine Funktion $f^M \colon \underbrace{M \times \cdots \times M}_{st(f)} \to M$;*

- *für jedes Relationssymbol R eine Teilmenge $R^M \subseteq \underbrace{M \times \cdots \times M}_{st(R)}$;*
- *für jedes Konstantensymbol c ein Element $c^M \in M$.*

Beispiel: Ist G eine Gruppe, so ist G (auf natürliche Weise) eine L_{Grp}-Struktur:
$\circ^G : G \times G \to G$ ist die Verknüpfung, $({}^{-1})^G : G \to G$ ist die Inversenabbildung und $e^G \in G$ ist das neutrale Element.

Anmerkung: ${}^{-1}$ und e sind in der Gruppensprache nicht so wichtig, da in einer Gruppe das Inverse und das neutrale Element durch die Verknüpfung sowieso eindeutig bestimmt sind. Trotzdem ist es üblich, Symbole dafür in die Sprache zu tun.

Noch eine Anmerkung: Statt $\circ^G$, $({}^{-1})^G$ und e^G schreibt man meistens nur $\circ$, ${}^{-1}$, e.

Und noch eine Anmerkung: Nicht jede Struktur L_{Grp}-Struktur ist eine Gruppe. Dass etwas eine L_{Grp}-Struktur ist, besagt schließlich noch nichts darüber, ob die Gruppenaxiome gelten. (In sofern ist das Konzept einer L_{Grp}-Struktur bisher nur mäßig nützlich. Aber das werden wir später noch verbessern.)

Beispiel: Die **Ringsprache** ist $L_{Ring} = \{+, -, \cdot, 0, 1\}$. Hierbei sind $+$, $-$, $\cdot$ zweistellige Funktionssymbole und 0,1 sind Konstantensymbole. Wie bei den Gruppen ist jeder Ring auf natürliche Weise eine L_{Ring}-Struktur.

Beispiel: Wenn man einen Körper K als Struktur auffassen will, hat man einen Problem mit der Division, da $\frac{a}{0}$ nicht definiert ist (aber jedes zweistellige Funktionssymbol einer Funktion auf ganz $K \times K$ entsprechen soll). Zwei Lösungen:
1. Lösung: Nimm trotzdem $L_{Kp} = \{+, -, \cdot, /, 0, 1\}$ und definiere $a/0 = 0$ für alle $a \in K$. Natürlich wollen wir nicht wirklich, dass $a/0 = 0$ ist, aber diese Definition verwenden wir nur, damit K wirklich formal eine L_{Kp}-Struktur wird; in allen Anwendungen betrachten wir a/b dann immer nur, wenn $b \neq 0$ ist.
2. Lösung: Betrachte K einfach nur als L_{Ring}-Struktur. Da in einem Körper die Division durch die Multiplikation eindeutig festgelegt wird, ist das nicht wirklich ein Problem. (Diese 2. Lösung ist übrigens die üblichere.)

Beispiel: Die **Sprache der Ordnungen** (d.h. der angeordnete Mengen) ist $L_{Ord} = \{\leq\}$. Hierbei ist $\leq$ ein zweistelliges Relationssymbol. Ist M eine

angeordnete Menge, so ist M auf naheliegende Art eine L_{Ord}-Struktur.

Anmerkung: In Def. 1.13 hatten wir Relationen auf M als Teilmengen von $M \times M$ definiert. Im Sinne von Defn. 2.2 sind das also 2-stellige Relationen.

Beispiel: Vektorräume: Frage: Wie kann man einen K-Vektorraum V als Struktur auffassen? Dazu gibt es mehrere Möglichkeiten. Eine ist die folgende: Nimm als Grundmenge der Struktur die disjunkte Vereinigung $M := K \dot\cup V$. Als Sprache nehmen wir $\{+_{\mathrm{KP}}, -_{\mathrm{KP}}, \cdot_{\mathrm{KP}}, 0_{\mathrm{KP}}, 1_{\mathrm{KP}}, +_{\mathrm{VR}}, -_{\mathrm{VR}}, 0_{\mathrm{VR}}, \cdot_{Skal}, \mathrm{KP}, \mathrm{VR}\}$. Hierbei soll $+_{\mathrm{KP}}, -_{\mathrm{KP}}, \cdot_{\mathrm{KP}}, 0_{\mathrm{KP}}, 1_{\mathrm{KP}}$ die Ring-Sprache auf K sein, $+_{\mathrm{VR}}, -_{\mathrm{VR}}, 0_{\mathrm{VR}}$ soll die Addition, Subtraktion und das neutrale Element auf V sein und $\cdot_{Skal}$ soll die Skalarmultiplikation $K \times V \to V$ sein. Dort, wo diese Funktionen nicht definiert sind, setzen wir sie einfach auf 0 (oder so), z.B.:

$$a +^M_{\mathrm{KP}} b = \begin{cases} a + b & \text{falls } a, b \in K \\ 0 & \text{sonst.} \end{cases}$$

Zusätzlich sollten wir noch irgendwie sicherstellen, dass man in der Struktur M ablesen kann, welche Teilmenge der Körper ist und welche Teilmenge der Vektorraum. Deswegen gibt es in der Sprache noch zwei einstellige Prädikate KP, VR mit $\mathrm{KP}^M = K$, $\mathrm{VR}^M = V$.

Bisher ist der Begriff einer Struktur noch nicht sehr nützlich, da z.B. bei L_{Grp}-Strukturen nicht unterschieden wird zwischen Gruppen und Strukturen, die die Gruppenaxiome nicht erfüllen. Um das Problem zu beheben, führen wir spezielle Formeln und Aussagen ein, die über Strukturen reden. In diesen Formeln dürfen dann die Symbole aus der entsprechenden Sprache vorkommen. 3.7.2013

Beispiel: Wenn wir mit $L_{Ring} = \{+, -, \cdot, 0, 1\}$ arbeiten, ist „$\exists x : x \cdot x = y$“ eine Formel. Ist K ein Körper, so definiert diese Formel eine Eigenschaft von Elementen von K, nämlich: Ist y ein Quadrat?

Ein anderes Beispiel in L_{Ring} ist „$\exists x : x \cdot x = 1 + 1 + 1$“; dies ist eine Formel ohne freie Variablen, also eine Aussage. Ob die Aussage wahr oder falsch ist, hängt aber von der Struktur ab, in der wir sie betrachten. Wenn die Struktur ein Körper K ist, dann ist die Aussage wahr genau dann wenn $\sqrt{3}$ in K liegt.

Wenn wir solche Formeln und Aussagen eingeführt haben, können wir dann z.B. auch die Körperaxiome als Aussagen ausdrücken. Z.B.: „$\forall x\,(x \neq 0 \Rightarrow \exists y\, x \cdot y = 1)$“

defn.LTF **Definition 2.4** *Sei L eine Sprache. L-**Terme** und L-**Formeln** sind Zeichenketten bestehend aus den folgenden Zeichen.*

- *die logischen Symbole $\wedge$, $\vee$, $\Rightarrow$, $\neg$, $\forall$, $\exists$, $=$, Klammern, Komma*
- *(Symbole für) Variablen*
- *die Symbole aus L.*

Die Zeichenketten müssen nach folgenden Regeln aufgebaut sein.

1. *Jede Variable x ist ein L-Term. Jedes Konstantensymbol c in L ist ein L-Term.*
2. *1 Sind $t_1, \ldots, t_m$ L-Terme und ist f ein m-stelliges Funktionssymbol in L, so ist $f(t_1, \ldots, t_m)$ ein L-Term.*
3. *Sind t_1, t_2 L-Terme, so ist $t_1 = t_2$ eine L-Formel.*
4. *Sind $t_1, \ldots, t_m$ L-Terme und ist R ein m-stelliges Relationssymbol in L, so ist $R(t_1, \ldots, t_m)$ eine L-Formel.*
5. *Sind ψ_1 und ψ_2 Formeln, so sind $(\psi_1 \wedge \psi_2)$, $(\psi_1 \vee \psi_2)$, $(\psi_1 \Rightarrow \psi_2)$, $\neg\psi_1$ Formeln.*
6. *Ist ψ eine Formel und x eine Variable, so sind $\forall x\, \psi$, $\exists x\, \psi$ Formeln.*

Definition 2.5 *Wir definieren die **freien Variablen** von Termen und Formeln.*

1. *Im Term x (wobei x eine Variable ist) ist x die einzige freie Variable. Der Term c (wobei c ein Konstantensymbol ist) hat keine freien Variablen.*
2. *Eine Var ist frei in $f(t_1, \ldots, t_m)$ wenn sie frei in (mindestens) einem der t_i ist.*
3. *$t_1 = t_2$ entsprechend.*
4. *$R(t_1, \ldots, t_m)$ entsprechend.*
5. *$(\psi_1 \wedge \psi_2)$, $(\psi_1 \vee \psi_2)$, $(\psi_1 \Rightarrow \psi_2)$, $\neg\psi_1$ entsprechend (mit ψ_i statt t_i)*
6. *Die Variable x ist nicht frei in $\forall x\, \psi$ bzw. $\exists x\, \psi$; für alle anderen Variablen y gilt: y ist frei in $\forall x\, \psi$ bzw. $\exists x\, \psi$ genau dann, wenn y frei in ψ ist.*

Sind $x_1, \ldots, x_n$ alle freien Variablen von einem Term t oder einer Formel ϕ, so schreiben wir (wie gehabt) $t(x_1, \ldots, x_n)$ bzw. $\phi(x_1, \ldots, x_n)$. Wir erlauben in Zukunft auch, $\phi(x_1, \ldots, x_n)$ zu schreiben, wenn nur ein Teil der Variablen $x_1, \ldots, x_n$ frei in ϕ sind. (Anschaulich soll ϕ über die nicht-freien Variablen dann einfach keine Aussage machen.)

*Eine L-**Aussage** ist eine L-Formel ohne freie Variablen.*

Unser Beispiel „$\exists x : x \cdot x = 1 + 1 + 1$“ ist eine L_{Kp}-Aussage. Ganz formal gesehen müsste es

$$\underbrace{\exists x \underbrace{\underbrace{\cdot(x,x)}_{\substack{\text{Term mit}\\ \text{freier Var. } x}} = \underbrace{+(1,+(1,1))}_{\text{Term ohne freie Var}}}_{\text{Fml mit freier Var } x}}_{\text{Fml. ohne freie Var.}}$$

geschrieben werden, aber ganz so streng wollen wir nicht sein. Wir verwenden auch wieder andere Abkürzungen wie $\iff$, $\neq$, $\exists x_1, x_2$:, Klammern weglassen, etc.

Jetzt definieren wir formal, 1was Terme, Formeln und Aussagen bedeuten sollen.

Definition 2.6 *Sei M eine L-Struktur und seien $a_1, \ldots, a_n \in M$. Wir verwenden zur Abkürzung die Notation $\underline{a} = (a_1, \ldots, a_n)$.*

*Ist $t(x_1, \ldots, x_n)$ ein L-Term, so definieren wir die **Interpretation** $t^M(\underline{a})$ von t in M wie folgt: (Anschaulich: Setze $\underline{a}$ in t ein und rechne es aus.)*

1. *Falls $t = x_i$ ist $t^M(\underline{a}) = a_i$.*
   Falls $t = c$ ist $t^M(\underline{a}) = c^M$.
2. *Falls $t = f(t_1, \ldots, t_m)$, so ist $t^M(\underline{a}) = f^M(t_1^M(\underline{a}), \ldots, t_m^M(\underline{a}))$.*

*Ist $\phi(x_1, \ldots, x_n)$ eine L-Formel, so sagen wir, dass $\phi(a_1, \ldots, a_n)$ **wahr ist in** M (Notation: $M \vDash \phi(a_1, \ldots, a_n)$), wenn gilt:*

3. *Falls $\phi =$ „$t_1 = t_2$“: $M \vDash \phi(\underline{a}) \iff t_1^M(\underline{a}) = t_2^M(\underline{a})$.*
4. *Falls $\phi =$ „$R(t_1, \ldots, t_m)$“: $M \vDash \phi(\underline{a}) \iff (t_1^M(\underline{a}), \ldots, t_m^M(\underline{a})) \in R^M$.*
5. *Falls $\phi =$ „$(\psi_1 \wedge \psi_2)$“, ...: so wie man es erwarten würde*

6. *Falls* $\phi(x_1, \ldots, x_n) =$ „$\forall y\, \psi(x_1, \ldots, x_n, y)$“*:* $M \vDash \phi(\underline{a}) \iff$ *für alle* $b \in M$ *gilt* $M \vDash \psi(\underline{a}, b)$*.* „$\exists$“ *entsprechend wenn es ein* $b \in M$ *gibt mit* $M \vDash \psi(\underline{a}, b)$*.*

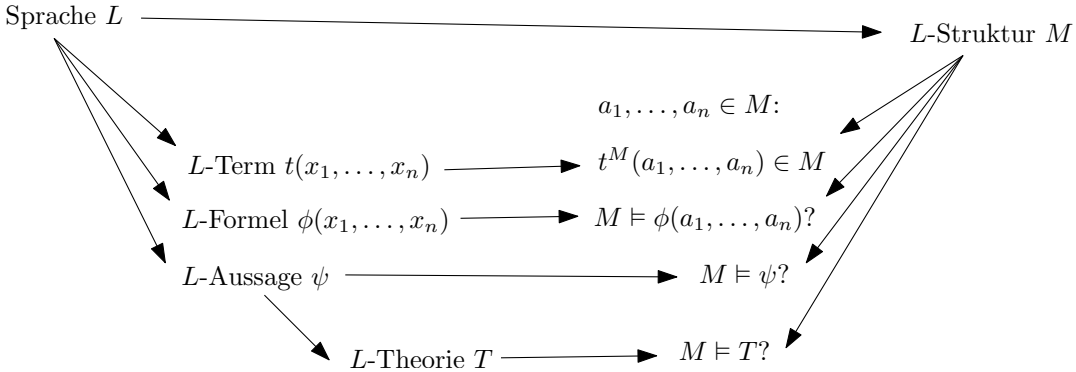
Bemerkung: Hier ist es wichtig, dass Quantoren immer über (alle) Elemente der Struktur laufen.
Beispiel: Betrachte die L_{Ring}-Formel $\phi(x) =$„$\exists y\, y + y = x$“. Ob $\phi(1)$ wahr ist, hängt von der Struktur ab, in der man das betrachtet. Es gilt z.B. $\mathbb{Q} \models \phi(1)$ aber nicht $\mathbb{Z} \models \phi(1)$.
Insbesondere ist es auch nicht möglich, Quantoren zu haben, bei denen die Variable für eine Teilmenge der Struktur steht. Aussagen der Form „$\forall A \subseteq M : \ldots$“ (für eine L-Struktur M) lassen sich also in der Sprache der Mengenlehre formulieren (wenn man die Struktur geeignet kodiert), aber nicht als L-Aussagen.

Ein paar Beispiele von Dingen, die man mit solchen Formeln ausdrücken kann. (Zur Definition dieser Dinge siehe LA II-Vorlesung.) Es gibt L_{Ring}-Formeln ϕ_i, so dass für jeden Ring R das folgende gilt:
$R \models \phi_1(a) \iff a \in R^\times$ ($\phi_1(x) =$„$\exists y\, x \cdot y = 1$“)
$R \models \phi_2(a, b) \iff a \mid b$ ($\phi_2(x, y) =$„$\exists z\, x \cdot z = y$“)
$R \models \phi_3(a) \iff a$ ist irreduzibel ($\phi_3(x) =$„$\forall y, z : (x = y \cdot z \Rightarrow \phi_1(y) \vee \phi_1(z))$“)
$R \models \phi_4(a) \iff a$ ist prim ($\phi_4(x) =$„$\forall y, z : (\phi_2(x, y \cdot z) \Rightarrow (\phi_2(x, y) \vee \phi_2(x, z)))$“)

In LA wurde gezeigt: aus prim folgt irreduzibel. Dies ist eine L_{Ring}-Aussage: $\phi_5 =$„$\forall x\, (\phi_4(x) \Rightarrow \phi_3(x))$“
Was in LA gezeigt wurde, kann man also anders ausdrücken als: Für jeden Ring R gilt $R \models \phi_5$.

Definition 2.7 *Eine Menge* T *von* L*-Aussagen wird* L-***Theorie*** *genannt. Wir schreiben* $M \vDash T$ *wenn* $M \vDash \phi$ *für jedes* $\phi \in T$ *gilt. Wir sagen „*M *ist ein* ***Modell*** *der Theorie* T*“.*

Übersicht:



Beispiel: Jedes Gruppenaxiom ist eine L_{Grp}-Aussage. Die **Theorie der Gruppen** T_{Grp} ist die Menge der Gruppenaxiome (als L_{Grp}-Aussagen):

$$\begin{aligned} T_{Grp} = \{&\forall x, y, z : (x \circ y) \circ z = x \circ (y \circ z) \\ &\forall x : (x \circ e = x \wedge e \circ x = x) \\ &\forall x : (x \circ x^{-1} = e \wedge x^{-1} \circ x = e)\} \end{aligned}$$

Für L_{Grp}-Stukturen G gilt: G ist eine Gruppe genau dann wenn $G \vDash T_{Grp}$.

Entsprechend: Die Theorie der Ringe T_{Ring} ist die L_{Ring}-Theorie bestehend aus den Ring-Axiomen; die Theorie der Körper ist die L_{Ring}-Theorie bestehend aus den Körper-Axiomen, etc.

Was kann man noch so mit Theorien ausdrücken?

1. Sei $L = \emptyset$. Frage: Gibt es eine L-Theorie T, so dass $M \vDash T \iff M$ hat mindestens 2 Elemente?
   Antwort: $T = \{\exists x_1, x_2 : x_1 \neq x_2\}$
2. Frage: Gibt es eine L-Theorie T, so dass $M \vDash T \iff M$ hat genau 2 Elemente?
   Antwort: $T = \{\exists (x_1, x_2 : x_1 \neq x_2 \wedge \forall x_3 : (x_3 = x_1 \vee x_3 = x_2))\}$
3. Gibt es eine L-Theorie T_∞, so dass $M \models T_\infty \iff M$ ist unendlich?
   Antwort: T_∞ besteht aus den Aussagen

   $$\phi_n := \exists x_1, \ldots, x_n : x_1 \neq x_2 \wedge x_1 \neq x_3 \wedge \cdots \wedge x_1 \neq x_n \wedge \cdots \wedge x_{n-1} \neq x_n$$

   für alle n.

(Für eine Struktur M gilt $M \models \phi_n$ genau dann wenn M mindestens n Elemente enthält. Also gilt $M \models T_\infty$ genau dann, wenn M unendlich ist.)

4. Gibt es eine einfachere Antwort auf Frage 3 wenn $L = \{f\}$ ist für ein einstelliges Funktionssymbol f? Antwort: Jein. Man kann ausdrücken, dass f injektiv aber nicht surjektiv ist:

$$T = \{\forall x, y : (f(x) = f(y) \Rightarrow x = y),$$
$$\exists x : \neg\exists y : f(y) = x\}$$

Daraus folgt, dass jedes Modell von T unendlich ist; allerdings ist nicht jede unendliche L-Struktur ein Modell von T.

Noch eine Anmerkung: Frage 3 lässt sich wirklich nur mit einer unendlichen Menge T lösen. Solche unendlichen Mengen sind auch der eigentliche Grund, weshalb wir überhaupt Theorien definiert haben. Wenn man nur endliche Theorien betrachtet, kann man genauso gut alle Aussagen der Theorie mit „$\wedge$“ verknüpfen, so dass man nur eine einzige Aussage hat.

Zurück zum Beispiel aus LA II: Was gezeigt wurde, ist also: Für jede L_{Ring}-Struktur R gilt: Falls $R \models T_{Ring}$, dann $R \models \phi_5$ (wobei ϕ_5 die Aussage „irred $\Rightarrow$ prim“ war). Anders ausgedrückt: T_{Ring} „impliziert“ ϕ_5 im Sinne der folgenden Definition.

Definition 2.8 *Eine L-Theorie T **impliziert** eine L-Aussage ϕ, wenn ϕ in jedem Modell von T wahr ist. (d.h. für jede L-Struktur M gilt: Falls $M \vDash T$, dann auch $M \vDash \phi$).*

Diese Art der Implikation war gemeint, als wir vorige Woche gesagt hatten, dass eine Aussage „aus rein logischen Gründen“ aus einer anderen Aussage folgt.

Beispiel: T_{Ring} impliziert „aus prim folgt irreduzibel“. 10.7.2013

Beispiel: $T = T_{Grp}$ impliziert $e^{-1} = e$.

Beispiel: $T = \emptyset$ impliziert $\forall x\, x = x$.

2.2 Der Gödelsche Vollständigkeitssatz

Für den Gödelschen Vollständigkeitssatz Satz ist es nützlich, alle Aussagen noch etwas zu vereinfachen. Wir fassen $\alpha \vee \beta$ als Abkürzung für $\neg(\neg\alpha \wedge \neg\beta)$ auf und $\exists x\, \alpha$ als Abkürzung für $\neg\forall x\, \neg\alpha$.

Definition 2.9 *Sei L eine Sprache. Dann sei H_L (die „Axiome des Hilbertkalküls“) die folgende Menge von L-Aussagen. Hierbei ist $\underline{x}$ eine Kurzschreibweise für $x_1, \ldots, x_n$, α, β, γ sind beliebige L-Formeln mit den angegebenen freien Variablen und t ist ein L-Term.*

1. $\forall \underline{x} : \big(\big(\alpha(\underline{x}) \Rightarrow (\beta(\underline{x}) \Rightarrow \gamma(\underline{x}))\big) \Rightarrow \big((\alpha(\underline{x}) \Rightarrow \beta(\underline{x})) \Rightarrow (\alpha(\underline{x}) \Rightarrow \gamma(\underline{x}))\big)\big)$
2. $\forall \underline{x} : \big(\alpha(\underline{x}) \Rightarrow (\beta(\underline{x}) \Rightarrow (\alpha(\underline{x}) \wedge \beta(\underline{x})))\big)$
3. $\forall \underline{x} : \big((\alpha(\underline{x}) \wedge \beta(\underline{x})) \Rightarrow \alpha(\underline{x})\big)$
4. $\forall \underline{x} : \big((\alpha(\underline{x}) \wedge \beta(\underline{x})) \Rightarrow \beta(\underline{x})\big)$
5. $\forall \underline{x} : \big((\alpha(\underline{x}) \Rightarrow \neg\beta(\underline{x})) \Rightarrow (\beta(\underline{x}) \Rightarrow \neg\alpha(\underline{x}))\big)$
6. $\forall \underline{x} : \big(\forall y\, \alpha(\underline{x}, y) \Rightarrow \alpha(\underline{x}, t(\underline{x}))\big)$
7. $\forall \underline{x} : \big(\alpha(\underline{x}) \Rightarrow \forall y\, \alpha(\underline{x})\big)$
8. $\forall \underline{x} : \big(\forall y\, (\alpha(\underline{x}, y) \Rightarrow \beta(\underline{x}, y)) \Rightarrow (\forall y\, \alpha(\underline{x}, y) \Rightarrow \forall y\, (\beta(\underline{x}, y))\big)$
9. $\forall y : y = y$
10. $\forall \underline{x}, y, z : \big(y = z \Rightarrow (\alpha(\underline{x}, y, z) \Rightarrow \alpha(\underline{x}, y, y))\big)$

satz.goedel

Satz 2.10 *(Gödelscher Volständigkeitssatz) Sei L eine Sprache, T eine L-Theorie und ϕ eine L-Aussage. Wir nehmen an, dass in den Aussagen von T und in ϕ kein „$\vee$“ und kein „$\exists$“ vorkommen.*

Dann sind äquivalent:

1. *T impliziert ϕ.*
2. *ϕ lässt sich in endliche vielen Schritten aus $T \cup H_L$ mit Hilfe des Modus Ponens herleiten, d.h.:*
   Es gibt L-Aussagen $\phi_1, \ldots, \phi_n$ mit $\phi_n = \phi$, und für jedes $i \leq n$ gibt es eine L-Aussage ψ, so dass sowohl ψ, als auch „$\psi \Rightarrow \phi_i$“ in $T \cup H_L \cup \{\phi_1, \ldots, \phi_{i-1}\}$ liegen.

*Die Folge $\phi_1, \ldots, \phi_n$ heißt **formaler Beweis** von ϕ aus T.*

Beweis: Siehe Logik-Vorlesung.

Beispiel: Man versuche, $\forall x \forall y \alpha(x, y)$ aus $\forall y \forall x \alpha(x, y)$ herzuleiten.

Anwendung auf die Mengenlehre:
In Def. 1.1 hatten wir „Formeln in der Sprache der Mengenlehre“ definiert. Nach unserer neuen Definition sind das genau die L_{Me}-Formeln, wobei $L_{Me} = \{\in\}$ ist und $\in$ ein zweistelliges Relationssymbol ist.
Die Axiome von ZFC bilden eine L_{Me}-Theorie T_{ZFC}.
Es folgt: Alles, was von T_{ZFC} impliziert wird, lässt sich mit dem Modus Ponens aus $H_{L_{Me}} \cup T_{ZFC}$ ableiten.
Umgekehrt könnte man jetzt also definieren:

Ziel 2.11 *Ein formaler Beweis eines mathematischen Satzes ϕ (formuliert als L_{Me}-Aussage) ist ein formaler Beweis von ϕ im Sinne von Satz 2.10 mit $T = T_{ZFC}$.*

Ein paar Anmerkungen:

- In der Praxis ist es natürlich völlig unpraktikabel, Beweise so aufzuschreiben, aber es ist beruhigend zu wissen, dass es wenigstens theoretisch möglich ist, präzise zu definieren, was ein Beweis ist. Außerdem sollte man zumindest theoretisch in der Lage sein, einen „normalen“ Beweis in einen formalen zu übersetzen. (Damit man dazu wirklich in der Lage ist, muss man allerdings noch den Beweis von Satz 2.10 kennen; dieser Beweis sagt einem, wie man, wenn T ϕ impliziert, den entsprechenden formalen Beweis von ϕ aus T konstruiert.)
- Etwas verwirrend: T_{ZFC} impliziert ϕ heißt: In jedem Modell M von T_{ZFC} gilt ϕ. So ein M ist eine Menge mit einer zweistelligen Relation $a \in^M b$; diese Relation besagt nicht wirklich $a \in b$-Relation, aber sie „tut so als ob“, da sie ja die ZFC-Axiome erfüllt. Dadurch kann man die gesamte Mathematik auch innerhalb von M betreiben.
- Wie wir gesehen haben (Kontinuumshypothese: $\aleph_0 = 2^{\aleph_0}$??), ist nicht so ganz klar, ob T_{ZFC} wirklich die „richtige“ Menge von Axiomen ist. Für die meiste Mathematik reicht es aber aus.

2.3 Anwendungen vom Vollständigkeitssatz

Der Vollständigkeitssatz hat eine sehr nützliche Folgerung:

Korollar 2.12 *(Kompaktheitssatz) Wenn eine L-Theorie T eine L-Aussage ϕ impliziert, dann gibt es schon eine endliche Teilmenge $T_0 \subseteq T$, die ϕ impliziert.*

Beweis: In dem formalen Beweis von ϕ aus T kommen nur endlich viele Aussagen aus T vor. Sei T_0 diese endliche Menge von Aussagen. □

Anmerkung: Es gibt ein ganzes Teilgebiet der Logik, das hauptsächlich auf diesem Satz beruht, nämlich die Modelltheorie.

1. Anwendung:

Wir hatten die Theorie $T_\infty = \{\phi_n \mid n \in \mathbb{N}\}$ gesehen, deren Modelle genau die unendlichen Mengen M sind. (Erinnerung: ϕ_n besagt, dass das Modell mindestens n Elemente hat.)

Frage: Gibt es auch eine endliche Theorie T', deren Modelle genau die unendlichen Mengen sind?
Antwort: nein.

Annahme: Es gäbe eine solche endliche Theorie $T' = \{\psi_1, \dots, \psi_n\}$. Setze $\psi := \psi_1 \wedge \dots \wedge \psi_n$. OBdA $T' = \{\psi\}$.

In jedem Modell von T_∞ gilt ψ. Also: T_∞ impiziert ψ. Aus dem Kompaktheitssatz folgt: Es gibt eine endliche Teilmenge $T_0 = \{\phi_{n_1}, \dots, \phi_{n_k}\} \subseteq T$, die ψ impliziert. T_0 hat endliche Modelle (nämlich jede Struktur mit mindestens $\max\{n_1, \dots, n_k\}$ vielen Elementen); diese Modelle sind dann auch Modelle von T'. Das ist ein Wiederspruch dazu, dass alle Modelle von T' unendlich sein sollten. □

2. Anwendung: „Non-standard Analysis“

Konstruktion von „unendlich großen ganzen Zahlen“:

Betrachte $\mathbb{Z}$ als L-Struktur mit $L = L_{Ring} \cup \{\leq, \dots\}$. (Die Pünktchen heißen: Man darf noch beliebige weitere Dinge zur Sprache hinzufügen.)

Behauptung: Es gibt einen Ring ${}^*\mathbb{Z}$, der „sich (a) ganz ähnlich wie die ganzen Zahlen verhält aber (b) unendlich große Zahlen enthält“. Genauer:

(a) *Jede* L-Aussage, die in $\mathbb{Z}$ gilt, gilt auch in ${}^*\mathbb{Z}$.
(b) Es gibt ein $c \in \mathbb{Z}^*$ mit $c > n$ für alle $n \in \mathbb{N}$.

Beweis:

Definiere $L' := L \cup \{c\}$, wobei c ein Konstantensymbol ist, und betrachte die folgenden L'-Theorien.
Sei $T_{(a)}$ die Menge *aller* L-Aussagen, die in $\mathbb{Z}$ wahr sind, also $T_{(a)} = \{\phi \mid \mathbb{Z} \models \phi\}$.
Sei $T_{(b)} := \{c > 1, c > 1 + 1, c > 1 + 1 + 1, \dots\}$.
Was wir suchen ist also einfach nur ein Modell ${}^*\mathbb{Z}$ von $T := T_{(a)} \cup T_{(b)}$. (Dass ${}^*\mathbb{Z}$ dann ein Ring ist, ist klar, da $T_{Ring} \subseteq T_{(a)}$.)

Anders ausgedrückt: Zu zeigen: Es gibt eine L'-Struktur, die ein Modell von T ist. Annahme, so eine Struktur gibt es nicht (d.h. T hat überhaupt kein Modell).

Dann gilt in jedem Modell von T die Aussage $0 = 1$. Also: T impliziert $0 = 1$.

Nach dem Kompaktheitssatz gibt es eine endliche Teilmenge $T_0 \subseteq T$ mit: T_0 impliziert $0 = 1$.

Behauptung: $\mathbb{Z}$ kann so als L'-Struktur aufgefasst werden, dass es ein Modell von T_0 ist. (Wenn wir das zeigen können, haben wir einen Widerspruch, da nicht $\mathbb{Z} \models 0 = 1$ gilt.)

$\mathbb{Z}$ ist bereits eine L-Struktur. Um es zu einer L'-Struktur zu machen, müssen wir noch festlegen, was $c^{\mathbb{Z}}$ sein soll. Erste Feststellung: $\mathbb{Z}$ ist auf jeden Fall ein Modell von $T_{(a)} \cap T_0$; bleibt also nur noch, sich drum zu kümmern, dass $\mathbb{Z}$ auch ein Modell von $T_{(b)} \cap T_0$ ist. Diese Schnittmenge besteht aus endlich vielen der Aussagen der Form „$c > 1 + \dots + 1$“. Diese Aussagen gelten alle in $\mathbb{Z}$, wenn wir $c^{\mathbb{Z}}$ hinreichend groß wählen. □

Wir haben jetzt also unsere Struktur ${}^*\mathbb{Z}$, die sich so ähnlich verhält wie die normalen ganzen Zahlen, die aber unendlich große Zahlen enthält. (Ein $a \in {}^*\mathbb{Z}$ heißt unendlich groß, wenn $a > n$ ist für jedes $n \in \mathbb{N}$.) Die unendlich großen Zahlen in ${}^*\mathbb{Z}$ haben einen Bezug zu $\mathbb{Z}$: Für jede beliebige L-Formel $\phi(x)$ sind äquivalent:
(a) Es gibt unendlich viele $n \in \mathbb{N}$ mit $\mathbb{Z} \models \phi(n)$
(b) Es gibt ein unendlich großes $a \in {}^*\mathbb{Z}$ mit ${}^*\mathbb{Z} \models \phi(a)$

Beweis dieser Äquivalenz:

„(a) $\Rightarrow$ (b)“:
Aus (a) folgt, dass es zu jeder natürlichen (oder ganzen) Zahl eine größere Zahl n gibt, für die $\phi(n)$ gilt. Anders ausgedrückt: Die L-Aussage $\psi :=$ „$\forall m : \exists n > m : \phi(n)$“ gilt in $\mathbb{Z}$. Also ist $\psi \in T_{(a)}$, und damit gilt ψ auch in ${}^*\mathbb{Z}$, d.h. für jedes $m \in {}^*\mathbb{Z}$ gibt es ein noch größeres $n \in {}^*\mathbb{Z}$, so dass ${}^*\mathbb{Z} \models \phi(n)$ gilt. Wähle für m jetzt einfach irgend eine unendlich große Zahl. Dann ist auch n unendlich groß.

„(b) $\Rightarrow$ (a)“:
Annahme, es gäbe nur endlich viele $n \in \mathbb{N}$ mit $\mathbb{Z} \models \phi(n)$.
Dann gibt es insbesondere ein $N \in \mathbb{N}$ so dass $\phi(n)$ falsch ist für alle $n > N$. Wir schreiben N als $1 + \cdots + 1$. Dann haben wir eine L-Aussage „$\forall n > 1 + \cdots + 1 : \neg\phi(n)$“, die in $\mathbb{Z}$ gilt. Also gilt sie auch in ${}^*\mathbb{Z}$. Das ist aber ein Widerspruch zu (b), da so ein unendlich großes a insbesondere größer als N ist. $\square$

Anwendung der 2. Anwendung:

Eine der großen offenen Vermutungen der Zahlentheorie ist:

Primzahlzwillingsvermutung: Es gibt unendlich viele Primzahlzwillinge, d.h. unendlich viele $n \in \mathbb{N}$, so dass sowohl n als auch $n + 2$ prim sind.

Dass eine Zahl prim ist, lässt sich als L-Formel schreiben: $\phi(x) =$ „$x > 0 \wedge \forall n > 0 : (n \mid x \Rightarrow (n = 1 \vee n = x))$“ (wobei $n \mid x$ eine Abkürzung ist für „$\exists m : n \cdot m = x$“.)

Damit lässt sich „Primzahlzwilling“ auch als Formel ausdrücken: $\phi'(x) =$ „$\phi(x) \wedge \phi(x + 2)$“.

Aus der vorigen Äquivalenz folgt, dass die Primzahlzwillingsvermutung äquivalent ist zu: Es gibt in ${}^*\mathbb{Z}$ unendliche große Primzahlzwillinge.

Anders ausgedrückt: Anstatt unendlich viele Primzahlzwillinge finden zu müssen, müssen wir jetzt nur noch ein einziges finden... das aber dafür unendlich groß sein muss.

Das sieht beeindruckend aus und klingt nach einer starken Vereinfachung; allerdings ist das neue Problem in Wirklichkeit überhaupt nicht einfacher.

(Trotzdem sind die unendlich großen ganzen Zahlen manchmal nützlich. Und die gleiche Konstruktion kann man auch z.B. mit $\mathbb{Q}$ oder $\mathbb{R}$ machen. Wenn man sie mit $\mathbb{R}$ macht, kann man einige Definitionen aus der Analysis mit Hilfe von unendlich großen und unendlich kleinen Zahlen einfacher formulieren – daher der Name Non-standard *Analysis*.)