Grundlagen der Mathematik

Mathias Schacht

Fachbereich Mathematik
Universität Hamburg

WS 2011/12

Stand: 1. Dezember 2011

Vorwort

Diese Folien behandeln in Kurzform einige Grundlagen der Mathematik ausgehend von der axiomatischen Mengenlehre nach Zermelo, Fraenkel und anderen und entstanden für die Vorlesung Lineare Algebra und Analytische Geometrie im Wintersemester 2011/12 an der Universität Hamburg.

Große Teile basieren auf dem Vorlesungsskript von Reinhard Diestel zur gleichnamigen Vorlesung.

Aufgrund der zeitlichen Beschränkungen konnten viele wichtige Themen, wie z. B. Kardinalzahlen, Ordinalzahlen, Theorie der Wohlordnungen, nur sehr kurz oder gar nicht behandelt werden.

Eine empfehlenswerte und umfassende *Einführung in die Mengenlehre* findet man zum Beispiel in dem gleichnamigen Buch von Ebbinghaus:

- H.-D. Ebbinghaus, *Einführung in die Mengenlehre*,
  Spektrum Akademischer Verlag, 4. Auflage, 2003

Übersicht

Kapitel 1

Naive Mengenlehre und Russels Paradoxon

Naive Mengenlehre

Fragen im 19. Jahrhundert:

- Was sind die Grundlagen der Mathematik/Arithmetik?
- Was sind Zahlen? Was sind Mengen? Darf es unendliche Mengen geben?

Idee/Definition (Ende 19. Jahrhundert, Cantor 1895)

Mengen sind ungeordnete Zusammenfassungen von wohlunterschiedenen Objekten (unseres Denkens) zu einem Ganzen.

Beispiele: $\{10^{10}, 1, \pi, 19, 2001\}$, Menge der natürlichen Zahlen, $\{A, x, 1, B\}$

Definition (Frege 1893)

Für jedes sprachliche Prädikat P gibt es die **Menge** M_P aller der Objekte O, auf die das Prädikat P zutrifft

$$M_P = \{O\colon\ P(O)\}.$$

Objekte O für die $P(O)$ gilt, heißen **Elemente von** M_P

$$O \in M_P\,.$$

Russels Paradoxon

Antinomie (Russel 1903)

Sei P das Prädikat „x enthält sich nicht selbst als Element," d. h.

$$M_P = \{O\colon\ O \notin O\}.$$

Widerspruch: $M_P \notin M_P$ genau dann, wenn $M_P \in M_P$.

Beweis: Auf der einen Seite erhalten wir

$$\begin{aligned} M_P \notin M_P &\Rightarrow M_P \text{ enthält sich nicht selbst als Element} \\ &\Rightarrow P(M_P) \text{ gilt } \Rightarrow M_P \in M_P \qquad ↯ \end{aligned}$$

und auf der anderen Seite erhalten wir

$$\begin{aligned} M_P \in M_P &\Rightarrow M_P \text{ enthält sich selbst als Element} \\ &\Rightarrow P(M_P) \text{ gilt nicht } \Rightarrow M_P \notin M_P \qquad ↯ \quad \square \end{aligned}$$

$\Longrightarrow$ M_P kann nicht existieren

Freges Ansatz ist nicht widerspruchsfrei!

Auflösung des Paradoxons

Probleme in Freges Definition:

- Was ist ein Prädikat? Wann ist ein Prädikat „wahr“, wann „gilt“ es?
- Was sind Objekte? Gibt es eine „Grundmenge“ aller Objekte?

Ausweg:

- Formalisierung mathematischer Sprache (**Aussagen**) und **Regeln**
  $\longrightarrow$ mathematische Logik
- Benennung als wahr angenommener Grundaussagen (**Axiome**)
  $\longrightarrow$ axiomatische Mengenlehre
- der Wahrheitswert aller anderen Aussagen wird formal mit Hilfe der Regeln aus den Axiomen hergeleitet (**Beweis**) $\longrightarrow$ Mathematik

Probleme:

- (innere) Widerspruchsfreiheit der Regeln und Axiome — unentscheidbar
- Vollständigkeit – Sind alle wahren Aussagen beweisbar? — Nein, GÖDEL

Bemerkungen

Idee

Das mathematische „Universum“ besteht ausschließlich aus *Mengen*, ist also ein System von Mengen. Jede Menge besteht aus wohlunterschiedenen Elementen, welche wiederum Mengen sind. Mengen stehen zu einander in Beziehung:

- $M \in N$, „die Menge N enthält die Menge M als Element,“

$$N = \{\dots, M, \dots\}.$$

- $M \subseteq N$, „die Menge N enthält die Menge M als Teilmenge,“
  d. h. jedes Element von M ist auch in N als Element enthalten.

Wir schreiben $M = N$, wenn sowohl $M \subseteq N$ als auch $N \subseteq M$ gilt.

Die Axiome der Mengenlehre beschreiben, welche „Grundmengen“ es gibt und wie man aus gegebenen Mengen neue Mengen erhält.

Bsp.: $M = \{m, n, o\}$, $N_1 = \{a, b, \dots, z\}$, $N_2 = \big\{\{a, b, c\}, \{b, c, d\}, \dots, \{x, y, z\}\big\}$
Dann gilt:

$$M \subseteq N_1\,, \quad M \notin N_1\,, \quad M \not\subseteq N_2\,, \quad M \in N_2\,.$$

Kapitel 2

Aussagenlogik

Aussagenlogik

Definition (Aussagen)

Aussagen sind Zeichenfolgen (Ausdrücke) bestehend aus (u. U. verzierten) lateinischen, griechischen, hebräischen, ... „Buchstaben" (Bezeichner) und Symbolen (,), {, }, [,], $\in$, $\subseteq$, $=$, $:$, $\neg$, $\vee$, $\wedge$, $\Rightarrow$, $\Leftrightarrow$.

Hierbei liest man

$:$ als *so dass*,	$\neg$ als *nicht*,
$\vee$ als *oder*,	$\wedge$ als *und*,
$\Rightarrow$ als *wenn ..., dann ...*,	$\Leftrightarrow$ als ... *genau dann, wenn ...*.

- Für je zwei Mengen A und B sind die Ausdrücke „$A \in B$" und „$A \subseteq B$" **primitive Aussagen**.
- Für zwei Aussagen p und q sind die Ausdrücke „$\neg p$", „$p \vee q$", „$p \wedge q$", „$p \Rightarrow q$" und „$p \Leftrightarrow q$" **zusammengesetzte Aussagen**.

Wahrheitsgehalt von Aussagen

Definition (Wahrheitswerte)

- *Primitive Aussagen* der Form „$A \in B$" (bzw. „$A \subseteq B$") sind **wahr**, wenn die Mengen A und B in der Beziehung $A \in B$ (bzw. $A \subseteq B$) stehen und ansonsten sind sie **falsch**.
- Für aus Aussagen p und q *zusammengesetzte Aussagen* gilt:

$$\neg p \text{ ist } \begin{cases} \textbf{wahr} & \text{wenn } p \text{ falsch ist,} \\ \textbf{falsch} & \text{sonst, d. h. wenn } p \text{ wahr ist,} \end{cases}$$

$$p \vee q \text{ ist } \begin{cases} \textbf{wahr} & \text{wenn mindestens eine der Aussagen } p \text{ oder } q \text{ wahr ist,} \\ \textbf{falsch} & \text{sonst, d. h. wenn keine der Aussagen } p \text{ und } q \text{ wahr ist,} \end{cases}$$

$$p \wedge q \text{ ist } \begin{cases} \textbf{wahr} & \text{wenn beide Aussagen } p \text{ und } q \text{ wahr sind,} \\ \textbf{falsch} & \text{sonst, d. h. wenn höchstens eine der Aussagen } p,\ q \text{ wahr ist,} \end{cases}$$

$$p \Rightarrow q \text{ ist } \begin{cases} \textbf{wahr} & \text{wenn } q \text{ wahr ist oder wenn } p \text{ falsch ist,} \\ \textbf{falsch} & \text{sonst, d. h. wenn } p \text{ wahr und } q \text{ falsch ist,} \end{cases}$$

$$p \Leftrightarrow q \text{ ist } \begin{cases} \textbf{wahr} & \text{wenn } p \text{ und } q \text{ beide wahr oder wenn beide falsch sind,} \\ \textbf{falsch} & \text{sonst, d. h. wenn } p \text{ und } q \text{ unterschiedliche W'werte haben.} \end{cases}$$

Reductio ad absurdum

Widerspruchsbeweis bzw. indirekter Beweis

Mit Hilfe der Implikation ($\Rightarrow$, wenn ..., dann ...) kann eine Aussage p durch **Widerspruch** bewiesen werden. Dafür muss für eine bekannte falsche Aussage q die Implikation

$$(\neg p) \Rightarrow q$$

bewiesen werden, d. h. man beweist die Richtigkeit der Aussage

„wenn p falsch ist, dann ist q wahr."

Da q aber falsch ist, kann p somit nicht falsch sein, also muss p wahr sein.

Bsp.: $p =$„$\sqrt{2}$ ist irrational" und $q =$„es gibt teilerfremde a, b für die a/b kürzbar ist"

- q ist offensichtlich falsch
- Angenommen $\neg p$ ist wahr $\Rightarrow$ $\sqrt{2} = a/b$ für teilerfremde natürliche Zahlen a, b"

$\Rightarrow$ $2b^2 = a^2 \Rightarrow 2$ teilt a^2

$\Rightarrow$ da 2 eine Primzahl ist, teilt 2 somit auch a, d. h. $a = 2a_1$ für geeignetes a_1

$\Rightarrow$ $2b^2 = a^2 = 4a_1^2 \Rightarrow b^2 = 2a_1^2 \Rightarrow 2$ teilt $b^2 \Rightarrow 2$ teilt b, d. h. $b = 2b_1$

$\Rightarrow$ $a/b = (2a_1)/(2b_1) = a_1/b_1 \Rightarrow q$ ist wahr $\lightning$

- Also muss $\neg p$ falsch sein und somit ist p wahr, d. h. $\sqrt{2}$ ist irrational $\square$

Aussageformen

Definition (Aussageform)

Ersetzt man in einer Aussage eine oder mehrere darin auftretende Bezeichnungen für Mengen durch (als „besonders" vereinbarte und sonst in der Aussage nicht verwendete) Symbole, die wir **freie Variablen** nennen werden, und zwar für jede ersetzte Mengenbezeichnung all ihre Vorkommnisse durch die gleiche Variable, so nennt man den dadurch entstehenden Ausdruck eine **Aussageform**.

Beispiel: Seien A, B, C Mengen und x eine freie Variable. Ersetzt man B durch x in der Aussage

$$p = (A \in B) \vee (B \subseteq C)\,,$$

so erhält man die Aussageform

$$p(x) = (A \in x) \vee (x \subseteq C)\,,$$

die alle die Mengen „beschreibt", die A als Element enthalten oder eine Teilmenge von C sind. Allerdings sind

$$p(x) = (x \in B) \vee (B \subseteq x) \quad \text{und} \quad p(x) = (A \in x) \vee (B \subseteq C)$$

keine Aussageform, welche aus p gewonnen werden können. (Warum?)

Quantoren: $\forall$ und $\exists$

Definition (Allaussagen und Existenzaussagen)

Sei $p(x)$ eine Aussageform. Dann ist

- $(\forall x)p(x)$ eine Aussage; die **Allaussage**.
- $(\exists x)p(x)$ eine Aussage; die **Existenzaussage**.

Die freie Variable x in $p(x)$ heißt dann **gebundene Variable** in der All-/Existenzaussage.

In All-/Existenzaussagen kann durch Einführung einer neuen Variablen eine neue Aussageform gebildet werden, die durch einen weiteren Quantor wieder gebunden werden kann.

Definition (Wahrheitswerte von All- und Existenzaussagen)

Für eine Aussageform $p(x)$ gilt:

$$(\forall x)p(x) \text{ ist } \begin{cases} \textbf{wahr} & \text{wenn } p(M) \text{ für jede Menge } M \text{ wahr ist} \\ \textbf{falsch} & \text{sonst, d. h. wenn es eine Menge } M \text{ gibt für die } p(M) \text{ falsch ist,} \end{cases}$$

$$(\exists x)p(x) \text{ ist } \begin{cases} \textbf{wahr} & \text{wenn es eine Menge } M \text{ gibt für die } p(M) \text{ wahr ist} \\ \textbf{falsch} & \text{sonst, d. h. } p(M) \text{ für jede Menge } M \text{ falsch ist.} \end{cases}$$

Bemerkungen

Für Aussagen p und q und eine Aussageform $p(x)$ gelten:

$$\begin{aligned}
\neg(p \vee q) &\Leftrightarrow \big((\neg p) \wedge (\neg q)\big)\,, & \neg(p \wedge q) &\Leftrightarrow \big((\neg p) \vee (\neg q)\big)\,,\\
\big(p \Rightarrow q\big) &\Leftrightarrow \big(\neg q \Rightarrow \neg p\big)\,, & (p \Rightarrow \neg q) &\Leftrightarrow \big(q \Rightarrow \neg p)\,,\\
\neg\big((\forall x) p(x)\big) &\Leftrightarrow \big((\exists x)\neg p(x)\big)\,, & \neg\big((\exists x) p(x)\big) &\Leftrightarrow \big((\forall x)\neg p(x)\big)\,.
\end{aligned}$$

Für eine Menge M schreiben wir abkürzend:

$$\begin{aligned}
(\forall x \in M)\, p(x) \quad &\text{für} \quad (\forall x)\big(x \in M \Rightarrow p(x)\big)\,,\\
(\exists x \in M)\, p(x) \quad &\text{für} \quad (\exists x)\big(x \in M \wedge p(x)\big)\,.
\end{aligned}$$

Insbesondere ist $(\forall x \in M)p(x)$ für alle Aussageformen $p(x)$ wahr, falls M keine Elemente enthält.

Mengen und Klassen

Für eine Aussageform $p(x)$ ist im Frege'schen Sinne die „Zusammenfassung“ $\{M\colon\ p(M)\}$ aller Mengen M, für die $p(M)$ gilt, eine Menge und für die Aussageform $x \notin x$ ergibt sich Russels Paradoxon. Die folgenden Axiome werden diese „Mengenbildung“ nicht zulassen.

Zusammenfassungen der Form $\{M\colon\ p(M)\}$ bezeichnet man als **Klassen**. Nicht alle Klassen sind Mengen und Klassen die keine Mengen sind (wie z. B. die Russel'sche Klasse $\{M\colon\ M \notin M\}$) heißen **echte Klassen**.

Kapitel 3

Axiomatische Mengenlehre

Axiome der Mengenlehre Teil 1

1. **Existenz der leeren Menge**: Es existiert eine Menge die kein Element enthält.
$$(\exists x)(\forall y)(y \notin x)$$

2. **Extensionalitätsaxiom**: Zwei Mengen sind genau dann gleich, wenn sie die gleichen Elemente enthalten.
$$(\forall x)(\forall y)\Big((x = y) \Leftrightarrow \Big((\forall z)\big((z \in x) \Leftrightarrow (z \in y)\big)\Big)\Big)$$

3. **Paarmengenaxiom**: Für je zwei Mengen A, B existiert die Menge $\{A, B\}$.
$$(\forall x)(\forall y)(\exists z)(\forall u)\Big((u \in z) \Leftrightarrow \big((u = x) \vee (u = y)\big)\Big)$$

4. **Vereinigungsmengenaxiom**: Für jede Menge A gibt es eine Menge $\bigcup A$ deren Elemente die Elemente der Elemente von A sind.
$$(\forall x)(\exists y)(\forall z)\Big((z \in y) \Leftrightarrow \big((\exists u)\big((u \in x) \wedge (z \in u)\big)\big)\Big)$$

5. **Potenzmengenaxiom**: Für jede Menge A existiert die **Potenzmenge** $\mathcal{P}(A)$ die alle Teilmengen von A als Elemente enthält.
$$(\forall x)(\exists y)(\forall z)\Big((z \in y) \Leftrightarrow \big((\forall u \in z)(u \in x)\big)\Big)$$

6. **Sondierungsaxiom**: Für jede Menge A und jede Aussageform $p(x)$ existiert die Menge $\{A' \in A\colon\ p(A')\}$, die Teilmenge von A deren Elemente $p(x)$ erfüllen.
$$(\forall x)(\exists y)(\forall z)\Big((z \in y) \Leftrightarrow (z \in x) \wedge p(z)\Big)$$

Folgerungen aus den ersten sechs Axiomen

- Aus den ersten beiden Axiomen ergibt sich, dass es genaue eine **leere Menge** gibt, welche wir mit $\emptyset$ bezeichnen.
- Wegen des Extensionalitätsaxioms enthält jede Menge jedes ihrer Elemente genau einmal. Genauer, da $\{A, B, B\}$ und $\{A, B\}$ dieselben Elemente enthalten gilt $\{A, B, B\} = \{A, B\}$.
- Das Paarmengenaxiom kann auch für den Fall $B = A$ angewandt werden. Dann besagt es (zusammen mit dem Extensionalitätsaxiom), dass $\{A, A\} = \{A\}$ für jede Menge A eine Menge ist.
- Das Paarmengenaxiom zusammen mit dem Vereinigungsaxiom ergibt, dass die Vereinigung der Elemente zweier Mengen wieder eine Menge ist. D. h. für alle Mengen A und B gibt es die Menge
$$A \cup B := \bigcup \{A, B\},$$
welche alle Elemente aus A und alle Elemente aus B als Elemente enthält.
- Das Vereinigungsaxiom zusammen mit dem Sondierungsaxiom ergibt für jede Menge A die Existenz der Schnittmenge $\bigcap A$, welches nur die Elemente enthält die in jedem Element von A enthalten sind
$$\bigcap A := \left\{A'' \in \bigcup A \colon\ (\forall A' \in A)(A'' \in A')\right\}.$$
Anstelle von $\bigcap\{A, B\}$ schreiben wir $A \cap B$.
Falls $A \cap B = \emptyset$, dann sind die beiden Mengen A und B **disjunkt**.
- Eine weitere Folgerung des Sondierungsaxioms ist die Existenz der **Differenz(menge)** zweier Mengen A und B
$$A \setminus B := \{A' \in A \colon\ A' \notin B\}.$$

Axiome der Mengenlehre   Teil 2

7 **Unendlichkeitsaxiom**: Es gibt eine Menge N, die die leere Menge als Element enthält und für jede Menge A, die ein Element von N ist, auch den **Nachfolger** $A^+ := A \cup \{A\}$ in N als Element enthält.

$$(\exists x)\Big((\emptyset \in x) \wedge (\forall y \in x)((y \cup \{y\}) \in x)\Big)$$

8 **Ersetzungsaxiom**: Das „Bild einer Menge unter einer Funktion" ist eine Menge. Für jede Aussagenform $p(x, y)$ mit der Eigenschaft, dass für jede Menge A genau eine Menge B existiert für die $p(A, B)$ gilt, und für jede Menge M ist die Zusammenfassung der N', für die eine $N \in M$ mit $p(N, N')$ existiert, eine Menge.

$$(\forall x)(\exists y)(\forall z)\big((z \in y) \Leftrightarrow ((\exists u \in x)p(u, z))\big)$$

9 **Fundierungsaxiom**: Jede nicht leere Menge A enthält ein Element A', deren Schnitt mit A leer ist.

$$\big((\forall x)(x \neq \emptyset)\big) \Rightarrow \big((\exists y \in x)(\forall z \in y)(z \notin x)\big)$$

10 **Auswahlaxiom**: Für jede nicht leere Menge A bestehend aus paarweise disjunkten nicht leeren Mengen existiert eine Menge B, die aus jeder Menge $A' \in A$ genau ein Element enthält.

$$(\forall x)\Big(\big((\forall y \in x)(y \neq \emptyset)\big) \wedge (\forall y \in x)(\forall z \in x)\big((y \neq z) \Rightarrow (y \cap z = \emptyset)\big)\Big)$$
$$\Rightarrow (\exists u)(\forall y \in x)(\exists! z \in y)(z \in u)$$

Hierbei steht $\exists!$ für „es existiert genau ein", d. h. $(\exists! x)p(x)$ ist genau dann **wahr**, wenn die Aussage $(\exists x)\big(p(x) \wedge (\forall y)((y \neq x) \Rightarrow \neg p(y))\big)$ wahr ist.

Bemerkungen

- Streng genommen darf man in den formalen Beschreibungen der Axiome (7-10) nicht die leere Menge, $\cup$, $\cap$ benutzen. Man kann (mit etwas Übung) überprüfen, dass es „reine" Aussagen gibt, die genau dasselbe besagen.
- Axiome 1-7 gehen auf die Arbeiten von Zermelo zurück und das Ersetzungs- und das Fundierungsaxiom wurden von Fraenkel, Skolem und von Neumann hinzugefügt. Axiome 1-9 werden nach Zermelo und Fraenkel als **ZF** bezeichnet. Das Auswahlaxiom (Axiom of **C**hoice) wird manchmal auf Grund seiner Konsequenzen kritisch gesehen. (Z. B. wird in Beweisen manchmal extra darauf hingewiesen, wenn Konsequenzen des Auswahlaxioms benötigt werden.) Axiome 1-10 werden typischerweise mit **ZFC** bezeichnet.
- Es folgt aus dem Fundierungsaxioms (zusammen mit dem Paarmengenaxiom), dass für Mengen A und B niemals sowohl $A \in B$, als auch $B \in A$ gelten kann. Insbesondere gibt es keine Menge A mit $A \in A$.

$\Rightarrow$ „Menge aller Mengen" ist keine Menge und ist eine echte Klasse

$\Rightarrow$ Vermeidung von Russels Paradoxon

Kapitel 4

Natürliche Zahlen

Induktive Mengen

Definition (induktive Menge)

Eine Menge N heißt **induktiv**, falls N die Eigenschaft des Unendlichkeitsaxioms erfüllt, d. h. $\emptyset \in N$ und für alle $A \in N$ ist der **Nachfolger** $A^+ := A \cup \{A\}$ ein Element von N.

Lemma 1

Falls alle Elemente von $A \neq \emptyset$ induktiv sind, dann ist $\bigcap A$ induktiv.
Insbesondere ist die Schnittmenge zweier induktiver Mengen wieder induktiv.

Beweis.

- Da alle Elemente von A induktive Mengen sind, gilt $\emptyset \in A'$ für alle $A' \in A$.
  $\Rightarrow \emptyset \in \bigcap A$ ✓
- Sei $B \in \bigcap A$ beliebig.
  $\Rightarrow B \in A'$ für alle $A' \in A$
  Da alle Elemente von A induktive Mengen sind, gilt $B^+ \in A'$ für alle $A' \in A$.
  $\Rightarrow B^+ \in \bigcap A$ ✓

$\square$

Satz 2

Es gibt genau eine induktive Menge, die Teilmenge einer jeden induktiven Menge ist.

Beweis.

- Unendlichkeitsaxiom $\Rightarrow$ es existiert eine induktive Menge A
- Potenzmengen- und Sondierungsaxiom $\Rightarrow$ es gibt $B := \{B' \in \mathcal{P}(A) \colon\ B' \text{ induktiv}\}$
- da $A \in B$, gilt $B \neq \emptyset$ und somit ist wegen Lemma 1 die Menge $C := \bigcap B$ induktiv

Beh.: Die Menge C hat die gesuchte Eigenschaft.

„$\subseteq$" Sei D eine beliebige induktive Menge.
$\Rightarrow$ Teilmenge $D \cap A$ von A ist induktiv (Lemma 1) $\Rightarrow (D \cap A) \in B$
$\Rightarrow C \subseteq (D \cap A) \Rightarrow C \subseteq D$ ✓

„$\exists!$" Angenommen C' ist induktive Menge, die in jeder induktiven Menge enthalten ist.
$\Rightarrow$ insbesondere $C' \subseteq C$, aber es gilt $C \subseteq C'$ (wegen „$\subseteq$"-Teil oben)
$\Rightarrow C' = C$ nach dem Extensionalitätsaxiom ✓

$\square$

Natürliche Zahlen

Satz 2

Es gibt genau eine induktive Menge, die Teilmenge einer jeden induktiven Menge ist.

Bemerkung: Jede induktive Menge enthält die Elemente $\emptyset$, $\{\emptyset\}$, $\{\emptyset, \{\emptyset\}\}$, $\{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}$, usw. und die Menge aus Satz 2 enthält auch keine anderen.

Definition (natürliche Zahlen - $\mathbb{N}$)

Die induktive Menge aus Satz 0.1 identifizieren wir mit der Menge der **natürlichen Zahlen**, welche wir mit $\mathbb{N}$ bezeichnen. D. h. jedes Element der induktiven Menge $\mathbb{N}$ entspricht einer natürlichen Zahl.

Wir führen folgende (vereinfachende) Schreibweisen ein:

$0 := \emptyset = \{\}$, kleinste natürliche Zahl (hier)

$1 := 0^+ = \{\emptyset\} = \{0\}$,

$2 := 1^+ = \{\emptyset, \{\emptyset\}\} = \{0, 1\}$,

$3 := 2^+ = \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\} = \{0, 1, 2\}, \ldots$

Wir sagen eine natürliche Zahl n ist **kleiner** (bzw. **kleiner gleich**) einer natürlichen Zahl m und schreiben $n < m$ (bzw. $n \leq m$), falls gilt $n \in m$ (bzw. $n \in m^+$).

Beweisprinzip der vollständigen Induktion

Korollar 3

Jede induktive Teilmenge von $\mathbb{N}$ ist gleich $\mathbb{N}$.

Beweis.

Falls $M \subseteq \mathbb{N}$ induktiv ist, dann gilt wegen Satz 2 und der Definition von $\mathbb{N}$ auch $\mathbb{N} \subseteq M$ und somit wegen des Extensionalitätsaxioms auch $M = \mathbb{N}$. $\square$

Korollar 4 (vollständige Induktion)

Sei $p(x)$ eine Aussageform. Falls

Induktionsanfang: $p(0)$ wahr ist (d. h. $p(\emptyset)$ ist wahr) und

Induktionsschritt: für alle $n \in \mathbb{N}$ gilt die Implikation: $p(n) \Rightarrow p(n^+)$,

dann gilt $p(n)$ für alle $n \in \mathbb{N}$.

Beweis.

Nach dem Induktionsanfang und dem Induktionsschritt folgt, dass die Menge der $n \in \mathbb{N}$ für die $p(n)$ gilt eine induktive Teilmenge von $\mathbb{N}$ ist. Also folgt Korollar 4 wegen Korollar 3. $\square$

Beispiel - vollständige Induktion

Korollar 4 (vollständige Induktion)

Sei $p(x)$ eine Aussageform. Falls

Induktionsanfang: $p(0)$ wahr ist (d. h. $p(\emptyset)$ ist wahr) und

Induktionsschritt: für alle $n \in \mathbb{N}$ gilt die Implikation: $p(n) \Rightarrow p(n^+)$,

dann gilt $p(n)$ für alle $n \in \mathbb{N}$.

Beispiele: (gewohnte Arithmetik der natürlichen Zahlen aus der Schule vorausgesetzt)

Beh.: Die Summe der natürlichen Zahlen $\leq n$ ist $\frac{n(n+1)}{2}$.

Induktionsanfang ($n = 0$): $0 = \frac{0 \cdot (0+1)}{2}$ ✓

Induktionsannahme $(*)$ (für n): es gelte $0 + 1 + \cdots + n = \frac{n(n+1)}{2}$

Induktionsschritt (von n nach $n + 1$):

$$0 + 1 + \cdots + n + (n+1) = (0 + 1 + \cdots + n) + (n+1) \overset{(*)}{=} \frac{n(n+1)}{2} + (n+1)$$

$$= \frac{n(n+1) + 2(n+1)}{2} = \frac{(n+2)(n+1)}{2} = \frac{(n+1)(n+2)}{2} \quad \checkmark$$

$\square$

Varianten vollständiger Induktion

Varianten

1. Induktionsanfang (IA) für n_0 und Induktionsschritt (IS) von jedem $n \geq n_0$ nach n^+
   $\Rightarrow p(n)$ gilt für alle $n \in \mathbb{N}$ mit $n \geq n_0$
2. IA für n_0 und n_0^+ und IS für jedes $n \geq n_0$ von n und n^+ nach $(n^+)^+$
   $\Rightarrow p(n)$ gilt für alle $n \in \mathbb{N}$ mit $n \geq n_0$
3. IA für n_0 und IS für jedes $n \geq n_0$ gilt die Implikation $(p(n_0) \wedge \cdots \wedge p(n)) \Rightarrow p(n^+)$
   $\Rightarrow p(n)$ gilt für alle $n \in \mathbb{N}$ mit $n \geq n_0$
4. Doppelte Induktion: Aussage $(\forall m \in \mathbb{N})(\forall n \in \mathbb{N}) p(m, n)$

   (i) Zeige: $p(0, 0)$ (IA)

   (ii) Zeige für alle m, $n \in \mathbb{N}$: $p(m, n) \Rightarrow p(m, n^+)$ (innerer IS)

   (iii) Zeige für alle $m \in \mathbb{N}$: $\big((\forall n \in \mathbb{N}) p(m, n)\big) \Rightarrow p(m^+, 0)$ (äußerer IS)

Bemerkungen:

- es gibt offensichtliche Verallgemeinerungen von 2 und 4
- oftmals lässt sich Doppelinduktion vermeiden und durch einfache Induktion nach $m + n$ ersetzen

Vorgänger

Definition (Vorgänger)

Falls $m^+ = n$, dann heißt m **Vorgänger** von n.

Satz 5

Für jede natürliche Zahl $n \neq 0$ gibt es genau einen Vorgänger n^- mit $(n^-)^+ = n$.

Beweis.

„$\exists$" Annahme: $n \in \mathbb{N}$ mit $n \neq 0$ hat keinen Vorgänger
$\Rightarrow$ $\mathbb{N} \setminus \{n\}$ ist induktive Menge
$\Rightarrow$ Widerspruch zu Korollar 3 ✓

„$\exists!$" Annahme: $n = m_1^+$ und $n = m_2^+$ mit $m_1 \neq m_2$
$\Rightarrow$ $n = m_1 \cup \{m_1\}$ und $n = m_2 \cup \{m_2\}$, also $m_1 \in n$ und $m_2 \in n$
$\Rightarrow$ da $m_1 \neq m_2$ gilt $m_2 \in n \setminus \{m_1\}$ und wegen $n \setminus \{m_1\} = m_1$, folgt $m_2 \in m_1$
$\Rightarrow$ gleiche Argumentation mit m_1 und m_2 vertauscht ergibt $m_1 \in m_2$
$\Rightarrow$ Widerspruch in **ZFC** (siehe Bemerkungen nach den Axiomen) ✓

□

Addition in $\mathbb{N}$

Definition (Addition „+“)

Wir definieren rekursiv die **Summe** $n + m$ zweier natürlicher Zahlen n und m wie folgt:

$$m + n := \begin{cases} 0, & \text{falls } m = 0 \text{ und } n = 0, \\ m, & \text{falls } m > 0 \text{ und } n = 0, \\ n, & \text{falls } m = 0 \text{ und } n > 0, \\ ((m^- + n^-)^+)^+, & \text{sonst, d. h. falls } m > 0 \text{ und } n > 0. \end{cases}$$

Insbesondere gilt: $0 + 1 = 1 = 0^+$ und für alle $m > 0$

$$m + 1 = ((m^- + 0)^+)^+ = ((m^-)^+)^+ = m^+ .$$

Satz 6

Die Addition auf $\mathbb{N}$ ist **kommutativ**, d. h. $m + n = n + m$ für alle $m, n \in \mathbb{N}$.

Beweis.

O.B.d.A. sei $m \leq n$ (Warum?). Wir führen Induktion nach n. Für den (IA) sei $n = 0$.
Dann ist $m = 0$ und $m + n = 0 + 0 = 0 = 0 + 0 = n + m$. ✓
Sei nun $n > 0$ und wir nehmen an (Induktionsannahme), dass der Satz bereits für n^- gilt.
Falls $m = 0$ dann folgt aus der Definition $0 + n = n = n + 0$.
Falls $m > 0$, dann folgt aus der Induktionsannahme $m^- + n^- = n^- + m^-$ und somit gilt
$m + n = ((m^- + n^-)^+)^+ = ((n^- + m^-)^+)^+ = n + m$. □

Multiplikation in $\mathbb{N}$

Definition (Multiplikation „·“)

Wir definieren rekursiv das **Produkt** $n \cdot m$ zweier natürlicher Zahlen n und m wie folgt:

$$m \cdot n := \begin{cases} 0, & \text{falls } m = 0 \text{ oder } n = 0, \\ \big((m^- \cdot n^-) + (m^- + n^-)\big) + 1, & \text{sonst, d. h. falls } m > 0 \text{ und } n > 0. \end{cases}$$

Insbesondere: $0 \cdot 1 = 0$ und für alle $m > 0$ gilt

$$m \cdot 1 = ((m^- \cdot 0) + (m^- + 0)) + 1 = (0 + m^-)^+ = (m^-)^+ = m\,.$$

Wir schreiben oftmals abkürzend mn an Stelle von $m \cdot n$.

Satz 7

Die Multiplikation auf $\mathbb{N}$ ist **kommutativ**, d. h. $mn = nm$ für alle $m, n \in \mathbb{N}$.

Beweis.

Sehr ähnlich wie der Beweis von Satz 6. (Tipp: Nutze die Symmetrie der etwas umständlichen Definition der Multiplikation aus.) □

Rechenregeln in $\mathbb{N}$

Satz 8

Die Addition und die Multiplikation in $\mathbb{N}$ sind **assoziativ** und es gilt das **Distributivgesetz**. D. h. für alle a, b, $c \in \mathbb{N}$ gilt:

- $(a + b) + c = a + (b + c)$, — Assoziativität der Addition
- $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ und — Assoziativität der Multiplikation
- $(a + b) \cdot c = (a \cdot c) + (b \cdot c)$. — Distributivgesetz

Notation

- wegen der Assoziativität können wir bei Summen und Produkten auf Klammern verzichten
- bei ungeklammerten gemischten Termen gilt „Punktrechnung vor Strichrechnung“
- wir schreiben $\sum_{i=1}^{k} x_i$ für $x_1 + \cdots + x_k$
- wir schreiben $\prod_{i=1}^{k} x_i$ für $x_1 \cdot \cdots \cdot x_k$
- die leere Summe (z. B. $\sum_{i=1}^{0} x_i$) ergibt 0 und das leere Produkt ergibt 1

Für natürliche Zahlen $a \geq 0$ und $b \geq 1$ zeigen wir erst

$$a + b = (a + b^-)^+ \,. \tag{1}$$

Die Aussage ist offensichtlich, falls $a = 0$ und von nun an nehmen wir an, dass $a \geq 1$.
Wir führen nun Induktion nach b. Falls $b = 1$, dann gilt $a + b = a + 1 = a^+$ und $(a + b^-)^+ = (a + 0)^+ = a^+$, was den Induktionsanfang ergibt. Für den Induktionsschritt (von b nach $b + 1 = b^+$) beobachten wir

$$a + b^+ \overset{\text{Def.}}{=} ((a^- + b)^+)^+ \overset{\text{I.V.}}{=} (((a^- + b^-)^+)^+)^+ \,.$$

Auf der anderen Seite gilt

$$(a + (b^+)^-)^+ = (a + b)^+ \overset{\text{Def.}}{=} (((a^- + b^-)^+)^+)^+ \,,$$

womit (1) bewiesen ist.

Assoziativität von „+“: (Induktion nach c)
Die Fälle $c = 0$ (Induktionsanfang) und $b = 0$ sind offensichtlich. Der Induktionsschritt von c^- nach c folgt durch

$$\begin{aligned}(a+b)+c &\overset{\text{Def.}}{=} (((a+b)^- + c^-)^+)^+ \overset{(1)}{=} (((a+b^-)+c^-)^+)^+ \\ &\overset{\text{I.V.}}{=} ((a+(b^-+c^-))^+)^+ \overset{(1)}{=} (a+(b^-+c^-)^+)^+ \\ &\overset{(1)}{=} (a+(b+c^-))^+ \overset{(1)}{=} a+(b+c^-)^+ \overset{(1)}{=} a+(b+c)\,.\end{aligned}$$

Distributivgesetz: (Induktion nach c)
Wieder sind die Fälle $c = 0$ (Induktionsanfang) und $b = 0$ offensichtlich. Der Induktionsschritt von c^- nach c folgt durch

$$\begin{aligned}(a+b)c &\overset{\text{Def.}}{=} (a+b)^- c^- + (a+b)^- + c^- + 1 \overset{(1)}{=} (a+b^-)\cdot c^- + a + b^- + c \\ &\overset{\text{I.V.}}{=} ac^- + b^- c^- + a + b^- + c = (ac^- + a) + (b^- c^- + b^-) + c \\ &\overset{\text{Def.}}{=} (ac^- + a\cdot 1) + (b^- c^- + b^- \cdot 1) + c \overset{\text{I.V.}}{=} a(c^- + 1) + b^-(c^- + 1) + c \\ &= ac + (b^- c + 1\cdot c) = ac + bc\,.\end{aligned}$$

Assoziativität von „·“: (Induktion nach c)
Wieder sind die Fälle $c = 0$ (Induktionsanfang) und $a = 0$ oder $b = 0$ offensichtlich. Der Induktionsschritt von c^- nach c folgt durch

$$
\begin{aligned}
(ab)c &\overset{\text{„}\cdot\text{“-Def.}}{=} \big((ab)^-c^- + ((ab)^- + c^-)\big) + 1 \\
&\overset{\text{A.+}}{=} ((ab)^-c^- + c^-) + ((ab)^- + 1) \\
&\overset{\text{„}\cdot\text{“-Def.}}{=} ((ab)^-c^- + 1 \cdot c^-) + ((ab)^- + 1) \\
&\overset{\text{D.G.}}{=} ((ab)^- + 1)c^- + ((ab)^- + 1) \\
&\overset{\text{„+“-Def.}}{=} (ab)c^- + ab \\
&\overset{\text{I.V.}}{=} a(bc^-) + ab \\
&\overset{\text{D.G.}}{=} a(bc^- + b) \\
&\overset{\text{„}\cdot\text{“-Def.}}{=} a(bc^- + b \cdot 1) \\
&\overset{\text{D.G.}}{=} a(b(c^- + 1)) \\
&\overset{\text{„+“-Def.}}{=} a(bc)\,.
\end{aligned}
$$

$\square$

Kapitel 5

Relationen und Funktionen

Geordnete Paare und kartesisches Produkt

Definition (Paar)

Eine Menge der Form $\{\{a\},\{a,b\}\}$ heißt **(geordnetes) Paar** (a,b).

Beispiele: $(b,a)=\{\{b\},\{b,a\}\}$ und $(a,a)=\{\{a\}\}$

Proposition 9

Zwei Paare (a,b) und (c,d) sind genau dann gleich, wenn $a=c$ und $b=d$.

Beweis. Übung. $\square$

Definition (Kartesisches Produkt)

Für Mengen A, B heißt

$$A\times B := \{(a,b)\colon\ a\in A \text{ und } b\in B\}$$

das **kartesische Produkt** (auch **Kreuzprodukt**) **von** A **und** B.
Statt $A\times A$ schreibt man auch A^2.
ACHTUNG: Bei der obigen Definition ist nicht klar, dass $A\times B$ eine Menge ist! Aber

$$A\times B=\Big\{C\in\mathcal{P}(\mathcal{P}(A\cup B))\colon\ (\exists a\in A)(\exists b\in B)\big(C=\{\{a\},\{a,b\}\}\big)\Big\}.$$

Relationen

Definition (Relation)

Eine Menge R von Paaren heißt **(zweistellige) Relation**. Für $(a, b) \in R$ schreibt man auch aRb. Falls $R \subseteq A^2$, dann ist R eine **Relation auf** A.

Definition (Eigenschaften von Relationen)

Eine Relation R auf A heißt

- **reflexiv**, falls $(a, a) \in R$ für alle $a \in A$.
- **symmetrisch**, falls für alle a, $b \in A$ gilt: $(a, b) \in R \Rightarrow (b, a) \in R$.
- **antisymmetrisch**, falls für alle a, $b \in A$ gilt: $\big((a, b) \in R$ und $(b, a) \in R\big) \Rightarrow a = b$.
- **transitiv**, falls für alle a, b, $c \in A$ gilt: $\big((a, b) \in R$ und $(b, c) \in R\big) \Rightarrow (a, c) \in R$.

Definition (Spezielle Relationen)

Eine Relation R auf A ist eine

- **Äquivalenzrelation**, falls R reflexiv, symmetrisch und transitiv ist.
- **Teilordnung** (manchmal auch **Halbordnung**, **Ordnung**, **Ordnungsrelation** genannt), falls R reflexiv, antisymmetrisch und transitiv ist.

Funktionen

Definition (Abbildungen und Funktion)

Eine Menge von Paaren f heißt **Abbildung**, falls für alle Paare (a, b) und (a', b') in f gilt: falls $a = a'$, dann $b = b'$.

- Für eine Abbildung $f \subseteq A \times B$ heißt A der **Definitionsbereich** (auch **Urbildbereich**) und B der **Wertebereich** (auch **Bildbereich**).
- Eine Abbildung $f \subseteq A \times B$ ist **auf (ganz)** A **definiert**, falls für jedes $a \in A$ ein $b \in B$ mit $(a, b) \in f$ existiert. Dann ist f eine **Funktion** und wir schreiben $f\colon A \to B$.
- Für zwei Mengen A und B ist
$$B^A := \{f \in \mathcal{P}(A \times B)\colon f\colon A \to B\}$$
die **Menge aller Funktionen von** A **nach** B.
- Für $(a, b) \in f \subseteq A \times B$ schreiben wir auch $f(a) = b$ oder $f\colon a \mapsto b$.
  - Dann heißt b **Bild** (auch **Wert**) **von** a **(unter** f**)** und a heißt **Urbild von** b **(unter** f**)**.
  - Die Menge $\{b \in B\colon \exists a \in A\colon f(a) = b\}$ ist das **Bild von** f und die Menge $\{a \in A\colon \exists b \in B\colon f(a) = b\}$ ist das **Urbild von** f.
  - Allgemeiner für Teilmengen $A' \subseteq A$ und $B' \subseteq B$ ist
$$f(A') := \{b \in B\colon \exists a \in A'\colon f(a) = b\}$$
das **Bild von** A' **(unter** f**)** und
$$f^{-1}(B') := \{a \in A\colon \exists b \in B'\colon f(a) = b\}$$
ist das **Urbild von** B' **(unter** f**)**.

Spezielle Funktionen

Definition (injektiv, surjektiv, bijektiv)

Eine Abbildung $f \subseteq A \times B$ heißt

- **injektiv**, falls für alle a, a' im Urbild mit $a \neq a'$ gilt: $f(a) \neq f(a')$.
- **surjektiv**, falls das Bild von f ganz B ist.
- **bijektiv**, falls f injektiv und surjektiv ist.

Beispiel: Für jede Menge A gibt es eine (natürliche / offensichtliche / triviale / kanonische) Bijektion φ zwischen $2^A = \{0,1\}^A$ und der Potenzmenge $\mathcal{P}(A)$:

$$\varphi\colon \{0,1\}^A \to \mathcal{P}(A)\,,$$

definiert für jede Funktion $f\colon A \to \{0,1\}$ durch

$$\varphi(f) = \{a \in A\colon f(a) = 1\}\,.$$

Den Teilmengen A' von A entsprechen die Funktionen $\varphi^{-1}(A') \in 2^A$.

Wegen dieser Bijektion wird die Potenzmenge von A oft auch mit 2^A bezeichnet.

Identität und Umkehrabbildung

Definition (Identität - id)

Für eine Menge A bezeichnen wir die Funktion $\mathrm{id}_A\colon A \to A$ definiert durch $a \mapsto a$ für alle $a \in A$ als **Identität auf** A. (Offensichtlich ist id_A eine Bijektion.)

Definition (Umkehrabbildung - f^{-1})

Für jede injektive Abbildung $f \subseteq A \times B$ ist auch

$$f^{-1} := \{(b, a) \in B \times A\colon (a, b) \in f\}$$

eine injektive Abbildung (Beweis!). Diese Abbildung heißt **Umkehrabbildung von** f.

Die Abbildung f^{-1} kann natürlich nur surjektiv sein, wenn f auf ganz A definiert ist. Tatsächlich kann man zeigen, dass falls die Funktion $f\colon A \to B$ bijektiv ist, dann ist $f^{-1}\colon B \to A$ auch bijektiv.

ACHTUNG: Entspricht $f^{-1}(B')$ für $B' \subseteq B$ hier dem aus der Definition von Funktion? Ja, denn

$$\{a \in A\colon \exists b \in B'\colon f(a) = b\} \overset{\text{Def. } f}{=} f^{-1}(B') \overset{\text{Def. } f^{-1}}{=} \{a \in A\colon \exists b \in B'\colon f^{-1}(b) = a\}.$$

Operationen mit Funktionen

Definition (Einschränkung - $f|_{A'}$)

Für eine Abbildung $f \subseteq A \times B$ und $A' \subseteq A$ heißt

$$f|_{A'} := f \cap (A' \times B) = \{(a,b) \in f \colon a \in A'\}$$

die **Einschränkung** (auch **Restriktion**) **von** f **auf** A'.

Definition (Verkettung - $g \circ f$)

Für Abbildungen $f \subseteq A \times B$ und $g \subseteq B \times C$ heißt die für jedes a, welches im Definitionsbereich von f liegt und für das $f(a)$ im Definitionsbereich von g liegt, durch

$$a \mapsto g(f(a))$$

definierte Abbildung $g \circ f \subseteq A \times C$ (sprich „g nach f“) die **Verkettung** (auch **Komposition** oder **Hinereinanderausführung**) **der Abbildungen** f **und** g.

Falls $f \colon A \to B$ und $g \colon B \to C$, dann gilt $g \circ f \colon A \to C$.

Kartesisches Produkt

Definition (n-Tupel, Indexmenge)

Sei A eine Menge und $n \in \mathbb{N}$

- Die Notation A^2 wurde zweimal eingeführt (einmal als kartesisches Produkt $A \times A$ und einmal $A^{\{0,1\}}$ als Menge der Funktionen von $\{0,1\}$ nach A.

  Tatsächlich gibt es eine offensichtlich Bijektion φ zwischen diesen beiden Mengen, welche für alle $(a, a') \in A \times A$ durch

  $$\varphi\colon\ (a, a') \mapsto f \in A^{\{0,1\}} \quad \text{mit } f(0) = a \text{ und } f(1) = a'$$

  definiert ist. Deswegen ist diese „Doppelbedeutung" vernachlässigbar.
- Allgemeiner für alle $n \geq 2$ heißt die Menge A^n **n-faches kartesisches Produkt** und die Elemente von A^n heißen **n-Tupel** (Tripel, Quadrupel, Quintupel, ... für $n = 3, 4, 5, \dots$).
- Analog zur Schreibweise für Paare beschreibt man ein n-Tupel (Funktion von $\{0, \dots, n-1\}$ nach A) meist durch Angabe seiner Bilder a_i der Elemente $i = 0, \dots, n-1$ in der Form $(a_0, \dots, a_{n-1})$.
- Noch allgemeiner für eine Menge $\mathcal{I}$ (hier auch **Indexmenge** genannt) deren Elemente wir uns als Indizes vorstellen, heißt $A^{\mathcal{I}}$ auch kartesisches Produkt und man schreibt für $f \in A^{\mathcal{I}}$ an Stelle von $f(i) = a_i$ für alle $i \in \mathcal{I}$ auch $f = (a_i)_{i \in \mathcal{I}}$.

Allgemeines kartesisches Produkt

Definition (Kartesiches Produkt - allgemeiner Fall)

Sei $\mathcal{I}$ eine Menge (Indexmenge) und für jedes $i \in \mathcal{I}$ sei A_i eine Menge. Dann gilt:

- $\mathcal{A} = \{A_i\colon\ i \in \mathcal{I}\}$ ist eine Menge und (folgt aus dem Ersetzungsaxiom)
- $A = \bigcup \mathcal{A}$ ist eine Menge. (folgt aus dem Vereinigungsaxiom)

Wir definieren das **kartesische Produkt der A_i mit $i \in \mathcal{I}$** als

$$\prod_{i \in \mathcal{I}} A_i := \left\{ f \in A^{\mathcal{I}}\colon\ f(i) \in A_i \text{ für alle } i \in \mathcal{I} \right\}.$$

Bemerkung: Interessanterweise braucht man das Auswahlaxiom, um allgemein zeigen zu können, dass

$$\prod_{i \in \mathcal{I}} A_i \neq \emptyset$$

falls $A_i \neq \emptyset$ für alle $i \in \mathcal{I}$. (Warum braucht man $A_i \neq \emptyset$ für alle $i \in \mathcal{I}$ hier?)

Kapitel 6

Äquivalenzrelationen

Äquivalenzrelationen (reflexiv, symmetrisch, transitiv)

Definition (Partition)

Eine Menge $\mathcal{A}$ von Teilmengen einer Menge A heißt **Partition** (oder **Zerlegung**) **von** A, wenn die Elemente von $\mathcal{A}$ nicht-leer sind, paarweise disjunkt sind, und es gilt

$$\bigcup \mathcal{A} = A\,.$$

Bemerkung: Disjunkte Vereinigungen werden wir manchmal mit einem Punkt über dem Vereinigungszeichen anzeigen (z. B. $\dot{\bigcup}\mathcal{A}$, $A \dot{\cup} B$, ...).

Satz 10

Für jede Menge A gilt

(*i*) für jede Partition $\mathcal{A}$ von A ist durch

$$x \sim_{\mathcal{A}} y :\Leftrightarrow\ \exists A' \in \mathcal{A}\colon\ x, y \in A'$$

eine Äquivalenzrelation definiert.

(*ii*) für jede Äquivalenzrelation $\sim$ auf A gibt es genau eine Partition $\mathcal{A}$ von A mit $\sim\, = \,\sim_{\mathcal{A}}$.

Beweis von Satz 10 (i)

Sei $\mathcal{A}$ eine Partition von A und $\sim_{\mathcal{A}}$ wie in der Behauptung definiert. Wir zeigen, dass $\sim_{\mathcal{A}}$ reflexiv, symmetrisch und transitiv ist.

Reflexivität: Sei $a \in A$. Da $A = \bigcup \mathcal{A}$, existiert $A' \in \mathcal{A}$ mit $a \in A'$ und somit $a \sim_{\mathcal{A}} a$.

Symmetrie: Seien a, $b \in A$ mit $a \sim_{\mathcal{A}} b$. D. h. es gibt $A' \in \mathcal{A}$ mit a, $b \in A'$ und somit $b \sim_{\mathcal{A}} a$.

Transitivität: Seien a, b und $c \in A$ mit $a \sim_{\mathcal{A}} b$ und $b \sim_{\mathcal{A}} c$. Nach Definition von $\sim_{\mathcal{A}}$ gibt es A' und $A'' \in \mathcal{A}$ mit a, $b \in A'$ und b, $c \in A''$. Also gilt $b \in A' \cap A''$ und da $\mathcal{A}$ eine Partition ist (paarweise disjunkte Elemente), folgt $A' = A''$. Somit enthält A' neben a und b auch c und es folgt $a \sim_{\mathcal{A}} c$.

$\checkmark$

Beweis von Satz 10 (ii) — Teil 1

Sei $\sim$ eine Äquivalenzrelation auf A.
Zuerst zeigen wir die Existenz einer Partition $\mathcal{A}$ und dann die Eindeutigkeit.

Definition von $\mathcal{A}$: Wir setzen $\mathcal{A} := \{A_a\colon\ a \in A\}$, wobei für jedes $a \in A$

$$A_a := \{b \in A\colon\ a \sim b\}\,.$$

$\mathcal{A}$ ist Partition: Wir müssen zeigen, dass die Mengen in $\mathcal{A}$ nicht-leer sind, paarweise disjunkt sind und ihre Vereinigung ganz A ergibt.

nicht-leer und $\bigcup \mathcal{A} = A$: Da $\sim$ reflexiv ist, gilt $a \sim a$ für jedes $a \in A$ und somit gilt $a \in A_a$. Also ist A_a nicht-leer für jedes $a \in A$ und $\bigcup \mathcal{A}$ enthält jedes $a \in A$, also $\bigcup \mathcal{A} = A$.

disjunkt: Seien A' und A'' Mengen aus $\mathcal{A}$ und sei $a \in A' \cap A''$.
Aus der Definition von $\mathcal{A}$ folgt, dass es $a' \in A$ und $a'' \in A$ gibt, so dass $A' = A_{a'}$ und $A'' = A_{a''}$. Wegen $a \in A_{a'} \cap A_{a''}$, folgt $a' \sim a$ und $a'' \sim a$ und aus der Symmetrie und Transitivität von $\sim$ ergibt sich $a' \sim a''$.
Wir zeigen nun $A' \subseteq A''$. Dafür sei $b \in A'$ beliebig. Es gilt also $a' \sim b$ und wegen der Symmetrie von $\sim$ auch $b \sim a'$. Da wir bereits $a' \sim a''$ gezeigt hatten, folgt wegen der Transitivität auch $b \sim a''$ und eine weitere Anwendung der Symmetrie ergibt $a'' \sim b$. Also ist $b \in A_{a''} = A''$.
Da $b \in A'$ beliebig war, gilt $A' \subseteq A''$. Analoge Argumentation zeigt auch $A'' \subseteq A'$ und somit $A' = A''$, falls $A' \cap A'' \neq \emptyset$.

Beweis von Satz 10 (ii) Teil 2

Als nächstes zeigen wir $\sim \, = \, \sim_{\mathcal{A}}$ und dann die Eindeutigkeit von $\mathcal{A}$.

$\sim \, \subseteq \, \sim_{\mathcal{A}}$: Sei $a \sim b$, also $(a, b) \in \, \sim$. Dann gilt a, $b \in A_a$ und aus der Definition von $\sim_{\mathcal{A}}$ (angewandt für $A' = A_a$) folgt $a \sim_{\mathcal{A}} b$, also $(a, b) \in \, \sim_{\mathcal{A}}$.

$\sim_{\mathcal{A}} \, \subseteq \, \sim$: Sei nun $a \sim_{\mathcal{A}} b$, also $(a, b) \in \, \sim_{\mathcal{A}}$. Dann existiert ein $A' \in \mathcal{A}$ mit a, $b \in A'$.
Wegen der Definition von $\mathcal{A}$ gibt es ein $a' \in A$ mit $A' = A_{a'}$.
Da also a, b aus A' sind, folgt $a' \sim a$ und $a' \sim b$ und mit Symmetrie und Transitivität von $\sim$ auch $a \sim b$. D. h. $(a, b) \in \, \sim$ wie gewünscht.

Eindeutigkeit: Sei $\mathcal{B}$ eine weitere Partition mit $\sim_{\mathcal{B}} \, = \, \sim$. Aus dem bereits Gezeigten folgt also $\sim_{\mathcal{B}} \, = \, \sim \, = \, \sim_{\mathcal{A}}$ und somit gilt für alle a, $b \in A$

$$a \sim_{\mathcal{B}} b \quad \Leftrightarrow \quad a \sim b \quad \Leftrightarrow \quad a \sim_{\mathcal{A}} b\,.$$

Folglich gilt für alle $a \in A$ auch

$$B_a := \{b \in A\colon\ a \sim_{\mathcal{B}} b\} = \{b \in A\colon\ a \sim b\} = A_a\,.$$

Somit ist $\{B_a\colon\ a \in A\} = \mathcal{A}$.
Des Weiteren ist B_a offensichtlich eine Teilmenge der Menge $B' \in \mathcal{B}$, die a enthält. Aber wegen der Transitivität von $\sim_{\mathcal{B}}$ gilt tatsächlich $B_a = B'$. D. h. $\{B_a\colon\ a \in A\} = \mathcal{B}$, also $\mathcal{B} = \mathcal{A}$ was den Beweis von Satz 10 (ii) abschließt.

$\square$

Äquivalenzklassen

Definition (Äquivalenzklassen)

Sei $\sim$ eine Äquivalenzrelation auf A.

- Die eindeutig bestimmte Partition $\mathcal{A}$ aus Satz 10 (ii) bezeichnet man mit $A/{\sim}$ und sie heißt **Faktormenge** (auch **Quotientenmenge**).
- Die Elemente von $A/{\sim}$ heißen **Äquivalenzklassen**, welche man mit $[a]$ (manchmal auch $\overline{a}$) statt A_a bezeichnet.
- Die Elemente einer Äquivalenzklasse sind die **Repräsentanten** dieser Äquivalenzklasse und wir sagen sie sind **äquivalent** zueinander.
- Zwei Elemente a und $b \in A$ repräsentieren also die gleiche Äquivalenzklasse genau dann, wenn sie äquivalent sind
$$[a] = [b] \quad \Leftrightarrow \quad a \sim b\,.$$
- Die Funktion $a \mapsto [a]$ heißt **kanonische Projektion** von A nach $A/{\sim}$.

Beispiel: Partitioniert man $\mathbb{N}$ in die geraden und ungeraden Zahlen und bezeichnet diese Partition mit $\mathcal{A}$, so ist $\sim_{\mathcal{A}}$ die Äquivalenzrelation mit zwei Äquivalenzklassen und zwei Zahlen sind genau denn äquivalent, wenn sie die gleiche Parität haben. Jede ungerade Zahl repräsentiert die Äquivalenzklasse der ungeraden Zahlen usw.

Wie macht man Funktionen injektiv?

Satz 11

Sei $f\colon A \longrightarrow B$ eine Funktion. Für $a, a' \in A$ definiere die Relation $\sim$ durch

$$a \sim a' \quad :\Leftrightarrow \quad f(a) = f(a')\,.$$

Dann ist $\sim$ eine Äquivalenzrelation und $[a] \mapsto f(a)$ eine injektive Funktion $g\colon A/{\sim} \longrightarrow B$.

Sei κ die kanonische Projektion von $\sim$. Dann besagt der Satz, es gibt inj. g mit $f = g \circ \kappa$

$$\begin{tikzcd}
A \arrow[rr, "f"] \arrow[dr, "\kappa"'] & & B \\
& A/{\sim} \arrow[ur, "g"'] &
\end{tikzcd}$$

Beweis.

Zu zeigen ist:

1. $\sim$ ist eine Äquivalenzrelation, ✓
2. g ist wohldefiniert, d. h. $g([a])$ ist unabhängig vom gewählten Repräsentanten! ✓
3. g ist injektiv. ✓

□

Von Quasiordnungen zu Teilordnungen

Definition (Quasiordnung)

Eine reflexive und transitive Relation heißt **Quasiordnung**.

Satz 12

Für jede Quasiordnung $\preccurlyeq$ auf einer Menge A ist durch

$$a \sim b \quad :\Leftrightarrow \quad (a \preccurlyeq b \text{ und } b \preccurlyeq a)$$

eine Äquivalenzrelation auf A definiert. Auf $A/{\sim}$ definiert dann

$$[a] \leq [b] \quad :\Leftrightarrow \quad a \preccurlyeq b$$

eine Teilordnung.

Bemerkung: Die Idee hinter den Sätzen 11 und 12 ist weit verbreitet in der Mathematik.

Die offensichtlichen „Ursachen werden ausfaktorisiert“. So werden alle Urbilder a, a' von f, die gegen die Injektivität verstoßen, in Satz 11 äquivalent gemacht. Genauso werden alle symmetrischen Paare der Quasiordnung aus Satz 12 in $\sim$ „gleichgesetzt“.

Beweis von Satz 12

Der Beweis hat drei Teile:

1. $\sim$ ist eine Äquivalenzrelation,
2. $\leq$ ist wohldefiniert und
3. $\leq$ ist eine Teilordnung.

zu 1: Reflexivität und Transitivität vererben sich von $\preccurlyeq$ und Symmetrie folgt von der Definition von $\sim$.

zu 2: Es ist zu zeigen, dass die Definition unabhängig von den gewählten Repräsentanten ist. D. h. für alle $a' \in [a]$ und $b' \in [b]$ muss gelten:

$$a \preccurlyeq b \quad \Leftrightarrow \quad a' \preccurlyeq b'\,.$$

Es gilt: $a' \in [a] \Rightarrow a' \sim a \Rightarrow a' \preccurlyeq a$ und $a \preccurlyeq a'$.
Ebenso $b' \in [b] \Rightarrow b' \preccurlyeq b$ und $b \preccurlyeq b'$.
Wegen der Transitivität von $\preccurlyeq$ gilt also $a \preccurlyeq b \Rightarrow a' \preccurlyeq a \preccurlyeq b \preccurlyeq b' \Rightarrow a' \preccurlyeq b'$ und ebenso $b \preccurlyeq a \Rightarrow b' \preccurlyeq a'$.

zu 3: Reflexivität und Transitivität vererben sich von $\preccurlyeq$.
Für die Antisymmetrie seien $a, b \in A$ mit $[a] \leq [b]$ und $[b] \leq [a]$. Aus der Definition von $\leq$ folgern wir $a \preccurlyeq b \preccurlyeq a$ und somit $a \sim b$, also $[a] = [b]$. $\square$

Kapitel 7

Ordnungsrelationen und Lemma von Zorn

Teilordnungen (reflexiv, antisymmetrisch, transitiv)

Definition (Notation)

Sei $(A, \leq)$ eine Teilordnung, d. h. $\leq$ ist eine Teilordnung auf A.

- Elemente a, b heißen **(durch $\leq$) vergleichbar**, wenn $a \leq b$ oder $b \leq a$ gilt und sonst heißen sie **unvergleichbar**.
- Für $a \leq b$ schreiben wir alternativ auch $b \geq a$.
- Falls $a \leq b$ und $a \neq b$, dann schreiben wir auch $a < b$ bzw. $b > a$.
- Wir sagen die Menge A ist durch $\leq$ **(teilweise) geordnet**.

Beispiel: Für jede Menge A ist $\mathcal{P}(A)$ durch $\subseteq$ teilweise geordnet.

Proposition 13

Sei R eine Teilordnung auf A und $B \subseteq A$. Dann ist $R \cap B^2$ wieder eine Teilordnung. Sie heißt die durch R auf B **induzierte** Teilordnung.

Beweis.

Reflexivität, Antisymmetrie und Transitivität vererben sich von R auf $R \cap B^2$. $\square$

Vollständige Ordnung, Extrema, Wohlordnung

Definition (Vollständige Ordnungen und Ketten)

Sei $(A, \leq)$ eine Teilordnung.

- Die Relation $\leq$ heißt **vollständige** (oder **lineare**) Ordnung (oder auch **Totalordnung**) auf A, wenn je zwei Elemente von A durch $\leq$ vergleichbar sind.
- Eine Teilmenge $B \subseteq A$ heißt **Kette** (bezüglich $\leq$), wenn $\leq$ auf B eine vollständige Ordnung induziert.

Definition (Extrema)

Sei $(A, \leq)$ eine Teilordnung. Ein Element $a \in A$ heißt

- **maximal** (bzw. **minimal**) in A, wenn es kein $b \in A$ mit $a < b$ (bzw. $b < a$) gibt.
- **größtes** (bzw. **kleinstes**) Element in A, wenn $\forall b \in A$ gilt $b \leq a$ (bzw. $a \leq b$).
- **obere** (bzw. **untere**) **Schranke** für eine Menge B, wenn $\forall b \in B$ gilt $b \leq a$ (bzw. $a \leq b$).

Bemerkungen:

- obere (bzw. untere) Schranken a von B müssen nicht in B liegen
- größte (bzw. kleinste) Elemente sind immer eindeutig bestimmt (Antisymmetrie!)
- $\max A$ (bzw. $\min A$) bezeichnen das größte (bzw. kleinste) Element von $A \subseteq X$ (in der induzierten Teilordnung) falls es existiert

Definition (Wohlordnungen)

Eine vollständige Ordnung auf A heißt **Wohlordnung**, falls jede nicht-leere Teilmenge B von A ein (in der induzierten Ordnung) kleinstes Element enthält, welches mit $\min B$ bezeichnet wird.

Zorns Lemma, Wohlordnungssatz und Auswahlaxiom

Satz 14 (Zorn'sche Lemma – Zorn 1935, Kuratowski 1922)

Hat in einer teilweise geordneten nicht leeren Menge X jede Kette eine obere (bzw. untere) Schranke, dann enthält X ein maximales (bzw. minimales) Element.

Satz 15 (Wohlordnungssatz)

Für jede Menge existiert eine Wohlordnung. □

Bemerkungen:

- Das Zorn'sche Lemma, der Wohlordnungssatz und das Auswahlaxiom sind äquivalent.

  D. h. in dem Axiomensystem **ZFC** kann man das Auswahlaxiom durch Zorns Lemma oder auch durch den Wohlordnungssatz ersetzen und erhält ein gleichmächtiges Axiomensystem.

Beweis von Zorns Lemma – Vorbereitungen Teil 1

Definition (Auswahlfunktion)

Eine Funktion $f\colon A \to \bigcup A$ heißt **Auswahlfunktion**, wenn sie jeder nicht-leeren Menge $B \in A$ ein Element $f(B) \in B$ zuordnet.

Proposition 16

Für jede Menge A gibt es eine Auswahlfunktion.

Beweis.

- Ersetzungsaxioms $\Rightarrow A' = \{\{B\} \times B\colon\ B \in A \text{ mit } B \neq \emptyset\}$ ist eine Menge
- Elemente von A' sind paarweise disjunkt
- Auswahlaxiom $\Rightarrow$ es gibt eine Menge F mit der Eigenschaft: für jedes $B' \in A'$ enthält F genau ein Element aus B'
- jedes $B' \in A'$ hat die Form $B' = \{B\} \times B = \{(B, b)\colon\ b \in B\}$ für ein $B \in A$

$\Rightarrow$ F enthält für jedes $B \in A$ genau ein Element der Form (B, b) mit $b \in B$

$\Rightarrow$ Auswahlfunktion $f \subseteq F$ existiert $(f = F \cap (\bigcup A'))$ $\square$

Bemerkung: Der Übergang von F nach f ist nötig, da in der hier gewählten Formulierung des Auswahlaxioms nicht gefordert wird, dass F aus nichts weiter besteht, als den eindeutigen Elementen aus jeder Menge aus A'.

Beweis von Zorns Lemma – Vorbereitungen Teil 2

Definition (Anfangsstücke)

Sei $(X, \leq)$ eine Teilordnung (Menge X mit Teilordnung $\leq$ auf X). Eine Teilmenge $A \subseteq X$ heißt **Anfangsstück von** X, falls alle $x \in X$ mit $x \leq a$ für ein $a \in A$ auch in A enthalten sind.

Beobachtung: Falls $\leq$ eine Wohlordnung auf X definiert und $A \subseteq X$, dann existiert $y = \min(X \setminus A)$ und A ist genau dann ein Anfangsstück, wenn $A = \{x \in X \colon x < y\}$.

Proposition 17

Sei $(X, \leq)$ eine Teilordnung und sei $\mathscr{K}$ eine Menge von Ketten in X die durch $\leq$ wohlgeordnet sind. Falls alle Ketten K und $L \in \mathscr{K}$ die Eigenschaft haben, dass eine das Anfangsstück der anderen ist (in der jeweils induzierten Teilordnung), dann gilt

1. jede Kette $K \in \mathscr{K}$ ist Anfangsstück von $Y := \bigcup \mathscr{K} \subseteq X$ und
2. Y ist durch $\leq$ wohlgeordnet.

Beweis.

Wir schreiben $K \preccurlyeq L$, falls K ein Anfangsstück von $(L, \leq)$ ist.

1. Sei $K \in \mathscr{K}$ und $x \in Y \setminus K$ mit $x \leq y \in K \Rightarrow \exists L \in \mathscr{K}$ mit $x \in L \Rightarrow K \preccurlyeq L \Rightarrow x \in K$ ↯
2. Seien x, $y \in Y$ mit $x \in K \in \mathscr{K}$ und $y \in L \in \mathscr{K}$ und o. B. d. A. $K \preccurlyeq L$.
   $\Rightarrow$ entweder ($y \in L \setminus K$ und damit $y > x$) oder (x, $y \in K$ und somit vergleichbar) ✓
   Sei $Z \subseteq Y \Rightarrow \exists K \in \mathscr{K}$ mit $Z \cap K \neq \emptyset$ und wir setzen $z_0 = \min(Z \cap K)$
   Sei $z \in Z$. Falls $z \in Z \cap K$, dann $z_0 \leq z$. Falls $z \in L \setminus K \Rightarrow K \preccurlyeq L \Rightarrow z > z_0$. ✓

□

Knesers Beweis von Zorns Lemma

Widerspruchsbeweis: Sei $(X, \leq)$ Teilordnung ohne maximales Element, für die für jede Kette eine obere Schranke existiert. Wir fixieren

f eine Auswahlfunktion von $\mathcal{P}(X)$

und für wohlgeordnete Ketten K (Teilmenge von X die durch $\leq$ wohlgeordnet wird) und $y \in K$

$K_{<y} := \{z \in K \colon z < y\}$ Teilkette unterhalb y

$K_{>} := \{x \in X \colon x > y \text{ für alle } y \in K\} \neq \emptyset$ Menge der oberen Schranken von K in $X \setminus K$

$g(K) := f(K_{>})$, beachte: $g(\emptyset) = f(X)$

- wohlgeordnete Kette K ist g-**bestimmt**, falls für alle $y \in K$ gilt $y = g(K_{<y})$.

Behauptung: Von je zwei g-bestimmten Ketten K und L ist eine das Anfangsstück der anderen.

Beweis der Behauptung.

- Sei J die Vereinigung aller Anfangsstücke von X die Anfangsstücke von K und von L sind.

$\Rightarrow$ J ist inklusionsmaximales Anfangsstück von K und von L

- Angenommen $J \neq K$ und $J \neq L$ (sonst wären wir fertig)

$\Rightarrow$ es gibt $y_K = \min(K \setminus J)$ und $y_L = \min(L \setminus J)$, da K und L wohlgeordnet sind

$\Rightarrow$ $y_K = g(J) = y_L$, da K und L g-bestimmt sind

$\Rightarrow$ $J \cup \{y_K\} = J \cup \{y_L\} \supsetneq J$ ist Anfangsstück von K und L $\quad$ ↯ J ist inklusionsmaximal $\square$

Sei Y die Vereinigung aller g-bestimmten Ketten.

- Proposition 17 $\Rightarrow$ Y ist eine Kette
- Y ist inklusionsmaximale g-bestimmte Kette (Warum ist Y wieder g-bestimmt?)
- Aber: $Y \cup \{g(Y)\} \supsetneq Y$ ist ebenfalls g-bestimmte Kette ↯ $\square$

Vollständige Ordnung $(\mathbb{N}, \leq)$

Erinnerung: $m \leq n \;:\Leftrightarrow\; m \in n^+$
Beobachtung: $m \in n \Rightarrow m \subseteq n$ (Beweis: Induktion)

Proposition 18

Das auf $\mathbb{N}$ bereits definierte $\leq$ ist eine vollständige Ordnung auf $\mathbb{N}$.

Beweis.

Reflexivität: $n^+ = n \cup \{n\} \Rightarrow n \in n^+ \Rightarrow n \leq n$ ✓

Antisymmetrie: $m \leq n$ und $n \leq m \Rightarrow m \in n^+ = n \cup \{n\}$ und $n \in m \cup \{m\}$
falls $m \neq n$, dann $m \in n$ und $n \in m$ $\lightning$ (Fundierungsaxiom)

Transitivität: $\ell \leq m$ und $m \leq n \Rightarrow$ falls $\ell \neq m$ und $m \neq n$, dann $\ell \in m$ und $m \in n$ und wegen der Beobachtung $\ell \in m \subseteq n \Rightarrow \ell \leq n$

Vollständigkeit: Induktiv über m: $\forall n \in \mathbb{N} : m \in n$ oder $m = n$ oder $n \in m$.

$m = 0 = \emptyset$: $n = 0$: ✓ $n \to n^+$: $n^+ = n \cup \{n\} \supset n \overset{\text{IA}}{\Longrightarrow} \emptyset \in n$ oder $n = \emptyset \Rightarrow \emptyset \in n^+$ ✓
$m \to m^+$, $n \in \mathbb{N}$: IA $\Rightarrow m \in n$ oder $m = n$ oder $n \in m$
falls $m = n$, dann $n \in m^+$ ✓
falls $n \in m$, dann $n \in m \subset m^+$ ✓
falls $m \in n$, beweise induktiv über n, dass dann $m^+ = n$ oder $m^+ \in n$: ($n = 0$ klar)
$n \to n^+$: $m \in n^+ \Rightarrow m \in n$ oder $m = n \overset{\text{IA}(n)}{\Longrightarrow} (m^+ = n$ oder $m^+ \in n)$ oder $m^+ = n^+$
$\Longrightarrow m^+ \in n^+$ oder $m^+ = n^+$ ✓

□

Wohlordnung $(\mathbb{N}, \leq)$

Korollar 19

Die vollständige Ordnung $(N, \leq)$ ist eine Wohlordnung.

Beweis.

Angenommen, $M \subseteq \mathbb{N}$ habe kein kleinstes Element.

Wir zeigen mit Induktion, dass $n \notin M$ gilt für alle $n \in \mathbb{N}$. Dann ist M leer, wie behauptet.

Es sei $n \in \mathbb{N}$ gegeben. Wir nehmen $m \notin M$ für alle $m < n$ an (IA) und zeigen $n \notin M$.

Wäre $n \in M$, so wäre n nach Induktionsannahme minimal mit dieser Eigenschaft in $\mathbb{N}$, und damit erst recht in $M \subseteq \mathbb{N}$. Als minimales Element von M wäre n aber auch sein kleinstes, denn die von $\mathbb{N}$ auf M induzierte Ordnung ist auch auf M vollständig. Dies widerspricht der Voraussetzung. Somit gilt $n \notin M$, wie behauptet. $\square$

Kapitel 8

Mächtigkeiten, Kardinalitäten

Mächtigkeiten

Definition (Kardinalitäten)

Für Mengen A und B schreiben wir:

- $|A| = |B|$, falls es eine bijektive Funktion $f\colon A \to B$ gibt. Die Mengen A und B heißen dann **gleichmächtig**.
- $|A| \leq |B|$, falls es eine injektive Funktion $f\colon A \to B$ gibt.
- $|A| < |B|$, falls $|A| \leq |B|$ gilt aber nicht $|A| = |B|$.

Für $n \in \mathbb{N}$ schreiben wir $|A| = n$ statt $|A| = |n|$.

Beispiele:

- $|A| = 1001$ bedeutet, dass es eine bijektive Funktion von A nach $\{0, \dots, 1000\}$ gibt.
- $|\mathbb{N}| = |\mathbb{N} \setminus \{0\}|$, da $n \mapsto n^+$ eine bijektive Funktion ist (Injektivität folgt aus der Eindeutigkeit des Vorgängers und Surjektivität mit Induktion).
- $|\mathbb{N} \times \mathbb{N}| = |\mathbb{N}|$, da z. B. $(x, y) \mapsto \frac{1}{2}(x + y)(x + y + 1) + y$ eine bijektive Funktion zwischen den beiden Mengen ist.

Gibt es $|A| \neq |B|$, obwohl $|A| \leq |B| \leq |A|$?

Satz 20 (Cantor, Schröder, Bernstein 1895-97; Dedekind 1887)

Für je zwei Mengen A und B folgt aus $|A| \leq |B|$ und $|B| \leq |A|$, dass $|A| = |B|$.

Beweis.

Seien also $f\colon A \to B$ und $g\colon B \to A$ injektive Funktionen. Da wegen der Injektivität von f gilt $|A| = |f(A)|$, können wir o. B. d. A. annehmen, dass $A \subseteq B$ und $f = \mathrm{id}_A$. Setze

$$C = \bigcap \Big\{ D \in \mathcal{P}(B)\colon (B \setminus A) \subseteq D \text{ und } g(D) \subseteq D \Big\}.$$

Da $g(B) \subseteq B$ und $B \supseteq (B \setminus A)$ erfolgt der Schnitt nicht über die leere Menge und somit gilt C ist inklusionsminimal mit den beiden Eigenschaften $C \supseteq (B \setminus A)$ und $g(C) \subseteq C$, d. h. jede Menge $C' \subseteq B$ mit denselben beiden Eigenschaften enthält C als Teilmenge.

- $g(B) \subseteq A \Rightarrow g(C) \subseteq C \cap A$, d. h. $g|_C\colon C \to C \cap A$ ist injektiv
- falls $x \in (C \cap A) \setminus g(C)$, dann widerspricht $C' = C \setminus \{x\}$ der Minimalität von C

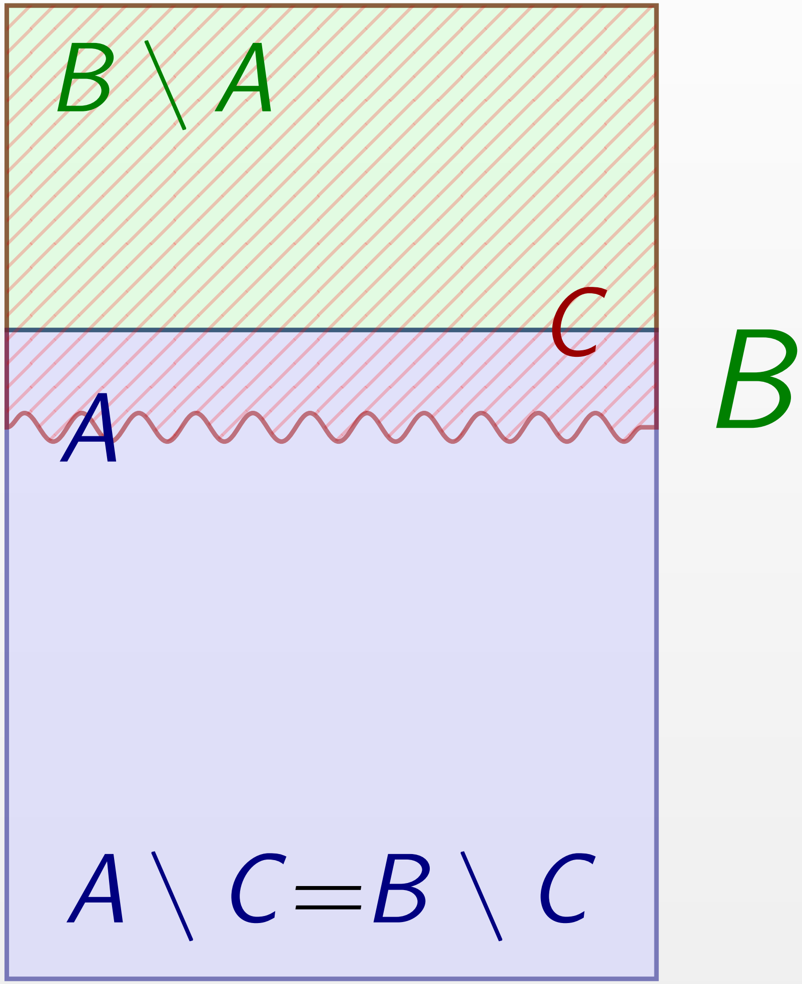
$\Rightarrow$ $g(C) = C \cap A \Rightarrow g|_C$ ist bijektiv

$\Rightarrow$ die Funktion h definiert durch

$$x \mapsto \begin{cases} g(x), & x \in C\,, \\ x, & x \in B \setminus C\,, \end{cases}$$

ist injektiv, auf ganz B definiert und hat als Bild $(C \cap A) \cup (B \setminus C) = A$, da hier $B \setminus C = A \setminus C$ ist (siehe Bild auf der nächste Seite). $\square$

Gibt es $|A| \neq |B|$, obwohl $|A| \leq |B| \leq |A|$?



Kardinalitäten aller Mengen sind vergleichbar

Korollar 21

Für je zwei Mengen A und B gilt immer genau eine der drei Beziehungen $|A| < |B|$, $|A| = |B|$ oder $|A| > |B|$.

Beweis.

Nach Satz 20 reicht es zu zeigen, dass es eine injektive Funktion $A \to B$ oder eine injektive Funktion $B \to A$ gibt.

Wir werden das Lemma von Zorn anwenden. Sei $\mathcal{F} \subseteq \mathcal{P}(A \times B)$ die Menge aller injektiven Abbildungen $f \subseteq A \times B$. Insbesondere muss f nicht auf ganz A definiert sein.

Dann definiert $\subseteq$ eine Teilordnung auf der Menge dieser Abbildungen. Hierbei gilt $f \subseteq g$, falls das Urbild X von f eine Teilmenge vom Urbild von g ist und $f(x) = g(x)$ für alle $x \in X$.

Für eine Kette $K \subseteq \mathcal{F}$ ist deswegen $f_K := \bigcup K$ wieder eine injektive Abbildung aus $\mathcal{F}$ und somit hat jede Kette in $\mathcal{F}$ eine obere Schranke.

Aufgrund von Zorns Lemma gibt es ein maximales injektives $f_M \in \mathcal{F}$. Dann muss gelten, entweder f_M ist auf ganz A definiert und dann sind wir fertig, oder $f_M(A) = B$. Im letzteren Fall ist aber f_M^{-1} eine injektive Funktion von B nach A. □

Größere Mengen und unendliche Mengen

Satz 22 (Cantor 1892)

Für jede Menge A gilt $|A| < |\mathcal{P}(A)|$.

Beweis.

„$\leq$“ $a \mapsto \{a\}$ ist injektive Funktion von A nach $\mathcal{P}(A)$ ✓

„$\neq$“ Angenommen $g\colon A \to \mathcal{P}(A)$ ist surjektiv und sei $A' = \{a \in A\colon a \notin g(a)\}$

$\Rightarrow$ es gibt $a' \in A$ mit $g(a') = A'$, aber dann: $a' \in A' = g(a') \Leftrightarrow a' \notin A'$ ↯ □

Bemerkung: Dieser Beweis inspirierte Russell zu seinem Paradoxon.

Definition (endlich, unendlich, abzählbar, überabzählbar)

Eine Menge A heißt

1. **unendlich** wenn sie zu einer echten Teilmenge von sich gleichmächtig ist und sonst heißt sie **endlich**.
2. **abzählbar**, wenn sie zu einer Teilmenge von $\mathbb{N}$ gleichmächtig ist und sonst heißt sie **überabzählbar**.
3. **abzählbar unendlich**, wenn sie zu $\mathbb{N}$ gleichmächtig ist und eine bijektive Funktion von $\mathbb{N}$ nach A heißt **Aufzählung** von A.

Endliche Mengen

Satz 23

Eine Menge A ist genau dann endlich, wenn es ein $n \in \mathbb{N}$ mit $|A| = n$ gibt.

Beweis (Skizze).

„$\Leftarrow$“ Es ist hinreichend zu zeigen, dass für jedes $n \in \mathbb{N}$ die Menge n endlich ist.
Widerspruchsbeweis:
Sei n die kleinste natürliche Zahl, so dass $n = \{0, \dots, n-1\}$ unendlich ist.
($(\mathbb{N}, \leq)$ ist wohlgeordnet und deswegen muss es ein solches n geben)
$\Rightarrow$ n kann injektiv auf n^- abgebildet werden
$\Rightarrow$ n ist unendlich und $|n| \leq |n^-|$, also ist auch n^- unendlich ↯

„$\Rightarrow$“ Falls $A = \emptyset$, dann ist $A = 0$ und somit $|A| = |0| = 0$. Sei A also nicht-leer und für jedes $n \in \mathbb{N}$ definieren wir rekursiv eine Funktion $f_n \colon n \longrightarrow A$ durch

$$f_{n^+}(m) = f_n(m) \quad \text{für alle } m \leq n$$

und falls $a \in A \setminus \{f_n(0), f_n(1), \dots, f_n(n)\}$ existiert, dann setze

$$f_{n^+}(n^+) = a \quad \text{und} \quad f_{n^+}(n^+) = f_{n^+}(0) = f_n(0) = \dots = f_0(0) \quad \text{sonst.}$$

$\Rightarrow$ f_n ist injektiv genau dann, wenn $|f_n^{-1}(0)| = 1$.
Dann ist $f := \bigcup_{n \in \mathbb{N}} f_n$ eine Funktion von $\mathbb{N}$ nach A mit $f|_n \equiv f_n$ für alle $n \in \mathbb{N}$.
Da A endlich und $\mathbb{N}$ unendlich ist, ist f nicht injektiv.
$\Rightarrow$ Es existiert kleinstes $n \in \mathbb{N}$, so dass f_{n^+} nicht injektiv ist. (Warum?)
$\Rightarrow$ f_n ist injektiv und surjektiv und somit $|A| = n$. □

Kapitel 9

Ganze, rationale und reelle Zahlen

Ganze Zahlen

Idee:

- Die Umkehroperation der Addition, die Subtraktion, kann nicht beliebig innerhalb von $\mathbb{N}$ definiert werden. Z. B. $7 - 12$ liegt nicht in $\mathbb{N}$.
- Erweitere $\mathbb{N}$, um Abgeschlossenheit bezüglich der Subtraktion zu erhalten.
- Definiere die ganze Zahl z als Menge der Paare von natürlichen Zahlen (a, b) mit „$a - b = z$“ (z. B. $(7, 12)$ und $(0, 5)$ sind Repräsentanten von -5).
- Da es aber kein „$-$“ in $\mathbb{N}$ gibt, drücken wir diese Beziehung innerhalb von $\mathbb{N}$ durch „umstellen“ wie folgt aus

$$„\, a - b = a' - b' \,“ \qquad \Leftrightarrow \qquad a + b' = a' + b\,.$$

- Damit definieren wir eine Äquivalenzrelation auf $\mathbb{N}^2$ deren Äquivalenzklassen den ganzen Zahlen entsprechen.

Ganze Zahlen

formale Definition Idee

Definition ($\mathbb{Z}$)

Durch

$$(a,b) \sim (a',b') :\Leftrightarrow a+b' = a'+b \qquad \text{„}a-b=a'-b'\text{“}$$

wird auf $\mathbb{N}^2$ eine Äquivalenzrelation definiert.

Wir bezeichnen die Faktormenge $\mathbb{N}^2/\sim$ mit $\mathbb{Z}$ und nennen ihre Elemente die **ganzen Zahlen**. Ganze Zahlen der Form $[(n,0)]$ bezeichnen wir kürzer durch die natürliche Zahl n und ganze Zahlen der Form $[(0,n)]$ als $-n$.

Die Operationen $+$ und $\cdot$ und die vollständige Ordnung $\leq$ von $\mathbb{N}$ erweitert man auf ganz $\mathbb{Z}$

$$[(a,b)] +_{\mathbb{Z}} [(a',b')] :\Leftrightarrow [(a+a', b+b')] \qquad \text{„}(a-b)+(a'-b')=(a+a')-(b+b')\text{“}$$

$$[(a,b)] \cdot_{\mathbb{Z}} [(a',b')] :\Leftrightarrow [(a\cdot a'+b\cdot b', a\cdot b'+b\cdot a')] \qquad \text{„}(a-b)\cdot(a'-b')=(a\cdot a'+b\cdot b')-(a\cdot b'+b\cdot a')\text{“}$$

und

$$[(a,b)] \leq_{\mathbb{Z}} [(a',b')] :\Leftrightarrow a+b' \leq a'+b \qquad \text{„}(a-b)\leq(a'-b')\text{“}$$

Bemerkung: Man kann zeigen, dass diese Operationen wohldefiniert sind (Übung).

Rationale Zahlen

Idee:

- Vervollständige $\mathbb{Z}$, um Abgeschlossenheit bezüglich der Division zu erhalten.
- Definiere die rationale Zahl q durch ihre Bruchdarstellungen, d. h. das Paar von ganzen Zahlen (a, b) mit $b \neq 0$ soll die rationale Zahl $q = a/b$ repräsentieren und verschiedene Bruchdarstellungen der Selben Zahl q werden gleich (äquivalent) gesetzt.
- Ähnlich wie bei der Darstellung von „$-$“, stellen wir um

$$„\frac{a}{b} = \frac{a'}{b'}“ \qquad \Leftrightarrow \qquad a \cdot_{\mathbb{Z}} b' = a' \cdot_{\mathbb{Z}} b\,.$$

- Damit definieren wir eine Äquivalenzrelation auf $\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$ deren Äquivalenzklassen den rationalen Zahlen entsprechen.

Rationale Zahlen

Definition ($\mathbb{Q}$)

Durch

$$(a,b) \approx (a',b') \;:\Leftrightarrow\; a \cdot_{\mathbb{Z}} b' = a' \cdot_{\mathbb{Z}} b \qquad \text{„}\frac{a}{b} = \frac{a'}{b'}\text{“}$$

wird auf $\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$ eine Äquivalenzrelation definiert.

Wir bezeichnen die Faktormenge $(\mathbb{Z} \times (\mathbb{Z} \setminus \{0\}))/{\approx}$ mit $\mathbb{Q}$ und nennen ihre Elemente die **rationalen Zahlen**. Rationale Zahlen der Form $[(z,1)]$ bezeichnen wir kürzer durch die ganze Zahl z und rationale Zahlen der Form $[(1,z)]$ als $1/z$.

Die Operationen $+_{\mathbb{Z}}$ und $\cdot_{\mathbb{Z}}$ und die vollständige Ordnung $\leq_{\mathbb{Z}}$ aus $\mathbb{Z}$ erweitert man auf ganz $\mathbb{Q}$

$$[(a,b)] +_{\mathbb{Q}} [(a',b')] \;:\Leftrightarrow\; [(a \cdot_{\mathbb{Z}} b' +_{\mathbb{Z}} a' \cdot_{\mathbb{Z}} b\,,\; b \cdot_{\mathbb{Z}} b')] \qquad \text{„}\frac{a}{b} + \frac{a'}{b'} = \frac{a \cdot b' + a' \cdot b}{b \cdot b'}\text{“}$$

$$[(a,b)] \cdot_{\mathbb{Q}} [(a',b')] \;:\Leftrightarrow\; [(a \cdot_{\mathbb{Z}} a'\,,\; b \cdot_{\mathbb{Z}} b')] \qquad \text{„}\frac{a}{b} \cdot \frac{a'}{b'} = \frac{a \cdot a'}{b \cdot b'}\text{“}$$

und

$$[(a,b)] \leq_{\mathbb{Q}} [(a',b')] \;:\Leftrightarrow\; a \cdot_{\mathbb{Z}} b' \leq a' \cdot_{\mathbb{Z}} b \qquad \text{„}\frac{a}{b} \leq \frac{a'}{b'}\text{“}$$

Bemerkung: Man kann zeigen, dass diese Operationen wohldefiniert sind.

Cauchy-Folgen

Definition (Nullfolge, Konvergenz, Cauchy-Folge)

Sei $(q_n)_{n\in\mathbb{N}} \in \mathbb{Q}^{\mathbb{N}}$ eine Folge rationaler Zahlen und $q \in \mathbb{Q}$. Die Folge $(q_n)_{n\in\mathbb{N}}$ heißt

- **Nullfolge**, falls für jede natürliche Zahl $m \geq 1$ ein Index $n_0 \in \mathbb{N}$ existiert, so dass für alle $n_1 \geq n_0$ gilt
$$-\frac{1}{m} \leq q_n \leq \frac{1}{m}\,.$$
- **konvergent gegen** q (geschrieben $q_n \to q$ bzw. $\lim_{n\to\infty} q_n = q$), falls $(p_n)_{n\in\mathbb{N}}$, definiert durch $p_n := q_n - q$, eine Nullfolge ist.
- **Cauchy-Folge**, falls für jede natürliche Zahl $m \geq 1$ ein Index $n_0 \in \mathbb{N}$ existiert, so dass für alle $n_1, n_2 \geq n_0$ gilt
$$-\frac{1}{m} \leq q_{n_1} - q_{n_2} \leq \frac{1}{m}\,.$$

Bemerkung: Aus der Definition folgt, dass eine Folge genau dann eine Nullfolge ist, wenn sie gegen 0 konvergiert.

Arithmetik von Cauchy-Folgen

Proposition 24

Seien $(p_n)_{n\in\mathbb{N}}$ und $(q_n)_{n\in\mathbb{N}}$ Cauchy-Folgen. Dann gilt

1. $(p_n + q_n)_{n\in\mathbb{N}}$ ist eine Cauchy-Folge und
2. $(p_n \cdot q_n)_{n\in\mathbb{N}}$ ist eine Cauchy-Folge.

Beweis.

1. Sei $m \geq 1$. Da $(p_n)_{n\in\mathbb{N}}$ und $(q_n)_{n\in\mathbb{N}}$ Cauchy-Folgen sind, gibt es für $M = 2m$ Indizes $N_{0,p}$ und $N_{0,q}$, so dass insbesondere für alle n_1, $n_2 \geq n_0 := \max\{N_{0,p}, N_{0,q}\}$ gilt
$$-\frac{1}{M} = -\frac{1}{2m} \leq p_{n_1} - p_{n_2} \leq \frac{1}{2m} = \frac{1}{M} \quad \text{und} \quad -\frac{1}{M} = -\frac{1}{2m} \leq q_{n_1} - q_{n_2} \leq \frac{1}{2m} = \frac{1}{M}$$
und somit
$$-\frac{1}{m} = -\frac{1}{2m} - \frac{1}{2m} \leq (p_{n_1} - p_{n_2}) + (q_{n_1} - q_{n_2}) = (p_{n_1} + q_{n_1}) - (p_{n_2} + q_{n_2}) \leq \frac{1}{2m} + \frac{1}{2m} = \frac{1}{m}\,.$$
Da $m \geq 1$ beliebig war, ist also $(p_n + q_n)_{n\in\mathbb{N}}$ eine Cauchy-Folge.
2. Sei $m \geq 1$. Zuerst wählen wir einen Index N groß genug, so dass für alle $n \geq N$ gilt $p_n \leq p_N + 1$ und $q_n \leq q_N + 1$. Als nächstes wählen wir $n_0 \geq N$ (in Abhängigkeit von p_N, q_N und m) groß genug, so dass für alle n_1 und $n_2 \geq n_0$ gilt
$$|p_{n_1} - p_{n_2}| \leq \frac{1}{2m(|q_N| + 1)} \quad \text{und} \quad |q_{n_1} - q_{n_2}| \leq \frac{1}{2m(|p_N| + 1)}\,,$$
wobei für jedes $x \in \mathbb{Q}$ der **Absolutbetrag** $|x|$ von x durch $|x| := \max\{x, -x\}$ definiert ist.
Somit folgt mit $p_{n_1}q_{n_1} - p_{n_2}q_{n_2} = (p_{n_1} - p_{n_2})q_{n_1} + (q_{n_1} - q_{n_2})p_{n_2}$ dann auch
$$|p_{n_1}q_{n_1} - p_{n_2}q_{n_2}| \leq \frac{q_{n_1}}{2m(|q_N|+1)} + \frac{p_{n_2}}{2m(|p_N|+1)} \leq \frac{1}{2m} + \frac{1}{2m} \leq \frac{1}{m}\,.$$

□

Unvollständigkeit von $\mathbb{Q}$

Proposition 25

Jede konvergente Folge ist eine Cauchy-Folge, aber die Umkehrung gilt nicht in $\mathbb{Q}$.

Beweis (konvergent $\Rightarrow$ Cauchy).

Sei $(q_n)_{n\in\mathbb{N}}$ eine Folge die gegen $q \in \mathbb{Q}$ konvergiert. Dann gibt es für jedes $m \geq 1$ ein n_0, so dass $|q_n - q| \leq \frac{1}{2m}$ für jedes $n \geq n_0$. Somit gilt für alle $n_1, n_2 \geq n_0$

$$
\begin{aligned}
|q_{n_1} - q_{n_2}| &= |q_{n_1} - q + q - q_{n_2}| \\
&\overset{(*)}{\leq} |q_{n_1} - q| + |q - q_{n_2}| \\
&\leq \frac{1}{2m} + \frac{1}{2m} \\
&= \frac{1}{m}
\end{aligned}
$$

und $(q_n)_{n\in\mathbb{N}}$ ist deswegen eine Cauchy-Folge. ✓

Bem.: Die einfach zu prüfende Ungleichung $(*)$ heißt auch **Dreiecksungleichung**.

Unvollständigkeit von $\mathbb{Q}$

Proposition 25

Jede konvergente Folge ist eine Cauchy-Folge, aber die Umkehrung gilt nicht in $\mathbb{Q}$.

Beweis (Beispiel nicht-konvergenter Cauchy-Folgen).

Setze $s_0 = 1$ und $t_0 = 2$ und für $n \geq 1$ sei $q_{n-1} = (s_{n-1} + t_{n-1})/2$ und

$$s_n = \begin{cases} q_{n-1}, & \text{falls } q_{n-1}^2 < 2, \\ s_{n-1}, & \text{sonst,} \end{cases} \quad \text{und} \quad t_n = \begin{cases} t_{n-1}, & \text{falls } q_{n-1}^2 < 2, \\ q_{n-1}, & \text{sonst.} \end{cases}$$

Aus der Definition folgt für alle $n \in \mathbb{N}$

- $s_n,\ t_n \in \mathbb{Q}$,
- $s_n < t_n$ und $s_n^2 < 2 < t_n^2$, da für keine rationale Zahl q gilt $q^2 = 2$,
- $s_n \leq s_{n+1}$ und $t_{n+1} \leq t_n$
  $\Rightarrow s_0 \leq s_1 \leq \cdots \leq s_n \leq \cdots <$ „$\sqrt{2}$“ $< \cdots \leq t_n \leq \cdots \leq t_1 \leq t_0$
- $t_n - s_n = (t_{n-1} - s_{n-1})/2 \Rightarrow t_n - s_n = (t_0 - s_0)/2^n = 1/2^n$
  $\Rightarrow |s_{n_1} - s_{n_2}| \leq 1/2^n$ und $|t_{n_1} - t_{n_2}| \leq 1/2^n$ für all $n_1,\ n_2 \geq n$
  $\Rightarrow (s_n)_{n\in\mathbb{N}}$ und $(t_n)_{n\in\mathbb{N}}$ sind Cauchy-Folgen in $\mathbb{Q}$
- $(t_n - s_n)_{n\in\mathbb{N}}$ ist Nullfolge $\Rightarrow$ möglicher Grenzwert r von (s_n) und (t_n) muss $r^2 = 2$ erfüllen $\Rightarrow$ Cauchy-Folgen (s_n) und (t_n) konvergieren nicht in $\mathbb{Q}$ ✓

Reelle Zahlen

Idee:

- Vervollständige $\mathbb{Q}$, so dass jede Cauchy-Folge konvergiert. Als Nebeneffekt werden wir auf diese Weise z. B. Wurzeln beliebiger nicht-negativer rationaler Zahlen bekommen. Tatsächlich sind die reellen Zahlen ein „viel größerer“ Zahlbereich als nur „$\mathbb{Q}$ plus Wurzeln rationaler Zahlen“.
- Definiere die reelle Zahl r als Grenzwert aller Cauchy-Folgen rationaler Zahlen die „gegen r konvergieren“, d. h. r entspricht einer Äquivalenzklasse von Cauchy-Folgen deren punktweise Differenz eine Nullfolge ist.
  Genauer für zwei Cauchy-Folgen $\mathbf{p} = (p_n)_{n\in\mathbb{N}}$ und $\mathbf{q} = (q_n)_{n\in\mathbb{N}} \in \mathbb{Q}^{\mathbb{N}}$ sei $\mathbf{p} - \mathbf{q} = (p_n - q_n)_{n\in\mathbb{N}}$

$$\text{„}\mathbf{p}\text{ und }\mathbf{q}\text{ haben gleichen Grenzwert“} \quad \Leftrightarrow \quad \mathbf{p} - \mathbf{q} \text{ ist eine Nullfolge}$$

- Damit definieren wir eine Äquivalenzrelation auf der Menge der rationalen Cauchy-Folgen deren Äquivalenzklassen dann den reelen Zahlen entsprechen.
- Diese Art der Vervollständigung wird auch allgemeiner z. B. bei vollständigen metrische Räumen verwendet.

Reelle Zahlen

Definition ($\mathbb{R}$)

Durch

$$\mathbf{p} \dot{\approx} \mathbf{q} \;:\Leftrightarrow\; \mathbf{p} - \mathbf{q} \to 0$$

wird auf der Menge der rationalen Cauchy-Folgen eine Äquivalenzrelation definiert.

Wir bezeichnen die Faktormenge mit $\mathbb{R}$ und nennen ihre Elemente die **reellen Zahlen**. Reelle Zahlen der Form $[(q)_{n\in\mathbb{N}}]$ für $q \in \mathbb{Q}$ bezeichnen wir kürzer durch die rationale Zahl q.

Die Operationen $+_\mathbb{Q}$ und $\cdot_\mathbb{Q}$ und die vollständige Ordnung $\leq_\mathbb{Q}$ aus $\mathbb{Q}$ erweitert man auf ganz $\mathbb{R}$, indem man für rationale Cauchy-Folgen $\mathbf{p} = (p_n)_{n\in\mathbb{N}}$ und $\mathbf{q} = (q_n)_{n\in\mathbb{N}}$ folgendes setzt

$$\begin{aligned} [\mathbf{p}] +_\mathbb{R} [\mathbf{q}] \;&:\Leftrightarrow\; [(p_n +_\mathbb{Q} q_n)_{n\in\mathbb{N}}] \\ [\mathbf{p}] \cdot_\mathbb{R} [\mathbf{q}] \;&:\Leftrightarrow\; [(p_n \cdot_\mathbb{Q} q_n)_{n\in\mathbb{N}}] \end{aligned}$$

und

$$[\mathbf{p}] \leq_\mathbb{R} [\mathbf{q}] \;:\Leftrightarrow\; (p_n - q_n)_{n\in\mathbb{N}} \to 0 \text{ oder } p_n <_\mathbb{Q} q_n \text{ für alle bis auf endlich viele } n \in \mathbb{N}.$$

Bemerkung: Auf Grund von Proposition 24 sind $(p_n +_\mathbb{Q} q_n)_{n\in\mathbb{N}}$ und $(p_n \cdot_\mathbb{Q} q_n)_{n\in\mathbb{N}}$ tatsächlich Cauchy-Folgen und man kann zeigen, dass $+_\mathbb{R}$, $\cdot_\mathbb{R}$ und $\leq_\mathbb{R}$ wohldefiniert sind. Per Definition konvergieren rationale Cauchy-Folgen in $\mathbb{R}$ (also ist $\sqrt{2} \in \mathbb{R}$, z. B. wegen der Folgen (s_n) und (t_n) aus Proposition 25) und man kann zeigen, dass reelle Cauchy-Folgen (analog definiert wie rationale) auch in $\mathbb{R}$ konvergieren. D. h. $\mathbb{R}$ ist vollständig.

$\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R}$?

Streng genommen geht aus den vorangegangenen Definitionen von $\mathbb{Z}$, $\mathbb{Q}$ und $\mathbb{R}$ nicht hervor, dass $\mathbb{N}$ eine Teilmenge von $\mathbb{Z}$ oder $\mathbb{Z}$ eine Teilmenge von $\mathbb{Q}$ oder $\mathbb{Q}$ eine Teilmenge von $\mathbb{R}$ ist. Zum Beispiel wurde $\mathbb{Z}$ als die Faktormenge einer Äquivalenzrelation auf $\mathbb{N} \times \mathbb{N}$ definiert und diese Faktormenge enthält $\mathbb{N}$ nicht!

Auf der anderen Seite, haben wir eine injektive Funktion $n \mapsto [(n, 0)]$ von $\mathbb{N}$ in diese Faktormenge angegeben, für die sich die auf $\mathbb{N}$ definierte Addition und Multiplikation erhält, z. B. für die Addition ergibt sich aus der Definition sofort für alle natürlichen Zahlen ℓ, m und n, dass $\ell + m = n$ genau dann gilt, wenn $[(\ell, 0)] +_{\mathbb{Z}} [(m, 0)] = [(n, 0)]$. Diese Einbettung von $\mathbb{N}$ erlaubt es $\mathbb{N}$ als Teilmenge von $\mathbb{Z}$ zu betrachten und wir werden von nun an $\mathbb{N}$ immer als diese Teilmenge von $\mathbb{Z}$ ansehen.

Genauso kann mit Hilfe der Funktion $z \mapsto [(z, 1)]$ die Menge der ganzen Zahlen in $\mathbb{Q}$ eingebettet werden, welche wiederum durch $q \mapsto [(q)_{n\in\mathbb{N}}]$ als eine Teilmenge von $\mathbb{R}$ aufgefasst werden kann. Von nun an werden wir auf Grund dieser Einbettungen sowohl die rationalen, als auch die ganzen und die natürlichen Zahlen als durch $\leq$ vollständig geordnete Teilmengen der reellen Zahlen betrachten und die Addition und Multiplikation einfach mit $+$ und $\cdot$ bezeichnen. Insbesondere gilt also

$$\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R}.$$

$|\mathbb{N}| = |\mathbb{Z}| = |\mathbb{Q}| < |\mathbb{R}|$

Satz 26 (Cantor 1874)

$\mathbb{R}$ ist überabzählbar.

Beweis.

Wir zeigen $|\mathcal{P}(\mathbb{N})| \leq |\mathbb{R}|$ und auf Grund von Satz 22 folgt dann

$$|\mathbb{N}| < |\mathcal{P}(\mathbb{N})| \leq |\mathbb{R}|\,,$$

also $\mathbb{R}$ ist nicht abzählbar und somit überabzählbar.

Wir verwenden hier die übliche Dezimaldarstellung der reellen Zahlen (ohne diese formal einzuführen) und betrachten die folgende Funktion $f\colon \mathcal{P}(\mathbb{N}) \to \mathbb{R}$ definiert für jedes $A \subseteq \mathbb{N}$ durch

$$f(A) = x_A \text{ mit } 0 \leq x_A \leq 1/9\,,$$

wobei die reelle Zahl $x_A = 0{,}x_{A,1}x_{A,2}\dots$ an der n-ten Dezimalstelle $x_{A,n}$ hinter dem Komma 1 ist, falls $n \in A$, und 0 sonst.

Da es für zwei verschiedene Mengen A und $B \subseteq \mathbb{N}$ ein kleinstes $n \in \mathbb{N}$ gibt, welches in genau einer der Mengen A oder B enthalten ist, ist $x_A \neq x_B$. Somit ist f injektiv und

$$|\mathcal{P}(\mathbb{N})| \leq |\{x \in \mathbb{R}\colon 0 \leq x \leq 1/9\}| \leq |\mathbb{R}|\,.$$