LINEARE ALGEBRA

FABIAN HEBESTREIT

Contents

1. Aussagen

Um später im Ernstfall eine präzise Sprache zu ermöglichen, beginnen wir mit etwas Vokabular, das wir der Alltagssprache entreißen:

1.1. **Konvention** Eine *Aussage (statement)* ist ein Satz, der eindeutigerweise entweder *wahr (true)* oder *falsch (false)* ist.

1.2. **Beispiel** Typische Beispiele, die dieser Konvention sicherlich genügen sind:

(1) Jede natürliche Zahl ist gerade.
(2) 6 ist durch 3 ohne Rest teilbar.
(3) 34 ist größer als 27.
(4) 27 ist größer als 34.

Diese Aussagen, so sind wir uns hoffentlich alle einig, sind in Reihenfolge falsch, wahr, wahr und falsch. Einige schon eher problematische Beispiele sind

(1) Milch kommt aus Tieren.
(2) Franz hat eine Brille auf.
(3) 7 ist meine Lieblingszahl.

aber Alltagsaussagen wie diese sind selten präzise genug um wirklich Aussagen im Sinne obiger Konvention zu sein (wie steht es um Hafermilch oder Sonnenmilch? Hat man eine Brille auch auf, wenn man sie nicht auf der Nase trägt, sondern in die Haare hochgeschoben hat? Was bedeutet eigentlich dieses "Lieblings-" genau? Definitv keine Beispiele sind:

(1) Ich lüge gerade.
(2) Es regnet.
(3) Franziska hat graue Haare.

Der erste Satz ist eine Variante des berühmten Paradox des Epimenides: Ist die getroffene Aussage wahr, so muss sie eine Lüge sein, und daher in Wahrheit falsch. Ist die getroffene hingegen Aussage falsch, so ist sie nicht gelogen, muss also wahr sein. Ergo können wir nicht sinnvoll einen Wahrheitsgehalt zuweisen. Der zweite Satz ist viel zu vage: Regnet es jetzt gerade oder manchmal? Zählt Niesel schon als Regen? Und über welchen Ort wird überhaupt geredet. Der dritte Fall ist ähnlich: In der Alltagssprache meint man mit "hat graue Haare" manchmal, dass alle Haare einer

Person grau sind, und manchmal nur dass einige Haare grau, aber durchaus noch braune, blonde, oder auch hell-pinke Haare auf dem Kopf zu finden sind. Wieder viel zu ungenau.

Eine erste große Herausforderung wird es nun sein sich daran zu gewöhnen, sehr scharf zwischen Aussagen im Sinne obiger Konvention und Alltagssprache zu trennen. Wir werden im weiteren im wesentlichen nur Aussagen erlauben um über mathematische Inhalte zu reden, allein schon um Missverständnisse zu vermeiden. Ich wünschte mir manchmal, dies wäre auch eine Alltagskonvention so...

1.3. **Konstruktion** Sind A und B zwei Aussagen, so konstruieren wir zweie neue Aussagen

$$(A) \vee (B) \quad \text{and} \quad (A) \wedge (B),$$

die *Disjunktion (disjunction)* bzw. *Konjunktion (conjunction)* von A und B: Ihre Wahrheitswerte sind durch folgende Vorschriften gegeben:

$$(A) \vee (B) \quad \text{ist} \quad \begin{cases} \text{wahr} & \text{falls } A \text{ und } B \text{ beide wahr sind} \\ \text{wahr} & \text{falls } A \text{ wahr ist und } B \text{ falsch} \\ \text{wahr} & \text{falls } A \text{ falsch ist und } B \text{ wahr} \\ \text{falsch} & \text{falls } A \text{ und } B \text{ falsch sind.} \end{cases}$$

$$(A) \wedge (B) \quad \text{ist} \quad \begin{cases} \text{wahr} & \text{falls } A \text{ und } B \text{ beide wahr sind} \\ \text{falsch} & \text{falls } A \text{ wahr ist und } B \text{ falsch} \\ \text{falsch} & \text{falls } A \text{ falsch ist und } B \text{ wahr} \\ \text{falsch} & \text{falls } A \text{ und } B \text{ falsch sind.} \end{cases}$$

Diese Konstruktion formalisiert die Alltagsbegriffe "und" und "oder". Man stellt die Vorschriften häufig als Wahrheitstafeln dar:

B \ A	w	f
w	w	w
f	w	f

$(A) \vee (B)$

B \ A	w	f
w	w	f
f	f	f

$(A) \wedge (B)$

1.4. **Warnung** Konjunktion und Diskjunktion enthalten keinerlei Hinweise auf logische, kausale oder sonstige Zusammenhänge zwischen den teilnehmenden Aussagen, anders als man dies aus dem Alltag kennt. Ein schönes Beispielsind etwa die zwei Sätze:

Er begang eine Straftat und ging ins Gefängnis.

Er ging ins Gefängnis und begang eine Straftat.

Intuitiv würden viele von uns aus dem ersten Satz wohl ablesen, dass die erwähnte Straftat der Grund für den Gefängnisgang ist (und insbesondere etwa bemerkt wurde), wohingegen man in den zweiten Satz eher hineinliest, dass der arme Protagonist wohl mittlerweile mindestens zweimal abseits des Gesetzes tätig war. Nichts davon ist aber wirklich gesagt, und von solchen Assoziation müssen Sie sich befreien. Die beiden Aussagen

(Er begang eine Straftat) $\wedge$ (Er ging ins Gefängnis)

(Er ging ins Gefängnis) $\wedge$ (Er begang eine Straftat)

sind für uns inhaltsgleich (sofern wir uns denn für den Zwecke dieses Beispiels einigen wollen wollen, dass "Er begang eine Straftat" und "Er ging ins Gefängnis" wirklich Aussagen sind).

Trotz dieser Diskrepanz werden wir häufig (A) *und* (B) anstatt $(A \wedge B)$ und (A) *oder* (B) anstatt $(A) \vee (B)$.

1.5. **Beispiel** (1) Hier sind zwei wahre Aussagen:
   (a) (34 ist größer als 27) und (rot ist eine Farbe).
   (b) (27 ist größer als 34) oder (rot ist eine Farbe).

(2) Im Sinne obiger Konstruktion muss die Antwort auf die Frage "Möchtest du Tee oder Kaffee" wohl "Ja" oder "Nein" lauten, je nachdem, welches von (Tee oder Kaffee) und (nichts) man denn will.
(3) Die Klammung, die beim verbinden von nur zwei Aussagen erstmal unnötig und vielleicht etwas nervig erscheint, ist enorm wichtig, sobald Disjunktion und Konjunktion beide im Spiel sind: Die beiden Aussagen

$$((A) \wedge (B)) \vee (C) \quad \text{und} \quad (A) \wedge ((B) \vee (C))$$

können sehr verschieden sein:

Paul went to the loo and did a number one or number two.

Nur bei einer Klammerung ist sichergestellt, dass Paul mit seiner Notdurft den Lokus erreicht hat.

1.6. **Konstruktion** Eine weitere wichtige Art aus alten Aussagen neue zu produzieren ist die *Negation (negation)*: Zu einer Aussage A bilden wir die Aussage $\neg(A)$, deren Wahrheitwert durch

$$\neg(A) \quad \text{ist} \quad \begin{cases} \text{falsch} & \text{falls } A \text{ wahr ist} \\ \text{wahr} & \text{falls } A \text{ falsch ist.} \end{cases}$$

Sie formalisiert den Alltagsbegriff "nicht" oder "Gegenteil von" und hat die Wahrheitstafel

A	w	f
	f	w

$\neg(A)$

1.7. **Beispiel** (1) ¬(Jede natürliche Zahl ist gerade) ist inhaltsgleich zu (Es gibt ungerade natürliche Zahlen), und ist natürlich wahr.
(2) ¬(Hans ist ein Untergebener von Lisa) hat den gleichen Gehalt wie (Hans ist kein Untergebener von Lisa), aber nicht unbedingt wie (Lisa ist eine Untergebene von Hans): Etwa könnten sie beide gleichen Rang haben.

Aus den Bausteinen $\wedge, \vee, \neg$ lassen sich viele andere Operationen zusammensetzen. Ein Beispiel ist die *Exklusivdisjunktion (exclusive disjunction)* $(A) \times (B)$, die definiert ist als

$$((A) \vee (B)) \wedge (\neg((A) \wedge (B))).$$

Etwas kürzer schreibt man in solchen Fällen gern

$$(A) \times (B) := ((A) \vee (B)) \wedge (\neg((A) \wedge (B)));$$

das Zeichen $:=$ ist als "ist definiert als" zu lesen und bedeutet, dass die linke Seite eine Abkürzende Schreibweise für die rechte Seite ist; man sollte diese Zeichen als ein einzelnes lesen, das nicht aus : und = zusammengesetzt ist (historisch kommt es natürlich daher).

Wichtiger als das in der Mathematik recht ungebräuchliche "exklusiv-oder" sind:

1.8. **Definition** Sind A und B Aussagen so setzen wir:

$$(A) \Rightarrow (B) := (\neg(A)) \vee (B)$$
$$(A) \Leftarrow (B) := (B) \Rightarrow (A)$$
$$(A) \Leftrightarrow (B) := ((A) \Rightarrow (B)) \wedge ((A) \Leftarrow (B))$$

Die ersten beiden nennt man *Implikationen (implications)* und die dritte *Äquivalenz (equivalence)*.

Gelesen werden Äquivalenzen als "genau dann, wenn" und die Implikationen demzufolge als "dann" (⇒) und "wenn" (⇐). Die Wahrheitstabellen lauten:

B \ A	w	f
w	w	w
f	f	w

B \ A	w	f
w	w	f
f	w	w

B \ A	w	f
w	w	f
f	f	w

$$(A) \Rightarrow (B) \qquad (A) \Leftarrow (B) \qquad (A) \Leftrightarrow (B)$$

1.9. **Warnung** Noch mehr als bei "und" und "oder" gibt es in vielen von uns den Impuls bei $(A) \Rightarrow (B)$ eine Kausalität in die Aussage hineinzulesen. Widerstehen Sie ihm. So ist etwa

$$(\text{Rot ist eine Farbe}) \Rightarrow (34 \text{ ist größer als } 27)$$

eine wahre Aussage, aber die Größe von 34 hat sicherlich nichts mit der Farbigkeit von rot zu tun.

Insbesondere gilt: Eine falsche Aussage impliziert jede Aussage. Nehmen Sie sich diese Weisheit zu Herzen: Es reicht ein einziger Fehler in einer Argumentationskette um das ganze Konstrukt zum Einsturz zu bringen.

Es gelten nun eine Myriade Rechenregeln für all diese Operationen. Um sie alle aufzuschreiben, sei noch vereinbart, dass w and f eine *Tautologie* und eine *Antinomie*, also eine wahre und eine falsche Aussage bezeichnen.

1.10. **Satz** *Sind A, B und C Aussagen so gelten*

(1) Assoziativität (associativity)

$$[((A) \vee (B)) \vee (C)] \Longleftrightarrow [(A) \vee ((B) \vee (C))] \quad \textit{und} \quad [((A) \wedge (B)) \wedge (C)] \Longleftrightarrow [(A) \wedge ((B) \wedge (C))]$$

(2) Kommutativität (commutativity)

$$[(A) \vee (B)] \Longleftrightarrow [(B) \vee (A)] \quad \textit{und} \quad [(A) \wedge (B)] \Longleftrightarrow [(B) \wedge (A)]$$

(3) Neutralität (neutrality)

$$[(A) \vee f] \Longleftrightarrow (A) \quad \textit{und} \quad [(A) \wedge w] \Longleftrightarrow (A)$$

(4) Absorption (absorption)

$$(A) \vee w \quad \textit{und} \quad \neg((A) \wedge f)$$

(5) Idempotenz (idempotency)

$$\neg(\neg(A)) \Longleftrightarrow (A)$$

(6) tertium non datur (law of the excluded middle)

$$(A) \vee (\neg(A)) \quad \textit{und} \quad \neg((A) \wedge \neg(A))$$

(7) de Morghan'schen Gesetze (de Morghan's laws)

$$[\neg((A) \vee (B))] \Longleftrightarrow [(\neg(A)) \wedge (\neg(B))] \quad \textit{und} \quad [\neg((A) \wedge (B))] \Longleftrightarrow [(\neg(A)) \vee (\neg(B))]$$

(8) Distributivität (distributivity)

$$[(A) \wedge ((B) \vee (C))] \Longleftrightarrow [((A) \wedge (B)) \vee ((A) \wedge (C))] \quad \textit{und} \quad [(A) \vee ((B) \wedge (C))] \Longleftrightarrow [((A) \vee (B)) \wedge ((A) \vee (C))]$$

(9) Transitivität (transivity)

$$[((A) \Rightarrow (B)) \wedge ((B) \Rightarrow (C))] \Longrightarrow [(A) \Rightarrow (C)]$$

(10) Substitution (substitution)

$$[(A) \Rightarrow (B)] \Longrightarrow [((A) \vee (C)) \Rightarrow ((B) \vee (C))]$$

$$[(A) \Rightarrow (B)] \Longrightarrow [((A) \wedge (C)) \Rightarrow ((B) \wedge (C))]$$

(11) Umkehrschluss (contraposition)

$$[(A) \Rightarrow (B)] \Longleftrightarrow [(\neg(B)) \Rightarrow (\neg(A))]$$

Die Assoziativität erlaubt es uns im weiteren viel der Klammern um Aussagen wegzulassen. So werden wir etwa eher $(A) \wedge (B) \wedge (C)$ schreiben und damit eine der äquivalenten Aussage in (1) meinen. In Wahrheit werden wir meist sogar $A \wedge B \wedge C$ schreiben und die Klammern nur setzen, wenn sie Verwirrung vermeiden (etwa wenn eine der Aussagen A, B oder C selbst wieder eine Disjunktion enthalten, sodass die Warnung 1.5 (3) zuschlägt. .

Beweis. Diese Regeln lassen sich alle durch simple Fallunterscheidung nachweisen. Am einfachsten sind wohl die beiden Absorptionsgesetze. Für sie reichen ein direkter Blick in die Wahrheitstabellen. Und das Idempotenzgesetz is nicht schwerer: Ist A wahr, so ist $\neg(A)$ falsch, ergo $\neg(\neg(A))$ wieder wahr, und ähnlich ist, falls A falsch ist, $\neg(A)$ wahr und dann $\neg(\neg(A))$ wieder falsch. Ein Blick in die Wahrheitstabelle Äquivalent zeigt dann aber, dass sowohl zwei wahre als auch zwei falsche Aussage eine wahre Aussage liefern. Die Neutralitätsgesetze sind auch einfach: Ist A wahr so nach Blick in die Wahrheitstabelle der Disjunktion auch $(A) \vee w$ und ist A falsch, so auch $(A) \vee w$, und wieder beendet ein Blick in die Wahrheitstabelle der Äquivalenz den Nachweis. Ähnliches für die Version der Konjugation. Um zu sehen, dass es etwas drittes nicht gibt, beobachten wir, dass immer genau eine der Aussagen A und $\neg(A)$ wahr ist, was durch Blick in die Wahrheitstabelle der Disjunktion verrät, dass $(A) \vee (\neq (A))$ immer wahr ist und in die der Konjugation, dass $(A) \wedge (\neg(A))$ nie wahr ist.

Für die Kommutativität stellt man fest, dass die Wahrheitstabelle von Disjunktion und Konjugation sich bei Vertauschen von A und B nicht verändern. Für die de Morghan'schen Gesetze ergeben sich für das erste und zweite jeweils auf beiden Seiten die Wahrheitstabellen

B \ A	w	f
w	f	f
f	f	w

B \ A	w	f
w	f	w
f	w	w

Assoziativität und Distributivität ergeben sich, indem man etwa Wahrheitstabellen erst C als wahr annimmt, und dann Wahrheitstabellen anfertigt, und dann ähnliches falls C falsch ist. Im ersten Fall, also falls C wahr ist ergeben sich in den vier Gesetzen jeweils

B \ A	w	f
w	w	w
f	w	w

B \ A	w	f
w	w	f
f	f	f

Assoziativitätsgesetze mit C wahr

B \ A	w	f
w	w	f
f	w	f

B \ A	w	f
w	w	w
f	w	f

Distrubutivitätsgesetzte mit C wahr

als Wahrheitstabellen beider Seiten, und falls C falsch ist erhalten wir

B \ A	w	f
w	w	w
f	w	f

B \ A	w	f
w	f	f
f	f	f

Assoziativitätsgesetze mit C falsch

B \ A	w	f
w	w	f
f	f	f

B \ A	w	f
w	w	f
f	w	f

Distrubutivitätsgesetzte mit C falsch

Damit bleiben noch die ersten beiden Substitutionsregeln und die Transitivität. Für die ersten beiden Substitutionsgesetze lauten die Wahrheitstabellen für die rechten Seiten der Implikationen

B \ A	w	f
w	w	w
f	w	w

B \ A	w	f
w	w	f
f	f	w

Rechte Seiten der Substitutionsgesetze mit C wahr

B \ A	w	f
w	w	f
f	f	w

B \ A	w	f
w	w	w
f	w	w

Rechte Seiten der Substitutionsgesetze mit C falsch

In allen Fällen taucht hier nur ein Eintrag "wahr" auf, wenn dieser auch in $(A) \Leftrightarrow (B)$ auftaucht. Das dritte Substitutionsgesetz ergibt sich wieder direkt durch einen Blick auf die Wahrheitstafel der Äquivalenz. Der Umkehrschluss folgt wieder direkt durch scharfes Hinsehen in der Wahrheitstafel der Implikation.

Zuletzt machen wir für die Transitivität eine Fallunterscheidung in B: Die Negation der linken Seite hat die Wahrheitstafel

C \ A	w	f
w	f	f
f	w	w

mit B wahr

B \ A	w	f
w	w	f
f	w	f

mit B falsch

In jedem Fall liefert die eintragsweise Disjunktion mit

C \ A	w	f
w	w	w
f	f	w

$$(A) \Rightarrow (C)$$

immer eine wahre Aussage. □

Hiermit haben wir nun wohl das Standardarsenal an Methoden zur Verfügung eine Aussage A als wahr nachzuweisen: Die leichteste Methode ist es eine schon als wahr bekannte Aussage zu finden und zu zeigen, dass $B \Rightarrow A$ wahr ist. Dann zeigt ein Blick in die Wahrheitstabelle der Implikation sofort, dass auch A wahr sein muss. Die Transitivität erlaubt es, hierfür noch weitere Aussagen zwischen zu schalten, also neben der wahren Aussage B etwa noch eine Aussage C zu finden und $B \Rightarrow C$ und $C \Rightarrow A$ als wahr nachzuweisen. Dann folgt nämlich $B \Rightarrow A$ und damit auch A. In diesem Fall spricht man oft von C als einem Zwischenschritt im Beweis von A.

Auf einem anderen Wege ist es etwa möglich, um A als wahr nachzuweisen, den Umkehrschluss zu verwenden: Hierzu muss man eine wahre Aussage B finden und nachweisen dass $\neg(A) \Rightarrow \neg(B)$ gilt. Es folgt dann nämlich $B \Rightarrow A$ und A folgt. Man spricht in diesem Fall von einem Beweis durch Widerspruch.

1.11. **Beispiel** Nachdem man Gesetze (1) - (10) nachgewiesen hat, kann man etwa den Umkehrschluss anstatt wie oben durch Blick auf die Wahrheitstafeln auch auf diese Weise herleiten: Ausgeschrieben bedeutet

$$(*) := \big([(A) \Rightarrow (B)] \Longrightarrow [(\neg(B)) \Rightarrow (\neg(A))]\big)$$

(und das ist eine Hälfte der Behauptung des Umkehrschlusses) dass

$$\neg(\neg A \vee B) \vee (\neg(\neg B) \vee \neg A).$$

Wegen des Idempotenzgesetzes gilt $\neg(\neg B) \Leftrightarrow B$, sodass eine Anwendung des Substitutionsgesetzes

$$[\neg(\neg A \vee B) \vee (B \vee \neg A)] \Longrightarrow (*)$$

liefert. Aber aufgrund des Kommutativitätsgesetzes gilt $[B \vee \neg A] \Longleftrightarrow [\neg A \vee B]$ und demzufolge liefert das Substitutionsgesetz

$$[\neg(\neg A \vee B) \vee (\neg A \vee B)] \Longrightarrow [\neg(\neg A \vee B) \vee (B \vee \neg A)]$$

und dann das Transitivitätsgesetz

$$[\neg(\neg A \vee B) \vee (\neg A \vee B)] \Longrightarrow (*).$$

Aber $\neg(\neg A \vee B) \vee (\neg A \vee B)$ ist wahr, da tertium non datur (etwas drittes gibt es nicht). Also ist auch $(*)$ wahr.

Das ist natürlich an dieser Stelle noch um einiges komplizierter als der Blick in die Wahrheitstafel, aber im Weiteren wird das letztere keine Option mehr sein. Um den Text etwas kürzer

(und hoffentlich auch verständlicher) zu machen, lässt die Anwendungen von Substitution und Transitivität meist implizit und schreibt diesen Beweis etwa einfach wie folgt auf:

$$\begin{aligned}\neg(\neg A \vee B) \vee (\neg A \vee B)] &\Longrightarrow [\neg(\neg A \vee B) \vee (B \vee \neg A)] \\ &\Longrightarrow [\neg(\neg A \vee B) \vee (\neg(\neg B) \vee \neg A)]\end{aligned}$$

wobei im ersten Schritt Kommutativität und im zweiten Schritt Idempotenz benutzt wird, und die Ursprungsaussage wegen tertium non datur wahr ist.

Schon etwas besser.

2. Prädikate

2.1. **Konvention** Ein *Prädikat (predicate)* P ist ein Satz, der einen oder mehrere Platzhalter (oder Variablen) enthält, zusammen mit einem *Definitionsbereich (domain of definition)*, derart dass durch Einsetzen eines jeden Objektes d aus dem Definitionsbereich für den Platzhalter eine Aussage $P(d)$ entsteht.

2.2. **Beispiel**
(1) "x ist gerade" mit Variable x und Definitionsbereich die natürlichen Zahlen. Anstatt (x ist gerade)(5) schreiben wir natürlich "5 ist gerade". Das ist übrigends falsch.
(2) "x ist gerade" mit Variable x und Definitionsbereich die Bäume ist kein Beispiel. Was soll es schon heißen einen Baum durch 2 zu teilen? Oder wann ist ein Baum sonst gerade?
(3) "x ist gerade" mit Variablen x und y und Definitionsbereich die natürlichen Zahlen (für x) und die Bäume (für y). Insbesondere müssen die Variablen eines Prädikates nicht wirklich in ihm vorkommen.
(4) "y ist gerade" mit Variable x und Definitionsbereich die natürlichen Zahlen ist wieder kein Beispiel. Was soll y denn sein, wenn es nicht die Variable des Prädikats ist?

Der Sinn und Zweck von Prädikaten ist es, aus ihnen Aussagen zu gewinnen. Zum einen hat man natürlich die einzelnen Aussagen $P(d)$, aber interessant wird das ganze durch:

2.3. **Konstruktion** Ist P ein Prädikat mit Variable x, so bilden wir zwei neue Aussagen

$$\forall x \text{ in } D\colon P \quad \text{und} \quad \exists x \text{ in } D\colon P$$

die *Universal-* und *Existenzquantifizierung (universal-* und existence quantification) von P, deren Wahrheitswerte gegeben sind durch

$$\forall x \text{ in } D\colon P \quad \text{ist} \quad \begin{cases}\text{wahr} & \text{falls } P(d) \text{ für jedes Objekt } d \text{ des Definitionsbereiches von } P \text{ wahr ist} \\ \text{falsch} & \text{falls } P(d) \text{ für mindestens ein Objekt } d \text{ des Definitionsbereiches falsch ist.}\end{cases}$$

$$\exists x \text{ in } D\colon P \quad \text{ist} \quad \begin{cases}\text{wahr} & \text{falls } P(d) \text{ für mindestens ein Objekt } d \text{ des Definitionsbereiches wahr ist} \\ \text{falsch} & \text{falls } P(d) \text{ für jedes Objekt } d \text{ des Definitionsbereiches von } P \text{ falsch ist.}\end{cases}$$

Häufig lässt man den Definitionsbereich auch implizit und schreibt nur

$$\forall x\colon P \quad \text{und} \quad \exists x\colon P$$

Hat ein Prädikat mehrere Variable, etwa x, y, so kann man $\forall x\colon P$ und $\exists x\colon P$ ebenfalls bilden (man spricht von partieller Quantifizierung) und erhält ein neues Prädikat, nun mit Variable y, deren Definitionsbereich sich nicht ändert. Es ist so definiert, dass $(\forall x\colon P)(d)$ für ein d aus dem Definitionsbereich von y wahr ist genau dann, wenn $P(d', d)$ für alle d' aus dem Definitionsbereich von x wahr ist, und ähnliches für partielle Existenzquantifikation.

Insbesondere kann man für ein Prädikat P mit Variablen x, y doppelt quantifizieren und die Aussagen

$$\forall x\colon (\forall y\colon P) \quad \text{and} \quad \forall x\colon (\exists y\colon P) \quad \text{and} \quad \exists x\colon (\forall y\colon P) \quad \text{and} \quad \exists x\colon (\exists y\colon P)$$

bilden. Durch Schachtelung von Ausdrücke der mittleren Sorte kann man schnell recht komplexe Aussagen erzeugen. Auch hier spart man sich wann immer möglich die Klammern und auch den ersten der Doppelpunkte schreibt man nur aus, wenn er beim Lesen hilft.

2.4. **Beispiel** (1) "x ist kleiner als y" ist ein zweistelliges Prädikat mit Variablen x, y und Definitionsbereichen die natürlichen Zahlen. Die Aussagen $(\exists x, y\colon x$ ist kleiner als $y)$ und $(\forall x \exists y\colon x$ ist kleiner als $y)$ sind wahr, wohingegen die Aussagen $(\exists y \forall x\colon x$ ist kleiner als $y)$ und $(\forall x, y\colon x$ ist kleiner als $y)$ falsch sind. Machen Sie sich dies gerade bei den mittleren beiden wirklich klar: Zu jeder natürlichen Zahl d gibt es eine größere (etwa $d + 17$), aber es gibt keine natürliche Zahl, die größer als alle anderen ist.

(2) Bei Schachproblemen gibt es Brettisituationen, die man mit "Weiß gewinnt in zwei Zügen" bezeichnet. Das ist schon ein Beispiel einer nicht mehr ganz simplen Aussage: Sie entfaltet sich zu

$$\exists \text{ Zug von Weiß } x\colon \forall \text{ Züge von Schwarz } y\colon \exists \text{ Zug von Weiß } z\colon$$

Nach Durchführung der Züge x, dann y, dann z ist Schwarz Schachmatt.

(3) Geschachtelte Quantoren und Aussagen sind mehr die Norm als die Ausnahme in der Mathematik: Die Definition der Stetigkeit für eine Funktion $f\colon \mathbb{R} \to \mathbb{R}$ in der Analysis I wird einmal

$$\forall x \in \mathbb{R} \forall \epsilon > 0 \exists \delta > 0 \forall y \in \mathbb{R}\colon |x - y| < \delta \Rightarrow |f(x) - f(y)| < \epsilon$$

lauten. Gewöhnen Sie sich also lieber schnell daran.

Prädikate können genau wie Aussagen verknüpft werden: Sind P und Q Prädikate mit gleichen Variablen und Definitionsbereichen so können wir die Prädikat $P \vee Q$ und $P \wedge Q$ deren Wahrheitswert bei einem Objekt d sinnvollerweise $P(d) \vee Q(d)$ bzw. $P(d) \wedge Q(d)$ sind.

Wieder gelten ein Haufen Rechenregeln:

2.5. **Satz** *Sind P und Q Prädikate mit Variable x und gleichem Definitionsbereich und R ein Prädikat mit Variablen x, y, so gelten folgende Aussagen:*

(1)

$$\neg(\forall x\colon P) \iff (\exists x\colon \neg P) \quad \textit{und} \quad \neg(\exists x\colon P) \iff (\forall x\colon \neg P)$$

(2)

$$(\forall x\colon P \wedge Q) \iff (\forall x\colon P) \wedge (\forall x\colon Q) \quad \textit{und} \quad (\exists x\colon P \vee Q) \iff (\exists x\colon P) \vee (\exists x\colon Q)$$

(3)

$$(\forall x\colon P \vee Q) \impliedby (\forall x\colon P) \vee (\forall x\colon Q) \quad \textit{und} \quad (\exists x\colon P \wedge Q) \implies (\exists x\colon P) \wedge (\exists x\colon Q)$$

(4)

$$\forall x \forall y\colon R \iff \forall y \forall x\colon R \quad \textit{und} \quad \exists x \exists y\colon R \iff \exists y \exists x\colon R$$

(5)

$$\exists x \forall y\colon R \implies \forall y \exists x\colon R$$

Beweis. Es verhält sich ähnlich zum Beweis von Satz 1.10: Die meisten Punkte erhält man durch scharfes Hinsehen und Fallunterscheidung. Etwa den ersten: Ist die Aussage auf der linken Seite korrekt, so ist es falsch, dass P für alle x gilt. Ergo muss es ein x geben für das P nicht gilt, was genau die Behauptung der rechten Seite ist. Es folgt nach Inspektion der Wahrheitstafel der Implikation, dass $\neg(\forall x\colon P) \implies (\exists x\colon \neg P)$. Ist andersherum die rechte Aussage wahr, gibt es ein x, für das P falsch ist. Aber dann stimmt ja sicherlich nicht, dass P für alle x gilt. Dies zeigt $(\exists x\colon \neg P) \implies \neg(\forall x\colon P)$. Die zweite Behauptung folgt analog.

Für den zweiten Punkt sind die getroffenen Aussagen hoffentlich ebenfalls offensichtlich: Etwa sind bei der linken Aussage beide Seiten genau dann wahr, wenn P und Q beide für alle x stimmen.

Etwas interessanter sind die Aussagen in Punkt (3), in den im allgemeinen jeweils nur eine Implikation gilt. Es ist klar, dass $(\forall c\colon P) \Rightarrow (\forall x\colon P \vee Q)$ und ähnliches mit Q anstelle des ersten $P's$, einfach weil ja generell $P(d) \Rightarrow P(d) \vee Q(d)$. Aber allgemein gilt

$$(A \Rightarrow C) \wedge (B \Rightarrow C) \iff (A \vee B \Rightarrow C)$$

wie Sie auf dem ersten Übungszettel nachweisen müssen. Setzen wir für A, B, C die drei Aussagen

$$(\forall c\colon P), (\forall c\colon Q), (\forall c\colon P \vee Q)$$

ein haben wir gerade die linke Seite verifiziert und die rechte folgt wie gewünscht. Die zweite Behauptung ist analog.

Zur vierten Behauptung weiß ich gar nichts zu sagen, so offensichtlich ist sie.

Interessant ist nochmal die letzte: Die linke Seite besagt, dass ein x gibt, dass für jedes y dazu führt dass R wahr ist. Aber dann gibt es ja zu jedem y auch wirklich dieses x was R wahr macht. Andersherum gilt das nicht: Bei Wahrheit der rechten Aussage könnte es zu verschiedenen y's verschiedene x'e geben, die R wahrmachen, auf der linken Seite reicht das nicht. □

2.6. **Warnung** In der Alltagssprache lässt man Quantoren oft implizit

Schnee ist weiß. Der Mann hat graues Haar.

Im ersten Falle scheint mir, man meint wohl "Aller Schnee ist weiß". Insbesondere ist dann ¬(Schnee ist weiß) die Aussage "Es gibt Schnee, der nicht weiß ist." und *nicht* (!!!) "Schnee ist nicht-weiß." Im zweiten Fall scheinen mir wohl beide Interpretationen

Alle Haare des Mannes sind grau. und Mindestens ein Haar des Mannes ist grau.

alltagskompatibel und ich nehme an, es gibt einige unter Ihnen, die intuitiv auf die eine, und einige, die es intuitiv auf die andere Weise interpretieren würden. Dies sind sehr verschiedene Aussagen. Noch seltsamer wird es, wenn man die "Aussage" negiert: Im ersten Fall ergibt sich

Mindestens ein Haar des Mannes ist nicht grau. und Kein Haar des Mannes ist grau.

Welche Bedeutung würden Sie intuitiv dem Satz "Der Mann hat nicht graues Haar." zuordnen? Mussten Sie vielleicht sogar das Camp wechseln?

Das Beispiel soll jedenfalls verdeutlichen, dass das unsere unrpäzise Alltagssprache ein großes (und wohl auch täglich genutzes) Potenzial für Verwirrungen und Missverständnisse bietet. Fügt man nun auch noch unseren Hang zum Hinzufügen von Zusammenhängen wie in Warnung 1.4 hinzu, erhält man ein unheiliges Gebräu bei dem es eher ein Wunder ist, dass überhaupt irgendwer irgendwen anders manchmal versteht (man überlege sich nur, welchen komplexes Konstrukt ein simples Wort wie "trotzdem" vermitteln soll).

Der Sinn und Zweck der formalen Sprache, die wir eingeführt haben ist es jedenfalls solchen Problemen vorzubeugen und präzise Argumente auch dann zu ermöglichen, wenn wir es mal mit wirklich komplizierten Aussagen zu tun bekommen.

Von vielen Aussagen weiß man bis heute nicht, ob sie wahr sind. Ein berühmtes Beispiel ist Goldbach's Vermutung:

$$\forall x\colon (\exists w\colon 2w = x \wedge w \geqslant 1) \Longrightarrow \big(\exists y, z\colon x = y + z$$

$$\wedge[\forall n, m\colon y = n \cdot m \Rightarrow (n = 1 \vee m = 1)] \wedge [\forall n, m\colon z = n \cdot m \Rightarrow (n = 1 \vee m = 1)]\big)$$

wobei alle Quantifikationen über die natürlichen Zahlen laufen. Oder mit anderen Worten: Jede gerade Zahl, die größer als 2 ist, ist Summe von zwei Primzahlen.

3. Mengen

Nun wo wir etwas sprechen gelernt haben, wenden wir uns als nächstes den Objekten zu, über die wir sprechen wollen:

3.1. **Konvention** (Cantor 1894) Eine *Menge (set)* M ist eine Zusammenfassung bestimmter, wohlunterschiedener Objekte unserer Anschauung oder unseres Denkens zu einem Ganzen.

Man nennt diese Objekte x die *Elemente (elements)* von M und schreibt $x \in M$. Wir nennen zwei Element $x, y \in M$ *gleich (equal)* und schreiben hierfür $x = y$, falls sich nicht unterscheidbar sind, und sonst $x \neq y$.

Man nennt N eine *Teilmenge (subset)* von M und schreibt $N \subseteq M$, falls jedes Element von N auch in M enthalten ist, in Formeln $\forall x\colon x \in N \Rightarrow x \in M$, quantifiziert über die Elemente von N.

Zwei Mengen M und N definieren wir als *gleich (equal)* und schreiben $M = N$, falls sie die gleichen Elemente enthalten, also falls $M \subseteq N$ und $N \subseteq M$.

Schlussendlich setzten wir noch

$$N \subsetneq M := N \subseteq M \wedge N \neq M$$

und sagen, dass N in diesem Fall eine *eigentliche (proper)* Teilmenge von M ist.

3.2. **Remark** Als der deutsche Mathematiker Georg Cantor (1845-1918) diese Definitionen, zusammen mit dem Begriff der Mächtigkeit (den wir in ein paar wenigen Vorlesungen kennen lernen werden) einführte, kam dies einer Revolution gleich, da er es ermöglichte auch unendliche Menge endlich rigoros zu studieren ohne nur auf die Intuition zurückzugreifen; Cantor selbst wollte eigentlich Mengen reeller Zahlen studieren, auf denen bestimmte Reihen konvergieren und bedurfte hierfür einer neuen Sprache, die sich dann verselbstständigt hat. Der ebenfalls deutsche Mathematiker David Hilbert (1862-1943) sagte knapp 30 Jahre nach dem Erscheinen von Cantors Arbeit einmal:

"Fruchtbaren Begriffsbildungen und Schlußweisen wollen wir, wo immer nur die geringste Aussicht sich bietet, sorgfältig nachspüren und sie pflegen, stützen und gebrauchsfähig machen. Aus dem Paradies, das Cantor uns geschaffen, soll uns niemand vertreiben können. Es ist nötig, durchweg dieselbe Sicherheit des Schließens herzustellen, wie sie in der gewöhnlichen niederen Zahlentheorie vorhanden ist, an der niemand zweifelt und wo Widersprüche und Paradoxien nur durch unsere Unaufmerksamkeit entstehen. Die Erreichung dieser Ziele ist offenbar nur möglich, wenn uns die volle Aufklärung über das Wesen des Unendlichen gelingt."

3.3. **Beispiel** (1) die Menge alle Kühe.
(2) die Menge aller Rechtshänder im Raum.
(3) die Mengen der natürlichen, ganzen, rationalen, reellen, p-adischen und komplexen Zahlen

Etwas ernsthafter: Eine Menge M nennen wir *leer (empty)* falls sie keine Elemente hat, also falls gilt

$$\forall x \colon x \notin \varnothing.$$

Wir beobachten sofort, dass wenn zwei Mengen M und N dieser Bedingung genügen, so gilt $M = N$. Oder mit anderen Worten es gibt nur eine leere Menge. Wir bezeichnen sie mit $\varnothing$.

3.4. **Beispiel** (1) Für jede Menge M gelten $\varnothing \subseteq M$ und $M \subseteq M$.
(2) Ist P ein Prädikat mit einer Variablen mit Definitionsbereich (die Elemente von) M, so kann man die Teilmenge

$$\{m \in M \mid P(m)\} \subseteq M$$

all derer Elemente $m \in M$ bilden, so dass $P(m)$ wahr ist. Andersherum ist für eine Teilmenge $N \subseteq M$ der Ausdruck $x \in N$ ein Prädikat mit Variable x und Definitionsbereich M.

Besteht der Definitionsbereich eines Prädikats P mit Variable m aus den Elementen einer Menge M so schreibt man in der Regel $\forall m \in M \colon P$ und $\exists m \in M \colon P$ bei der Quantifizierung.

(3) Ist $N \subseteq M$, so bezeichnet man die Teilmenge

$$M \backslash N := \{m \in M \mid m \notin N\}$$

als das *Komplement (complement)* von N in M.

(4) Möchte man gegebene Objekte zu einer Menge zusammenfassen benutzt man ebenfalls { }, etwa man bezeichnet für $x \in M$ die Teilmenge

$$\{m \in M \mid x = m\} \subseteq M$$

mit $\{x\}$. Ähnlich schreibt man $\{x, y\}$ für

$$\{m \in M \mid x = m \vee m = y\} \subseteq M$$

und so weiter. Es gilt insbesondere immer $\{x, y\} = \{y, x\}$, eine Reihenfolge oder ähnliches haben Mengen nicht. In der gesamten Diskussion ist durchaus zugelassen, dass $x = y$ gilt. In diesem Falle gelten auch $\{y\} = \{x, y\} = \{x\}$, sonst natürlich nicht.

(5) Es ist $\varnothing$ wohl zu unterscheiden von $\{\varnothing\}$. Die letztere Menge hat ein Element! Nämlich $\varnothing$. Die vordere nicht.
(6) Etwa gilt {natürliche Zahlen}\{gerade Zahlen} = {ungerade Zahlen}.

3.5. **Definition** Ist M eine Menge, so ist ihre *Potenzmenge (power set)* $\mathcal{P}(M)$ die Menge aller ihrer Teilmengen, also

$$\forall x\colon x \in \mathcal{P}(M) \Leftrightarrow x \subseteq M.$$

Ist $X \subseteq \mathcal{P}(M)$ eine Teilmenge, so definieren wir ihre *Vereinigung (union)* und *Durchschnitt (intersection)* als

$$\bigcup X := \{m \in M \mid \exists U \in X\colon m \in U\} \quad \text{and} \quad \bigcap X := \{m \in M \mid \forall U \in X\colon m \in U\}$$

Häufig schreibt man auch $\bigcup_{U\in X} U$ anstatt $\bigcup X$, was für so manches Gehirn etwas leichter zu parsen zu sein scheint. Wir werden das bestimmt öfter sehen. Definitiv benutzen werden wir

$$U \cup V := \bigcup\{U, V\} \quad \text{and} \quad U \cap V := \bigcap\{U, V\}$$

für zwei Teilmengen $U, V \subseteq M$. Zwei Teilmenge von M mit $U \cap V = \varnothing$ heißen *disjunkt (disjoint)*.

3.6. **Beispiel** (1) Es gelten

$$\mathcal{P}(\varnothing) = \{\varnothing\}$$
$$\mathcal{P}(\{\varnothing\}) = \{\varnothing, \{\varnothing\}\}$$
$$\mathcal{P}(\{\varnothing, \{\varnothing\}\}) = \{\varnothing, \{\varnothing\}, \{\{\varnothing\}\}, \{\varnothing, \{\varnothing\}\}\}$$

oder allgemeiner

$$\mathcal{P}(\{x\}) = \{\varnothing, \{x\}\} \quad \text{und} \quad \mathcal{P}(\{x, y\}) = \{\varnothing, \{x\}, \{y\}, \{x, y\}\}$$

für je zwei Elemente $x, y \in M$.

(2) Es gelten

$$\{1,2,3\} \cup \{2,3,4\} = \{1,2,3,4\} \quad \text{und} \quad \{1,2,3\} \cap \{2,3,4\} = \{2,3\}.$$
$$\bigcup\{\{1,2,3\},\{2,3,4\},\{3,4,5\}\} = \{1,2,3,4,5\} \quad \text{und} \quad \bigcap\{\{1,2,3\},\{2,3,4\},\{3,4,5\}\} = \{3\}.$$

Wieder gibt es eine Myriade Rechenregeln; hier eine Auswahl:

3.7. **Satz** *Für $U, V, W \subseteq M$ und $X, Y \subseteq \mathcal{P}(M)$ gelten:*

(1)
$$U \cup (M\backslash U) = M \quad \textit{und} \quad U \cap (M\backslash U) = \varnothing$$

(2)
$$M\backslash(U \cup V) = (M\backslash U) \cap (M\backslash V) \quad \textit{and} \quad M\backslash(U \cap V) = (M\backslash U) \cup (M\backslash V)$$

(3)
$$\bigcup\{U\} = U = \bigcap\{U\}$$

(4)
$$\bigcup \varnothing = \varnothing \quad \textit{und} \quad \bigcap \varnothing = M$$

(5)
$$\bigcup \mathcal{P}(M) = M \quad \textit{und} \quad \bigcap \mathcal{P}(M) = \varnothing$$

(6)
$$\bigcup X \cup \bigcup Y = \bigcup(X \cup Y) \quad \textit{und} \quad \bigcap X \cap \bigcap Y = \bigcap(X \cup Y)$$

insbesondere
$$(U \cup V) \cup W = U \cup (V \cup W) \quad \textit{und} \quad (U \cap V) \cap W = U \cap (V \cap W)$$

und
$$X \subseteq Y \Longrightarrow \bigcup X \subseteq \bigcup Y \quad \textit{und} \quad \bigcap Y \subseteq \bigcap X$$

und

(7)

$$\bigcap X \cup \bigcap Y = \bigcap \{N \subseteq M \mid \exists U \in X, U' \in Y \colon N = U \cup U'\}$$

und

$$\bigcup X \cap \bigcup Y = \bigcup \{N \subseteq M \mid \exists U \in X, U' \in Y \colon N = U \cap U'\}$$

insbesondere

$$(U \cup V) \cap W = (U \cap W) \cup (V \cap W) \quad \textit{und} \quad (U \cap V) \cup W = (U \cup W) \cap (V \cup W)$$

Beweis. Fangen wir mit der linken Aussage in (1) an: Für $U \cup (M \backslash U) \subseteq M$ müssen wir zeigen, dass $m \in U \vee m \in M \backslash U \Rightarrow m \in M$. Aber nach einer Übungsaufgabe ist das das gleiche wie zu zeigen, dass $m \in U \Rightarrow m \in M$ und $m \in M \backslash U \Rightarrow M$. Diese Aussage sind aber beide per definition (von U und $\backslash$) wahr. Für die umgekehrte Inlusion $M \subseteq U \cup M \backslash U$ müssen wir zeigen $m \in M \Rightarrow m \in U \vee m \in M \backslash U$. Aber wieder nach Übung können wir stattdessen, $m \in M \wedge m \notin U \Rightarrow m \in M \backslash U$ zeigen, was wieder nach Definition von $M \backslash U$ wahr ist.

Für die zweite Aussage $U \cap (M \backslash U) = \varnothing$ müssen wir zeigen, dass $U \cap (M \backslash U)$ leer ist. Mit anderen Worten, dass für alle $x \in M$ die Aussage $x \in U \wedge x \in M \backslash U$ falsch ist. Aber das is wieder nach Definition von $\backslash$ wahr, da tertium non datur.

Aussage (2) ist eine Übungsaufgabe werden.

Aussagen (3) sind direkt per Definition klar. Numero (4) ist amüsant: Die linke Gleichung folgt, da es per Definition für kein $x \in M$ eine Menge $U \in \varnothing$ gibt, mit $x \in U$: Es gibt ja einfach überhaupt kein $U \in \varnothing$, also ist $\bigcup \varnothing$ leer. Für die rechte stellen wir fest, dass aber für jedes $U \in \varnothing$ gilt $x \in U$, wieder weil es ja gar kein solches U gibt. Also ist $x \in \bigcap \varnothing$ und damit $M \subseteq \bigcap \varnothing$. Die andere Inklusion gilt per definitionem. Das Argument für (5) ist simpler: Für jedes $x \in M$ bezeugt $M \in \mathcal{P}(M)$, dass auch $x \in \bigcup \mathcal{P}(M)$, und $M \backslash \{x\} \in \mathcal{P}(M)$, dass $x \notin \bigcap \mathcal{P}(M)$.

Für Aussage (6) müssen wir zeigen, dass $x \in \bigcup X \vee x \in \bigcup Y$ genau dann gilt, wenn $x \in \bigcup X \cup Y$. Wir verwenden wie in (1) die Übungsaufgabe vom ersten Zettel, um für die Hinrichtung stattdessen $x \in \bigcup X \Rightarrow x \in \bigcup X \cup Y$ und $x \in \bigcup Y \Rightarrow x \in \bigcup X \cup Y$ zeigen zu dürfen. Aber das ist klar: Gibt es ein $U \in X$ mit $x \in U$, so gilt ja auch $U \in X \cup Y$, und analog für $U \in Y$. Für die Rückrichtung reicht es ebenfalls nach der Übungsaufgabe zu zeigen, dass $(\exists U \in X \cup Y \colon x \in U) \wedge \neg(\exists U \in Y \colon x \in U)$ impliziert, dass $x \in \bigcup X$. Aber auch das ist richtig: Die linke Seite der Konjunktion ist $(\exists U \in X \colon x \in U) \vee (\exists U \in X \colon x \in U)$, also die gesamte Konjunktion nach Distrubutivität und tertium non datur, sogar äquivalent zu $(\exists U \in X \colon x \in U)$, also in der Tat $x \in \bigcup X$.

Die linke der weiteren Behauptungen ergibt sich nun durch

$$(U \cup V) \cup W = \bigcup \{U, V\} \cup \bigcup \{W\} = \bigcup \{U, V, W\} = \bigcup \{U\} \cup \bigcup \{V, W\} = U \cup (V \cup W)$$

und die zweite durch

$$\bigcup X \subseteq \bigcup X \cup \bigcup (Y \backslash X) = \bigcup (Y \cup (Y \backslash X)) = \bigcup Y.$$

Die Behauptungen über Durchschnitte erhält man ähnlich.

Ich nutze den Beweis von der ersten Behauptung von (7) schlußendlich, um noch einmal einen Beweis soweit zu formalisieren, dass man ihn gerade noch lesen kann. Ein Beweis der für den menschlichen Konsum gedacht ist, folgt am Ende. Die zweite Behauptung nachzuweisen wird eine Übungsaufgabe.

Die Behauptung $\bigcap X \cup \bigcap Y \subseteq \bigcap \{N \subseteq M \mid \exists U \in X, U' \in Y \colon N = U \cup U'\}$ ist per Definition die Aussage:

$$(*) \qquad \forall x \in M \colon (x \in \bigcap X \cup \bigcap Y) \Rightarrow (x \in \bigcap \{N \subseteq M \mid \exists U \in X, U' \in Y \colon N = U \cup U'\}).$$

Zuerst beobachten, dass nach Definition von $\cup$ gilt:

$$x \in \bigcap X \cup \bigcap Y \iff (x \in \bigcap X) \vee (x \in \bigcap Y)$$

Also ist $(*)$ nach Substitution in 1.10 äquivalent zu

$$\forall x \in M \colon [(x \in \bigcap X) \vee (x \in \bigcap Y)] \Rightarrow (x \in \bigcap \{N \subseteq M \mid \exists U \in X, U' \in Y \colon N = U \cup U'\})$$

Aber nach dem ersten Übungszettel ist die äquivalent zu

$$\forall x \in M\colon [(x \in \bigcap X) \Rightarrow (x \in \bigcap \{N \subseteq M \mid \exists U \in X, U' \in Y\colon N = U \cup U'\})]$$
$$\wedge [(x \in \bigcap Y) \Rightarrow (x \in \bigcap \{N \subseteq M \mid \exists U \in X, U' \in Y\colon N = U \cup U'\})]$$

Und dies, und damit nach Transitivität auch $(*)$, ist nach 2.5 (2) wiederum zu

$$[\forall x \in M\colon (x \in \bigcap X) \Rightarrow (x \in \bigcap \{N \subseteq M \mid \exists U \in X, U' \in Y\colon N = U \cup U'\})]$$
$$\wedge [\forall x \in M\colon (x \in \bigcap Y) \Rightarrow (x \in \bigcap \{N \subseteq M \mid \exists U \in X, U' \in Y\colon N = U \cup U'\})]$$

äquivalent. Es reicht also diese beiden Aussagen als wahr nachzuweisen. Zeigen wir die erste, also

$$(**) \qquad \forall x \in M\colon (x \in \bigcap X) \Rightarrow (x \in \bigcap \{N \subseteq M \mid \exists U \in X, U' \in Y\colon N = U \cup U'\})$$

die zweite ist völlig analog. Nach Einsetzen der Definitionen des Durchschnitts lautet $(**)$

$$\forall x \in M\colon [\forall U \in X\colon x \in U] \Rightarrow [\forall U \in X\colon \forall U' \in Y\colon x \in U \cup U']$$

Einsetzten der Definition von $\cup$ wird dies weiter zu

$$(***) \qquad \forall x \in M\colon [\forall U \in X\colon x \in U] \Rightarrow [\forall U \in X\colon \forall U' \in Y\colon (x \in U) \vee (x \in U')],$$

was wir nun als wahr nachweisen müssen. Aber sicherlich gilt

$$[\forall U \in X\colon x \in U] \Rightarrow [\forall U \in X\colon x \in U] \vee [\forall U' \in Y\colon x \in U']$$

($A \Rightarrow A \vee B$ ist sicherlich für je zwei Aussage A und B wahr: etwa ist es nach dem ersten Übungszettel äquivalent zu $A \wedge \neg A \Rightarrow B$ und $A \wedge \neg A$ ist falsch) und nach 2.5 (3) gilt auch

$$[\forall U \in X\colon x \in U] \vee [\forall U' \in Y\colon x \in U'] \Rightarrow [\forall U \in X\colon \forall U' \in Y\colon (x \in U) \vee (x \in U')],$$

sodass eine letzte Anwendung von Transitivität $(***)$ liefert. Damit haben wir

$$\bigcap X \cup \bigcap Y \subseteq \bigcap \{N \subseteq M \mid \exists U \in X, U' \in Y\colon N = U \cup U'\}$$

nachgewiesen.

Bleibt noch die andere Inklusion

$$(\times) \qquad \bigcap \{N \subseteq M \mid \exists U \in X, U' \in Y\colon N = U \cup U'\} \subseteq \bigcap X \cup \bigcap Y$$

zu zeigen. Dies lautet ausgeschrieben

$$\forall x \in M\colon [\forall U \in X\colon \forall U' \in Y\colon x \in U \vee x \in U'] \Longrightarrow [\forall U \in X\colon x \in U] \vee [\forall U' \in Y\colon x \in U']$$

Aber wieder nach dem ersten Übungszettel ist dies äquivalent zu

$$\forall x \in M\colon [\forall U \in X\colon \forall U' \in Y\colon x \in U \vee x \in U'] \wedge \neg [\forall U \in X\colon x \in U] \Longrightarrow [\forall U' \in Y\colon x \in U']$$

was nach 2.5 (1) (und natürlich Substitution aus 1.10) äquivalent ist zu

$$(\times\times) \qquad \forall x \in M\colon [\forall U \in X\colon \forall U' \in Y\colon x \in U \vee x \in U'] \wedge [\exists U \in X\colon x \notin U] \Longrightarrow [\forall U' \in Y\colon x \in U'],$$

was wir nun als wahr nachweisen müssen. Aber für je zwei Prädikate P und Q mit gleichem Definitionsbereich gilt:

$$(\forall x\colon P) \wedge (\exists x\colon Q) \Rightarrow (\exists x\colon P \wedge Q)$$

(zum einen ist das offensichtlich, zum andern gilt es auf dem zweiten Übungszettel einen symbolischen Beweis zu finden). Setzen wir dies ein erhalten wir

$$[\forall U \in X\colon (\forall U' \in Y\colon x \in U \vee x \in U')] \wedge [\exists U \in X\colon x \notin U]$$
$$\Longrightarrow \exists U \in X\colon \forall U' \in Y\colon x \notin U \wedge (x \in U \vee x \in U')$$

und es gilt

$$x \notin U \wedge (x \in U \vee x \in U') \Longleftrightarrow (x \notin U \wedge x \in U) \vee (x \notin U \wedge x \in U') \Longleftrightarrow (x \notin U \wedge x \in U') \Longrightarrow x \in U'$$

nach Distributivität aus 1.10, was nach Transivität durch Substitution $(\times\times)$ liefert. Uff.

Hier noch die menschenfreundlichere Art das gleiche in natürlicher Sprache zu formulieren (machen Sie sich klar, dass hier wirklich das gleiche passiert). Wir zeigen zuerst, dass die linke in der rechte Seite enthalten ist. Dafür gilt es also wieder zu zeigen, dass $\bigcap X$ und $\bigcap Y$ in der rechten

Seite liegen. Nehmen wir also etwa ein Element $x \in M$, mit $x \in U$ für alle $U \in X$. Dann gilt für jedes $U' \in Y$ sicherlich $x \in U \cup U'$, also ist x in der rechten Seite enthalten. Analog für $x \in V \in Y$. Für die umgekehrte Inklusion benutzen wir wieder die Umformulierung den Übungszettels und müssen zeigen, dass ein $x \in M$, mit $x \in U \cup U'$ für alle $U \in X$ und $U' \in Y$, das aber nicht in $\bigcap X$ liegt, in $\bigcap Y$ liegen muss. Aber nicht in $\bigcap X$ zu liegen, bedeutet dass es ein $U \in X$ gibt, so dass $x \notin U$. Da aber per Annahme $x \in U \cup U'$ für alle $U' \in Y$ gilt, muss also $x \in U'$ liegen.

Ich hoffe der Kontrast in der Länge macht deutlich, wie dicht mathematische Texte meist geschrieben sind. Auch hier: Gewöhnen Sie sich lieber schnell daran, es wird nicht besser. □

Zuletzt noch eine nützliche Abkürzung, die vieles einfach macht, und eine Anmerkung, die vieles komplizierter macht:

3.8. **Definition** Ist P ein einstelliges Prädikat mit Variable x und Definitionsbereich M, M eine Menge, so setzen wir

$$\exists! x \in M \colon P := (\exists m \in M \colon P(m)) \wedge (\forall m, m' \in M \colon (P(m) \wedge P(m')) \Rightarrow m = m').$$

Gelesen wird $\exists!$ als "es existiert genau ein".

3.9. **Remark** Man mag nun auf die furchtbare Idee kommen, in allem Überschwung diejenige Menge S zu bilden, deren Elemente genau alle Mengen sind. Dann kann man beobachten, dass $S \in S$ gilt. Überrascht, mag man dann noch versuchen die Teilmenge

$$T := \{M \in S \mid M \notin M\}$$

zu betrachten und sich dann zu fragen, ob $T \in T$. Jetzt explodiert aber alles: Ist nämlich $T \in T$, so gilt nach Definition $T \notin T$. Und gilt aber $T \notin T$, so doch per definition doch $T \in T$. Dieses Paradox heißt die Russel'sche Antinomie und zeigt, dass es die Menge S nicht geben kann (Cantor's Paradies hat also doch seine Grenzen).

Um solchen Problemen vorzubeugen, fasst man Mengen heutzutage formal nicht mehr durch Cantor's (doch recht vage) Konvention 3.1, sondern rein axiomatisch. Eine genau Diskussion würde uns hier zu viel Zeit und Platz kosten; das Stichwort zum Weiterlesen sind die Zermelo-Fraenkel-Axiome. Für uns ist der Schluss erstmal, dass man nur die Konstruktionen durchführen sollte, die in diesem Kapitel angegeben sind, und keine solch wilden Experimente wie S.

4. Ordnungsrelationen

4.1. **Definition** Das *kartesische Produkt (cartesian product)* $M \times N$ zweier Mengen M und N ist die Menge der Paare (x, y) mit $x \in M$ und $y \in N$. Die Gleichheit von Paaren wiederum ist so definiert, dass

$$\forall x, x' \in M, y, y' \in N \colon (x, y) = (x', y') \Leftrightarrow (x = x') \wedge (y = y').$$

Benannt ist das kartesische Produkt nach dem französischen Mathematiker René Descartes (1596 - 1650) der zuerst die heute ebenfalls als kartesisch bekannten Koordinaten einführte um Punkte in der Ebene zu lokalisieren (in der Notation oben, die Ebene also als $\mathbb{R} \times \mathbb{R}$ identifizierte). Falsch geschrieben als Adjektiv im mathematischen Sprachgebrauch zu erscheinen ist in gewissen Weise wohl die höchste Ehre, die einem Mathematiker zu Teil werden kann. Von Descartes stammt auch der berühmte Ausspruch "Cogito, ergo sum!" (Ich denke, also bin ich.), der ein wunderbares Beispiel ist, dass die bei Anfänger (und leider auch in der wirklich wahren Welt) beliebte Variante $(A \Rightarrow B) \Rightarrow (B \Rightarrow A)$ des Umkehrschlusses wirklich Murks ist. Es scheint zumindest immer häufiger, dass nicht jeder, der ist, auch wirklich denkt.

4.2. **Beispiel** (1) Gilt $M = \{x, y\}$, so gilt

$$M \times M = \{(x, x), (x, y), (y, x), (y, y)\}.$$

(2) Es gelten $M \times \varnothing = \varnothing = \varnothing \times M$.

4.3. **Definition** Eine *Relation (relation)* R zwischen zwei Mengen M und N (oder besser "zwischen den Elementen zweier Mengen M und N", aber das ist so lang) ist eine Teilmenge $R \subseteq M \times N$.

Man stelle sich hierbei R als die Menge derer Paare von Elementen zu die in der gegebenen Beziehung zu einander stehen. Folglich schreibt man häufig auch mRn anstatt $(m,n) \in R$. Gilt $M = N$ so spricht man meist von einer Relation auf M.

4.4. **Beispiel** (1) Die Gleichheitsrelation

$$\Delta_M = \{(m,m') \in M \mid m = m'\}$$

existiert auf jeder Menge M, ebenso wie

$$M \times M \backslash \Delta_M,$$

die Ungleichheit.

(2) Die trivialen Relationen

$$M \times N \subseteq M \times N \quad \text{and} \quad \varnothing \subseteq M \times N$$

für je zwei Mengen M und N.

(3) Größenvergleich $\geqslant$ und Teilbarkeit $|$ sind zwei Relationen auf den natürlichen Zahlen.

(4) Auf $\mathcal{P}(M)$ haben wir die Teilmengenrelation

$$\{(X,Y) \in \mathcal{P}(M) \mid X \subseteq Y\}.$$

Relationen kommen in verschiedensten Spielrichtungen. Wir werden in dieser under nächsten Vorlesung drei von ihnen genauer anschauen: Ordnungsrelationen, Funktionen und Äquivalenzrelationen.

4.5. **Definition** Eine Relation R auf einer Menge M heißt

(1) *reflexiv*, falls für alle $m \in M$ gilt mRm gilt,
(2) *transitiv*, falls für alle $m,n,k \in M$ gilt $(mRn \wedge nRk) \Rightarrow mRk$,
(3) *identitiv*, falls für alle $m,n \in M$ gilt $(mRn \wedge nRm) \Rightarrow n = m$,
(4) *total*, falls für alle $m,n \in M$ gilt $mRn \vee nRm$.

Eine Relation, die reflexiv, transitiv und identitiv ist heißt eine *partielle Ordnung (partial order)*. Ist sie zusätzlich total, so spricht man von einer *totalen Ordnung (total order)*.

Selten sich Autoren einig welches dieser Konzepte der Begriff "Ordnung" oder entweder "partiell" oder "total" davor bezeichnet. Ich werde daher versuchen ihn alleine zu vermeiden. Das Paar (M,R) wird zusammen übrigends häufig als *partiell/total geordnete Menge (partially/totally ordered set)* bezeichnet, wobei sich im englischen der Begriff *poset* für den ersten Fall durchgesetzt hat.

4.6. **Beispiel** (1) Die Teilmengenrelation auf $\mathcal{P}(M)$ ist für jede Menge M eine partielle Ordnung. Total ist sie genau auf $M = \varnothing$ und Mengen der Form $M = \{x\}$: Sobald es $x,y \in M$ gibt, mit $x \neq y$, gilt weder

$$\{x\} \subseteq \{y\} \quad \text{noch} \quad \{y\} \subseteq \{x\}.$$

(2) Ähnliches gilt typischer, wenn man eine Ansammlung Mitarbeiter nach dem Vorgesetztsein ordnet: Dies ist eine partielle, aber nur in etwas seltsamen Firmen eine totale Ordnung.

(3) Die Gleichheitsrelation ist eine (sehr sehr) partielle Ordnung, die nicht total ist sobald M zwei verschiedene Elemente hat.

(4) Die leere Relation $\varnothing$ ist nur auf der leeren Menge eine partielle Ordnung (sonst ist sie nicht reflexiv), und die volle Relation $M \times M$ ist nur eine partielle Ordnung falls $M = \varnothing$ oder $M = \{x\}$ (sonst ist sie nicht identitiv).

(5) Die Ordnung nach der Größe ist eine totale Ordnung auf den natürlichen, ganzen, rationalen und auch reellen Zahlen (visualisiert im üblichen Zahlenstrahl).

(6) Teilbarkeit ist eine weitere partielle, aber nicht totale Ordnung auf den natürlichen Zahlen (es gilt schließlich weder 2 die 3 noch 3 die 2).

(7) Ist N eine Teilmenge von M und R eine partielle bzw. totale Ordnung auf M, so ist $R \cap N \times N$ wieder eine partielle bzw. totale Ordnung auf N. Man spricht von der auf N *eingeschränkten Ordnung (restricted order)*. Es kann passieren, dass diese total ist,

obwohl R es auf ganz M nicht ist. In diesem Falle nennt man N eine *Kette (chain)* von M.

(8) Ist R eine partielle Ordnung auf M, so auch $R^{\mathrm{rev}} = \{(m, m') \in M \times M \mid (m', m) \in R\}$. Eine Ordnungsrelation weiß also nicht intrinsisch, ob nun die rechte oder die linke Seite "größer" ist. Weitere Begriffe werden wir aber immer so festlegen, als wäre in n das "größere" Element falls mRn.

4.7. **Definition** Sei R eine partielle Ordnung auf M und $m \in M$. Das Element m heißt ein *größtes/kleinstes (largest/smallest)* Element von M, falls für alle $m' \in M$ gilt $m'Rm$ bzw. mRm', und *maximal/minimal*, falls für alle $m' \in M$ gilt $mRm' \Rightarrow m = m'$ bzw. $m'Rm \Rightarrow m' = m$.

Oft erweitert man diese Definition noch zu einer relativen Version: Ist $N \subseteq M$, so heißt m *obere/untere Schranke (upper/lower bound)* für N falls für alle $n \in N$ gilt nRm bzw. mRn gilt. Beachte, dass hierbei m kein Element von N sein muss.

4.8. **Beobachtung** Ist M von R partiell geordnet, so gilt:

(1) M hat höchstens ein größtes Element (also sind $x, y \in M$ größt, so folgt $x = y$).
(2) Jedes größte Element von M ist auch maximal.
(3) Besitzt M ein größtes Element, so ist jedes maximale Element von M auch größt.
(4) Ist M durch R total geordnet, so ist ebenfalls jedes maximale Element von M auch größt.

In Abwesenheit eines größten Elements, kann es in einer nur partiell geordneten Menge aber viele maximale Elemente geben, wie wir im nächsten Beispiel sehen werden.

Beweis. Die ersten beiden Aussagen folgen direkt aus der Identivität: Sind x und y beide größt, so gilt xRy weil y größt ist, und yRx weil x größt ist. Ergo $x = y$, also (1). Und für (2), ist x größt, und xRy, so gilt weil ja auch yRx gilt, wieder $x = y$. Für Aussage (3) sei $x \in M$ größt, und $y \in M$ maximal. Dann gilt wegen dem ersten yRx und damit dann wegen dem zweiten $x = y$, insbesondere ist y also auch größt. Für Aussage (4) sei $x \in M$ maximal. Dann muss wegen Totalität für alle $y \in M$ mindestens eins von xRy und yRx gelten. Aber xRy gilt nur für $y = x$, und in diesem Fall gilt auch yRx wegen Reflexivität. In allen anderen Fällen muss dann aber yRx gelten. □

4.9. **Beispiel**

(1) M ist das größte Element von $\mathcal{P}(M)$ und $\varnothing$ das kleinste.
(2) In $\mathcal{P}(M)\backslash\{M\}$ ist für jedes $x \in M$ das Element $M\backslash\{x\} \in \mathcal{P}(M)\backslash\{M\}$ maximal, aber sobald M zwei verschiedene Elemente erhält nicht größt: Falls $x \neq y$ gilt weder $M\backslash\{x\} \subseteq M\backslash\{y\}$ noch $M\backslash\{y\} \subseteq M\backslash\{x\}$.
(3) Jede Teilmenge der natürlichen Zahlen besitzt unter Größenvergleich ein kleinstes Element. Die natürlichen Zahlen besitzen aber kein maximales, erst recht kein größtes Element.
(4) Betrachten wir die natürlichen Zahlen mit der Teilbarkeitsrelation so ist 1 die kleinste natürliche Zahl und 0 die größte. In der Teilmenge $\{\text{natürliche Zahlen}\}\backslash\{0, 1\}$ sind genau die Primzahlen die minimalen Elemente und es gibt keine maximalen (erst recht keine größten) Elemente. Die maximalen Elemente von $\{2, 3, 4, 5, 6\}$ sind 4, 5 und 6, insbesondere gibt es kein größtes Element.

Hier schon einmal formulieren möchte ich einen hochgradig nicht-trivialen Satz, mit dem wir uns wahrscheinlich später noch beschäftigen müssen.

4.10. **Theorem** (Zorn'sches Lemma, 1933) *Besitzt jede Kette einer partiell geordneten Menge M eine obere Schranke, so besitzt M ein maximales Element.*

Spielen sie etwas mit dieser Aussage um sich zu überzeugen, dass sie nicht offensichtlich ist. Es ist irgendwie beeindruckend, was man mit so wenigen Begriffen, wie wir sie nun erst haben, schon an Komplexität erreichen kann. Unabhängig vom Amerikaner Max Zorn (1906 - 1993) bewies übrigends der Pole Kazimierz Kuratowski (1896 - 1980) diesen Satz schon 1922, aber der Namen zeugt davon, dass dies lange in der westlichen Welt nicht allgemein bekannt war.

5. Funktionen

Wir kommen zur zweiten Sorte Relationen, die wir genauer betrachten wollen:

5.1. **Definition** Eine Relation $R \subseteq M \times N$ heißt *Funktion* oder *Abbildung (function/map)* falls gilt:

$$\forall m \in M \exists! n \in N \colon mRn.$$

Man notiert R in diesem Falle auch also $R \colon M \to N$, und schreibt $R(m) = n$ anstatt mRn (n ist per definitionem ja eindeutig bestimmt. Die Menge M heißt die *Quelle (source)* von R und N das *Ziel (target)* von R.

Eine weiter Eigenheit der Sprache ist es, dass man häufig sagt, man beweist, dass eine Funktion *wohldefiniert (well-defined)* ist, anstatt zu sagen, dass man beweist, dass eine Relation eine Funktion ist. Auch das ist der Historie geschuldet. Wir bezeichnen mit

$$\mathrm{F}(M,N) := \{R \subseteq M \times N \mid R \text{ ist eine Funktion } M \to N\}$$

die Menge der Funktionen $M \to N$.

Man stelle sich eine Funktion immer so vor, dass sie jedem Element der Quelle genau ein Element des Ziels zuordnet und schreibt daher auch $m \mapsto R(m)$; man beachte die Unterschied zwischen dem Pfeil $\to$ in der Deklaration einer Funktion, und dem Pfeil $\mapsto$ hier. Diese Zuordnung muss aber erstmal in keinster Weise durch eine irgendwie geartete aufschreibbare Vorschrift erfolgen.

5.2. **Remark** Wir beobachten direkt, dass für zwei Funktionen $f, g \colon M \to N$ gilt, dass $f = g$ genau dann, wenn $f(m) = g(m)$ für alle $m \in M$: Die rechte Seite besagt ja ausgeschrieben nichts anderes als $f(m) = n$ genau dann, wenn $g(m) = n$ für alle $m \in M$ und $n \in N$, und das übersetzt sich zu $(m,n) \in f \Leftrightarrow (m,n) \in g$, sodass die Gleichheitsdefinition für Mengen zuschlägt.

Ebenso gilt, dass $f \subseteq g \Rightarrow f = g$ für zwei Funktionen $f, g \colon M \to N$: Um $g \subseteq f$ zu zeigen, sei $(m,n) \in g$. Dann gibt es nach Existenzteil der Wohldefiniertheit von f ein $n \in N$ mit $(m,n') \in f$, und damit auch $(m,n') \in g$. Wegen des Eindeutigkeitsteils der Wohldefiniertheit von g gilt dann aber $n = n'$ und somit $(m,n) \in f$, was zu zeigen war.

5.3. **Beispiel**

(1) Die Gleichheitsrelation $\Delta_M \subseteq M \times M$ ist eine Funktion. In diesem Gewand bezeichnet man sie meist mit id_M, die *Identität (identity)* auf M. In Zeichen:

$$\mathrm{id}_M \colon M \longrightarrow M, \quad m \longmapsto m.$$

(2) Gegeben $x \in N$, so definiert

$$\{(m,n) \in M \times N \mid n = x\}$$

eine Funktion, die *konstante Funktion (constant function)* const_x mit Wert X. In Zeichen:

$$\mathrm{const}_x^M \colon M \longrightarrow N, \quad m \longmapsto x.$$

Achtung: Meist lässt man den Index M aus der Notation und schreibt nur const_x. Es gibt also durchaus viele Funktionen, die auch den Namen const_x hören.

(3) Für $x \in M$ definiert

$$\{(m,n) \in M \times N \mid m = x\}$$

hingegen nur dann eine Funktion, wenn $M = \{x\}$ und $N = \{y\}$ für ein $y \in N$.

(4) Ist M durch R partiell geordnet, so setzen (nur für die Dauer dieses Beispiels)

$$K(M,R) = \{N \subseteq M \mid N \text{ hat ein kleinstes Element bzgl. } R\}$$

Dann definiert

$$\{(N,m) \in K(M,R) \times M \mid m \text{ ist kleinstes Element von } N \text{ bzgl. } R\}$$

wegen Beobachtung 4.8 die Minimumsfunktion, in Zeichen

$$\min \colon K(M,R) \longrightarrow M, \quad N \longmapsto \min(N).$$

Ähnliches gilt für die Maximumsfunktion.

Dass sich die Bezeichnung "Minimumsfunktion" durchgesetzt hat, obwohl sie doch kleinste Element auswählt, ist nicht auf meinem Mist gewachsen.

(5) Ist $f\colon M \to N$ eine Funktion, so können wir zwei neue Funktionen

$$\mathrm{Im}_f\colon \mathcal{P}(M) \to \mathcal{P}(N) \quad \text{und} \quad \mathrm{Pre}_f\colon \mathcal{P}(N) \to \mathcal{P}(M)$$

definieren durch

$$U \longmapsto \{n \in N \mid \exists u \in U\colon f(u) = n\} \quad \text{und} \quad V \longmapsto \{m \in m \mid f(m) \in V\}$$

Sie heißen die *Bild- (image)* und *Urbildfunktion (preimage)* von f. Generell bezeichnet man auch

$$\mathrm{Im}(f) \coloneqq \mathrm{Im}_f(M) = \{n \in N \mid \exists m \in M\colon f(m) = n\}$$

als das Bild von f.

(6) Für $M = A \cup B$ mit $A \cap B = \varnothing$ und Funktionen $f\colon A \to N$ und $g\colon B \to N$ ist auch $h \coloneqq f \cup g \subseteq M \times N$ eine Funktion ist. Man schreibt sie als häufig als

$$h\colon M \longrightarrow N, \quad m \longmapsto \begin{cases} f(m) & m \in A \\ g(m) & m \in B \end{cases},$$

und spricht davon dass h stückweise definiert ist.

Etwa können wir so durch $\mathrm{const}_n^A \cup \mathrm{const}_{n'}^B$ eine Funktion definieren, die nicht mehr ganz konstant ist (zumindest wenn $n \neq n'$).

Allgemeiner kann man Funktionen stückweise auf einer Partition von M im Sinne der Definition 6.6 unten definieren.

Interessantere Funktionen, wie Addition, Multiplikation, Exponentiation auf den natürlichen Zahlen, Sinus, Kosinus und Polynome auf den reellen Zahlen und vieles mehr sind Beispiele, die wir uns in den Anfängervorlesungen nun Stück für Stück nähern wollen.

5.4. **Definition** Sind $R \subseteq M \times N$ und $S \subseteq N \times P$ Relationen, so setzen wir

$$S \circ R = \{(m, p) \in M \times P \mid \exists n \in N\colon mRn \wedge nSp\},$$

die *Komposition (composition)* von R mit S.

5.5. **Lemma** *Sind $R \subseteq M \times N$ und $S \subseteq N \times P$ Funktionen, so auch $S \circ R$. Desweiteren gelten für und $p \in P$*

$$S \circ \mathrm{id}_N = S \quad \textit{und} \quad \mathrm{id}_N \circ R = R$$

und

$$S \circ \mathrm{const}_n = \mathrm{const}_{S(n)} \quad \textit{und} \quad \mathrm{const}_p \circ R = \mathrm{const}_p.$$

Wenn man das auseinander schraubt gilt also per definitionem $(S \circ R)(m) = S(R(m))$. Und Achtung: In der letzten Gleichung des Lemmas bezeichnen die beiden const_p's verschiedene Abbildungen: Die linke hat Quelle N, die rechte Quelle M. Es scheint vielen (inklusive mir) so zu gehen, dass die Komposition $S \circ R$ irgendwie "falschherum" erscheint (man liest es gern als "erst S, dann R"), aber die Kovention, dass $S \circ R$ in Wahrheit "S nach R" bedeutet, liegt zu tief, als dass wir daran etwas ändern könnten. Der Grund ist wieder historisch: Man schreibt eben $f(x)$ und nicht $x(f)$ für den Wert einer Funktion f auf einem Element x und das erzwingt diese Konvention.

Beweis. Das ist eine Übungsaufgabe auf dem drittel Zettel. □

5.6. **Remark** Transitivität einer Relation R bedeutet genau $R \circ R \subseteq R$.

5.7. **Beobachtung** Sind $f\colon M \to N, g\colon N \to T$ und $h\colon T \to S$ Abbildungen so gilt $h \circ (g \circ f) = (h \circ g) \circ f$. Wir rechnen nämlich

$$[h \circ (g \circ f)](m) = h((g \circ f)(m)) = h(g(f(m))) = (h \circ g)(f(m)) = [(h \circ g) \circ f](m)$$

für jedes $m \in M$. Wie zuvor können wir beim Komponieren also die Klammern weglassen.

5.8. **Definition** Eine Funktion $f\colon M \to N$ heißt *umkehrbar (invertible)* falls es eine Funktion $g\colon N \to M$ gibt, so dass

$$f \circ g = \mathrm{id}_N \quad \text{und} \quad g \circ f = \mathrm{id}_M.$$

5.9. **Satz** *Eine Abbildung $f\colon M \to N$ ist umkehrbar genau dann, wenn sie*

(1) injektiv*, das heißt $\forall m, m' \in M\colon f(m) = f(m') \Rightarrow m = m'$, und*
(2) surjektiv*, das heißt $\forall n \in N \exists m \in M\colon f(m) = n$*

ist. In diesem Fall nennt man sie auch bijektiv *und ein g, dass die Umkehrbarkeit von f bezeugt ist eindeutig bestimmt. Es heißt die* Umkehrfunktion (inverse function) *von f, und wird mit f^{-1} bezeichnet.*

Eine andere Art Bijektivität auszudrücken ist, dass für alle $n \in N$ ein $m \in M$ existiert, so dass $\mathrm{Pre}_f(\{n\}) = \{m\}$. Direkt aus der Definition folgt auch, dass für invertierbares f auch f^{-1} invertierbar ist mit $(f^{-1})^{-1} = f$.

Beweis. Wir zeigen zunächst einmal, dass f bijektiv wirklich f umkehrbar impliziert. Ist f bijektiv, dann ist nämlich $f^{\mathrm{rev}} \subseteq N \times M$ ebenfalls eine Funktion, diesmal aber $N \to M$: Sei nämlich $n \in N$. Dann gibt es wegen Surjektivität ein $m \in n$ mit $f(m) = n$, also formal $(m, n) \in f$, und damit $(n, m) \in f^{\mathrm{rev}}$. Dies zeigt den Existenzteil der Wohldefiniertheit. Für den Eindeutigkeitsteil seien andererseits $(n, m) \in f^{\mathrm{rev}}$ und $(n, m') \in f^{\mathrm{rev}}$. Dann folgt $(m, n) \in f$ und $(m', n) \in f$, mit anderen Worten $f(m) = n = f(m')$, was wegen der Injektivität von f, wie gewünscht $m = m'$ impliziert.

Wir behaupten weiter, dass f^{rev} eine Umkehrfunktion von f ist: Um $f^{\mathrm{rev}} \circ f = \mathrm{id}_M$ nachzuweisen, benutzen wir das zweite Kriterium aus 5.2 und zeigen $\Delta_M \subseteq f^{\mathrm{rev}} \circ f$. Aber zu $(m, m) \in \Delta_M$ gilt $(m, f(m)) \in f$ und $(f(m), m) \in f^{\mathrm{rev}}$, was zeigt, dass $(m, m) \in f^{\mathrm{rev}} \circ f$. Um auch $f \circ f^{\mathrm{rev}} = \mathrm{id}_N$ analog einzusehen, beobachten wir, dass es für jedes $n \in N$ ein $m \in M$ gibt mit $f(m) = n$. Mit anderen Worten es gelten dann $(n, m) \in f^{\mathrm{rev}}$ und $(m, n) \in f$, was $(n, n) \in f \circ f^{\mathrm{rev}}$ zeigt.

Die restlichen Behauptungen der Proposition sind Spezialfälle der beiden folgenden Lemmata. □

5.10. **Lemma** *Seien $f\colon M \to N$ und $g\colon N \to T$ Abbildungen. Dann gilt*

(1) Sind f und g injektiv bzw. surjektiv, so ist auch $g \circ f$ injektiv bzw. surjektiv.
(2) Ist $g \circ f$ injektiv, so ist auch f injektiv.
(3) Ist $g \circ f$ surjektiv, so ist auch g surjektiv.

Proof. Das ist eine Übungsaufgabe auf dem dritten Zettel. □

5.11. **Lemma** *Sind $f\colon M \to N$ und $g, h\colon N \to M$ Abbildungen mit $g \circ f = \mathrm{id}_M$ und $f \circ h = \mathrm{id}_N$. Dann folgt $g = h$.*

Proof. Es gilt

$$h = \mathrm{id}_M \circ h = (g \circ f) \circ h = g \circ (f \circ h) = g \circ \mathrm{id}_N = g.$$

□

5.12. **Beispiel** Um ein illustratives Beispiel zu haben greifen wir etwas vor und schauen uns die Quadratur q mit $x \mapsto x^2$ auf verschiedenen Zahlmengen an:

(1) als Abbildung $q\colon$ {natürliche Zahlen} → {natürliche Zahlen} ist sie injektiv, aber nicht surjektiv,
(2) als Abbildung {ganze Zahlen} → {ganze Zahlen} ist sie weder injektiv noch surjektiv,
(3) ebenso als Abbildung {rationale Zahlen} → {rationale Zahlen},
(4) und auch als Abbildung {reelle Zahlen} → {reelle Zahlen}, aber
(5) als Abbildung {positive reelle Zahlen} → {positive reelle Zahlen} ist sie sogar bijektiv; eine Umkehrabbildung ist genau durch das Ziehen von zweiten Wurzeln gegeben,
(6) als Abbildung {komplexe Zahlen} → {komplexe Zahlen} ist sie schließlich surjektiv, aber nicht injektiv.

Wir charakterisieren nun noch Abbildungen die nur injektiv oder surjektiv sind:

5.13. **Satz** *Sei $f\colon M \to N$ eine Abbildung. Dann sind äquivalent:*

(1) f ist injektiv.
(2) Für alle Abbildungen $g, g'\colon T \to M$ gilt $f \circ g = f \circ g' \Rightarrow g = g'$.
(3) Für alle Abbildungen $g, g'\colon M \to M$ gilt $f \circ g = f \circ g' \Rightarrow g = g'$.

Diese Aussagen werden impliziert von

(4) Es gibt eine Abbildung $h\colon N \to M$ mit $h \circ f = \mathrm{id}_M$.

und gilt $M \neq \varnothing$, so ist die vierte ebenfalls äquivalent zu den anderen.

Proof. Wir zeigen zunächst (1) $\Rightarrow$ (2): Per Annahme gilt für alle $m \in M$, dass $f(g(t)) = f(g'(t))$, also wegen Injektivität von f auch $g(t) = g'(t)$ also nach dem Kriterium oben $g = g'$. (2) $\Rightarrow$ (3) ist klar: Das dritte ist ja der Spezialfall $T = M$ des zweiten. Alsdann beweisen wir (3) $\Rightarrow$ (1) per Umkehrschluss. Nehmen wir also an, dass $f(m) = f(m')$ gilt mit $m \neq m'$. Dann definieren wir eine Funktion

$$s\colon M \longrightarrow M, \quad x \longmapsto \begin{cases} m & x = m' \\ m' & x = m \\ x & \text{sonst} \end{cases}$$

Es gilt dann $f \circ s = f = f \circ \mathrm{id}_M$, aber $s \neq \mathrm{id}_M$. Per Transitivität folgt nun, dass (1), (2) und (3) wirklich äquivalent sind (man nennt das einen Ringschluss). Als nächstes beweisen wir (4) $\Rightarrow$ (1): Gilt nämlich $f(m) = f(m')$ für $m, m' \in M$, so folgt

$$m = \mathrm{id}_M(m) = (h \circ f)(m) = h(f(m)) = h(f(m')) = (h \circ f)(m') = \mathrm{id}_M(m') = m'$$

wie gewünscht.

Zuletzt bleibt (1) $\Rightarrow$ (4) im Falle, dass $M \neq \varnothing$. Hierzu beobachten wir zunächst, dass f sich zu einer Abbildung $f'\colon M \to \mathrm{Im}(f)$ einschränkt, was nicht anderes bedeutet als dass $f \subseteq M \times \mathrm{Im}(f)$ gilt, und auch so aufgefasst immer noch die Wohldefiniertheitseigenschaft erfüllt. Aber per definitionem ist f' nun surjektiv, und sicherlich immer noch injektiv. Also hat f nach dem (schon bewiesenen Teil von) Proposition 5.9 eine Umkehrfunktion $h'\colon \mathrm{Im}(f) \to M$. Schnappen wir uns nun ein $x \in M$ (M ist ja nicht leer!), so können wir definieren

$$h\colon N \longrightarrow M, \quad n \longmapsto \begin{cases} h'(n) & n \in \mathrm{Im}(f) \\ x & \text{sonst} \end{cases}$$

Dieses h erfüllt dann offensichtlich das gewünschte: Für $m \in M$ gilt

$$(h \circ f)(m) = h(f(m)) = h'(f(m)) = m$$

per Konstruktion. □

5.14. **Satz** *Sei $f\colon M \to N$ eine Abbildung. Dann sind äquivalent:*

(1) f ist surjektiv.
(2) Für alle Abbildungen $g, g'\colon N \to T$ gilt $g \circ f = g' \circ f \Rightarrow g = g'$.
(3) Es gibt eine Abbildung $h\colon N \to M$ mit $f \circ h = \mathrm{id}_N$.

Diese implizieren

(4) Für alle Abbildungen $g, g'\colon N \to N$ gilt $g \circ f = g' \circ f \Rightarrow g = g'$.

und falls $M \neq \varnothing$ sind sie auch äquivalent zur vierten.

Proof. Wieder fangen wir mit (1) $\Rightarrow$ (2) an: Ist $n \in N$, so gibt es per Annahme ein $m \in M$ mit $f(m) = n$. Damit rechnen wir

$$g(n) = g(f(m)) = (g \circ f)(m) = (g' \circ f)(m) = g'(f(m)) = g'(n)$$

und damit $g = g'$. (2) $\Rightarrow$ (4) ist wieder trivial, ebenso (2) $\Rightarrow$ (1) falls $M = \varnothing$. (4) $\Rightarrow$ (1) falls $M \neq \varnothing$, zeigen wir wieder per Umkehrschluss. Nehmen wir also an f ist nicht surjektiv, etwa

weil $x \in N \backslash \mathrm{Im}(f)$. Weil $M \neq \varnothing$ folgt $\mathrm{Im}(f) \neq \varnothing$. Sei also $y \in \mathrm{Im}(f)$, sodass insbesondere $x \neq y$. Wir betrachten dann die Abbildung

$$s \colon N \longrightarrow N, \quad n \longmapsto \begin{cases} y & n = x \\ n & \text{sonst} \end{cases}$$

Es gilt dann $s \circ f = f = \mathrm{id}_N \circ f$, aber $s \neq \mathrm{id}_N$.

Alsdann zeigen wir noch (3) $\Rightarrow$ (1): Für $n \in N$ gilt

$$n = \mathrm{id}_N(n) = (f \circ h)(n) = f(h(n))$$

was zeigt, dass man $h(n)$ als Urbild von n wählen kann, ergo ist f surjektiv. Zuletzt kommen wir zu (1) $\Rightarrow$ (3): Hier wähle man zu jedem $n \in N$ ein $m \in M$ mit $f(m) = n$ und konstruiere die gesuchte Abbildung h, indem man n auf solch ein m schicke... □

Der letzte Punkt des vorigen Beweises ist, wie Sie hoffentlich merken, sehr vage. Dies hat einen guten Grund: Die Aussage lässt sich mit den bisher etablierten Mitteln nicht nachweisen, sie ist eine Grundwahrheit, ähnlich der Existenz von Potenzmengen oder kartesischer Produkte. Die grundlegende Aussage ist formalisiert im folgenden Satz; in obigen Beweis wendet man ihn auf

$$g = \mathrm{Pre}_f \circ \{-\} \colon N \longrightarrow \mathcal{P}(M), \quad n \longmapsto \mathrm{Pre}_f(\{n\})$$

an.

5.15. **Fakt** (Auswahlprinzip (axiom of choice)) Gegeben sei eine Abbildung $g \colon N \to \mathcal{P}(M)$, so dass $g(n) \neq \varnothing$ für jedes $n \in N$. Dann existiert eine Abbildung $h \colon N \to M$ mit $h(n) \in g(n)$ für alle $n \in N$.

So ein h heißt eine *Auswahlfunktion (choice function)* für g. Um sich die Problematik klarer zu machen, stelle man sich einen großen Schrank mit Schubladen vor (besonders gut ist es, sich einen unendlichen Schrank vorzustellen, aber das ist vielleicht etwas schwer) mit einem Paar Socken in jeder Schublade. Ist dann M die Menge der Schubladen und N die Menge der Socken, so gibt es eine offensichtliche Funktion $M \to \mathcal{P}(N)$, die jeder Schublade ihren Inhalt (also eine zweielementige Menge von Socken) zuordnet. Eine Auswahlfunktion sucht nun in jeder Schublade einen Socken aus. Mit Schuhen anstatt Socken wäre es einfach so eine Funktion anzugeben: Man nehme immer den linken Schuh. Da sich die beiden Socken eines Paares aber nicht unterscheiden (oder wir das zumindest für unser Gedankenexperiment einmal annehmen wollen), gibt es keine Möglichkeit eine Auswahlfunktion irgendwie wirklich zu *konstruieren*. Trotzdem sind wir es hoffentlich alle hinreichend gewohnt, Socken aus Schubladen zu nehmen, dass die *Existenz* einer Auswahlfunktion offensichtlich scheint.

Dass es wirklich unmöglich ist Auswahlfunktionen im Allgemeinen auf irgendeine Art zu konstruieren, bewies 1963 der Amerikaner Paul Cohen (1934 - 2007), er erhielt hierfür 1966 die Fields-Medaille) nachdem der Österreicher Kurt Gödel (1906 - 1978) schon 1938 gezeigt hatte, dass die allgemeine Existenz von Auswahlfunktion anzunehmen der Mathematik keine Widersprüche hinzufügt. Gödel hatte zuvor allgemein gezeigt, dass sich, sind hinreichend viele Grundannahmen einmal gemacht, *immer* Aussagen konstruieren lassen, zu denen sich kein Gegenbeispiel konstruieren lässt, die aber auch nicht beweisbar sind; dies ist der Gödel'sche Unvollständigkeitssatz, einer der Grundpfeiler der modernen Logik. In der Tat werden Sie im Laufe ihres Studiums wahrscheinlich mehrere weitere solcher Aussagen kennenlernen. Die berühmtesten sind vielleicht die Kontinuumshypothese und Whiteheads Problem, aber nun hat uns dieser Ausflug weit genug von der Heimat entführt.

Als direkte Konsequenz der beiden Sätze erhalten wir:

5.16. **Korollar** *Sind A und B nicht-leere Mengen, so gilt: Es gibt eine Injektion $A \to B$ genau dann, wenn es eine Surjektion $B \to A$ gibt.*

5.17. **Definition** Wir sagen eine Menge M heißt *mächtiger (more potent)* als eine Menge N, falls es eine Injektion $N \to M$ gibt. Man schreibt $M \preccurlyeq N$. Die zwei Menge heißt *gleichmächtig (equipotent)*, falls es eine Bijektion $M \to N$ gibt. Wir werden hierfür $M \cong N$ schreiben.

Wir beenden diesen Abschnitt wieder mit zwei Sätzen, deren Beweise wir erst später führen werden:

5.18. **Theorem** *(Satz von Schröder und Bernstein, 1897) Sind A und B Mengen und existieren sowohl eine Injektion $A \to B$ und eine Injektion $B \to A$, so existiert auch eine Bijektion $A \to B$. Mit anderen Worten $A \leqslant B$ und $B \leqslant A$ implizieren $A \cong B$.*

5.19. **Theorem** *(Zermelo'scher Vergleichbarkeitssatz, 1904) Sind A und B Mengen, so existiert eine Injektion $A \to B$ oder eine Injektion $B \to A$. Mit anderen Worten $A \leqslant B$ oder $B \leqslant A$.*

Beide Sätze waren von Cantor schon in seiner ursprünglichen Arbeit, die den Begriff der Menge wie oben formulierte, vermutet worden. Felix Bernstein (1878 - 1956) bewies den ersten in seiner unter Cantor geschriebenen Doktorarbeit; Ernst Schröder (1841 - 1902) gab unabhängig und beinahe gleichzeitig ebenfalls einen Beweis. Der Vergleichbarkeitssatz benötigt übrigends (wie auch da Zorn'sche Lemma) das Auswahlaxiom und es war Ernst Zermelo (1871 - 1953) der es genau zu genau diesem Zweck das ersten Mal explizit formulierte, und mit den Worten "Dieses logische Prinzip läßt sich zwar nicht auf ein noch einfacheres zurückführen, wird aber in der mathematischen Deduktion überall unbedenklich angewendet." kommentierte (alle drei waren Deutsche): Die Auswahl von Elementen war vor seiner expliziten Diskussion (sogar von ihm selbst) als völlig selbstverständliche Beweismethode betrachtet worden und so wollen wir es von nun an auch wieder halten. Eine Begründung des ersten Teils gab er nicht und es dauerte in der Tat beinahe 60 Jahre bis Cohen Zermelos Behauptung beweisen konnte.

6. Äquivalenzrelationen

Wir wenden uns nun der dritte Sorte Relationen zu, die wir betrachten wollen:

6.1. **Definition** Eine Relation R auf einer Menge M heißt *Äquivalenzrelation (equivalence relation)* falls sie

(1) *reflexiv*, also für alle $m \in M$ gilt mRm gilt,
(2) *transitiv*, also für alle $m, n, k \in M$ gilt $(mRn \wedge nRk) \Rightarrow mRk$, und
(3) *symmetrisch* ist, also für alle $m, n \in M$ gilt $mRn \Rightarrow nRm$.

Reflexivität und Transitivität sind uns natürlich schon bei den Ordnungsrelationen begegnet.

6.2. **Beispiel**
(1) Die Gleichheitsrelation Δ_M ist auf jeder Menge eine Äquivalenzrelation (sie ist die einzige Äquivalenzrelation, die gleichzeitig eine partielle Ordnung ist). Ebenso ist die Allrelation $M \times M \subseteq M \times M$ eine Äquivalenzrelation.
(2) Ist $f\colon M \to N$ eine Abbildung und R eine Äquivalenzrelation (etwa die Gleichheit) auf N, so ist
$$f^*R := \{(m, m') \in M \times M \mid (f(m), f(m')) \in R\}$$
ein Äquivalenzrelation auf M. Für partielle/totale Ordnungen S stimmt das Analog nur für injektive Abbildungen f: Sonst ist f^*S nicht mehr identitiv. Man stelle sich etwa vor, dass f eine bestimmte Größe oder ähnliches der Elemente von M beschreibt. Dann gilt $m(f^*\Delta_N)m'$ genau dann, wenn $f(m) = f(m')$, also die gleiche Größe haben. Als informelles Beispiel ist etwa "gleichschwer" eine Äquivalenzrelation auf der Menge aller Menschen.
(3) Auf diese Weise lassen sich viele interessante Äquivalenzrelationen bauen. Fixieren wir beispielsweise eine natürliche Zahl $d \neq 0$, so nennt man zwei natürliche Zahlen n und m *äquivalent modulo d*, geschrieben $n \equiv_d m$, wenn sie den gleichen Rest bei Division mit d lassen; die Division mit Rest definiert schließlich eine Funktion {natürliche Zahlen} $\to \{0, 1, 2, \ldots, d-1\}$.
(4) Auf $\mathcal{P}(M)$ is die Gleichmächtigkeit eine äquivalenzrelation: Reflexivität folgt aus der Existenz der Identitätsabbildungen, Transivität aus (1) von Lemma 5.10, und Symmetrie aus der Existenz von Umkehrfunktionen.

Der Zweck von Äquivalenzrelationen ist es Mengen zu partionieren. Dazu haben wir:

6.3. **Definition** Gegeben eine Äquivalenzrelation R auf M heißen die nicht-leeren maximalen Elemente von

$$\{E \subseteq M \mid \forall m, m' \in E \colon mRm'\}$$

bzgl. der Teilmengenrelation die *Äquivalenzklassen (equivalence class)* von R. Die Menge der Äquivalenzklassen von R bezeichnet man mit $M/R \subseteq \mathcal{P}(M)$.

6.4. **Lemma** *Gegeben eine Äquivalenzrelation R auf M. Dann existiert zu jedem $m \in M$ genau eine Äquivalenzklasse $E \subseteq M$ mit $m \in E$, nämlich $E = \{x \in M \mid mRx\}$. Insbesondere ist*

$$\{(m, E) \in M \times M/R \mid m \in E\}$$

eine Funktion.

Man bezeichnet diese Funktion häufig mit $[-]_R \colon M \to M/R$. Es gilt dann mRm' genau dann, wenn $[m]_R = [m']_R$.

Beweis. Zur Existenz: Gegeben $x \in M$ bildet $[x]_R = \{m \in M \mid mRx\}$ wirklich eine Äquivalenzklasse mit $x \in [x]_R$ (letzteres wegen Reflexivität): Sind $m, m' \in [x]_R$, so gelten per definitionem mRx und $m'Rx$, also wegen Symmetrie auch xRm' und dann wegen Transitivität auch mRm', und erfüllt $[x]_R \subseteq E \subseteq \mathcal{P}(M)$ ebenfalls $m, m' \in E \Rightarrow mRm'$, gilt wegen $x \in [x]_R \subseteq E$ für alle $m \in E$ auf jeden Fall mRx und damit $E \subseteq [x]_R$. Also gilt dann $E = [x]_R$, was genau sagt, dass $[x]_R$ maximal ist. Dieses Argument zeigt auch die Eindeutigkeit: Ist E maximal und enthält x, so gilt auch $[x]_R \subseteq E$, und weil $[x]_R$ ja schon maximal ist, dann auch $E = [x]_R$. □

6.5. **Beispiel**
(1) Die Äquivalenzklassen der Gleichheitsrelation sind die Einpunktmengen $\{x\}$ für $x \in M$. Insbesondere ist $[-]_{\Delta_M} \colon M \to M/\Delta_M$ bijektiv. Die Allrelation hat nur eine Äquivalenzklasse, nämlich M selbst, also $M/(M \times M) = \{M\}$.
(2) Für die Äquivalenz modulo d auf den natürlichen Zahlen gibt es genau die d Äquivalenzklassen $[0]_{\equiv_d}, [1]_{\equiv_d}, \ldots, [d-1]_{\equiv_d}$. Etwa gilt $[0]_{\equiv_2} = \{\text{gerade Zahlen}\}$ und $[1]_{\equiv_2} = \{\text{ungerade Zahlen}\}$.
(3) Die Menge $\{\varnothing\}$ ist eine Äquivalenzklasse der Gleichmächtigkeit auf $\mathcal{P}(M)$, ebenso die Menge aller Einpunktmengen in M, und die Menge aller Zweipunktmengen, etc.

Die Äquivalenzklassen bilden immer eine Partition von M in folgendem Sinne:

6.6. **Definition** Eine *Partition (partition)* einer Menge M ist eine Teilmenge $X \subseteq \mathcal{P}(M)$, derart dass

(1) $U \neq \varnothing$ für alle $U \in X$,
(2) $\bigcup X = M$, und
(3) für alle $U, U' \in X$ gilt $U \neq U' \Rightarrow U \cap U' = \varnothing$.

Der folgende Satz ist Hauptsatz dieses Kapitels und diesmal beweisen wir ihn direkt.

6.7. **Theorem** *Für jede Menge ist die Abbildung*

$$\{R \subseteq M \times M \mid R \textit{ ist Äquivalenzrelation}\} \longrightarrow \{X \subseteq \mathcal{P}(M) \mid X \textit{ ist Partition}\}, \quad R \longmapsto M/R$$

eine Bijektion.

Die Umkehrfunktion ist durch

$$X \longmapsto \{(m, m') \in M \times M \colon \exists U \in X \colon m, m' \in U\}$$

gegeben.

Proof. Zunächst zeigen wir, dass M/R wirklich für jede Äquivalenzrelation R eine Partition ist: Per definition sind Äquivalenzklassen nicht leer und nach Lemma 6.4 ist jedes Element von M in einer enthalten, also $\bigcup M/R = M$. Und sind E, E' Äquivalenzklassen und $x \in E \cap E'$, so gelten mRx und $m'Rx$ für alle $m \in E$ und $m' \in E'$. Demzufolge gilt auch mRm' und damit $m' \in E$ und $m \in E'$, was $E = E'$ zeigt.

Bezeichnen wir zur Abkürzung

$$\varphi(X) \coloneqq \{(m, m') \in M \times M \colon \exists U \in X \colon m, m' \in U\}.$$

Dann zeigen wir als erstes, dass $\varphi(X)$ wirklich eine Äquivalenzrelation ist. Reflexivität folgt direkt aus der zweiten Eigenschaft einer Partition, Transitität aus der dritten (gelten nämlich $x, y \in U$ und $y, z \in U'$ so ist $y \in U \cap U'$, demzufolge $U = U'$ und damit $x, z \in U$) und Symmetrie aus der Kommutativität von $\wedge$.

Nun gilt es noch $\varphi(M/R) = R$ und $M/\varphi(X) = X$ für alle Äquivalenzrelationen R und Partitionen X nachzuweisen. Die erste Aussage ist genau der Kommentar nach Lemma 6.4.

Für die zweite Aussage ist zu zeigen, dass genau die Elemente von X Äquivalenzklassen von $\varphi(X)$ sind. Zeigen wir zunächst, dass jedes $U \in X$ wirklich eine Äquivalenzklasse ist. Tautologischerweise gilt, dass für alle $m, m' \in U$ $m\varphi(X)m'$ gilt, und ist $U \subseteq V$ und für je zwei Elemente $m, m' \in V$ gilt $m\varphi(X)m'$, dann nehmen wir uns ein Element $xinU$ her (U ist wegen der ersten Eigenschaft einer Partition nicht leer), und erhalten $x\varphi(X)m$ für alle $m \in V$. Wegen der dritten Eigenschaft von X muss dies aber von U bezeugt werden, x ist ja in keinem anderen $U' \in X$ enthalten. Also $m \in U$ und demzufolge $U = V$ und demzufolge ist U eine Äquivalenzklasse. Ist andersherum E eine beliebige Äquivalenzklasse von $\varphi(X)$, so gibt es ein $x \in E$ und wegen der zweiten Eigenschaft von X ein $U \in X$ mit $x \in U$. Aber verschiedene Äquivalenzklassen sind nach dem ersten Teil des Beweises disjunkt, also folgt $E = U$. □

7. Die natürlichen Zahlen

Nach all diesen Vorbereitungen wenden wir uns endlich den ersten Objekten zu über die wir wirklich sprechen wollen, den Zahlen und fangen hier mit den natürlichen Zahlen an. Ein Problem ist natürlich, dass wir uns dafür im Prinzip erstmal einigen müssten, was eine Zahl wirklich ist. Eigentlich spielt das, wie Sie vielleicht schon in ihrem wirklich wahren Leben schon gemerkt haben aber gar keine Rolle. Man muss nicht so sehr wissen, was eine Zahl ist, man muss nur wissen wie man zählt. Dies formalisiert man wie folgt:

7.1. **Definition** (Peano, 1889) Ein *System natürlicher Zahlen (system of natural numbers)* oder auch eine *Peanomenge* besteht aus einer Menge N, einem Element $\alpha \in N$ und einer Funktion $s \colon N \to N$, derart dass

(1) s ist injektiv
(2) $\alpha \notin \mathrm{Im}(s)$
(3) $\forall A \subseteq N \colon (\alpha \in A \wedge (n \in A \Rightarrow s(n) \in A)) \Rightarrow A = N$.

Die Funktion s heißt die *Nachfolgefunktion (successor function)* und α die *Null (zero)* des Systems.

Informell besagen die drei Axiome also, dass man Weiterzählen (1) immer zu von Null verschiedenen Zahlen (2), (2) von verschiedenen Zahlen immer zu verschiedenen Zahlen und (3), das *Induktionsprinzip (principle of induction)*, man durch Weiterzählen von Null aus jede natürliche Zahl erreicht. Ich hoffe alle diese Eigenschaften leuchten ein. Es gilt mit anderen Worten informell gilt $N = \{\alpha, s(\alpha), s(s(\alpha)), s(s(s(\alpha))), \dots\}$ und die Definition oben formalisiert die Pünktchen.

Als fundamendalste Prinzip über die natürlichen Zahlen hat man dann:

7.2. **Theorem** (Rekursionsprinzip) *Gegeben ein System natürlicher Zahlen (N, α, s), eine Menge Y, eine Funktion $g \colon Y \to Y$ und ein Element $y \in Y$, so gibt es genau eine Abbildung $f \colon N \to Y$ mit*

$$f(\alpha) = y \quad \textit{and} \quad f \circ s = g \circ f.$$

Mit anderen Worten

$$f(\alpha) = y, \quad f(s(\alpha)) = g(f(\alpha)) = g(y), \quad f(s(s(\alpha))) = g(f(s(\alpha))) = g(g(y)), \quad \dots$$

Beweis.* Den Beweis gab es in der Analysisvorlesung. Der Vollständigkeit halber schreibe ich ihn hier noch einmal auf.

Zur Existenz: Man betrachte die Menge

$$B \coloneqq \{A \subseteq N \times Y \mid (\alpha, y) \in A \wedge (n, x) \in A \Rightarrow (s(n), g(x)) \in A\}.$$

Wir behaupten, dass $f := = \bigcap B$ eine Funktion ist.

Um das zu sehen, betrachten wir

$$C := \{n \in N \colon \exists! x \in Y \colon (n, x) \in f\}$$

und zeigen $C = N$ mithilfe des Induktionsprinzips. Dafür zeigen wir zunächst $\alpha \in C$. Per Definition gilt $(\alpha, y) \in f$ und da $N \times Y \backslash \{(\alpha, x)\} \in B$ (wegen des zweiten Peanoaxioms) für alle $x \in Y$ mit $x \neq y$ gilt, folgt $(\alpha, x) \notin f$ für solche x und damit $\alpha \in C$. Für die zweite Eigenschaft nehmen wir an $n \in C$ an und müssen $s(n) \in C$ zeigen. Per Annahme gilt dann $(n, x) \in f$ für genau ein $x \in Y$, und damit nach Definition $(s(n), g(x)) \in f$. Und für $z \in Y$ mit $z \neq g(x)$ gilt dann $f \backslash \{(s(n), z)\} \in B$ (wegen des ersten Peanoaxioms), und damit $(s(n), z) \notin f$, und damit $s(n) \in C$. Dies zeigt $C = N$ (wegen des dritten Peanoaxioms), und damit ist f eine Funktion.

Bleibt noch zu zeigen, dass f die zweite der gewünschten Eigenschaften hat; $f(\alpha) = y$ haben wir ja schon gesehen. Hierfür reicht es zu beobachten, dass $f \in B$ gilt (die zweite Bedingung aus der Definition von B sagt ja dann gerade $f(s(n)) = g(f(n))$ für alle $n \in N$). Aber $(n, x) \in f$ genau dann, wenn $(n, x) \in A$ für alle $A \in B$, was per Definition $(s(n), g(x) \in A$ für alle B impliziert, und damit $(s(n), g(x)) \in f$.

Zur Eindeutigkeit: Sind $f, f' \colon N \to X$ zwei Abbildungen, die die Bedingungen aus dem Theorem erfüllen, so betrachten wir

$$A := \{n \in N \mid f(n) = f(n')\}$$

und zeigen wieder $A = N$ mittels des Induktionsprinzips. Aus $f(\alpha) = y = f'(\alpha)$ folgt $\alpha \in A$ und gilt $n \in A$, so rechnen wir

$$f(s(n)) = g(f(n)) = g(f'(n)) = f'(s(n)),$$

was $s(n) \in A$ zeigt. □

Als unmittelbare Anwendung erhält man:

7.3. **Korollar** (Eindeutigkeit der natürlichen Zahlen) *Sind (N, α, s) und (M, β, t) Systeme natürlicher Zahlen, so gibt es genau eine Abbildung $f \colon N \to M$ mit $f(\alpha) = \beta$ and $f \circ s = t \circ f$. Sie ist umkehrbar.*

Es gibt also genau eine Art zwischen zwei Systemen natürlicher Zahlen hin- und her zu übersetzen.

Beweis. Die Existenz und Eindeutigkeit folgt direkt aus dem Rekursionsprinzip (mit Quelle (N, α, s) und $X = M, x = \beta$ und $g = t$). Um die Umkehrbarkeit einzusehen, wende man den Existenzteils des Rekursionssatzes nochmal andersherum an (also mit Quelle (M, β, t) und $X = N, x = \alpha, g = s$) um eine Abbildung $f' \colon M \to N$ mit $f' \circ t = s \circ f'$ zu erhalten. Aber $f' \circ f \colon N \to N$ ist dann eine Abbildung mit $(f' \circ f)(\alpha) = f'(\beta) = \alpha$ und

$$f' \circ f \circ s = f' \circ t \circ f = s \circ f' \circ f.$$

Aber ebenso gilt $\mathrm{id}_N(\alpha) = \alpha$ und $\mathrm{id}_N \circ s = s \circ \mathrm{id}_N$, sodass die Eindeutigkeit im Rekursionssatz $f' \circ f = \mathrm{id}_N$ erzwingt. Ähnliches für $f \circ f'$ und id_M. □

Beschäftigen wir uns nun mit der Existenz von Systemen natürlicher Zahlen:

7.4. **Definition** (Dedekind, 1888) Eine Menge M heißt *endlich (finite)* falls gilt $\forall f \colon M \to M \colon f$ injektiv $\Leftrightarrow$ f surjektiv. Ansonsten heißt sie *unendlich (infinite).*

Per Definitionem ist die Menge N in einem System natürlicher Zahlen (N, α, s) unendlich: s ist injektiv, aber nicht surjektiv da $\alpha \neq \mathrm{Im}(s)$. Umgekehrt gilt:

7.5. **Lemma** (Existenz der natürlichen Zahlen) *Ist $f \colon M \to M$ injektiv und $x \in \mathrm{Im}(f)$, so hat die Menge*

$$\{X \subseteq M \colon x \in X \wedge (m \in X \Rightarrow f(m) \in X)\}$$

ein kleinstes Element N. Die Abbildung f schränkt sich zu einer Abbildung $s \colon N \to N$ ein, und (N, x, s) ist dann ein System natürlicher Zahlen.

Gibt es also überhaupt eine unendliche Menge (und daran glauben wir natürlich), so gibt es auch ein System natürlicher Zahlen.

Beweis.* Wieder gab es den Beweis in der Analysisvorlesung, und ich schreibe ihn hier der Vollständigkeit nochmal auf:

Wir setzen

$$A = \{X \subseteq M \colon x \in X \wedge (m \in X \Rightarrow f(m) \in X)\}.$$

und $N = \bigcap A$. Man überprüft leicht, dass $N \in A$ (ähnlich zur Behauptung, dass $\bigcap B \in B$ im Beweis des Rekursionsprinzips), und per Definition gilt $N \subseteq X$ für alle $X \in A$, sodass N wirklich ein kleinstes Element ist. Per Definition gilt $n \in N \Rightarrow f(n) \in N$, was zeigt, dass $s := f \cap N \times N$ eine Abbildung $s \colon N \to N$ definiert. Soviel zu den Vorüberlegungen.

Bleibt zu zeigen, dass (N, x, s) die Peanoaxiome erfüllt. Per Annahmen gilt $x \notin \mathrm{Im}_f$, also sicherlich $x \notin \mathrm{Im}_s$, und s ist als Einschränkung von f auch injektiv. Sei also zuletzt $B \subseteq N$, mit $x \in B$ und $m \in B \Rightarrow f(m) \in B$; wir müssen $B = N$ zeigen. Aber es gilt dann ja $B \in A$ und N ist das kleinste Element von A, also $N \subseteq B$ und damit $N = B$. □

Zusammen genommen erlauben uns die Existenz und Eindeutigkeit etwas missbräuchlich von *dem* System natürlicher Zahlen zu sprechen.

7.6. **Definition** Wir schreiben $\mathbb{N}$ für das System natürlicher Zahlen und 0 für sein Nullelement (und weiterhin s für die Nachfolgefunktion). Weiterhin sind heutzutage folgende Symbole gebräuchlich:

$$1 := s(0), 2 := s(1), 3 := s(2), 4 := s(3), 5 := s(4), 6 := s(5), 7 := s(6), 8 := s(7) \quad \text{und} \quad 9 := s(8)$$

Diese Anzahl fixer Symbole stimmt mit der Anzahl unserer Finger überein, was sicherlich kein Zufall ist. Natürlich kann man die natürlichen Zahlen ordnen:

7.7. **Theorem** *Es gibt genau eine partielle Ordnung $\leqslant$ auf $\mathbb{N}$, sodass $n \leqslant s(n)$ für alle $n \in \mathbb{N}$ gilt. Sie ist total, 0 ist ihr kleinstes Element und überhaupt hat jede nicht-leere Teilmenge von $\mathbb{N}$ ein kleinstes Element.*

Eine partiell geordnete Menge M, in der jede Teilmenge ein kleinstes Element hat, heißt *wohlgeordnet (well-ordered)*. Solche partiellen Ordnungen sind immer total: Man betrachte die zweielementigen Teilmengen von M. Offenbar ist jede Teilmenge einer wohlgeordneten Menge wieder wohlgeordnet.

Beweis.* Wieder gab es den Beweis in der Analysisvorlesung, und ich schreibe ihn hier der Vollständigkeit nochmal auf:

Zur Existenz: Für jedes $n \in \mathbb{N}$ hat

$$T(n) := \{A \subseteq \mathbb{N} \colon n \in A \wedge (m \in A \Rightarrow s(m) \in A)$$

ein kleinstes Element $S(n)$, nämlich seinen Durchschnitt, wie schon in den Beweisen des Rekursionsprinzips und der Existenz von $\mathbb{N}$. $S(n)$ ist die Menge der (iterierten) Nachfolger von n; beispielsweise gelten $S(0) = \mathbb{N}$ nach dem Induktionsprinzip.

Wir definieren nun

$$\leqslant := \{(n, m) \in \mathbb{N} \times \mathbb{N} \mid m \in S(n)\}.$$

Dann sind Reflexivität ist klar, ebenso wie $n \leqslant s(n)$.. Alle anderen Eigenschaften bedürfen etwas Vorbereitung. Zunächst beobachten wir $S(m) \subseteq S(n) \Leftrightarrow m \in S(n)$. Die Vorwärtsimplikation folgt aus $m \in S(m)$. Die Rückrichtung weil $m \in S(n)$ impliziert, dass $S(n) \in T(m)$, und damit $S(m) \subseteq S(n)$, weil $S(m)$ ja das kleinste Element von $T(m)$ ist. Diese Überlegung zeigt sofort die Transitivität, da $\subseteq$ eine transitive Relation ist.

Als nächstes zeigen wir $S(s(n)) = S(n) \backslash \{n\}$.

Zunächst gilt $S(s(n)) \cup \{n\} = S(n)$: Nach der gerade getroffenen Überlegung gilt sicherlich $S(s(n)) \subseteq S(n)$ und $\{n\} \subseteq S(n)$ sowieso, also ist die linke in der rechten Seite enthalten und andersherum gilt $S(s(n)) \cup \{n\} \in T(n)$, sodass die rechte in der linken liegt. Es muss also $S(s(n)) =$

$S(n)\backslash\{n\}$ oder $S(s(n)) = S(n)$ gelten und um den zweiten Fall auszuschließen beweisen wir noch $S(n)\backslash\{n\} \in T(s(n))$, sodass $S(s(n)) \subseteq S(n)\backslash\{n\}$. Dazu betrachten wir

$$B := \{n \in \mathbb{N} \mid S(n)\backslash\{n\} \in T(s(n))\}.$$

Dann gilt $0 \in B$ (nach dem zweiten von Peano's Axiomen), und falls $n \in B$ gilt, so hat man $S(s(n)) \subseteq S(n)\backslash\{n\}$, also insbesondere $n \notin S(s(n))$. Daraus folgt nun leicht $S(s(n))\backslash\{s(n)\} \in T(s(s(n)))$: Nach einer Aufgabe vom vierten Zettel gilt $s(s(n)) \neq s(n)$, sodass $s(s(n)) \in S(s(n))\backslash\{s(n)\}$ und falls $m \in S(s(n))\backslash\{s(n)\}$ so gilt sicher $s(m) \in S(s(n))$, und sollte $s(m) = s(n)$ so liefert die Injektivität von s, dass $n = m$, aber $n \notin S(s(n))$.

Als nächstes zeigen wir die Totalität, also dass immer entweder $S(n) \subseteq S(m)$ oder $S(m) \subseteq S(n)$ gilt. Wieder betrachten wir hierfür

$$A = \{n \in \mathbb{N} \mid \forall m \in \mathbb{N}\colon S(n) \subseteq S(m) \text{ oder } S(m) \subseteq S(n)\}$$

Dann gilt $S(m) \subseteq \mathbb{N} = S(0)$, also $0 \in A$. Sei dann $n \in A$ und $m \in \mathbb{N}$. Gilt $S(m) \subseteq S(n)$, so folgt wegen $S(s(n)) = S(n)\backslash\{n\}$ auch $S(m) \subseteq S(s(n))$, außer im Falle $n \in S(m)$. Aber in diesem Falle folgt, dann $S(n) \subseteq S(m)$ und dann sicherlich $S(s(n)) \subseteq S(n) \subseteq S(m)$, also in jedem Falle $s(n) \in A$. Also ist $\leqslant$ total.

Zu guter letzt bleibt noch die Identivität übrig: Mit anderen Worten gilt $S(n) = S(m)$ so folgt $n = m$. Wieder setzen wir

$$C := \{n \in \mathbb{N} \mid \forall m \in \mathbb{N}\colon S(n) = S(m) \Rightarrow n = m\}.$$

Für $m > 0$ ist $\mathbb{N}\backslash\{0\} \in T(0)$, also $0 \notin S(m)$ und damit $S(0) \neq S(m)$, ergo $0 \in C$. Ist dann $n \in C$, und $S(s(n)) = S(m)$, so ist $n \neq S(m)$, also $m \neq 0$. Dann gibt es ebenfalls nach einer Aufgabe des vierten Zettels ein $p \in \mathbb{N}$ mit $s(p) = m$ und damit

$$S(n)\backslash\{n\} = S(s(n)) = S(s(p)) = S(p)\backslash\{p\}.$$

Wegen Totalität gilt nun $S(p) \subseteq S(n)$ oder $S(n) \subseteq S(p)$. Nehmen wir etwa das erste an, so gilt $p \in S(n)$, also kann $p \notin S(n)\backslash\{n\}$ nur gelten, wenn $n = p$ ist, und andersherum ebenso.

Damit ist $\leqslant$ endlich als totale Ordnung auf $\mathbb{N}$ nachgewiesen. Wir berechnen dann noch die Mi

Zeigen wir nun noch, dass jede nicht-leere Teilmenge M ein kleinstes Element hat. Dazu sei

$$D := \{n \in \mathbb{N}\colon \forall M \subseteq \mathbb{N}\colon \exists i \leqslant n\colon i \in M \Rightarrow M \text{ hat kleinstes Element}\}$$

Dann gilt $0 \in D$, da 0 ja sogar kleinstes Element von ganz $\mathbb{N}$, erst recht von jedem $M \subseteq \mathbb{N}$ mit $0 \in M$. Gilt $n \in D$, und $M \subseteq \mathbb{N}$ mit $s(n) \in M$, so kann entweder $i \in M$ für ein $i \leqslant n$ gelten, sodass M nach Annahme ein kleinstes Element hat oder es ist $s(n)$ eben das kleinste Element von M.

Zur Eindeutigkeit: Ist R eine weitere partielle Ordnung auf $\mathbb{N}$ mit $nRs(n)$, so folgt $\{m \in \mathbb{N} \mid nRm\} \in T(n)$, und damit $S(n) \subseteq \{m \in \mathbb{N} \mid nRm\}$, mit anderen Worten $n \leqslant m \Rightarrow nRm$, und damit $\leqslant \subseteq R$. Gilt nun aber nRm, so gilt wegen der Totalität von $\leqslant$ mindestens eins von $n \leqslant m$ und $m \leqslant n$. Im zweiten Falle folgt mRn und damit $n = m$, also $n \leqslant m$ und damit $R \subseteq \leqslant$, was noch zu zeigen war. □

Die Ordnung erlaubt uns nun zu formulieren:

7.8. **Satz** (Allgemeines Rekursionsprinzip) *Seien X und Y Mengen, $y\colon X \to Y$ and*

$$g\colon \mathrm{F}(X \times \mathbb{N}, Y) \times X \times \mathbb{N} \to Y$$

eine Funktion die für alle $h, h'\colon X \times \mathbb{N} \to Y$ und $n \in \mathbb{N}$ die Implikation

$$(\forall i \leqslant n, x \in X\colon h(x,i) = h'(x,i)) \Longrightarrow \forall x \in X\colon g(h,x,n) = g(h',x,n)$$

erfüllt. Dann existiert genau eine Abbildung $f\colon X \times \mathbb{N} \to Y$ mit

$$f(x,0) = y(x) \quad \textit{and} \quad f(x,s(n)) = g(f,x,n)$$

für alle $n \in \mathbb{N}$ und $x \in X$.

Der Satz sieht erstmal sehr viel komplizierter aus als das (spezielle) Rekursionsprinzip, aber diese Allgemeinheit ist wirklich nötig, wie wir jetzt und auf dem Übungszettel und auch im folgenden Satz sehen werden.

Scharfes Hinsehen zeigt, dass die Bedinung die wir an g hier stellen besagt, dass der Wert von $g(f,x,n)$ nur von x,n und $f(0),f(1),f(2),\dots,f(n)$ abhängt, nicht aber von $f(s(n)),f(s(s(n))),\dots$. Das erkennt man hoffentlich direkt als notwendige Bedingung, dass das rekursive Definieren von $f(x,s(n))$ als $g(f,x,n)$ nicht selbstreferentiell oder schlimmer noch vorgreifend wird.

Beweis.* Diesen Beweis gab es zwar in der Analysisvorlesung nicht, aber ich habe ihn in der Vorlesung trotzdem übersprungen.

Wir leiten den Satz aus dem eigentlichen Rekursionsprinzip mit einem Trick her (den ich auch jedes Mal wieder nachlesen muss): Nämlich, wir wenden 7.2 auf die Menge $\bar{X} = \mathrm{F}(X\times\mathbb{N},Y)\times\mathbb{N}$ mit der Selbstabbildung $\bar{g}\colon \bar{X}\to\bar{X}$ gegeben durch

$$(h,n)\longmapsto\left((x,i)\mapsto\begin{cases}h(x,i) & i\leqslant n\\ g(h,x,n) & i>n\end{cases},s(n)\right)$$

und das Element $\bar{y}=((x,i)\mapsto y(x),0)$ an. Wir erhalten also eine Abbildung $\bar{f}\colon\mathbb{N}\to\bar{X}$ mit

$$\bar{f}(0)=\bar{y}\quad\text{and}\quad\bar{f}(s(n))=\bar{g}(\bar{f}(n)).$$

Bezeichnen wir nun den ersten Eintrag eines Paares $z=(m,n)\in M\times N$ der einfacheren Lesbarkeit halber einmal durchweg mit z_1 (also $z_1=m$) und den zweiten mit z_2 (also $z_2=n$), so können wir die gesuchte Funktion f durch

$$f(x,n)=(\bar{f}(n)_1)(x,n),$$

definieren. Bevor wir die gewünschten Eigenschaften nachweisen, beobachten wir als erstes, dass für alle $n\in\mathbb{N}$ gilt $\bar{f}(n)_2=n$: Ist nämlich $A=\{n\in\mathbb{N}\mid\bar{f}(n)_2=n\}$ so gilt per definitionem von $\bar{f}$, dass $0\in A$ und ist $n\in A$, so rechnen wir

$$\bar{f}(s(n))_2=\bar{g}(\bar{f}(n))_2=s(\bar{f}(n)_2)=s(n).$$

Nach Induktionsprinzip gilt also $A=\mathbb{N}$, was wir zeigen wollten. Nun zum Nachweis der Eigenschaften von f: Es gilt zum einen

$$f(x,0)=[\bar{f}(0)_1](x,0)=\bar{y}_1(x,0)=[(x,i)\mapsto y(x)](x,0)=y(x)$$

und zum anderen

$$\begin{aligned}f(x,s(n))&=[\bar{f}(s(n))_1](x,s(n))\\&=[\bar{g}(\bar{f}(n))_1](x,s(n))\\&=\left[(a,i)\mapsto\begin{cases}[\bar{f}(n)_1](a,i) & i\leqslant\bar{f}(n)_2\\ g(\bar{f}(n)_1),a,n) & i>\bar{f}(n)_2\end{cases}\right](x,s(n))\\&=\left[(a,i)\mapsto\begin{cases}[\bar{f}(n)_1](a,i) & i\leqslant\bar{n}\\ g(\bar{f}(n)_1),a,n) & i>\bar{n}\end{cases}\right](x,s(n))\\&=g(\bar{f}(n)_1,x,n)\end{aligned}$$

Wir behaupten nun, dass die Abbildung $\bar{f}(n)_1\colon X\times\mathbb{N}\to Y$ auf den Elementen (x,i) mit $x\in X$ und $i\leqslant n$ mit f selbst übereinstimmt. Sobald wir das gezeigt haben, kommt dann die Eigenschaft von g ins Spiel die wir noch nicht benutzt haben. Sie impliziert, dass dann wirklich $g(\bar{f}(n)_1,x,n)=g(f,x,n)$ gilt wie gewünscht. Die verbleibende Behauptung zeigen wir per Induktion: Sei nämlich

$$A=\{n\in\mathbb{N}\mid\forall x\in X,i\leqslant n\colon[\bar{f}(n)_1](x,i)=f(x,i)\}.$$

Dann gilt $0\in A$ weil

$$[\bar{f}(0)_1](x,0)=\bar{y}_1(x,0)=y(x)=f(x,0)$$

wie wir oben schon gerechnet hatten, und falls $n \in A$, so gilt für $i \leqslant s(n)$

$$\begin{aligned}
[\bar f(s(n))_1](x,i) &= [\bar g(\bar f(n))_1](x,i)\\
&= \left[(a,j) \mapsto \begin{cases}[\bar f(n)_1](a,j) & j \leqslant f(n)_2\\ g(\bar f(n)_1, a, n) & j > \bar f(n)_2\end{cases}\right](x,i)\\
&= \left[(a,j) \mapsto \begin{cases}[\bar f(n)_1](a,j) & j \leqslant n\\ g(\bar f(n)_1, a, n) & j > n\end{cases}\right](x,i)\\
&= \begin{cases}[\bar f(n)_1](x,i) & i \leqslant n\\ g(\bar f(n)_1, x, n) & i = s(\bar f(n)_2)\end{cases}\\
&= \begin{cases}f(x,i) & i \leqslant n\\ f(x,s(n)) & i = s(n)\end{cases}\\
&= f(x,i)
\end{aligned}$$

wobei wir im vorletzten Schritt für den ersten Fall die Annahme $n \in A$ benutzen und im zweiten Fall die schon gemacht Berechnung von $f(x,s(n))$ oben. Dies beendet den Nachweis, dass $n \in A \Rightarrow s(n) \in A$. Dann schlägt aber das Induktionsprinzip zu und wir erhalten $A = \mathbb{N}$, was den Beweis beendet, dass$f$ die gewünschten Eigenschaften hat, und damit den gesamten Existenzteil des Beweises.

Die Eindeutigkeit ist leichter: Sind $f, f' \colon X \times \mathbb{N} \to Y$ zwei Abbildungen, die die Bedingungen des Satzes erfüllen, so setzen wir:

$$B = \{n \in \mathbb{N} \mid \forall x \in X, i \leqslant n \colon f(x,i) = f'(x,i)\}.$$

Wieder gilt $0 \in B$ weil $f(x,0) = y(x) = f'(x,0)$ und falls $n \in B$ so gilt auch

$$f(x,s(n)) = g(f,x,n) = g(f',x,n) = f'(x,s(n))$$

wegen der angenommen Eigenschaft von g. □

Als erste Anwendung zeigen wir, dass Dedekind's Begriff der Endlichkeit mit dem etwas naheliegenderen in Termen der natürlichen Zahlen übereinstimmt (der Punkt von Dedekind's Definition ist aber gerade, dass sie keine Referenz zu den natürlichen Zahlen macht).

7.9. **Theorem** *Eine Menge M ist endlich genau dann, wenn es ein $n \in \mathbb{N}$ und eine Bijektion $\{k \in \mathbb{N} \mid k < n\} \to M$ gibt. Solch ein $n \in \mathbb{N}$ (nicht aber die Bijektion) ist eindeutig bestimmt, und heißt die* Anzahl (number) *(der Elemente) von M, geschrieben $|M|$. Für zwei endliche Mengen gilt $M \leqslant N$ genau dann, wenn $|M| \leqslant |N|$.*

Eine Menge ist unendlich genau dann, wenn es eine Injektion $\mathbb{N} \to M$ gibt.

Etwa gilt $|\varnothing| = 0$, $|\{0\}| = 1$ und $|\{0,1,3,5\}| = 4$. Eine Menge M, für die es eine Surjektion $\mathbb{N} \to M$ nennt man *abzählbar (countable)*, und es war eine der revolutionären Entdeckungen Cantors, dass es unendliche Mengen gibt, die nicht abzählbar sind. Weiteres dazu gibt es ebenfalls in der Analysisvorlesung.

Beweis.* Wieder gab es den Beweis in der Analysisvorlesung, und ich schreibe ihn hier der Vollständigkeit nochmal auf.

Als erstes zeigen wir die letzte Aussage. Dass es zu unendlichen Mengen M eine Injektion $\mathbb{N} \to M$ gibt, ist Teil von 7.5. Und hat man umgekehrt eine Injektion $f \colon \mathbb{N} \to M$, so definiert man eine Abbildung

$$M \longrightarrow M, \quad m \longmapsto \begin{cases} m & m \notin \operatorname{Im}_f\\ f(s(n)) & m = f(n)\end{cases}$$

die injektiv ist und $f(0)$ nicht trifft.

Als nächstes zeigen wir, dass die Mengen $\{k \in \mathbb{N} \mid k < n\}$ wirklich endlich sind. Dazu setzen wir natürlich

$$A = \{n \in \mathbb{N} \mid \{k \in \mathbb{N} \mid k < n\} \text{ ist endlich}\}.$$

Dann gilt $0 \in \mathbb{N}$, denn die eindeutig bestimmte Abbildung $\varnothing \to \varnothing$ ist sowohl injektiv als auch surjektiv. Und gilt $n \in A$ und $f\colon \{k \in \mathbb{N} \mid k < s(n)\} \to \{k \in \mathbb{N} \mid k < s(n)\}$ ist injektiv, so betrachten wir die Abbildung

$$\sigma\colon \{k \in \mathbb{N} \mid k < s(n)\} \to \{k \in \mathbb{N} \mid k < s(n)\}, \quad m \longrightarrow \begin{cases} f(s(n)) & i = s(n) \\ s(n) & i = f(s(n)) \\ i & i \neq s(n), f(s(n)) \end{cases}.$$

Sie ist offenbar bijektiv, und desmzufolge $\sigma \circ f$ immer noch injektiv nach 5.10. Aber es gilt $\sigma(f(s(n)) = s(n)$, sodass sich $\sigma \circ f$ zu einer (immer noch injektiven) Abbildung $\{k \in \mathbb{N} \mid k < n\} \to \{k \in \mathbb{N} \mid k < n\}$ einschränkt. Diese muss dann nach Annahme bijektiv sein, und dann ist es aber auch $\sigma \circ f$ in Gänze, und damit auch f. Den Fall, dass f als surjektiv ist kann man ähnlich beweisen, oder er folgt, indem man einen Schnitt h von f wählt wie in 5.14, beobachtet, dass dieser injektiv ist nach 5.13, ergo bijektiv nach dem gerade bewiesenen. Aber dann muss nach 5.11 auch f bijektiv sein. Das bedeutet $s(n) \in A$, und eine Anwendung des Induktionsprinzips beendet den Beweis.

Als drittes zeigt man, dass es für $n < m$ (also $n \leqslant m \wedge n \neq m$) keine Surjektion $\{k \in \mathbb{N} \mid k < n\} \to \{k \in \mathbb{N} \mid k < m\}$ gibt (oder dann äquivalent keine Injektion in die andere Richtung); dies ist das sogenannte *Schubfachprinzip (pidgeon hole principle)*. Es zeigt zu gleich, dass eine Menge höchstens eine Anzahl hat (dass alle endlichen Mengen eine Anzahl haben, zeigen wir erst im letzten Schritt), und dass $M \leqslant N$ genau dann, wenn $|M| \leqslant |N|$. Natürlich beweisen wir das Schubfachprinzip mit Induktion. Nämlich betrachten wir

$$C \coloneqq \{n \in \mathbb{N} \mid \forall n < m \in \mathbb{N}\colon \text{es existiert keine Surjektion} \{k \in \mathbb{N} \mid k < n\} \to \{k \in \mathbb{N} \mid k < m\}\}$$

Dann gilt $0 \in C$: Die leere Menge surjiziert nur auf die leere Menge. Und gilt $n \in C$, und $f\colon \{k \in \mathbb{N} \mid k < s(n)\} \to \{k \in \mathbb{N} \mid k < m\}$ eine Abbildung mit $s(n) < m$. Wir müssen zeigen, dass f nicht surjektiv ist. Liegt m nicht im Bild von f sind wir natürlich sofort fertig. Sonst sei $x < s(n)$ ein Urbild von m. Liefert

$$\tau\colon \{k \in \mathbb{N} \mid k < n\} \longrightarrow \{k \in \mathbb{N} \mid k < s(n)\} \backslash \{x\}, \quad a \longmapsto \begin{cases} i & i < x \\ s(i) & x \leqslant i \end{cases}$$

eine Bijektion, sodass per Induktionshypothese $f \circ \tau$ nicht surjektiv sein kann. Und liegt $y < m$ nicht im Bild von $f \circ \tau$, so liegt y auch nicht im Bild von f, da per Konstruktion ja $\mathrm{Im}_f = \mathrm{Im}_{f\circ\tau} \cup \{m\}$ gilt.

Als letztes beweisen wir, dass eine endliche Menge eine Bijektion zu einer der Mengen $\{k \in \mathbb{N} \mid k < n\}$ besitzt. Wir machen das mithilfe eines Umkehrschlusses. Sei also M eine Menge, die zu keinem $\{k \in \mathbb{N} \mid k < n\}$ in Bijektion steht. Wir werden zeigen, dass es eine Injektion $\mathbb{N} \to M$ gibt. Hierzu beobachten wir zuerst, dass es für jedes n zumindest eine Injektion $\{k \in \mathbb{N} \mid k < n\} \to M$ gibt. Dazu betrachten wir wieder die Menge B aller $n \in \mathbb{N}$ für die das wahr ist. Dann gilt $0 \in B$, da die eindeutige Abbildung $\varnothing \to M$ injektiv ist, und ist $f\colon \{k \in \mathbb{N} \mid k < n\} \to M$ injektiv, so ist f nach Annahme nicht surjektiv und für $x \notin \mathrm{Im}_f$ ist dann auch

$$\{k \in \mathbb{N} \mid k < s(n)\} \to M, \quad \begin{cases} f(i) & i \leqslant n \\ x & i = s(n) \end{cases}$$

injektiv, sodass $n \in B \Rightarrow s(n) \in B$, und damit $B = \mathbb{N}$ wie gewünscht. Das zeigt, dass man das Auswahlprinzip auf

$$\mathbb{N} \longrightarrow \mathcal{P}(\mathcal{P}(\mathbb{N} \times M)), \quad n \mapsto \{f \subseteq \mathbb{N} \times M \mid f \text{ ist eine injektive Funktion } \{k \in \mathbb{N} \mid k < n\} \to M\}$$

anwenden kann. Man erhält also eine Abbildung $u\colon \mathbb{N} \to \mathcal{P}(\mathbb{N}\times M)$ mit $u(n)\colon \{k \in \mathbb{N} \mid k < n\} \to M$ injektiv für alle $n \in \mathbb{N}$.

Nun definieren wir $f\colon \mathbb{N} \to M$ durch $f(0) = u_1(0)$ und informell indem wir $f(s(n))$ also $u_{s(n)}(i)$, wobei i das kleinste Element ist, derart dass $u_{s(n)}(i) \neq f(0), f(1), \ldots, f(n)$; so ein Element gibt

es dann genau nach dem eben bewiesenem Schubfachprinzip. Formal benutzen wir hierfür, dass allgemeine Rekursionsprinzip mit

$$g\colon \mathrm{F}(\mathbb{N}, M) \times \mathbb{N} \to M, \quad (h, n) \mapsto u_{s(n)}(\{\min\{i \leqslant s(n)\colon \forall j \leqslant n\colon u_{s(n)}(i) \neq h(j)\}).$$

Dass die resultierende Abbildung injektiv ist, ist hoffentlich klar. □

7.10. **Remark** Dieses Theorem enthält insbesondere den Satz von Schröder und Bernstein im Falle endlicher Mengen. Ich wiederhole noch einmal, dass es nicht wahr ist, dass jede unendliche Menge eine Injektion nach $\mathbb{N}$ besitzt.

Als nächstes wollen wir die üblichen Rechenoperationen diskutieren. Einführen werden sie mit dem Rekursionsprinzip. Die Addition ist aber etwa eine Abbildung $\mathbb{N} \times \mathbb{N} \to \mathbb{N}$, sodass es sich nicht direkt anwenden lässt. Wir brauchen:

7.11. **Korollar** *Es gibt eindeutige Funktionen* $\mathrm{add}\colon \mathbb{N}\times\mathbb{N} \to \mathbb{N}$ *und* $\mathrm{mult}\colon \mathbb{N}\times\mathbb{N} \to \mathbb{N}$*, die* Addition (addition) *und die* Multiplikation (multiplication)*, mit*

$$\mathrm{add}(m, 0) = n \quad \textit{und} \quad \mathrm{add}(m, s(n)) = s(\mathrm{add}(m, n))$$

und

$$\mathrm{mult}(m, 0) = 0 \quad \textit{und} \quad \mathrm{mult}(m, s(n)) = \mathrm{add}(m, \mathrm{mult}(m, n))$$

für alle $m, n \in \mathbb{N}$*.*

Wir werden natürlich meistens $n+m$ anstatt $\mathrm{add}(n, m)$ und $n \cdot m$ anstatt $\mathrm{mult}(n, m)$ schreiben.

Beweis. Für die Addition wende man das allgemeine Rekursionsprinzip mit $X = \mathbb{N} = Y, y = \mathrm{id}_{\mathbb{N}}$ und $g(h, x, n) = s(h(x, n))$ an. Für die Multiplikation wende man es mit $X = \mathbb{N} = Y, y = \mathrm{const}_0$ und $g(h, x, n) = \mathrm{add}(x, h(x, n))$ an. □

7.12. **Beispiel**

(1) Etwa haben wir

$$n + 1 = \mathrm{add}(n, s(0)) = s(\mathrm{add}(n, 0)) = s(n)$$
$$n + 2 = \mathrm{add}(n, s(1)) = s(\mathrm{add}(n, 1)) = s(n + 1) = s(s(n))$$

und so weiter,

(2) und auch

$$n \cdot 1 = \mathrm{mult}(n, s(0)) = \mathrm{add}(n, \mathrm{mult}(n, 0)) = \mathrm{add}(n, 0) = n$$
$$n \cdot 2 = \mathrm{mult}(n, s(1)) = \mathrm{add}(n, \mathrm{mult}(n, 1)) = \mathrm{add}(n, n) = n + n$$

et cetera.

(3) Ein konkretes Beispiel:

$$3 + 3 = 3 + s(2) = s(3 + 2) = s(3 + s(1)) = s(s(3 + 1))$$
$$= s(s(3 + s(0))) = s(s(s(3 + 0))) = s(s(s(3))) = s(s(4)) = s(5) = 6$$

wie hoffentlich auch alle erwartet haben.

Es gelten nun eine große Zahl Rechengesetze, die uns immer wieder begegnen werden und denen wir deshalb vorab Namen geben:

7.13. **Definition** Eine Menge M zusammen mit einer Abbildung

$$M \times M \to M, \quad (m, n) \longmapsto m * n,$$

einer sogenannten *Verknüpfung (composition)*, und einem Element $e \in M$ heißt *Monoid (monoid)*, falls für alle $m, n, k \in M$ gilt

(1) Assoziativität

$$(m * n) * k = m * (n * k)$$

(2) Neutralität

$$m * e = m = e * m$$

So ein Monoid heißt *abelsch*, wenn weiter gilt

(3) Kommutativität

$$m * n = n * m$$

Ist auf M auch noch eine partielle Ordnung $\preccurlyeq$ auf M gegeben, so sagt man $(M, \preccurlyeq, *, e)$ ist ein *partiell geordneter Monoid*, falls noch

(4) Monotonie

$$m \preccurlyeq n \Longrightarrow m * k \preccurlyeq n * k \quad \text{und} \quad k * m \preccurlyeq k * n$$

gilt. Ist stattdessen eine zweite Verknüpfung

$$M \times M \to M, \quad (m, n) \longmapsto m \times n,$$

und ein weiteres Element $f \in M$ gegeben, so nennt man das Tupel $(M, *, \times, e, f)$ eine *Halbring (semiring)*, falls

(1) $(M, *, e)$ ist ein kommutativer Monoid,
(2) $(M, \times, f)$ ist ein Monoid, und
(3) Distributivität

$$(m * n) \times k = (m \times k) * (n \times k)$$

und

$$m \times (n * k) = (m * n) \times (m * k)$$

gelten. So ein Halbring heißt kommutativ, wenn auch die zweite Verknüpfung kommutativ ist. Ein *partiell geordneter Halbring* besteht schließlich aus all dem obigen, ist also ein Tupel $(M, \preccurlyeq, *, \times, e, f)$ derart, dass

(1) $(M, *, \times, e, f)$ ist ein Halbring,
(2) Die Ordnung $\preccurlyeq$ macht $(M, *, e)$ zu einem geordneten Monoiden, und
(3) $m \preccurlyeq n$ und $e \preccurlyeq k \Longrightarrow m \times k \preccurlyeq n \times k$ und $k \times m \preccurlyeq k \times n$.

Uff.

Ringe (also nicht nur halbe) werden uns ebenfalls bald begegnen. Die Haupteigenschaften der Addition und Multiplikation lassen sich also Zusammenfassen durch folgenden Satz, der in gewisser Form sicherlich schon in der Antike bekannt war (und natürlich obige Definition in seiner Gänze motiviert):

7.14. **Satz** (nach Adam Riese) *Das Tupel* $(\mathbb{N}, \leqslant, +, \cdot, 0, 1)$ *bildet einen total geordneten kommutativen Halbring, mit*

$$a \leqslant b \Longleftrightarrow \exists c \in \mathbb{N} \colon b = a + c.$$

Desweiteren gelten immer

$$a + b = a + c \Longrightarrow b = c \quad \textit{und} \quad a \cdot b = a \cdot c \Longrightarrow b = c$$

solange $a \neq 0$.

In Anlehnung an diesen Satz bezeichnet man die erste der beiden Verknüpfungen in einem Ring meist auch als Addition und die zweite als Mulitplikation, obwohl sie mit der Addition und Multiplikation von Zahlen nicht viel gemein haben müssen. Und natürlich stammt der Satz *nicht* vom Mathematiker Adam Riese (1492 - 1559), aber ich finde die Sprechweise so nett.

Beweis.* Wieder ist der Beweis Teil der Analysisvorlesung und er steht hier nur der Vollständigkeit halber.

Es gibt viele Einzelpunkte, keiner von ihnen schwer. Fangen wir etwa mit der Assoziativität der Addition an. Hierzu betrachten wir

$$A = \{k \in \mathbb{N} \mid \forall m, n \in \mathbb{N} \colon (m + n) + k = m + (n + k)\}$$

Dann gilt $0 \in A$ weil

$$(m + n) + 0 = m + n = m + (n + 0).$$

Und ist $k \in A$ so folgt

$$(m + n) + s(k) = s((m + n) + k) = s(m + (n + k)) = m + s(n + k) = m + (n + s(k)).$$

Dann die Neutralität von 0: $m + 0 = m$ gilt per Definition. Für die andere Richtung betrachte man

$$B = \{k \in \mathbb{N} \mid 0 + k = k\}$$

dann gilt $0 \in B$ und ist $k \in B$, dann rechnen wir

$$0 + s(k) = s(0 + k) = s(k).$$

Für die Kommutativität der Addition brauchen wir zunächste eine Hilfsaussage: Nämlich, dass immer $s(k) + m = s(k + m)$ gilt. Hierfür betrachten wir

$$C = \{m \in \mathbb{N} \mid \forall k \in \mathbb{N} \colon s(k) + m = s(k + m)\}$$

Dann gilt $0 \in C$ wegen Neutralität und ist $m \in C$, so rechnen wir

$$s(k) + s(m) = s(s(k) + m) = s(s(k + m)) = s(k + s(m))$$

also $s(m) \in C$. Für die Kommutativität betrachte nun

$$D = \{k \in \mathbb{N} \mid \forall m \in \mathbb{N} \colon m + k = k + m\}$$

Wegen der Neutralität gilt $0 \in C$, und ist $k \in C$, so rechnen wir

$$m + s(k) = s(m + k) = s(k + m) = s(k) + m$$

wobei der letzte Schritt die Hilfsaussage benutzt.

Damit ist $(\mathbb{N}, +, 0)$ ein kommutativer Monoid. Als nächstes weisen wir die Distributivgesetze nach: Fürs erste betrachten wir

$$E = \{k \in \mathbb{N} \mid \forall m, n \in \mathbb{N} \colon (m + n) \cdot k = m \cdot k + n \cdot k\}$$

Dann gilt $0 \in E$, weil

$$(m + n) \cdot 0 = 0 = 0 + 0 = m \cdot 0 + n \cdot 0$$

und wenn $k \in E$ gilt, so rechnen wir

$$(m+n) \cdot s(k) = m+n+(m+n) \cdot k = m+n+m \cdot k+n \cdot k = m+m \cdot k+n+n \cdot k = m \cdot s(k)+n \cdot s(k),$$

wo wir die schon gezeigten Gesetze für die Addition benutzt haben. Für das zweite Distrubitvgesetz gehen wir ähnlich vor und betrachten

$$F = \{k \in \mathbb{N} \mid \forall m, n \in \mathbb{N} \colon m \cdot (n + k) = m \cdot n + m \cdot k\}$$

Dann gilt $0 \in F$, weil

$$m \cdot (n + 0) = m \cdot n = m \cdot n + 0 = m \cdot n + m \cdot 0$$

und ist $k \in F$, so rechnen wir

$$m \cdot (n+s(k)) = m \cdot s(n+k) = m+m \cdot (n+k) = m+m \cdot n+m \cdot k = m \cdot n+m+m \cdot k = m \cdot n+m \cdot s(k).$$

Als nächstes zeigen wir die Rechengesetze für die Multiplikation: Für die Neutralität haben wir $n \cdot 1 = n$ schon beobachtet und für die andere Richtung betrachten wir

$$G = \{n \in \mathbb{N} \mid 1 \cdot n = n\}.$$

Dann gilt $0 \in E$ per Definition und für $n \in E$ rechnen wir

$$1 \cdot s(n) = 1 + 1 \cdot n = 1 + n = s(0) + n = s(0 + n) = s(n)$$

nach dem Hilfssatz oben. Für die Kommutativität brauchen wir noch einen Hilfssatz, nämlich, dass $0 \cdot n = 0$ gilt. Dafür betrachten wir

$$H = \{n \in \mathbb{N} \mid 0 \cdot n = 0\}$$

Es gilt $0 \in H$ per Definition, und für $n \in H$ rechnen wir

$$0 \cdot s(n) = 0 + 0 \cdot n = 0 + 0 = 0.$$

Nun betrachten wir

$$I = \{n \in \mathbb{N} \mid \forall m \in \mathbb{N} \colon m \cdot n = n \cdot m\}.$$

Dann gilt $0 \in I$ nach obigem Hilfssatz, und für $n \in I$ rechnen wir

$$m \cdot s(n) = m + m \cdot n = 1 \cdot m + n \cdot m = (1 + n) \cdot m = s(n) \cdot m.$$

Für die Assoziativität zuletzt betrachten wir

$$J = \{k \in \mathbb{N} \mid \forall m, n \in \mathbb{N}\colon (m \cdot n) \cdot k = m \cdot (n \cdot k)\}$$

Dann gilt $0 \in E$, weil

$$(m \cdot n) \cdot 0 = 0 = m \cdot 0 = m \cdot (n \cdot 0)$$

und ist $k \in E$ so rechnen wir

$$(m{\cdot}n){\cdot}s(k) = m{\cdot}n{+}(m{\cdot}n){\cdot}k = m{\cdot}n{+}m{\cdot}(n{\cdot}k) = m{\cdot}(n{\cdot}1){+}m{\cdot}(n{\cdot}k) = m{\cdot}(n{\cdot}1{+}n{\cdot}k) = m{\cdot}(n{\cdot}(1{+}k)) = m{\cdot}(n{\cdot}s(k))$$

Damit ist $(\mathbb{N}, \cdot, 1)$ ein Monoid und $(\mathbb{N}, +, \cdot, 0, 1)$ ein kommutativer Halbring.

Dann zeigen wir den ersten Zusatz, nämlich, dass $a + (-)\colon \mathbb{N} \to \mathbb{N}$ für alle $a \in \mathbb{N}$ injektiv ist. Dafür betrachten wir

$$K = \{a \in \mathbb{N} \mid a + (-)\colon \mathbb{N} \to \mathbb{N} \text{ ist injektiv}\}.$$

Dann gilt $0 \in K$ weil $0 + (-) = \mathrm{id}_{\mathbb{N}}$ und falls $a \in K$ ist, und $s(a) + n = s(a) + m$, so folgt

$$a + 1 + n = s(a) + n = s(a) + m = a + 1 + m$$

und damit $s(n) = 1 + n = 1 + m = s(m)$ und dann $n = m$ da s injektiv ist.

Als nächstes zeigen wir die Charakterisierung der Ordnung in Termen der Addition. Dafür müssen wir nach dem Eindeutigkeitsteil von 7.7 nur nachweisen, dass

$$R = \{(a, b) \in \mathbb{N} \times \mathbb{N}\colon \exists c \in \mathbb{N}\colon b = a + c\}$$

eine partielle Ordnung ist mit $nRs(n)$. Hierzu verifizieren wir zuerst, dass sie kompatibel mit den Rechenoperationen ist: Letzteres ist klar wegen $s(n) = n + 1$. Dass $a = a + 0$ für alle $a \in \mathbb{N}$ gilt, zeigt die Reflexivität, und gelten $b = a + c$ und $b' = b + d$, so gilt

$$b' = b + d = a + (c + d)$$

was die Transitivität zeigt. Die Identitivität folgt, da wir bei $b = b' + d$ und $b' = b + c$

$$b' + 0 = b' = b + c = b' + d + c$$

rechnen können. Aber da die Abbildung $b' + (-)\colon \mathbb{N} \to \mathbb{N}$ injektiv ist, folgt $d + c = 0$. Nun betrachte man

$$X = \{c \in \mathbb{N} \mid \forall d \in \mathbb{N}\colon d + c = 0 \Rightarrow d = 0\}$$

Dann gilt wegen $d = d + 0$ zumindest $0 \in X$ und ist $c \in X$, so ist $c + s(d) = s(c + d) \neq 0$ nach dem zweiten Peanoaxiom, und deshalb folgt aus $d + s(c) = 0$ alles, insbesondere auch $d = 0$, sodass $s(c) \in K$. In obiger Situation folgt also aus $d + c = 0$ erst $c = 0$, aber dann auch $d = 0$ und damit $b = b'$. Damit ist R in der Tat eine partielle Ordnung, und damit gleich $\leqslant$.

Hieraus folgt leicht die Kompatibilität der Rechenoperationen mit der Ordnung: Gilt $m \leqslant n$ gibt es ein $a \in \mathbb{N}$ mit $n = m + a$, und dann gilt $n + k = m + a + k = m + k + a$, also $n + k \leqslant m + k$ und

$$n \cdot k = (m + a) \cdot k = m \cdot k + a \cdot k,$$

also $n \cdot k \leqslant m \cdot k$ (und wegen Kommutativität auch $k + n \leqslant k + m$ und $k \cdot n \leqslant k \cdot m$). Damit ist $(\mathbb{N}, \leqslant, +, \cdot, 0, 1)$ ein total geordneter Halbring.

Zuletzt sei $a \neq 0$ und $a \cdot n = a \cdot m$. Gilt dann etwa $n \leqslant m$, also $m = n + k$ für ein $k \in \mathbb{N}$, so rechnen wir

$$a \cdot n + 0 = a \cdot n = a \cdot m = a \cdot (n + k) = a \cdot n + a \cdot k$$

so dass wegen der Injektivität von $a \cdot n + (-)\colon \mathbb{N} \to \mathbb{N}$ auch

$$0 = a \cdot k.$$

Aber das ist nur möglich, wenn $k = 0$ gilt (was den Beweis beendet). Um diese letzte Behauptung zu sehen betrachten wir

$$L = \{k \in \mathbb{N} \mid a \cdot k > 0\} \cup \{0\}.$$

Dann gilt sicherlich $0 \in L$ und ist $k \in L$, dann kann entweder $k = 0$, in welchem Falle $0 < a = a \cdot 1 = a \cdot s(0)$ folgt, und sonst

$$0 < a \cdot k \leqslant a + a \cdot k = a \cdot s(k)$$

was in jedem Falle $s(k) \in L$ bedeutet. □

7.15. **Beispiel** Wir kennen schon einige weitere Monoide und Halbringe:

(1) Sowohl $(\mathcal{P}(M), \subseteq, \cup, \cap, \varnothing, M)$ als auch $(\mathcal{P}(M), \subseteq, \cap, \cup, M, \varnothing)$ bilden nach 3.7 partiell geordnete kommutative Halbringe. Dass man die Addition und Multiplikation in einem Halbring vertauschen kann und wieder einen erhält ist ein eher seltenes Phänomen; solche Halbringe nennt man *boolesch (boolean)* nach dem englischen Mathematiker George Boole (1815 - 1864), der sie 1847 einführte.

(2) Sicherlich ist zum Beispiel $(\mathbb{N}, \cdot, +, 1, 0)$ *kein* Halbring, da etwa
$$(1 \cdot 1) + 3 = 4 \neq 6 = (1 \cdot 3) + (1 \cdot 3)$$

(3) In den Halbringstrukturen auf der Potenzmenge gelten die beiden Kürzungsgesetze aus 7.14 ganz und gar nicht: $A \cup B = A \cup C$ impliziert nicht $B = C$, und ähnlich für Durchschnitte.

(4) $(\mathrm{F}(M, M), \circ, \mathrm{id}_M)$ ist nach 5.5 und 5.7 ebenfalls ein Monoid. Sobald M mehr als zwei Elemente besitzt ist er nicht kommutativ.

(5) Ist $(M, *, e)$ ein Monoid und X eine Menge, so können wir $\mathrm{F}(X, M)$ ebenfalls eine Verknüpfung geben indem wir $*_X \colon \mathrm{F}(X, M) \times \mathrm{F}(X, M) \to \mathrm{F}(X, M)$ durch
$$(f *_X g)(x) = f(x) * g(x)$$
definieren. Und in der Tat ist dann $(\mathrm{F}(X, M), *_X, \mathrm{const}_e)$ ebenfalls ein Monoid. Analog gilt: Ist $(R, *, \times, e, f)$ ein (kommutativer) Halbring, so auch $(\mathrm{F}(X, M), *_X, \times_X, \mathrm{const}_e, \mathrm{const}_f)$

(6) Sind $(M, *, e)$ und $(N, \times, e)$ Monoid, so erklären wir auf $M \times N$ eine Verknüpfung durch
$$((m, n), (m', n')) \longmapsto (m * m', n * n').$$
Diese liefert wieder eine Monoidstruktur mit (e, e') als neutralem Element.

(7) Auch die ganzen, rationalen, reellen und komplexen Zahlen bilden mit ihrer Addition und Multiplikation Halbringe.

Die Zusätze in 7.14 zeigen insbesondere, dass $x > y$ impliziert $x + z > y + z$ und $x \cdot z > y \cdot z$ falls $z > 0$. Damit erhalten wir sofort:

7.16. **Korollar** *Es gilt*
$$a + b = 0 \Longrightarrow a = 0 \wedge b = 0 \quad \textit{und} \quad a \cdot b = 1 \Longrightarrow a = 1 \wedge b = 1.$$
für je zwei natürlich Zahlen $a, b \in \mathbb{N}$.

Die erste Behauptung haben wir auch schon im Beweis von 7.14 durchgehen müssen, aber doppelt gemoppelt hält besser.

Beweis. Gilt etwa $a > 0$ so folgt $a + b > 0 + b = b \geqslant 0$, und ähnlich für b. Das zeigt die erste Behauptung. Für die zweite Behauptung sei dann $a \cdot b = 1$. Wäre $a = 0$ gilt $a \cdot b = 0 \neq 1$ und ähnlich wenn $b = 0$. Gilt aber $a > 1$ und $b \geqslant 1$ so, folgt $ab > 1 \cdot b = b \geqslant 1$. Also folgt $a = 1$ und damit auch $b = 1$. □

Und wir halten noch einen Fakt über die Ordnung fest, der sich leicht aus der Charakterisierung in 7.14 ergibt:

7.17. **Korollar** *Es gilt*
$$\min\{m \in \mathbb{N} \mid n < m\} = n + 1$$
für jede natürliche Zahl $n \in \mathbb{N}$.

Beweis. Wir zeigen die Behauptung zunächst für $n = 0$: Hierfür reicht es zu prüfen, dass $\{m \in \mathbb{N} \mid 1 \leqslant m\} \cup \{0\} = \mathbb{N}$, was unmittelbar aus dem Induktionsprinzip folgt. Für allgemeines n gilt nun $n < m$ genau dann, wenn es ein $0 \neq k \in \mathbb{N}$ gibt, mit $m = n + k$. Aber aus dem gerade schon bewiesenen Fall folgt $k \geqslant 1$ und somit $m = n + k \geqslant n + 1$. □

7.18. **Konstruktion** Der Zusatz von 7.14 zeigt, dass

$$\{(n,m,k) \in \mathbb{N} \times \mathbb{N} \times \mathbb{N} \mid n = m + k\}$$

eine Abbildung

$$-\colon \{(n,m) \in \mathbb{N} \times \mathbb{N} \mid m \leqslant n\} \to \mathbb{N}$$

definiert, die *Subtraktion (subtraction)*. Ähnliches gilt für die Multiplikation: Zunächst überlegt man sich, dass

$$\{(n,m) \in \mathbb{N} \times \mathbb{N} \mid \exists k \in \mathbb{N}\colon m = n \cdot k\}$$

eine partielle Ordnung auf $\mathbb{N}$ ist, die *Teilbarkeit (divisibility)*, geschrieben $n \mid m$; wir haben das in den Beispielen schonmal verwendet. Einzig die Identivität ist hier etwas subtil: Gilt $m = n \cdot k$ und $n = m \cdot l$, so folgt falls $m = 0$ gilt, sicher auch $n = 0 = m$. Ist $m \neq 0$, so folgt

$$m \cdot 1 = m = n \cdot k = m \cdot l \cdot k.$$

Also zeigt der Zusatz $l \cdot k = 1$, und damit $l = 1 = k$ nach 7.16, also $n = m$.

Nach 7.14 definiert auch

$$\{(n,m,k) \in \mathbb{N} \times \mathbb{N} \times \mathbb{N} \mid m \neq 0 \wedge n = m \cdot k\}$$

eine Funktion

$$/\colon \{(n,m) \in \mathbb{N} \times \mathbb{N} \mid m \neq 0 \wedge m \mid n\} \to \mathbb{N}$$

die *Division (division)*.

In einem Monoid $(M, *, e)$ kann man auch iterierte Verknüpfungen definieren:

7.19. **Konstruktion** Betrachte die Abbildung

$$g\colon \mathrm{F}(\mathrm{F}(\mathbb{N}, M) \times \mathbb{N}, M) \times \mathrm{F}(\mathbb{N}, M) \times \mathbb{N} \longrightarrow M, \quad (f,h,n) \longmapsto f(h,n) * h(s(n))$$

Dann existiert nach dem allgemeinen Rekursionsprinzip genau eine Abbildung $\circledast\colon \mathrm{F}(\mathbb{N}, M) \times \mathbb{N} \to M$ mit

$$\circledast(h,n) = g(\circledast, h, n) = \circledast(h,n) * h(s(n)) \quad \text{und} \quad \circledast(h,0) = e.$$

Informell gilt also

$$\circledast(h,n) = h(1) * h(2) * \cdots * h(n-1) * h(n);$$

das Symbol ist wirklich eine vergrößerte Version des Verknüpfungszeichen.

Ist nun I eine endliche, total geordnete Menge so gibt es laut einer Aufgabe auf dem vierten Aufgabenzettel genau eine monotone Bijektion $\tau\colon \{1, \dots, n\} \to I$. Ist $g\colon I \to M$ nun eine Abbildung, so definieren wir

$$\tilde{g}\colon \mathbb{N} \longrightarrow M, \quad i \longmapsto \begin{cases} g(\tau(i)) & 1 \leqslant i \leqslant n \\ e & \text{sonst} \end{cases}$$

und dann

$$\circledast_I g := \circledast(\tilde{g}, n).$$

Das gleiche funktioniert immer noch falls I unendlich ist, aber $\{i \in I\colon g(i) \neq e\}$ endlich. In diesem Fall sagt man, dass $g(i) = e$ für *fast alle* $i \in I$.

Ähnlich wie bei Durchschnitten schreibt man häufig auch $\circledast_{i \in I} g(i)$ oder ähnliches anstatt $\circledast_I g$. Gilt $I = \{k \in \mathbb{N} \mid n \leqslant k \leqslant m\}$ so schreibt man auch $\circledast_n^m g$ oder gar $\circledast_{i=n}^m g(i)$. Und ist die Verknüpfung des Monoiden mit $+$ bezeichnet, schreibt man meist $\sum_I h$ und ist sie mit $\cdot$ bezeichnet, so schreibt man $\prod_I h$.

7.20. **Beispiel** (1) Ist beispielsweise $q\colon \mathbb{N} \to \mathbb{N}, x \to x \cdot x$ die Quadratur, so gelten

$$\sum_{i=4}^{7} i^2 = \sum_{4}^{7} q = 4 \cdot 4 + 5 \cdot 5 + 6 \cdot 6 + 7 \cdot 7 \quad \text{and} \quad \prod_{i=4}^{7} i^2 = \prod_{4}^{7} q = 4 \cdot 4 \cdot 5 \cdot 5 \cdot 6 \cdot 6 \cdot 7 \cdot 7.$$

(2) Für einen Monoiden $(M, *, e)$ und $m \in M$ und $n \in \mathbb{N}$ setzt man

$$m^{*n} := *_1^n \mathrm{const}_m.$$

In den natürlichen Zahlen gilt etwa

$$n \cdot m = \sum_{i=1}^{m} n = m^{+n},$$

da beide Seiten per Konstruktion die gleiche Rekursion erfüllen. Deshalb schreibt man häufig allgemein $n \cdot m$ falls die Verknüpfung in M mit $+$ bezeichnet ist. Heißt die Verknüpfung des Monoiden $\cdot$, schreibt man meist nur n^m anstatt $n^{\cdot m}$.

(3) Im Monoiden $(\mathcal{P}(M), \cup, \varnothing)$ gilt für jede Funktion $g\colon I \to \mathcal{P}(M)$ wirklich

$$\bigcup_I g = \bigcup \mathrm{Im}_g,$$

wobei die linke Seite die iterierte Vereinigung im Sinne von 7.19 bezeichnet, und die rechte Seite die Vereinigung im Sinne von 3.5. Hierzu prüft man leicht, dass die Funktion

$$\mathrm{F}(\mathbb{N}, \mathcal{P}(M)) \times \mathbb{N} \longrightarrow \mathcal{P}(M), \quad (h, n) \longmapsto \bigcup h(\{k \in \mathbb{N}, k \leqslant n\})$$

die definieren Eigenschaften aus obiger Konstruktion erfüllt. Analoges gilt für Durchschnitte.

(4) Insbesondere gilt $A^{\cup n} = A = A^{\cap n}$ für alle $A \in \mathcal{P}(M)$ und $n \geqslant 1$.

(5) Für einen abelschen Monoiden $(M, *, e)$ hängt $*_I f$ für beliebiges $f\colon I \to M$ nicht von der Ordnung von I ab. Dies ist eine Übungsaufgabe auf dem vierten Zettel.

8. Die natürlichen Zahlen II

Die einfachste (und historisch auch erste) Art natürliche Zahlen darzustellen ist einfach mit Strichen: Also

$$1 = I, \quad 2 = II, \quad 3 = III, \quad \ldots, \quad 7 = IIIIIII, \ldots$$

was den Vorteil hat, sich nur ein Symbol merken zu müssen. Große Zahlen werden aber schnell lang. Mithilfe der iterierten Verknüfungen wollen wir uns nun zwei besseren Darstellungen von natürlichen Zahlen zuwenden. Die eine ist das Stellensystem, in dem Zahlen heutzutage üblicherweise notiert werden, die andere ist die Primfaktorzerlegung. Beide haben ihre Vor- und Nachteile und fußen auf der *Division mit Rest (division with remainder)*:

8.1. **Satz** *Sei $b \in \mathbb{N}$ mit $b \geqslant 1$. Dann gibt es zu jedem $n \in \mathbb{N}$ genau ein Paar $(q, r) \in \mathbb{N} \times \mathbb{N}$ mit*

$$n = q \cdot b + r \quad \textit{und} \quad r < b.$$

Insbesondere definiert

$$\{(n, r) \in \mathbb{N} \times \mathbb{N} \mid \exists q \in \mathbb{N}\colon n = q \cdot b + r \textit{ und } r < b\}$$

eine Funktion $\mathrm{rem}_b\colon \mathbb{N} \to \{k \in \mathbb{N}\colon k < b\}$.

Ebenso definiert

$$\{(n, q) \in \mathbb{N} \times \mathbb{N} \mid \exists r \in \mathbb{N}\colon n = q \cdot b + r \text{ und } r < b\}$$

eine Funktion. Man bezeichnet ihren Wert bei n häufig mit mit $\lfloor n/b \rfloor$. Man prüft leicht, dass sie die Division erweitert, also $\lfloor n/b \rfloor = n/b$ falls b ein Teiler von n ist.

Beweis. Natürlich zeigen wir das per Induktion. Sei A also die Menge aller $n \in \mathbb{N}$, für die die Behauptung stimmt. Dann gilt $0 \in A$: Sicherlich gilt $0 = 0 \cdot b + 0$, sodass $(0, 0)$ ein erlaubtes Paar für 0 ist, und gilt andersherum $0 = q \cdot b + r$, so folgt nach 7.16 $q \cdot b = 0$ und $r = 0$ und dann wegen der Kürzbarkeit von b auch $q = 0$.

Ist dann $n \in A$, also etwa $n = q \cdot b + r$ mit $r < b$, so gilt sicherlich

$$n + 1 = q \cdot b + r + 1.$$

Es gilt auf jeden Fall $r+1 \leqslant b$ nach 7.17. Gilt sogar $r+1 < b$ so ist $(q, r+1)$ ein erlaubtes Paar für $n+1$. Ist andererseits $r+1 = b$, so rechnen wir weiter

$$n+1 = q \cdot b + b = (q+1) \cdot b + 0$$

und finden dass $(q+1, 0)$ ein erlaubtes Paar für $n+1$ ist. Dies zeigt die Existenz einer Darstellung wie gewünscht. Zur Eindeutigkeit gelte

$$q' \cdot b + r' = n+1 = q \cdot b + r$$

mit $r', r < b$. Betrachen wir nun etwa den Fall $q' \leqslant q$ an. Dann folgt $q' \cdot b \leqslant q \cdot b$

$$r' = q \cdot b + r - q' \cdot b = r + (q - q') \cdot b.$$

Gilt nun aber $q' < q$, so folgt $q - q' \geqslant 1$ und damit

$$r = r + (q - q') \cdot b \geqslant r + b \geqslant b,$$

was der Annahme an r widerspricht, also muss $q' = q$ sein, und genauso schließt man im Fall $q \leqslant q'$. Aber wenn $q = q'$ gilt, so folgt aus

$$q \cdot b + r = q \cdot b + r'$$

auch $r = r'$. Dies zeigt $n+1 \in A$ und dann beendet das Induktionsprinzip den Beweis: Die letzten Behauptungen folgen nämlich direkt aus den Definitionen. □

8.2. **Theorem** (Stellenzerlegung) *Sei $b \geqslant 2$. Dann existiert zu jedem $n \in \mathbb{N}$ genau eine Abbildung*

$$a \colon \mathbb{N} \longrightarrow \{k \in \mathbb{N} \mid k < b\},$$

mit $a(i) = 0$ für fast alle $i \in \mathbb{N}$, und derart dass

$$n = \sum_i a(i) \cdot b^i.$$

Man beobachte, dass mit a auch die Funktion $i \mapsto a(i) \cdot b^i$ für fast alle i den Wert 0 annimmt, sodass die Summe wirklich definiert ist. Die Funktion a heißt die *b-adische Entwicklung* von n.

Der genaue Ursprung des Stellensystems ist (mir zumindest) nicht bekannt; es scheint häufig immer wieder unabhängig entdeckt worden zu sein. Archimedes hatte es wohl schon um das Jahr -250 einmal gefunden, aber langsame Verbreitung fand es erst um die erste Jahrtausendwende positiver Zeit (es war unabhängig etwa in China und Kombodscha und erfunden worden). In den europäischen Raum gelang diese Erkenntnis über Arabien erst wieder im 13. Jahrhundert und im deutschen Sprachraum fand es Verbreitung durch die Bücher von Adam Riese (daher auch der Ausspruch "nach Adam Riese"). Das Stellensystem bedarf unbedingt einer expliziten Null (man betrachtete lange die natürlichen Zahlen als bei 1 beginnend) und erst mit seiner Einführung war es möglich effizient mit den natürlichen Zahlen zu rechnen, was seinen Teil zum Aufstieg der Wissenschaft in der Aufklärung geleistet hat.

Der Beweis basiert außer der Division mit Rest noch auf folgendem:

8.3. **Satz** (Geometrische Summenformel) *Sei $(R, +, \cdot, 0, 1)$ ein Halbring. Dann gilt*

$$r \cdot \left(\sum_{i=0}^{n} r^{n-i} \cdot q^i \right) + q^{n+1} = \left(\sum_{i=0}^{n} r^{n-i} \cdot q^i \right) \cdot q + r^{n+1}$$

für alle $q, r \in R$ und $n \in \mathbb{N}$.

Es gibt extrem viele Anwendungen dieser Formel. Die klassischste ist wohl der Fall von $r = 1$ in den natürlichen Zahlen: Hier findet man

$$\left(\sum_{i=0}^{n} q^i \right) + q^{n+1} = q \cdot \left(\sum_{i=0}^{n} q^i \right) + 1$$

Ist nun $q \geqslant 1$, so folgt durch Kürzen

$$q^{n+1} = (q-1) \cdot \left(\sum_{i=0}^{n} q^i \right) + 1$$

und daher für $q \geqslant 2$

$$\frac{q^{n+1}-1}{q-1} = \sum_{i=0}^{n} q^i.$$

Allein, dass $q^{n+1}-1$ überhaupt durch $q-1$ teilbar ist, ist wohl nur für $q = 2, 3$ offensichtlich. In diesem Fall erhält man

$$\sum_{i=0}^{n} 2^i = 2^{n+1} - 1.$$

Beweis. Man rechnet schnell

$$r \cdot \left(\sum_{i=0}^{n} r^{n-i} \cdot q^i \right) + q^{n+1} = \left(\sum_{i=0}^{n} r^{n+1-i} \cdot q^i \right) + q^{n+1} = r^{n+1} + \left(\sum_{i=1}^{n} r^{n+1-i} \cdot q^i \right) + q^{n+1}$$

und ebenso

$$\left(\sum_{i=0}^{n} r^{n-i} q^i \right) \cdot q + r^{n+1} = \left(\sum_{i=0}^{n} r^{n-i} q^{i+1} \right) + r^{n+1} = q^{n+1} + \left(\sum_{i=0}^{n-1} r^{n-i} q^{i+1} \right) + r^{n+1}.$$

Aber für die beiden mittleren Terme gilt

$$\sum_{i=1}^{n} r^{n+1-i} q^i = \sum_{i=0}^{n-1} r^{n-i} q^{i+1};$$

in der Tat ist linke Seite unsere Definition der rechten, da $(-)+1 \colon \{0, \dots, n-1\} \to \{1, \dots, n\}$ eine monotone Bijektion ist. □

Beweis von Theorem 8.2. Zur Existenz: Natürlich per Induktion. Sei also A die Menge all derer natürlichen Zahlen die eine b-adische Entwicklung haben. Dann gilt sicherlich $0 \in A$: Wir haben $\sum \mathrm{const}_0 = 0$. Und liegt $n \in A$, etwa $n = \sum_i a_i b^i$ so sei

$$l \coloneqq \min\{i \in \mathbb{N} \mid a(i) + 1 < b\};$$

die Menge rechts ist nicht leer, da a nur für endliche viele i einen anderen Wert als 0 annimmt (und $b \geqslant 2$). Damit rechnen wir los

$$\begin{aligned} n+1 &= 1 + \sum_i a(i) b^i \\ &= 1 + \sum_{i=0}^{l-1} (b-1) b^i + a(l) b^l + \sum_{i>l} a(i) b^i \\ &= 1 + (b-1) \left(\sum_{i=0}^{l-1} b^i \right) + a(l) b^l + \sum_{i>l} a(i) b^i \\ &= b^l + a(l) b^l + \sum_{i>l} a(i) b^i \\ &= (a(l)+1) b^l + \sum_{i>l} a(i) b^i \end{aligned}$$

wobei wir in der Mitte einmal die geometrische Summenformel benutzt haben. Setzen wir also

$$\bar{a} \colon \mathbb{N} \longrightarrow \{k \in \mathbb{N} \mid k < b\}, \quad i \longmapsto \begin{cases} 0 & i < l \\ a(l)+1 & i = l \\ a(i) & l < i \end{cases}$$

So erhalten wir $\sum_i \bar{a}(i) b^i = n+1$ und damit $n+1 \in A$.

Zur Eindeutigkeit: Wir beobachten zunächst, dass der 0te Eintrag jeder b-adischen Entwicklung eindeutig bestimmt ist: Wir berechnen

$$\mathrm{rem}_b \left(\sum_i a(i) b^i \right) = \mathrm{rem}_b \left(a(0) + b \left(\sum_{i>0} a(i) b^{i-1} \right) \right) = a(0)$$

da ja in der Tat $a(0) < b$.

Sei nun $\sum_i a(i)b^i = n = \sum_i a'(i)b^i$. Betrachte dann $B = \{j \in \mathbb{N} \mid \forall i \leqslant j \colon a(i) = a'(i)\}$. Dann gilt $a(0) = \mathrm{rem}_b(n) = a'(0)$, also $0 \in B$. Und ist $j \in B$, so finden wir

$$\sum_i a(i+j+1)b^i = \sum_{j<i} a(i)b^{i-j} = \left(\sum_{j<i} a(i)b^j\right)/b^j = \left(\sum_i a(i)b^i - \sum_{i=0}^{j} a(i)b^i\right)/b^j = \left(n - \sum_{i=0}^{j} a(i)b^i\right)/b^j$$

und analog für die gestrichene Version. Da aber $\sum_{i=0}^{j} a(i)b^i = \sum_{i=0}^{j} a'(i)b^i$ per Annahme, folgt

$$\sum_i a(i+j+1)b^i = \sum_i a'(i+j+1)b^i.$$

Aber dies sind selber b-adische Entwicklungen, ergo folgt aus unserer Vorüberlegung $a(j+1) = a'(j+1)$ und damit $j+1 \in B$. Und dann schlägt das Induktionsprinzip zu. □

8.4. **Beispiel** Für gegebene Basis $b \geqslant 2$ bezeichnet man die zu einem $a \colon \mathbb{N} \to \{k \in \mathbb{N} \mid k < b\}$ gehörige Zahl oft mit $(a)_b$. Desweiteren, schreibt man häufig einfach die Werte von a in umgekehrter Reihung ohne Kommas hintereinander und lässt die Nullen am Anfang weg: Etwa

$$(425)_7 = 5 + 2 \cdot 7 + 4 \cdot 7^2$$

$$(10)_b = b, \quad (11)_b = b + 1, \quad \text{und} \quad (110)_b = b + b^2$$

$$(1s(9))_{s(s(9))} = s(9) + s(s(9)) = 2 \cdot s(9) + 1$$

Besonders häufig ist natürlich die Basis $b = s(9)$, man spricht vom *Dezimalsystem* und für genau diesen Fall haben wir genügend Symbole eingeführt. Man kürzt diesem Fall noch weiter ab, indem man die Basis aus der Notation weglässt. Also etwa

$$10 = s(9), \quad 11 = s(s(9)) \quad \text{und} \quad 21 = 2 \cdot 10 + 1.$$

Eine weiteres häufiges Beispiel ist $b = 2$ mit den Anfangszahlen

$$(0)_2 = 0, \quad (1)_2 = 1, \quad (10)_2 = 2, \quad (11)_2 = 3, \quad (100)_2 = 4, \quad (101)_2 = 5, \ldots$$

Dieses *Binärsystem* ist in der Informatik sehr viel gebräuchlicher als das Dezimalsystem.

Im Stellensystem ist es sehr leicht die Größe zweier Zahlen zu vergleichen und sowohl Addition als auch Multiplikation sind nicht schwer durchzuführen (das haben sie wahrscheinlich bis zum Verrecken in der Schule geübt). Es ist jedoch bis heute keine vollständige Beschreibung der Teilbarkeitsrelation im Stellensystem bekannt (und hierauf basiert die Sicherheit vieler Kryptographieverfahren). Um sich das Problem zu vergegenwärtigen, versuch sie einmal per Hand herauszufinden, ob

$$1893742374923487 \quad \text{durch} \quad 49381$$

teilbar oder gar eine Primzahl ist.

Kommen wir nun zur zweiten Art natürliche Zahlen darzustellen, bei der genau diese Eigenschaft sehr leicht abzulesen ist. Hierfür brauchen wir:

8.5. **Definition** Eine Zahl $p \in \mathbb{N}$, $p \neq 0, 1$, heißt *Primzahl (prime number)*, falls sie nur durch 1 und p teilbar ist.

Der folgende Satz heißt manchmal auch der *Fundamentalsatz der Arithmetik*.

8.6. **Theorem** (Primfaktorzerlegung) *Für jede natürliche Zahl $n \in \mathbb{N}$, $n \neq 0$, gibt es genau eine Abbildung $m \colon \{\text{Primzahlen}\} \to \mathbb{N}$ mit $m(i) = 0$ für fast alle $i \in \mathbb{N}$, so dass*

$$n = \prod_{p \ prim} p^{m(p)}.$$

Man beachte, dass die Funktion $p \mapsto p^{m(p)}$ für fast alle i den Wert 1 annimmt, sodass obiges Produkt wohldefiniert ist. Zum Beweis brauchen wir wieder noch etwas Hilfe:

8.7. **Satz** (Lemma des Euklid, -400) *Ist $p \in \mathbb{N}$ und $p \mid n \cdot m$, so folgt $p \mid n$ oder $p \mid m$.*

Allgemeiner folgt hieraus per Induktion (über k), dass wenn p ein beliebiges Produkt $\prod_{i=0}^{k} n_i$ teilt, dann teilt p schon eins der n_i: Die Aussage ist sicher wahr für $k = 0$ (dann kann p so ein Produkt nicht teilen), und teilt

$$\prod_{i=0}^{k+1} n_i = \left(\prod_{i=0}^{k} n_i\right) \cdot n_{k+1},$$

so teilt p nach obigen Lemma n_{k+1} oder $\prod_{i=0}^{k} n_i$ und hier schlägt die Induktionshypothese zu.

Beweis. Nehmen wir also an, dass p nicht n teilt und zeigen, dass dann $p \mid m$. Hierfür betrachten wir

$$A = \{i \in \mathbb{N} \mid i \neq 0 \wedge p \mid i \cdot m\}.$$

Die Menge A ist nicht leer (etwa gelten ja $n \in A$), und hat deshalb ein kleinstes Element $k \in A$ nach 7.7. Wir zeigen nun dass k jedes Element aus A teilt. Aber es gilt auch $p \in A$, also muss entweder $k = p$ oder $k = 1$ gelten. Aber es gilt $n \in A$, und p teilt n per Annahme nicht. Also muss $k = 1$ gelten, und damit teilt p nach Definition von A wie gewünscht m.

Zum Beweis der Behauptung sei $x \in A$. Dann können wir nach 8.1 $x = q \cdot k + r$ schreiben mit $r < k$. Per Definition gilt $x \cdot m = p \cdot a$ und $k \cdot m = p \cdot b$ für irgendwelche $a, b \in \mathbb{N}$, und wegen $x \geqslant k$ folgt $a \geqslant b$. Aber dann gilt

$$r \cdot m = (x - q \cdot k) \cdot m = x \cdot m - q \cdot k \cdot m = p \cdot a - q \cdot p \cdot b = p \cdot (a - q \cdot b).$$

Aber weil $r < k$ gilt, kann nicht $r \in A$ gelten, was $r = 0$ erzwingt und die Behauptung beweist. □

Beweis von Theorem 8.6. Betrachte $A = \{n \in \mathbb{N} \mid \forall 0 < i \leqslant n\colon i \text{ hat genau eine Primfaktorzerlegung}\}$. Dann gilt offenbar $0 \in A$. Ist nun $n \in A$, so unterscheiden wir drei Fälle. Ist $s(n)$ selbst prim, so gilt $s(n) \in A$ bezeugt von

$$p \longmapsto \begin{cases} 0 & p \neq s(n) \\ 1 & p = s(n) \end{cases},$$

und per Definition von Primzahlen kann es keine weitere Zerlegung von $s(n)$ geben. Ist $n = 0$, so haben wir $s(0) = 1 \in A$ bezeugt von $m = \text{const}_0$, und nach 7.16 kann es keine weitere Zerlegung geben. Ansonsten muss $s(n) = k \cdot l$ für $k, l \in \mathbb{N}$ mit $1 < k, l < n$. Dann haben aber k und l Primfaktorzerlegungen, etwa

$$k = \prod_{p \text{ prim}} p^{m(p)} \quad \text{und} \quad l = \prod_{p \text{ prim}} p^{m'(p)}$$

Es folgt, dass

$$s(n) = k \cdot l = \left(\prod_{p \text{ prim}} p^{m(p)}\right) \cdot \left(\prod_{p \text{ prim}} p^{m'(p)}\right) = \prod_{p \text{ prim}} p^{m(p)+m'(p)}.$$

Dies zeigt die Existenz einer Primfaktorzerlegung von $s(n)$. Nun noch zur Eindeutigkeit: Gilt

$$\prod_{p \text{ prim}} p^{m(p)} = s(n) = \prod_{p \text{ prim}} p^{m'(p)}$$

so sei q die kleinste Primzahl mit $m(q) \neq 0$ (wäre $m(q) = 0$ für alle Primzahlen q, so wäre $s(n) = 1$, aber den Fall haben wir schon abgeschlossen). Dann gilt $q \mid s(n)$. Nach Euklid's Lemma (oder dem Kommentar direkt danach) muss es dann zunächst einen Faktor $p^{m'(p)}$ der rechten Seite geben den q teilt. Das bedeutet nach 7.16 natürlich $m'(p) > 0$. Ist $m'(p) = 1$ bedeutet das $p \mid q$, und falls $m'(p) > 1$, so liefert eine zweite Anwendung von Euklid's Lemma ebenfalls $q \mid p$. Aber da p prim ist, bleibt also nur $q = p$. Also $m'(q) \geqslant 1$. Es folgt dann

$$\prod_{p \text{ prim}} p^{\bar{m}(p)} = s(n)/q = \prod_{p \text{ prim}} p^{\bar{m}'(p)}$$

für

$$\bar{m}\colon \{\text{Primzahlen}\} \longrightarrow \mathbb{N}, \quad p \longmapsto \begin{cases} m(p) & p \neq q \\ m(q) - 1 & p = q \end{cases}$$

und analogem $\bar{m}'$. Aber dies sind beides Primfaktorzerlegungen von$s(n)/q$ und weil $0 \neq s(n)/q < s(n)$ gibt es hiervon nur eine. Also folgt $\bar{m} = \bar{m}'$ und damit $m = m'$. Das zeigt $s(n) \in A$ und das Induktionsprinzip liefert die Behauptung. □

9. Die ganzen Zahlen

Wir haben in 7.18 gesehen, dass die Subtraktion in den natürlichen Zahlen nur manchmal funktioniert, etwa kann man nicht $2-4$ bilden. Die Idee der ganzen Zahlen ist es dies zu beheben. Zunächst etwas Terminologie:

9.1. **Definition** Ist $(M, *, e)$ ein Monoid, so heißt ein $m \in M$ eine *Einheit (unit)* falls es ein $m' \in M$ gibt mit

$$m' * m = e = m' * m.$$

So ein m' heißt *invers* zu m. Ein Monoid in dem jedes Element ein Inverses besitzt, heißt eine *Gruppe (group)*, und ein Halbring in dem die Addition eine Gruppenstruktur liefert heißt ein *Ring (ring)*.

So ein m' ist eindeutig bestimmt, da

$$m' = e * m' = m'' * m * m' = m''$$

wann immer m'' ebenfalls inverse zu m ist. Man schreibt m^{-1} (oder genauer m^{*-1}, aber das sieht oft sehr seltsam aus) für das Inverse. Wird die Vernüpfung als $+$ geschrieben so schreibt man $-m$ anstatt dem nun wirklich sehr seltsamen m^{+-1}.

9.2. **Beispiel**
(1) In jedem Monoiden $(M, *, e)$ ist e eine Einheit mit $e^{-1} = e$.
(2) In $(\mathbb{N}, +, 0)$ und $(\mathbb{N}, \cdot, 1)$ sind nur 0 bzw. 1 Einheiten nach 7.16.
(3) In $(\mathrm{F}(M, M), \circ, \mathrm{id}_M)$ ist ein Element f genau dann eine Einheit, wenn f bijektiv ist nach 5.9 und auch die Definition von f^{-1} dort passt zu der gerade gegebenen.

9.3. **Beobachtung** Sei $(M, *, e)$ ein Monoid. Dann sind äquivalent:
(1) $(M, *, e)$ ist eine Gruppe.
(2) Zu jeden $m, n \in M$ genau ein $k \in M$ gibt mit $m * k = n$.
(3) Zu jedem $m \in M$ gibt es ein $k \in M$ mit $m * k = e$.
(4) Zu jeden $m, n \in M$ genau ein $k \in M$ gibt mit $k * m = n$.
(5) Zu jedem $m \in M$ gibt es ein $k \in M$ mit $k * m = e$.

In diesem Fall definieren

$$\{(n, m, k) \in M \times M \times M \mid n = m * k\}$$

und

$$\{(n, m, k) \in M \times M \times M \mid n = k * m\}$$

Funktionen

$$M \times M \to M, \quad (n, m) \longmapsto m^{-1} * n \quad \text{und} \quad n * m^{-1}.$$

Ist M kommutativ so stimmt diese natürlich überein.

Der Monoid $(M, *, e)$ ist also eine Gruppe genau dann, wenn das Analog von Subtraktion bzw. Division (je nach Namen der Verknüpfung) uneingeschränkt möglich ist.

Beweis: Wir zeigen als erstes (1) ⇒ (2): Zur Existenz nehme man einfach $k = m^{-1} * n$. Zur Eindeutigkeit rechnet man

$$k = e * k = m^{-1} * m * k = m^{-1} * n = m^{-1} * m * k' = e * k' = k'$$

wann immer die mittleren beiden Gleichungen gelten. Natürlich gilt (2) ⇒ (3). Und dann (3) ⇒ (1): Wir müssen zeigen, dass auch $k * m$ gilt. Per Annahme gibt es aber zumindest ein $n \in M$ mit $k * n = e$. Dann rechnen wir aber

$$m = m * e = m * k * n = n.$$

Die Implikationen (1) ⇒ (2) ⇒ (3) ⇒ (1) sind vollständig analog. □

Einen Begriff von Zahl zu finden in dem man uneingeschränkt subtrahieren kann, ist die Grundidee der Erweiterung zu den ganzen Zahlen. Zur Formalisierung dieser Idee benötigen wir:

9.4. **Definition** Sind $(M, *, e)$ and $(M', *', e')$ Monoide, so heißt eine Funktion $f\colon M \to N$ ein *Monoidomomorphismus* falls

$$f(e) = e' \quad \text{and} \quad f(m * n) = f(m) *' f(n)$$

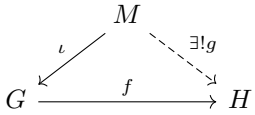
für alle $m, n \in M$. Sind $(R, *, \times, e, f)$ und $(R', *', \times', e', f')$ Halbringe, so heißt $f\colon R \to R'$ ein *Ringhomomorphismus*, falls f sowohl ein Monoidhomomorphismus $(R, *, e) \to (R', *', e')$ als auch $(R, \times, f) \to (R', \times', f')$ ist.

Ein Homomorphismus heißt ein *Mono-*, *Epi-* bzw. *Isomorphismus*, falls er injektiv, surjektiv bzw. bijektiv ist.

Wir formalisieren nun die Idee einer kleinsten Erweiterung zu einer Gruppe:

9.5. **Definition** Ist M ein Monoid, so heißt ein Paar bestehend aus einer Gruppe G und einem Monoidmonomorphismus $\iota M \to G$ eine *Gruppenvervollständigung (group completion)* von M, falls es für jede Gruppe H und jeden Monoidmonomorphismus $f\colon M \to H$ genau einen Monoidmonomorphismus $g\colon G \to H$ gibt, derart dass $g \circ \iota = f$.

Man zeichnet die Bedingung oft als



Wir zeigen als nächstes Eindeutigkeit und Existenz von Gruppenvervollständigungen:

9.6. **Lemma** (Eindeutigkeit von Gruppenvervollständigungen) *Sind $\iota\colon M \to G$ und $\iota'\colon M \to G'$ Gruppenvervollständigungen von M so gibt es genau einen Homomorphismus $f\colon G \to G'$ mit $f \circ \iota = \iota'$. Dieser ist ein Isomorphismus.*

Dies Lemma ist völlig analog zur Eindeutigkeit der natürlichen Zahlen. Wir sprechen von nun an also wieder missbräuchlich von *der* Gruppenvervollständigung von M und bezeichnen sie mit M^{grp}, sofern sie existiert, oder M_*^{grp} falls die Verknüpfung nicht aus dem Kontext klar ist.

9.7. **Theorem** (Existenz von Gruppenvervollständigungen) *Ein abelscher Monoid $(M, +, 0)$ besitzt eine Gruppenvervollständigung genau dann, wenn jedes Element in M gekürzt werden kann, also wenn für alle $m, n, k \in M$ gilt, dass $k + m = k + n \Rightarrow m = n$.*

Ist M geordnet, so trägt die Gruppenvervollständigung M^{grp} genau eine Ordnung, dass die Strukturabbildung $M \to M^{\mathrm{grp}}$ monoton ist. Trägt R eine Halbringstruktur, so erbt R_+^{grp}, derart dass $R \to \mathrm{R}^{\mathrm{grp}}$ ein Ringhomomorphismus ist.

Es gelten Verallgemeinerungen dieses Satzes auf nicht abelsche und nicht kürzbare Monoide, aber wir wollen uns mit dieser Version begnügen.

9.8. **Definition** Wir definieren den kommutativen, total geordneten Ring der *ganzen Zahlen (integers)* als $\mathbb{Z} := \mathbb{N}_+^{\mathrm{grp}}$.