EINFÜHRUNG IN DAS MATHEMATISCHE ARBEITEN

PAULA HILBERT UND DIRK PRAETORIUS

1. Was ist Mathematik?

Die normale Sprache im Alltag ist oft ungenau und missverständlich. Mathematik ist eine Sprache und eine Denkweise, um die üblichen Ungenauigkeiten und Missverständnisse zu vermeiden. Dies ist insbesondere in der Wissenschaft und Technik unumgänglich.

Die Mathematik macht allgemeingültige Aussagen über Mengen und abstrakte Strukturen (wie Zahlen, Abbildungen und Räume). Als Ausgangspunkt verwendet man gewisse Grundtatsachen, die sogenannten Axiome, die von allen akzeptiert (oder geglaubt) werden. Mittels klar festgelegter logischer Regeln werden aus den Axiomen weitere Aussagen abgeleitet, die damit wahr sein müssen. Dieses Vorgehen nennt man auch *logisches Schließen* oder *Beweis*.

Anders als andere Wissenschaften ist die Mathematik eine *exakte Wissenschaft*: Mathematische Sätze und Theorien sind unmissverständlich, unumstößlich, nachvollziehbar und für immer wahr. Die Mathematik arbeitet dabei mit abstrakten Begriffsbildungen, die aufgrund ihrer Allgemeinheit vielseitig anwendbar sind. Beispielsweise beschreibt die *Ableitung einer Funktion* das qualitative und quantitative Änderungsverhalten einer Funktion in vielfältigen Situationen.

Funktion	**Ableitung**
Ort eines Körpers zum Zeitpunkt t	Geschwindigkeit des Körpers
Temperatur als Funktion der Zeit t	Abkühlung oder Erwärmung des Körpers
Masse als Funktion des Ortes x	Massendichte

Es gibt viele verschiedene Teilgebiete der Mathematik, die Sie im Zuge des Studiums noch sehen werden. Am Anfang des Studiums begegnet Ihnen zunächst Folgendes:

- Grundlegende Objekte der *Analysis* sind der Aufbau des Zahlsystems, reelle Funktionen, Grenzwerte, Stetigkeit, Ableitung und Integral.
- Grundlegende Objekte der *Linearen Algebra* sind Vektorräume, lineare Abbildungen, Gleichungssysteme (und deren Lösungen) sowie die Eigenwerttheorie.

Die Aufgabe der *Einführung in das Mathematische Arbeiten* ist es, Ihnen eine Brücke von der Schulmathematik zur Universität zu schlagen.

2. Elementare Logik und logisches Schliessen

Jede mathematische Aussage hat einen **Wahrheitswert**: Sie ist entweder **wahr (w) oder falsch (f)**. Eine mathematische Aussage darf also falsch sein. Dies ist aber meist der uninteressante Fall. Außerdem gibt es Aussagen, bei denen nicht bekannt ist, ob sie wahr oder falsch sind, z.B. die Goldbachsche Vermutung, die der deutsche Mathematiker Christian Goldbach 1742 in einem Brief an seinen Schweizer Kollegen Leonhard Euler formuliert: *Jede gerade Zahl größer* 2 *ist die Summe zweier Primzahlen.*

Die elementare Logik nutzt die folgenden Verknüpfungen von Aussagen A und B, um neue Aussagen zu erzeugen (und zu bewerten):

Negation	$\neg A$	*nicht* A	entgegengesetzter Wahrheitswert zu A
Disjunktion	$A \vee B$	A *oder* B	Genau dann wahr, wenn mindestens A oder B wahr sind
Konjunktion	$A \wedge B$	A *und* B	Genau dann wahr, wenn sowohl A als auch B wahr sind
Implikation	$A \Rightarrow B$ $B \Leftarrow A$	*aus* A *folgt* B	Genau dann falsch, wenn A wahr und B falsch ist
Äquivalenz	$A \Leftrightarrow B$	A *und* B *sind äquivalent*	Genau dann wahr, wenn $A \Rightarrow B$ und $A \Leftarrow B$ gelten

Diese Regeln sind in den folgenden Wahrheitswert-Tabellen zusammengefasst:

- Negation

A	$\neg A$
w	f
f	w

- Disjunktion und Konjunktion

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

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

- Implikation und Äquivalenz

A	B	$A \Rightarrow B$	$A \Leftarrow B$	$A \Leftrightarrow B$
w	w	w	w	w
w	f	f	w	f
f	w	w	f	f
f	f	w	w	w

Beachten Sie den Unterschied zur Umgangssprache bei der Implikation. Umgangssprachlich geht es bei der Implikation („*Wenn..., dann ...!*“) um eine Kausalität. Mathematisch geht es bei der Implikation nur um die klar definierte Verknüpfung von Wahrheitswerten. Ist die **Prämisse** A einer Implikation $A \Rightarrow B$ falsch, so ist die Implikation wahr (unabhängig vom Wahrheitswert der **Konklusion** B). Die folgende Aussage ist also mathematisch wahr: *Wenn* $\pi = 3$ *ist, dann ist* 7 *eine gerade Zahl.*

Die genannten logischen Verknüpfungen formulieren die ersten Axiome des mathematischen Grundaufbaus. Formal muss man dabei nur $\neg$ und $\vee$ fordern, da sich die anderen Verknüpfungen $\wedge$, $\Rightarrow$ und $\Leftrightarrow$ aus diesen herleiten lassen, wie man in den folgenden Wahrheitswert-Tabellen sieht. Wir verwenden dabei die Konvention, das $\neg$ stärker bindet als die anderen logischen Verknüpfungen $\wedge$, $\vee$, $\Rightarrow$ und $\Leftrightarrow$. Um die Eindeutigkeit einer logischen Aussage zu garantieren, müssen ggf. Klammern gesetzt werden.

- $A \wedge B$ ist äquivalent zu $\neg(\neg A \vee \neg B)$, da sie stets denselben Wahrheitswert liefern:

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

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

- $A \Rightarrow B$ ist äquivalent zu $\neg A \vee B$, da sie stets denselben Wahrheitswert liefern:

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

A	B	$\neg A$	$\neg A \vee B$
w	w	f	w
w	f	f	f
f	w	w	w
f	f	w	w

- $A \Leftrightarrow B$ ist nach Definition äquivalent zu $(A \Rightarrow B) \wedge (A \Leftarrow B)$.

Mathematische Beweise basieren auf logischen Schlüssen, d.h. der stringenten Anwendung von allgemeingültigen Aussagen über mathematische Gegenstände, sogenannten **Tautologien**. Dies sind Verknüpfungen von Aussagen, die unabhängig vom Wahrheitswert ihrer Aussagen-logischen Teile immer wahr sind, beispielsweise

- $(A \wedge B) \Leftrightarrow (\neg(\neg A \vee \neg B))$,
- $(A \Rightarrow B) \Leftrightarrow (\neg A \vee B)$,

wie wir eben gesehen haben. Man kann Tautologien leicht mit Hilfe geeigneter Wahrheitswert-Tabellen überprüfen.

- **Tautologie vom ausgeschlossenen Dritten**: $A \vee \neg A$

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

Beispiel: *Es regnet (A) oder es regnet nicht ($\neg A$).*

- **Tautologie der Konjunktionsbeseitigung**: $(A \wedge B) \Rightarrow A$

A	B	$A \wedge B$	$(A \wedge B) \Rightarrow A$
w	w	w	w
w	f	f	w
f	w	f	w
f	f	f	w

Beispiel: *Wenn es regnet (A) und die Straße nass ist (B), dann regnet es (A).*

- **Tautologie der Disjunktionseinführung**: $A \Rightarrow (A \vee B)$

A	B	$A \vee B$	$A \Rightarrow (A \vee B)$
w	w	w	w
w	f	w	w
f	w	w	w
f	f	f	w

Beispiel: *Wenn es regnet (A), dann regnet es (A) oder die Straße ist nass (B).*

- **Tautologie von der Kontraposition**: $(A \Rightarrow B) \Leftrightarrow (\neg B \Rightarrow \neg A)$

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

Beispiel: *Die folgenden Aussagen sind äquivalent: Wenn es regnet (A), dann ist die Straße nass (B)! Wenn die Straße nicht nass ist ($\neg B$), dann regnet es nicht ($\neg A$)!*

- **Modus ponendo ponens**: $[A \wedge (A \Rightarrow B)] \Rightarrow B$

A	B	$A \Rightarrow B$	$A \wedge (A \Rightarrow B)$	$[A \wedge (A \Rightarrow B)] \Rightarrow B$
w	w	w	w	w
w	f	f	f	w
f	w	w	f	w
f	f	w	f	w

Beispiel: *Es regnet (A), und wenn es regnet, dann ist die Straße nass ($A \Rightarrow B$). Also ist die Straße nass (B).*

- Weitere Tautologien sehen Sie in der Übung.

3. Direkter und indirekter Beweis

Bei Beweisen unterscheidet man zwischen *direkten Beweisen* und *indirekten Beweisen*. Der **direkte Beweis** führt durch eine Folge von logischen Schlüssen zur Behauptung. Beim **indirekten Beweis** nimmt man an, die Behauptung B sei falsch und konstruiert dann mit logischen Schlüssen einen Widerspruch.

Dieser Abschnitt soll Ihnen erste Beispiele für direkte und indirekte Beweise im Rahmen der Schulmathematik präsentieren, wobei wir die natürliche Zahlen $\mathbb{N} = \{1, 2, 3, \dots\}$ und einige ihrer elementaren Eigenschaften als gegeben voraussetzen. Wir nutzen im Folgenden das Symbol $\in$ für Ist-ein-Element-von und schreiben $a \in \mathbb{N}$, um abzukürzen, dass a eine natürliche Zahl ist.

Um in der Mathematik klar zu formulieren, was an Notation oder Bezeichnungsweise vorausgesetzt wird, formuliert man üblicherweise *Definitionen*. Es ist wichtig, dass Definitionen klar und eindeutig sind, damit es nicht zu Missverständnissen kommt und damit klar ist, welche Eigenschaften die behandelten Objekte haben (d.h. was als wahr angenommen wird). Wenn man neue Notation definiert, dann verwendet man meist das Symbol $:=$, um zu betonen, dass dies keine Gleichheit im mathematisch-logischen Sinn ist, sondern eine Gleichheit aufgrund von Definition (siehe das **Produktsymbol** $\prod$ in Satz 3.4).

Definition 3.1. *Eine Zahl $t \in \mathbb{N}$ ist ein **Teiler** von $a \in \mathbb{N}$, wenn es eine Zahl $a' \in \mathbb{N}$ gibt mit $a = ta'$. Ferner ist t ein **echter Teiler** von a, wenn zusätzlich $1 < t < a$ gilt. Eine Zahl $p \in \mathbb{N}$ ist eine **Primzahl**, wenn $p \geq 2$ gilt und wenn 1 und p die einzigen Teiler von p sind, d.h. p hat keine echten Teiler. Eine Zahl $a \in \mathbb{N}$ ist **gerade**, wenn 2 ein Teiler von a ist. Anderenfalls ist sie **ungerade**.*

Unser erster Satz ist natürlich im Sinne der Schulmathematik offensichtlich. Der Beweis soll Ihnen zeigen, wie man stringent nach einer gegebenen Definition argumentiert. Außerdem illustriert er den *Beweis der Kontraposition*. Beachten Sie die erste Beweiszeile: *Sei $p \in \mathbb{N}$ mit $p \geq 3$*. Diese besagt gerade, dass p im Folgenden eine *beliebige* natürliche Zahl ≥ 3 ist. Beweise werden in diesem Skript immer mit dem Symbol $\square$ abgeschlossen

(d.h. an dieser Stelle ist der Beweis vollständig). Andere Mathematiker*innen schreiben auch *QED*, *qed*, oder *q.e.d.* (*lat.* quod erat demonstrandum) oder nutzen andere Symbole.

Satz 3.2. *Jede Primzahl $p \geq 3$ ist ungerade, d.h. 2 ist die einzige gerade Primzahl.*

Beweis. Sei $p \in \mathbb{N}$ mit $p \geq 3$. Wir müssen die Implikation [p Primzahl $\Rightarrow$ p ungerade] zeigen. Diese ist äquivalent zu ihrer Kontraposition [p gerade $\Rightarrow$ p nicht Primzahl]. Diese ist aber klar, denn jede gerade Zahl hat den Teiler 2 und wegen $p \geq 3$ gilt $p \neq 2$. □

Auch der folgende Satz ist natürlich im Sinne der Schulmathematik offensichtlich. Der Beweis soll Ihnen nur zeigen, dass man eine Äquivalenz (*genau dann, wenn...*) in der Regel dadurch zeigt, dass man beide Implikationen zeigt.

Satz 3.3. *Eine Zahl $a \in \mathbb{N}$ ist genau dann ungerade, wenn $a+1$ gerade ist.*

Beweis. Wir unterteilen den Beweis in drei Schritte.

Schritt 1 (a ungerade $\Rightarrow$ $a+1$ gerade). Sei $a \in \mathbb{N}$ ungerade, d.h. 2 ist kein Teiler von a. Also gilt $a \neq 2n$ für alle $n \in \mathbb{N}$. Dann gibt es ein minimales $n \in \mathbb{N}$ mit $a < 2n$. Aufgrund der Minimalität von n muss gelten, dass $2n - 2 = 2(n-1) \leq a < 2n$. Das $\leq$ muss dann sogar ein $<$ sein, denn für $=$ gilt

- entweder $n = 1$ und damit $a = 0$ (was nicht geht)
- oder $n > 1$ und damit wären 2 und $n-1$ Teiler von a (was auch nicht geht).

Also muss $<$ und damit $a = 2n - 1$ gelten, d.h. $a + 1 = 2n$ ist gerade.

Schritt 2 ($a+1$ gerade $\Rightarrow$ a ungerade). Sei $a \in \mathbb{N}$ mit $a+1$ gerade, d.h. es existiert $n \in \mathbb{N}$ mit $a + 1 = 2n$. Dann ist $a = 2n - 1$ nicht durch 2 teilbar und somit ungerade.

Schritt 3 (a ungerade $\Leftrightarrow$ $a+1$ gerade). Mit Schritt 1 und 2 haben wir gezeigt, dass beide Implikationen wahr sind. Also ist die Äquivalenz wahr. □

Kommentar. *Eine **Fallunterscheidung** wie im Beweis von Satz 3.3 kommt relativ häufig in Beweisen vor. Man muss dabei nur aufpassen, dass man alle formal möglichen Fälle berücksichtigt. Im Beweis von Satz 3.3 ist das sehr einfach, da für $n \in \mathbb{N}$ entweder $n = 1$ oder $n > 1$ gilt.*

Der folgende Satz formuliert die Existenz der Primfaktorzerlegung. Dazu nutzen wir einen indirekten Beweis, der auf der Tautologie vom ausgeschlossenen Dritten basiert. Im Zuge der vollständigen Induktion werden wir später einen alternativen Beweis sehen.

Satz 3.4 (Existenz der Primfaktorzerlegung). *Für jede Zahl $a \in \mathbb{N}$ mit $a \geq 2$ existieren $n \in \mathbb{N}$ und n-viele Primzahlen $p_1, \ldots, p_n \in \mathbb{N}$ mit $a = \prod_{j=1}^{n} p_j \coloneqq p_1 \cdot p_2 \cdots p_n$.*

Beweis. Wir nehmen an, die Aussage des Satzes ist falsch, d.h. es gibt mindestens eine natürliche Zahl ≥ 2, die sich nicht als Produkt von Primzahlen schreiben lässt. Da die natürlichen Zahlen nach unten beschränkt sind, existiert eine kleinste Zahl $a \in \mathbb{N}$ mit $a \geq 2$, die sich nicht als Produkt von Primzahlen schreiben lässt. Nach der Tautologie

vom ausgeschlossenen Dritten ist diese Zahl entweder eine Primzahl oder keine Primzahl. Wir machen wieder eine Fallunterscheidung:

Fall 1 (a ist eine Primzahl). Wäre a eine Primzahl, so wäre $n \coloneqq 1$ und $p_1 \coloneqq a$ eine Primfaktorzerlegung, d.h. $a = \prod_{j=1}^{1} p_j$. Aber a hat nach Wahl keine Primfaktorzerlegung, d.h. a ist keine Primzahl. Also kann dieser Fall nicht eintreten.

Fall 2 (a ist keine Primzahl). Dann gibt es echte Teiler $t, a' \in \mathbb{N}$ mit $a = ta'$. Da a die kleinste natürliche Zahl ohne Primfaktorzerlegung ist, haben t und a' Primfaktorzerlegungen, d.h. $t = p_1 \cdots p_k$ und $a' = p_{k+1} \cdots p_n$ für geeignete Primzahlen p_j und geeignete $k, n \in \mathbb{N}$. Dann hat aber a die Primfaktorzerlegung $a = ta' = p_1 \cdots p_n$. Wir bekommen also wieder einen Widerspruch dazu, dass a keine Primfaktorzerlegung hat. Also kann auch dieser Fall nicht eintreten.

Insgesamt muss also die Annahme, dass es natürliche Zahlen gibt, die sich nicht als Produkt von Primzahlen schreiben lassen, falsch sein. Also lässt sich jede natürliche Zahl als Produkt von Primzahlen schreiben, d.h. die Aussage des Satzes ist wahr □

Kommentar. *Im vorausgegangenen Beweis haben wir wie folgt argumentiert:*

> Wäre a eine Primzahl, so wäre $n \coloneqq 1$ und $p_1 \coloneqq a$ eine Primfaktorzerlegung. Aber a hat nach Wahl keine Primfaktorzerlegung, d.h. a ist keine Primzahl.

*Implizit handelt es sich dabei entweder um ein indirektes Argument (*Angenommen, dass a eine Primzahl ist. Dann hat a eine Primfaktorzerlegung. Dies liefert einen Widerspruch.*) oder (richtiger!) um die Verwendung der Kontraposition (*Jede Primzahl hat eine Primfaktorzerlegung. Da a keine Primfaktorzerlegung hat, ist a keine Primzahl*).*

Ein hübsches Beispiel für einen indirekten Beweis ist auch das folgende Resultat, das bereits auf Euklid zurückgeht. Weil das Resultat gewissermaßen mittels „einfacher Argumente“ aus der Existenz der Primfaktorzerlegung folgt, bezeichnen wir es als *Korollar* (des vorausgegangenen Satzes). Dabei ist wichtig festzuhalten, dass man bereits bewiesene mathematische Resultate (wie eben Satz 3.4) verwenden kann, darf und soll, wenn deren Voraussetzungen erfüllt sind.

Korollar 3.5. *Es gibt unendlich viele Primzahlen.*

Beweis. Wir nehmen an, die Aussage ist falsch, d.h. es gibt nur endlich viele Primzahlen $p_1, \ldots, p_n$. Wir definieren $q \coloneqq p_1 \cdot p_2 \cdots p_n + 1$. Dann gilt $q \in \mathbb{N}$. Ferner liefert Division durch $p_1, \ldots, p_n$ stets Rest 1, d.h. q ist durch keine Primzahl teilbar. Das ist aber ein Widerspruch zur Existenz der Primfaktorzerlegung von Satz 3.4. Also muss auch die Aussage, dass es nur endlich viele Primzahlen gibt, falsch sein. Also gibt es unendlich viele Primzahlen, d.h. die Aussage des Korollars ist wahr. □

Da für einen Teiler t von a immer $t \leq a$ ist, hat eine Zahl a nur endlich viele verschiedene Teiler. Da 1 ein Teiler aller Zahlen $a \in \mathbb{N}$ ist, ist die folgende Definition sinnvoll.

Definition 3.6. *Es sei g ein gemeinsamer Teiler von $a, b \in \mathbb{N}$, sodass für alle anderen gemeinsamen Teiler $t \in \mathbb{N}$ von a und b gilt $t \leq g$. Dann bezeichnet man g als* ***größten gemeinsamen Teiler*** *von a und b, und wir nutzen die Schreibweise $\mathsf{ggT}(a, b) := g$.*

Mathematische Aussagen (z.B. Sätze, Korollare) haben häufig die Form einer Implikation, d.h. es wird behauptet, dass die Aussage $A \Rightarrow B$ wahr ist: Wenn die Voraussetzung / Prämisse A wahr ist, dann ist auch B wahr. Falls A falsch ist, wird keine Aussage gemacht, ob B wahr ist. Dies ist auch der Fall im folgenden Resultat, das später nur als Hilfsresultat im Beweis von Satz 3.9 verwendet und deshalb als *Lemma* bezeichnet wird.

Lemma 3.7. *Es seien $a, b \in \mathbb{N}$ mit $a < b$. Dann gilt $\mathsf{ggT}(a, b) = \mathsf{ggT}(a, b - a)$, d.h. der größte gemeinsame Teiler von a und b ist auch der größte gemeinsame Teiler von a und $b - a$.*

Beweis. Wir unterteilen den Beweis in drei Schritte.

Schritt 1 ($\mathsf{ggT}(a, b) \leq \mathsf{ggT}(a, b - a)$). Zunächst sei $g \in \mathbb{N}$ ein Teiler von a und b, d.h. es gibt Zahlen $a', b' \in \mathbb{N}$ mit $a = ga'$ und $b = gb'$. Da $a < b$ gilt, gilt auch $a' < b'$ und deshalb $c' := b' - a' \in \mathbb{N}$ mit $b - a = gb' - ga' = gc'$. Wir haben also gezeigt, dass jeder Teiler von a und b auch ein Teiler von $b - a$ ist. Insbesondere ist $\mathsf{ggT}(a, b)$ ein Teiler von $b - a$ und somit $\mathsf{ggT}(a, b) \leq \mathsf{ggT}(a, b - a)$.

Schritt 2 ($\mathsf{ggT}(a, b - a) \leq \mathsf{ggT}(a, b)$). Nun sei $g \in \mathbb{N}$ ein Teiler von a und $b - a$, d.h. es gibt Zahlen $a', c' \in \mathbb{N}$ mit $a = ga'$ und $b - a = gc'$. Dann gilt $b = a + (b - a) = ga' + gc' = g(a' + c')$, d.h. g ist auch ein Teiler von b. Insbesondere ist $\mathsf{ggT}(a, b - a)$ ein Teiler von b und somit $\mathsf{ggT}(a, b - a) \leq \mathsf{ggT}(a, b)$.

Schritt 3. Da wir beide Ungleichungen gezeigt haben, folgt insgesamt die Behauptung: $\mathsf{ggT}(a, b) = \mathsf{ggT}(a, b - a)$. □

Das vorausgegangene Lemma erlaubt es, auf einfache Weise (und ohne Verwendung der Primfaktorzerlegung) den größten gemeinsamen Teiler zweier positiver ganzer Zahlen zu bestimmen:

Algorithmus 3.8 (Euklid). ***Input:*** *Es seien $a, b \in \mathbb{N}$ gegeben und $g := \mathsf{ggT}(a, b)$ gesucht.*

Wiederhole die folgenden Schritte (i)–(ii)*, bis $a = b$ gilt:*

(i) *Vertausche a und b, falls $a > b$.*

(ii) *Ersetze b durch $b - a$.*

Output: *Sobald der Algorithmus terminiert, ist $g = a = b$ der gesuchte Wert.*

Auch solche Algorithmen muss man mathematisch analysieren, um zu garantieren, dass sie wirklich das behauptete Ergebnis liefern. Mit Hilfe von Lemma 3.7 kann man zeigen, dass der Euklidische Algorithmus für alle $a, b \in \mathbb{N}$ in der Tat den größten gemeinsamen Teiler $\mathsf{ggT}(a, b)$ berechnet.

Satz 3.9. *Für alle $a, b \in \mathbb{N}$ bricht Algorithmus 3.8 nach endlich vielen Schritten ab und liefert den größten gemeinsamen Teiler* $\mathsf{ggT}(a, b)$.

Beweis. Wir gliedern den Beweis in drei Schritte.

Schritt 1 ($a = b$). Falls $a = b$ ist, gilt offensichtlich $\mathsf{ggT}(a, b) = a = b$, und Algorithmus 3.8 terminiert.

Schritt 2 ($a \neq b$). Falls $a \neq b$ ist, gilt natürlich $g = \mathsf{ggT}(a, b) = \mathsf{ggT}(b, a)$, d.h. Algorithmus 3.8(i) hat keinen Einfluss auf das gesuchte g und stellt sicher, dass wir wegen $a < b$ das Hilfsresultat aus Lemma 3.7 anwenden können: Es gilt also $g = \mathsf{ggT}(a, b - a)$, d.h. Algorithmus 3.8(ii) hat auch keine Auswirkung auf das gesuchte g.

Schritt 3 (Algorithmus 3.8 terminiert). Wir müssen uns nur noch überlegen, dass Algorithmus 3.8 nach endlich vielen Schritten mit $a = b$ abbricht: In jedem Durchlauf von Algorithmus 3.8(i)–(ii) mit $a \neq b$ erzwingen wir $b > a$ und überschreiben $b = \max(a, b)$ durch $b - a$. Wegen $a, b \in \mathbb{N}$ und $b > a$ gilt $b - a \in \mathbb{N}$ mit $b - a < b$. Also wird das Maximum $\max(a, b)$ um mindestens 1 kleiner. Da $\mathbb{N}$ nach unten durch 1 beschränkt ist, kann der Algorithmus nur endlich viele Schritte machen. Da er nur für $a = b$ abbricht, muss nach endlich vielen Schritten $a = b$ gelten, sodass Algorithmus 3.8 wirklich mit dem behaupteten Ergebnis terminiert. □

Kommentar. *Wie Sie beim Lesen der Beweise vermutlich gemerkt haben, handelt es sich bei Beweisen nicht um hohe Prosa. Um die Nachvollziehbarkeit zu erleichtern, verwenden wir kurze Sätze. Gleiche Argumente werden mit gleicher Wortwahl formuliert (d.h. bewusste Wortwiederholung). Aus diesem Grund sollten Argumente auch immer mit* „Weil. . . , gilt. . . “ *formuliert werden (anstelle von* „Es gilt. . . , weil. . . “*). In jedem Fall sind mathematische Formeln und logischen Aussagen in der mathematischen Schriftsprache immer Teile von vollständigen Sätzen (und insbesondere gelten die Regeln der Interpunktion).*

Kommentar. *Wie Sie in den vorausgegangenen Beweisen gesehen haben, verwendet ein* ***direkter Beweis*** *meistens den* Modus ponendo ponens*: Da die (als wahr vorausgesetzte) Voraussetzung A und die Implikation $A \Rightarrow B$ wahr sind, muss auch B wahr sein. Da B und die Implikation $B \Rightarrow C$ wahr sind, muss auch C wahr sein, etc; siehe beispielsweise den Beweis von Lemma 3.7. Manchmal kann/darf/muss man aber auch andere Tautologien verwenden, z.B. die Kontraposition im Beweis von Satz 3.2.*

Beim ***indirekten Beweis*** *nimmt man an, dass die Behauptung B falsch (f) ist. Man zeigt dann mittels logischer Schlüsse (d.h. wie beim direkten Beweis), dass unter der (als wahr vorausgesetzten) Voraussetzung A und der Annahme $\neg B$ die Implikation $[(A \wedge \neg B) \Rightarrow \mathsf{f}]$ wahr ist. Diese ist aber nach elementarer Aussagenlogik genau dann wahr, wenn $\neg B$ falsch und somit B wahr ist; siehe den Beweis von Satz 3.4 oder den Beweis von Korollar 3.5. Im Beweis von Satz 3.4 gibt es augenscheinlich keine Voraussetzungen*

(außer den „natürlichen“ Eigenschaften von $\mathbb{N}$). In einem solchem Fall ist A einfach als wahr (w) zu verstehen, sodass sich die gezeigte Implikation zu $[\neg B \Rightarrow \mathsf{f}]$ vereinfacht (und $\neg B$ als falsch beweist).

Kommentar. *Es ist wichtig, dass Sie zwischen der Tafelpräsentation in Ihren Vorlesungen (und Übungen) und der mathematischen Schriftsprache unterscheiden. Wenn man an der Tafel präsentiert, verwendet man häufig logische Symbole ungenau (insbesondere Implikation $\Rightarrow$ und Äquivalenz $\Leftrightarrow$), um die Präsentation abzukürzen, z.B.*

- $\Rightarrow$ *zur Abkürzung von:* „Daraus folgt, dass…“
- $\Leftrightarrow$ *zur Abkürzung von:* „Dies ist äquivalent zu…“

Viele Vortragende kürzen auch Definitionen ab, z.B.

- $\overset{\text{def}}{\Longleftrightarrow}$ *bzw.* $:\Longleftrightarrow$ *zur Abkürzung von:* „definiert als“ *oder* „gemäß Definition“

Sie sehen diese Unterschiede, wenn Sie in der Vorlesung mitschreiben und Ihre Mitschrift mit der Präsentation im zugehörigen Skript oder Buch vergleichen. Spätestens bei Seminararbeit und Bachelorarbeit müssen Sie jedenfalls die mathematische Schriftsprache korrekt verwenden.

---

4. Logische Quantoren und vollständige Induktion

Wie Sie in den vorausgegangenen Sätzen und Korollaren gesehen haben, nutzt die Mathematik häufig Formulierungen der Art:

- Für alle $n \in \mathbb{N}$…
- Es existiert ein $k \in \mathbb{N}$…

Die Schriftsprache tendiert dazu, bisweilen nicht eindeutig oder missverständlich zu sein. In der Mathematik ist aber gerade dies ein erklärtes Ziel. Aus diesem Grund gibt es die sogenannten **(logischen) Quantoren**: Wir unterscheiden den **All-Quantor** $\forall$ (*für alle*) und den **Existenz-Quantor** $\exists$ (*es existiert (mindestens) ein*). Ferner wird häufig die **eindeutige Existenz** mit $\exists!$ oder $\exists^1$ (*es existiert ein eindeutiges*) bezeichnet. Schließlich bezeichnet $\nexists$ oft die **Nicht-Existenz** (*es gibt kein*).

Ketten von Quantoren sind immer von links nach rechts zu lesen und in diesem Sinn eindeutig (z.B. $\forall T$ Topf $\exists D$ Deckel : … bedeutet: *„Für jeden Topf existiert ein Deckel, sodass…“* und eben nicht(!): *„Es existiert ein Deckel, der auf jeden Topf passt, sodass…“*) Viele Mathematiker*innen schreiben am Ende einer Quantorenkette den Doppelpunkt als Abkürzung von: *„sodass gilt…“*. Ein Beistrich nach einem Quantor wird meist als *„mit der Eigenschaft“* gelesen (vgl. Satz 4.3(iii)), manchmal schreibt man aber auch explizit *„mit“* statt des Beistrichs. Ferner verwendet man in der Regel die Konvention, dass die logischen Verknüpfungen $\neg$, $\wedge$, $\vee$, $\Rightarrow$ und $\Leftrightarrow$ stärker binden als die logischen Quantoren. Jenseits davon müssen Klammern gesetzt werden, um eine Aussage wirklich unmissverständlich zu formulieren.

Kommentar. *Es kann sinnvoll sein, bei Quantoren-Aussagen Klammern zu setzen, damit die Aussage eindeutig und klar ist. Beispielsweise sind die Aussagen*

- $\forall n \in \mathbb{N}:\ A(n) \Rightarrow B$ *(nach Konvention äquivalent zu* $\forall n \in \mathbb{N}:\ [A(n) \Rightarrow B]$*)*
- $\big[\forall n \in \mathbb{N} : A(n)\big] \Rightarrow B$

offensichtlich nicht äquivalent.

Bemerkung 4.1. *Im Folgenden sei $A(n)$ eine Aussage in Abhängigkeit einer natürlichen Zahl $n \in \mathbb{N}$.*

(i) *Die **All-Quantor-Aussage** $[\forall n \in \mathbb{N}:\ A(n)]$ ist nach Definition des Quantors genau dann wahr, wenn $A(n)$ für alle $n \in \mathbb{N}$ wahr ist, d.h. die Aussage entspricht einem iterierten Und: $A(1) \wedge A(2) \wedge A(3) \wedge \dots$.*

(ii) *Die **Existenz-Quantor-Aussage** $[\exists n \in \mathbb{N}:\ A(n)]$ ist nach Definition des Quantors genau dann wahr, wenn es (mindestens) ein $n \in \mathbb{N}$ gibt, für das $A(n)$ wahr ist, d.h. die Aussage entspricht einem iterierten Oder: $A(1) \vee A(2) \vee A(3) \vee \dots$.*

(iii) *Die All-Quantor-Aussage ist genau dann falsch, wenn es ein $n_0 \in \mathbb{N}$ gibt, für das $\neg A(n_0)$ wahr ist, d.h. es gilt*

$$\neg[\forall n \in \mathbb{N}:\ A(n)] \quad \Leftrightarrow \quad [\exists n_0 \in \mathbb{N} : \neg A(n_0)].$$

*Dieses n_0 bezeichnet man dann auch als **Gegenbeispiel** der All-Quantor-Aussage, weil $A(n_0)$ zeigt, dass die All-Quantor-Aussage falsch ist.*

(iv) *Insbesondere ist die Existenz-Quantor-Aussage genau dann falsch, wenn für alle $n \in \mathbb{N}$ gilt, dass $\neg A(n)$ wahr ist, d.h. es gilt*

$$\neg[\exists n_0 \in \mathbb{N}:\ A(n_0)] \quad \Leftrightarrow \quad [\forall n \in \mathbb{N} : \neg A(n)].$$

Nach Definition ist dies auch äquivalent zur Aussage, dass kein $n \in \mathbb{N}$ existiert mit $A(n)$, d.h.

$$[\nexists n_0 \in \mathbb{N}:\ A(n_0)] \quad \overset{\text{def}}{\Longleftrightarrow} \quad [\forall n \in \mathbb{N} : \neg A(n)].$$

Beispiel 4.2. *Eine Zahl $p \in \mathbb{N}$ ist genau dann eine Primzahl, wenn $p \geq 2$ gilt und wenn 1 und p die einzigen Teiler von p sind. Dies entspricht der Aussage*

$$(p \geq 2) \wedge \big[\forall n \in \mathbb{N}:\ \big((n \text{ teilt } p) \Rightarrow (n = 1 \vee n = p)\big)\big].$$

Also ist p keine Primzahl, wenn diese Aussage falsch ist. Mit der Tautologie $\big[\neg(A \wedge B) \Leftrightarrow (\neg A \vee \neg B)\big]$ ist p also keine Primzahl, wenn

$$\neg(p \geq 2) \vee \neg\big[\forall n \in \mathbb{N}:\ \big((n \text{ teilt } p) \Rightarrow (n = 1 \vee n = p)\big)\big].$$

Die Aussage $\neg(p \geq 2)$ ist äquivalent zu $p < 2$ und wegen $p \in \mathbb{N}$ deshalb zu $p = 1$. Also ist die Aussage, dass p keine Primzahl ist, äquivalent zu

$$p = 1 \vee \neg\big[\forall n \in \mathbb{N} : \big((n \text{ teilt } p) \Rightarrow (n = 1 \vee n = p)\big)\big].$$

Aufgrund der Negation der All-Quantor-Aussage ist dies äquivalent zu

$$p = 1 \vee \big[\exists n \in \mathbb{N} : \neg\big((n \text{ teilt } p) \Rightarrow (n = 1 \vee n = p)\big)\big].$$

Mit der Tautologie $\big[(A \Rightarrow B) \Leftrightarrow (\neg A \vee B)\big]$ *ist dies äquivalent zu*

$$p = 1 \vee \big[\exists n \in \mathbb{N} : \neg\big(\neg(n \text{ teilt } p) \vee n = 1 \vee n = p\big)\big].$$

Mit der Tautologie $\big[\neg(A \vee B \vee C) \Leftrightarrow (\neg A \wedge \neg B \wedge \neg C)\big]$ *ist dies abschließend äquivalent zu*

$$p = 1 \vee \big[\exists n \in \mathbb{N} : \big((n \text{ teilt } p) \wedge n \neq 1 \wedge n \neq p\big)\big].$$

Diese Aussage ist also dazu äquivalent, dass p keine Primzahl ist. □

Kommentar. *In einer Tafelpräsentation würde man Beispiel 4.2 vermutlich folgendermaßen abkürzen, um Schreibarbeit zu sparen: Für $p \in \mathbb{N}$ gilt nach Definition*

$$p \text{ Primzahl} \quad \overset{\text{def}}{\Longleftrightarrow} \quad (p \geq 2) \wedge \big[\forall n \in \mathbb{N} : \big((n \text{ teilt } p) \Rightarrow (n = 1 \vee n = p)\big)\big].$$

Durch Negation dieser Aussage erhalten wir die folgenden Äquivalenzen:

$$\begin{aligned} p \text{ keine Primzahl} &\Longleftrightarrow p = 1 \vee \neg\big[\forall n \in \mathbb{N} : \big((n \text{ teilt } p) \Rightarrow (n = 1 \vee n = p)\big)\big] \\ &\Longleftrightarrow p = 1 \vee \big[\exists n \in \mathbb{N} : \neg\big((n \text{ teilt } p) \Rightarrow (n = 1 \vee n = p)\big)\big] \\ &\Longleftrightarrow p = 1 \vee \big[\exists n \in \mathbb{N} : \neg\big(\neg(n \text{ teilt } p) \vee n = 1 \vee n = p\big)\big] \\ &\Longleftrightarrow p = 1 \vee \big[\exists n \in \mathbb{N} : \big((n \text{ teilt } p) \wedge n \neq 1 \wedge n \neq p\big)\big]. \end{aligned}$$

Beachten Sie, dass hier das Äquivalenz-Symbol $\Longleftrightarrow$ formal unsauber verwendet wird zur reinen Abkürzung der Präsentation: $[(A \Leftrightarrow B) \Leftrightarrow C]$ (was dort steht) ist natürlich nicht äquivalent zu $[(A \Leftrightarrow B) \wedge (B \Leftrightarrow C)]$ (was aber natürlich gemeint ist).

Kommentar. *Auch bei den logischen Quantoren ist es wichtig, dass Sie zwischen der Tafelpräsentation in Ihren Vorlesungen (und Übungen) und der mathematischen Schriftsprache unterscheiden. Häufig werden die Quantoren nur verwendet, um die Präsentation abzukürzen, z.B.*

- *$\forall x \in \mathbb{N}$ wird ans Ende eines Satzes oder einer Formel geschrieben zur Abkürzung von „für alle $x \in \mathbb{N}$“;*
- *$\exists x \in \mathbb{N}$ wird im Text verwendet, um abzukürzen, dass es ein x mit einer Eigenschaft gibt und dass dieses x im Folgenden auch betrachtet wird.*

Achten Sie auf die (ggf. formal unsaubere) Verwendung der Quantoren in Ihren Vorlesungen! Bei Seminararbeit und Bachelorarbeit müssen Sie jedenfalls die mathematische Schriftsprache korrekt verwenden, d.h. eine Quantor(en)-Aussage ist eine Aussage. Diese kann wahr oder falsch sein, mehr aber auch nicht!

Kommentar. *Unsere Notation und Verwendung von Quantoren ist in der Mathematik weithin verbreitet. Im Sinne der formalen Prädikatenlogik ist aber auch unsere Verwendung formal falsch. Die formale Prädikatenlogik schreibt*

$$\forall n : \big[n \in \mathbb{N} \Rightarrow A(n)\big] \qquad \text{(„Für alle } n \text{ gilt, dass } n \in \mathbb{N} \text{ auch } A(n) \text{ impliziert.“)}$$

anstelle von

$$\forall n \in \mathbb{N} : A(n) \qquad \text{(„Für alle } n \in \mathbb{N} \text{ gilt } A(n).\text{“)}.$$

Analog schreibt die formale Prädikatenlogik

$$\exists n : \big[n \in \mathbb{N} \wedge A(n)\big] \qquad \text{(„Es existiert ein } n \text{ mit } n \in \mathbb{N} \text{ und } A(n).\text{“)}$$

anstelle von

$$\exists n \in \mathbb{N} : A(n) \qquad \text{(„Es existiert ein } n \in \mathbb{N} \text{ mit } A(n).\text{“)}.$$

Sie sehen also, dass der Doppelpunkt in manchen Formeln eine Implikation (⇒) und in anderen Formeln ein logisches Und (∧) versteckt. In der mathematischen Praxis ist das aber wenig fehleranfällig.

Das *Beweisprinzip der vollständigen Induktion* ist eine Beweistechnik, um zu zeigen, dass eine Aussage der Form

$$\forall n \in \mathbb{N} : A(n)$$

wahr ist, d.h. man hat eine Aussage $A(n)$ in Abhängigkeit einer natürlichen Zahl $n \in \mathbb{N}$ und will zeigen, dass diese Aussage für alle $n \in \mathbb{N}$ wahr ist; siehe Beispiel 4.5 unten.

Im folgenden Satz bedeutet **paarweise äquivalent**, dass alle drei Äquivalenzen gelten: (i) ⇔ (ii), (i) ⇔ (iii) und (ii) ⇔ (iii). Da eine Äquivalenz $A \Leftrightarrow B$ von zwei Aussagen A und B nach Definition genau dann wahr ist, wenn beide Implikationen $A \Rightarrow B$ und $A \Leftarrow B$ wahr sind, könnte man also insgesamt sechs Implikationen zeigen. Es geht aber bisweilen effizienter. Wir werden in drei Schritten zeigen, dass die folgenden drei Implikationen gelten: (i) ⇒ (ii), (ii) ⇒ (iii) und (iii) ⇒ (i). Man bezeichnet dies als **Ringschluss**. Mittels elementarer Logik folgen aus diesen drei Implikationen tatsächlich die genannten drei Äquivalenzen, d.h. die Aussagen (i)–(iii) sind paarweise äquivalent.

Satz 4.3 (vollständige Induktion). *Es sei $A(n)$ eine Aussage in Abhängigkeit einer natürlichen Zahl $n \in \mathbb{N}$. Dann sind die folgenden drei Aussagen* (i)–(iii) *paarweise äquivalent:*

(i) *$A(n)$ ist wahr für alle $n \in \mathbb{N}$, d.h.*

$$\forall n \in \mathbb{N} : A(n).$$

(ii) ***Induktionsprinzip:*** *$A(1)$ ist wahr und für alle $n \in \mathbb{N}$ gilt: Wenn $A(n)$ wahr ist, dann ist auch $A(n+1)$ wahr, d.h.*

$$A(1) \wedge [\forall n \in \mathbb{N} : A(n) \Rightarrow A(n+1)]$$

(iii) ***Starkes Induktionsprinzip:*** *$A(1)$ ist wahr und für alle $n \in \mathbb{N}$ gilt: Wenn $A(k)$ wahr ist für alle $k = 1, \ldots, n$, dann ist auch $A(n+1)$ wahr, d.h.*

$$A(1) \wedge \big[\forall n \in \mathbb{N} : \big(\forall k \in \mathbb{N}, k \leq n : A(k)\big) \Rightarrow A(n+1)\big].$$

Beweis. **Schritt 1 ((i) ⇒ (ii)).** Wir setzen voraus, dass (i) wahr ist, d.h. $A(n)$ ist wahr für alle $n \in \mathbb{N}$. Insbesondere ist also $A(1)$ wahr. Für (ii) müssen wir noch für alle $n \in \mathbb{N}$ die Implikation $[A(n) \Rightarrow A(n+1)]$ zeigen. Diese ist aber klar, da für jedes $n \in \mathbb{N}$ nach Voraussetzung $A(n)$ und $A(n+1)$ wahr sind. Also gilt (ii).

Schritt 2 ((ii) ⇒ (iii)). Wir setzen voraus, dass (ii) wahr ist, d.h. $A(1)$ ist wahr und für alle $n \in \mathbb{N}$ gilt die Implikation $[A(n) \Rightarrow A(n+1)]$. Tatsächlich ist für (iii) nur noch die folgende Implikation für alle $n \in \mathbb{N}$ zu zeigen: $(A(1) \wedge \cdots \wedge A(n)) \Rightarrow A(n+1)$. Dies ist aber natürlich erfüllt, denn es gelten die Implikationen $[(A(1) \wedge \cdots \wedge A(n)) \Rightarrow A(n)]$ und nach Voraussetzung $[A(n) \Rightarrow A(n+1)]$.

Schritt 3 ((iii) ⇒ (i)). Wir setzen voraus, dass (iii) wahr ist. Damit ist zunächst $A(1)$ wahr. Wir nehmen an, dass die Aussage von (i) falsch ist, d.h. es gibt (mindestens) ein $n \in \mathbb{N}$, für das $A(n)$ falsch ist. Sei also N die kleinste natürliche Zahl, für die $A(N)$ falsch ist. Klarerweise gilt $N > 1$, denn $A(1)$ ist wahr. Aufgrund der Minimalität von N gilt ferner, dass $A(k)$ wahr ist für alle $k = 1, \ldots, N-1$. Dies steht aber im Widerspruch zu (iii): Für alle $n \in \mathbb{N}$ (und damit auch für $n = N-1$) muss $A(n+1)$ wahr sein (also $A(N)$ wahr sein), wenn $A(1) \wedge \cdots \wedge A(n)$ wahr ist. Also ist unsere Annahme falsch, d.h. (i) muss wahr sein. □

Bemerkung 4.4 (Beweisprinzip der vollständigen Induktion). *Nach Satz 4.3 kann man folgendermaßen vorgehen, wenn man zeigen will, dass eine Aussage $A(n)$ für alle $n \in \mathbb{N}$ wahr ist:*

(a) *Man zeigt zunächst im* ***Induktionsanfang****, dass $A(1)$ wahr ist. Dann macht man die* ***Induktionsvoraussetzung****, dass für ein beliebiges $n \in \mathbb{N}$ die Aussage $A(n)$ wahr ist. Im* ***Induktionsschritt*** *muss man zeigen, dass daraus bereits folgt, dass $A(n+1)$ wahr ist.*

(b) *Anstelle der schwachen Induktionsvoraussetzung aus* (a) *darf man auch die* ***starke Induktionsvoraussetzung*** *machen, dass für ein beliebiges $n \in \mathbb{N}$ die Aussagen $A(k)$ für alle $k = 1, \ldots, n$ wahr sind.*

Hat man den Induktionsschritt (mit Induktionsvoraussetzung in (a) *bzw. starker Induktionsvoraussetzung in* (b)*) gezeigt, so folgt aus der Äquivalenz* (i) ⇔ (ii) *bzw.* (i) ⇔ (iii) *in Satz 4.3, dass die Aussage $A(n)$ tatsächlich für alle $n \in \mathbb{N}$ wahr ist.*

Im Folgenden geben wir einige Beispiele für die vollständige Induktion, wobei wir im folgenden Beispiel 4.5 auch das **Summensymbol** $\sum$ als Notation einführen.

Beispiel 4.5. *Für $n \in \mathbb{N}$ betrachte die Summe $\sum_{j=1}^{n} j := 1 + 2 + 3 + \cdots + n$. Dann gilt*

$$\sum_{j=1}^{n} j = \frac{n(n+1)}{2} \quad \text{für alle } n \in \mathbb{N}.$$

Wir betrachten die Aussage $A(n)$, dass $\sum_{j=1}^{n} j = \frac{n(n+1)}{2}$ gilt. Wir wollen mittels vollständiger Induktion nach n beweisen, dass $A(n)$ für alle $n \in \mathbb{N}$ wahr ist.

Induktionsanfang: *Für $n = 1$ gilt $\sum_{j=1}^{n} j = \sum_{j=1}^{1} j = 1 = \frac{1\cdot 2}{2} = \frac{n(n+1)}{2}$, d.h. $A(1)$ ist wahr.*

Induktionsvoraussetzung: *Sei $n \in \mathbb{N}$. Es gelte $\sum_{j=1}^{n} j = \frac{n(n+1)}{2}$, d.h. $A(n)$ ist wahr.*

Induktionsschritt: *Wir müssen zeigen, dass $\sum_{j=1}^{n+1} j = \frac{(n+1)(n+2)}{2}$ gilt, d.h. $A(n+1)$ ist wahr. Dazu beobachten wir, dass laut Induktionsvoraussetzung gilt*

$$\sum_{j=1}^{n+1} j = (n+1) + \sum_{j=1}^{n} j = (n+1) + \frac{n(n+1)}{2} = \frac{2(n+1) + n(n+1)}{2} = \frac{(n+2)(n+1)}{2}.$$

Damit ist aber der Induktionsschritt gezeigt. Also gilt $\sum_{j=1}^{n} j = \frac{n(n+1)}{2}$ für alle $n \in \mathbb{N}$. □

Manchmal will man beweisen, dass eine Aussage für alle $n \in \mathbb{N}$ mit $n \geq n_0$ gilt. Auch dies geht mit vollständiger Induktion.

Korollar 4.6. *Sei $n_0 \in \mathbb{N}$. Ferner sei $A(n)$ eine Aussage in Abhängigkeit einer natürlichen Zahl $n \in \mathbb{N}$ mit $n \geq n_0$. Dann sind die folgenden drei Aussagen paarweise äquivalent:*

(i) *$A(n)$ ist wahr für alle $n \in \mathbb{N}$ mit $n \geq n_0$, d.h.*

$$\forall n \in \mathbb{N}, n \geq n_0 : \ A(n).$$

(ii) *$A(n_0)$ ist wahr und für alle $n \in \mathbb{N}$ mit $n \geq n_0$ gilt: Wenn $A(n)$ wahr ist, dann ist auch $A(n+1)$ wahr, d.h.*

$$A(n_0) \wedge \big(\forall n \in \mathbb{N}, n \geq n_0 : \ A(n) \Rightarrow A(n+1)\big)$$

(iii) *$A(n_0)$ ist wahr und für alle $n \in \mathbb{N}$ mit $n \geq n_0$ gilt: Wenn $A(k)$ wahr ist für alle $k = n_0, \dots, n$, dann ist auch $A(n+1)$ wahr, d.h.*

$$A(n_0) \wedge \big[\forall n \in \mathbb{N}, n \geq n_0 : \ \big(\forall k \in \mathbb{N}, n_0 \leq k \leq n : \ A(k)\big) \Rightarrow A(n+1)\big].$$

Beweis. Wir definieren die Aussage $\widetilde{A}(n) := A(n+n_0-1)$ für alle $n \in \mathbb{N}$. Dann gilt für die Aussagen $\widetilde{A}(\cdot)$ der Satz 4.3 über die vollständige Induktion. Wie man leicht sieht, ist die Aussage für $A(\cdot)$ von Korollar 4.6(i) äquivalent zu der Aussage für $\widetilde{A}(\cdot)$ von Satz 4.3(i), d.h. es gilt

$$[\forall n \in \mathbb{N}, n \geq n_0 : \ A(n)] \quad \Leftrightarrow \quad [\forall n \in \mathbb{N} : \ \widetilde{A}(n)]$$

Die analoge Äquivalenz gilt auch für die jeweiligen Aussagen (ii) und (iii) von Korollar 4.6 und Satz 4.3. Über die Äquivalenzen von Satz 4.3 erhält man also, dass auch die Aussagen (i)–(iii) von Korollar 4.6 paarweise äquivalent sind. □

Bemerkung 4.7. *Mit demselben Vorgehen wie in Korollar 4.6 kann man ein Induktionsprinzip herleiten, um eine Aussage $A(n)$ für alle $n \in \mathbb{Z} = \{0, \pm 1, \pm 2, \dots\}$ mit $n \geq n_0$ oder für alle $n \in \mathbb{Z}$ mit $n \leq n_0$ zu zeigen.*

Das folgende Beispiel nutzt das Induktionsprinzip nach Korollar 4.6(iii) für $n_0 = 2$, um einen alternativen Beweis von Satz 3.4 über die Existenz der Primfaktorzerlegung zu geben.

Beispiel 4.8. *Als Beispiel für die Anwendung der starken Induktionsvoraussetzung betrachten wir folgende Aussage für $n \in \mathbb{N}$ mit $n \geq 2$:*

$A(n)$*: Es existieren ein Index $k \in \mathbb{N}$ und Primzahlen $p_1, \dots, p_k \in \mathbb{N}$ mit $n = \prod_{j=1}^{k} p_j$.*

Wir nutzen nun vollständige Induktion, um zu zeigen, dass $A(n)$ für alle $n \in \mathbb{N}$ mit $n \geq 2$ wahr ist.

Induktionsanfang: *Für $n = 2$ geben $k := 1$ und $p_1 := n$ die Primfaktorzerlegung, d.h. $A(2)$ ist wahr.*

Induktionsvoraussetzung: *Sei $n \in \mathbb{N}$ mit $n \geq 2$. Es gelte, dass für jede Zahl $N \in \mathbb{N}$ mit $2 \leq N \leq n$ ein Index $k \in \mathbb{N}$ und k-viele Primzahlen $p_1, \dots, p_k \in \mathbb{N}$ existieren mit $N = \prod_{j=1}^{k} p_j$.*

Induktionsschritt: *Wir müssen zeigen, dass zu $n+1$ ein Index $k \in \mathbb{N}$ und Primzahlen $p_1, \dots, p_k \in \mathbb{N}$ existieren mit $n+1 = \prod_{j=1}^{k} p_j$. Dabei können zwei Fälle auftreten: Entweder ist $n+1$ eine Primzahl, oder $n+1$ ist keine Primzahl.*

Fall 1: *Falls $n+1$ eine Primzahl ist, so können wir wie beim Induktionsanfang argumentieren. Wir definieren $k := 1$ und $p_1 := n+1$ und haben die gesuchte Primfaktorzerlegung gefunden.*

Fall 2: *Falls $n+1$ keine Primzahl ist, hat $n+1$ zwei echte Teiler, d.h. $n+1 = ab$ mit $a, b \in \mathbb{N}$ und $2 \leq a, b < n+1$. Insbesondere können wir für a und b die Induktionsvoraussetzung anwenden, d.h. es gibt Indizes $\ell, m \in \mathbb{N}$ und Primzahlen $p_1, \dots, p_\ell$ sowie $q_1, \dots q_m$ mit $a = \prod_{j=1}^{\ell} p_j$ und $b = \prod_{j=1}^{m} q_j$. Definieren wir $k := \ell + m$ und $p_{\ell+j} := q_j$ für alle $j = 1, \dots, m$, so folgt (mit einem Index-Shift im Produkt bei $\stackrel{!}{=}$)*

$$n+1 = ab = \Big(\prod_{j=1}^{\ell} p_j\Big)\Big(\prod_{j=1}^{m} q_j\Big) = \Big(\prod_{j=1}^{\ell} p_j\Big)\Big(\prod_{j=1}^{m} p_{\ell+j}\Big) \stackrel{!}{=} \Big(\prod_{j=1}^{\ell} p_j\Big)\Big(\prod_{j=\ell+1}^{\ell+m} p_j\Big) = \prod_{j=1}^{k} p_j.$$

Auch in diesem Fall haben wir die gesuchte Primfaktorzerlegung gefunden. Damit ist der Induktionsschritt gezeigt, d.h. jedes $n \in \mathbb{N}$ mit $n \geq 2$ hat eine Primfaktorzerlegung. □

Kommentar. *Die Mathematik hat eine innere Ästhetik („elegante Beweise"), die schwer zu beschreiben ist, die Sie aber sicher im Zuge des Studiums wahrnehmen werden. Jedenfalls strebt man oft danach, einen Beweis so klar wie möglich und so kurz wie möglich hinzuschreiben. Im vorausgegangenen Beispiel könnte man zunächst beobachten, dass jede Primzahl eine (eindeutige) Primfaktorzerlegung hat. Dann wäre die Induktionsvoraussetzung als Spezialfall für $n = 2$ bereits verifiziert, und im Induktionsschritt dürften wir sofort voraussetzen, dass $n+1$ keine Primzahl ist.*

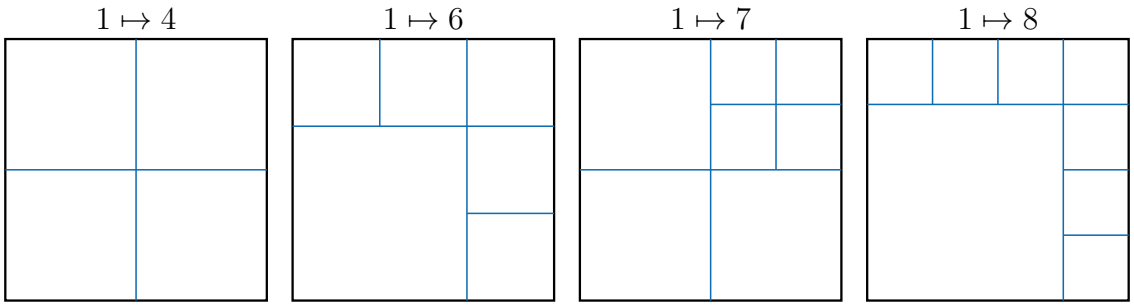


ABBILDUNG 1. Jedes Quadrat (schwarze Umrandung) lässt sich in 4, 6, 7 und 8 (nicht notwendigerweise gleich große) Quadrate unterteilen (blaue Unterteilungen). Beispiel 4.9 zeigt mittels vollständiger Induktion, dass sich jedes Quadrat deshalb in $n \geq 6$ viele (nicht notwendigerweise gleich große) Quadrate unterteilen lässt.

Die Allgemeinheit der Induktion erlaubt auch die Beweisführung für ganz unterschiedliche Fragestellungen. Manchmal braucht es auch ein wenig Idee, um die richtige Induktionsbehauptung zu formulieren.

Beispiel 4.9. *Wir betrachten die folgende Aussage für $n \in \mathbb{N}$ mit $n \geq 6$:*

$B(n)$: Jedes Quadrat lässt sich in n (nicht unbedingt gleich große) Quadrate unterteilen.

Unser Beweis basiert darauf, dass man jedes Quadrat in 4 Quadrate zerlegen kann, d.h. $1 \mapsto 4 = 1 + 3$; siehe Abbildung 1 (links). Um diese Idee in einem Induktionsschritt zu nutzen, muss man die Aussagen $B(6)$, $B(7)$ und $B(8)$ als Induktionsanfang nehmen. Wir betrachten also für $n \geq 8$ die Aussage $A(n) \coloneqq B(n-2) \wedge B(n-1) \wedge B(n)$, d.h. wir wollen im Folgenden

$$\forall n \in \mathbb{N}, n \geq 8 : A(n)$$

mittels vollständiger Induktion zeigen.

Induktionsanfang: *Anhand von Abbildung 1 sieht man, dass $B(6)$, $B(7)$ und $B(8)$ wahr sind. Also ist $A(8)$ wahr. Dies zeigt den Induktionsanfang $n = 8$.*

Induktionsvoraussetzung: *Sei $n \in \mathbb{N}$ mit $n \geq 8$. Die Aussage $A(n)$ sei wahr, d.h. jedes Quadrat lässt sich in $n-2$, $n-1$ und n Quadrate unterteilen.*

Induktionsschritt: *Wir müssen zeigen, dass $A(n+1)$ wahr ist. Nach Definition von $A(n+1)$ ist nur zu zeigen, dass $B(n+1)$ wahr ist, d.h. wir können ein Quadrat in $n+1$ Quadrate unterteilen. Zunächst teilen wir das Quadrat in 4 gleich große Quadrate; siehe Abbildung 1 (links). Nach Induktionsvoraussetzung ist $A(n)$ wahr und damit $B(n-2)$ wahr, d.h. wir können eines dieser vier Quadrate in $n-2$ Quadrate unterteilen. Insgesamt haben wir das Ausgangsquadrat in $3 + (n-2) = n+1$ Quadrate unterteilt. Damit ist der Induktionsschritt gezeigt. Also haben wir abschließend bewiesen, dass sich jedes Quadrat in $n \geq 6$ Quadrate unterteilen lässt.* □

Das abschließende Beispiel (mit falschem Beweis) zeigt, dass man bei der vollständigen Induktion sorgfältig arbeiten muss.

Beispiel 4.10. *Wir betrachten die folgende (offensichtlich falsche) Aussage:*

$A(n)$: In jeder Gruppe von $n \in \mathbb{N}$ Pferden haben alle Pferde dieselbe Farbe.

Wir „beweisen“ diese Aussage mittels vollständiger Induktion nach n.

Induktionsanfang: *Der Induktionsanfang $n = 1$ ist offensichtlich wahr.*

Induktionsvoraussetzung: *Sei $n \in \mathbb{N}$. Die Aussage $A(n)$ sei wahr.*

Induktionsschritt: *Wir müssen zeigen, dass $A(n+1)$ gilt. Seien dazu P und Q zwei Pferde der Gruppe von $n+1$ Pferden. Sei $\widehat{P}$ die Gruppe ohne P und $\widehat{Q}$ die Gruppe ohne Q. Dann sind $\widehat{P}$ und $\widehat{Q}$ zwei Gruppen mit jeweils n Pferden. Nach Induktionsvoraussetzung haben alle n Pferde in $\widehat{P}$ und $\widehat{Q}$ dieselbe Farbe. Also müssen alle Pferde aus der Gruppe mit $n+1$ Pferden dieselbe Farbe haben. „Damit ist die Aussage $A(n+1)$ bewiesen.“*

Wo ist der Fehler im Beweis? *Im Induktionsschritt nutzen wir implizit, dass es in der Gruppe neben P und Q noch ein drittes Pferd R gibt, sodass P und R (als Pferde der Gruppe $\widehat{Q}$) und Q und R (als Pferde der Gruppe $\widehat{P}$) dieselbe Farbe haben. Es muss also $n \geq 3$ gelten. Wir haben den Induktionsanfang aber für $n = 1$ gezeigt, und die Aussage $A(n)$ ist auch offensichtlich falsch für $n = 2$.*

Bemerkung 4.11. *Abschließend müssen wir noch festhalten, welche (aus der Schulmathematik bekannten) Eigenschaften von $\mathbb{N}$ wir in den letzten Abschnitten verwendet haben:*

- *Arithmetik (inkl. Kommutativ-, Assoziativ- und Distributivgesetzen),*
- *vollständige Kleiner-Größer-Ordnung (inkl. Verträglichkeit mit der Arithmetik),*
- *Existenz von minimalen Elementen.*

Formal müssen wir diese Eigenschaften noch verifizieren, wenn wir später die natürlichen Zahlen $\mathbb{N}$ konstruieren.

5. Mengen

Die moderne Mathematik basiert auf dem Begriff der Menge. Auch die Konstruktion der üblichen Zahlenmengen (mit ihrer Arithmetik und etwaigen Ordnungsrelationen) wie beispielsweise $\mathbb{N}$ werden Sie im Zuge der *Einführung ins Mathematische Arbeiten* (Konstruktion von $\mathbb{N}$) und der *Analysis 1* (Konstruktion von $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$) noch sehen. Der Einfachheit halber arbeiten wir hier mit dem Mengenbegriff von Georg Cantor.

Definition 5.1 (Cantor (1895)). *Eine **Menge** M ist eine ungeordnete Zusammenfassung von wohlbestimmten und wohlunterschiedenen Objekten zu einer Gesamtheit. Diese Objekte heißen **Elemente** von M. Ist M eine Menge und x ein Element von M, so schreiben wir $x \in M$. Ist M eine Menge und x kein Element von M, so schreiben wir $x \notin M$.*

Eine Möglichkeit Mengen darzustellen, ist die **aufzählende Schreibweise**, z.B.

$$M \coloneqq \{a, b, c, d, e\} \quad \text{oder} \quad M \coloneqq \{1, 3, 5, \dots\}.$$

Ist $A(x)$ eine Aussage über die Elemente x einer Menge M, so verwendet man auch eine **beschreibende Schreibweise**, z.B.

$$\{x \in M \mid A(x)\} \coloneqq \{x \in M \mid A(x) \text{ ist wahr}\} \coloneqq \{x \mid x \in M \text{ und } A(x) \text{ ist wahr}\}.$$

Aus der Schule kennen Sie die folgenden Zahlenmengen, die wir allerdings später mit dem obigen Mengenbegriff gewissermaßen aus dem Nichts heraus noch konstruieren wollen und werden:

- $\mathbb{N} \coloneqq \{1, 2, 3, \dots\}$ *natürliche Zahlen* (positive ganze Zahlen);
- $\mathbb{N}_0 \coloneqq \{0, 1, 2, \dots\}$ *natürliche Zahlen inklusive Null* (nicht-negative ganze Zahlen);
- $\mathbb{Z} \coloneqq \{0, 1, -1, 2, -2, \dots\} = \{\pm n \mid n \in \mathbb{N}_0\}$ *ganze Zahlen*;
- $\mathbb{Q} \coloneqq \{z/n \mid z \in \mathbb{Z}, n \in \mathbb{N}\}$ *rationale Zahlen*;
- $\mathbb{R}$ *reelle Zahlen*;
- $\mathbb{C} \coloneqq \{a + bi \mid a, b \in \mathbb{R}\}$ *komplexe Zahlen.*

Definition 5.2. *Zwei **Mengen A und B sind gleich**, wenn sie dieselben Elemente enthalten. Wir schreiben in diesem Fall $A = B$ mit dem üblichen Symbol $=$ für die Gleichheit. Sind zwei Mengen nicht gleich, so schreiben wir $A \neq B$. Eine Menge A ist eine **Teilmenge** von B, wenn jedes Element von A auch ein Element von B ist. In diesem Fall bezeichnet man **B als Obermenge von A** und schreibt $A \subseteq B$ bzw. $B \supseteq A$ mit den Symbolen $\subseteq$ und $\supseteq$ für die **Inklusion**. Ist A eine Teilmenge von B und $A \neq B$, so schreiben wir $A \subsetneq B$ bzw. $B \supsetneq A$ mit den Symbolen $\subsetneq$ und $\supsetneq$ für die **strikte Inklusion** (bzw. **echte Inklusion**). Schließlich bezeichnet $\emptyset \coloneqq \{\}$ die **leere Menge**.*

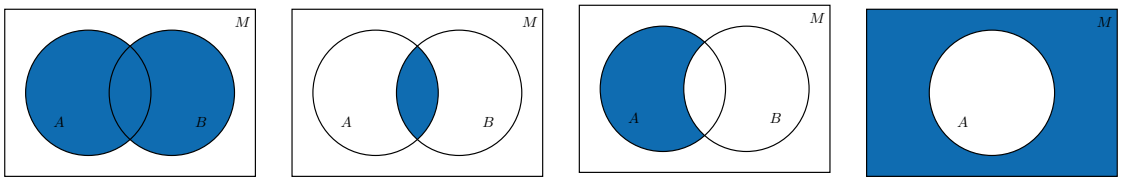
Kommentar. *Manche Mathematiker*innen schreiben $A \subsetneq B$ anstelle von $A \subsetneq B$. Je nach Autor*in wird das Symbol $A \subset B$ als $A \subseteq B$ oder $A \subsetneq B$ verstanden.*

Bemerkung 5.3. *Für jede Menge A gilt $\emptyset \subseteq A$ mit strikter Inklusion $\emptyset \subsetneq A$ für $A \neq \emptyset$. Ferner kann man Mengen von Mengen bilden, z.B. findet man häufig:* Sei $\mathbb{K} \in \{\mathbb{R}, \mathbb{C}\}$, *d.h. $\mathbb{K}$ bezeichnet entweder die Menge der reellen oder die Menge der komplexen Zahlen. Wenn wir später die natürlichen Zahlen $\mathbb{N}$ formal konstruieren, wird es wichtig sein, dass klarerweise $\emptyset \neq \{\emptyset\} \neq \{\emptyset, \{\emptyset\}\}$ gilt.*

Die folgenden Definitionen werden in Abbildung 2 in Form von sogenannten **Venn-Diagrammen** visualisiert.

Definition 5.4. *Für Mengen A und B definieren wir*

- *die **Vereinigung** $A \cup B \coloneqq \{x \mid (x \in A) \vee (x \in B)\}$, sprachlich: **$A$ vereinigt B**,*
- *den **Schnitt** $A \cap B \coloneqq \{x \mid (x \in A) \wedge (x \in B)\}$, sprachlich: **$A$ geschnitten B**,*



$A \cup B$ $A \cap B$ $A \backslash B$ A^{c}

ABBILDUNG 2. Venn-Diagramme für Vereinigung $A \cup B$, Schnitt $A \cap B$ und Differenz $A \backslash B$ von Mengen $A, B \subseteq M$ sowie Komplement A^{c} von A in M.

- *die* ***Differenz*** $A \backslash B := \{x \mid (x \in A) \wedge (x \notin B)\} = \{x \in A \mid x \notin B\}$, *sprachlich:* ***$A$ ohne B***.

Ist $A \subseteq M$ und die Menge M im Kontext klar, so bezeichnet

- $A^{\mathsf{c}} := M \backslash A$ *das* ***Komplement von A (in M)***.

Zwei Mengen A und B sind ***disjunkt****, wenn $A \cap B = \emptyset$.*

Beispiel 5.5. *Einfache Beispiele für Vereinigung, Schnitt und Differenz sind*

$$\{1,2,3\} \cup \{2,3,4\} = \{1,2,3,4\}, \quad \{1,2,3\} \cap \{2,3,4\} = \{2,3\}, \quad \{1,2,3\} \backslash \{2,3,4\} = \{1\}.$$

Sind die natürlichen Zahlen $\mathbb{N}$ die Gesamtmenge, so ist

$$G := \{2n \mid n \in \mathbb{N}\} := \{x \mid \exists n \in \mathbb{N} : x = 2n\} = \{2,4,6,\dots\}$$

die Menge der geraden Zahlen. Das Komplement

$$U := G^{\mathsf{c}} = \mathbb{N} \backslash G = \{1,3,5,\dots\} = \{x \mid \exists n \in \mathbb{N} : x = 2n-1\} =: \{2n-1 \mid n \in \mathbb{N}\}.$$

ist die Menge der ungeraden Zahlen. Gemäß Definition gilt $U \cap G = \emptyset$.

Auf Mengen gelten diverse Rechenregeln wie beispielsweise die *Distributivgesetze*. Gemäß Definition gilt eine Mengengleichheit $A = B$ genau dann, wenn beide Inklusionen $A \subseteq B$ und $A \supseteq B$ gelten. Will man eine Mengengleichheit zeigen, so zeigt man also (meistens), dass beide Inklusionen gelten.

Lemma 5.6. *Für beliebige Mengen A, B, C gelten*

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C), \tag{1}$$

$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C). \tag{2}$$

Beweis. Wir zeigen beide Inklusionen in (1). Die Gleichheit (2) folgt analog.

Schritt 1 (Inklusion $\subseteq$ in (1)). Um (1) zu zeigen, sei zunächst $x \in A \cap (B \cup C)$ beliebig. Nach Definition des Schnitts gilt $(x \in A) \wedge (x \in B \cup C)$. Nach Definition der

Vereinigung ist also $(x \in B) \vee (x \in C)$. Daraus ergibt sich also

$$(x \in A) \wedge (x \in B), \text{ d.h. } x \in A \cap B, \quad \text{oder} \quad (x \in A) \wedge (x \in C), \text{ d.h. } x \in A \cap C.$$

Insgesamt zeigt dies $(x \in A \cap B) \vee (x \in A \cap C)$ und damit $x \in (A \cap B) \cup (A \cap C)$. Da x beliebig war, erfüllt jedes $x \in A \cap (B \cup C)$ also $x \in (A \cap B) \cup (A \cap C)$ und somit gilt $A \cap (B \cup C) \subseteq (A \cap B) \cup (A \cap C)$.

Schritt 2 (Inklusion $\supseteq$ in (1)). Die andere Inklusion zeigt man analog. Sei dazu $x \in (A \cap B) \cup (A \cap C)$ beliebig. Nach Definition der Vereinigung gilt $(x \in A \cap B) \vee (x \in A \cap C)$. Insbesondere gilt also einerseits $x \in A$ und andererseits

$$x \in B \text{ oder } x \in C, \text{ d.h. } x \in B \cup C.$$

Insgesamt zeigt dies $(x \in A) \wedge (x \in B \cup C)$ und damit $x \in A \cap (B \cup C)$. Jedes $x \in (A \cap B) \cup (A \cap C)$ erfüllt also $x \in A \cap (B \cup C)$ und somit $(A \cap B) \cup (A \cap C) \subseteq A \cap (B \cup C)$.

Schritt 3 (Gleichheit = in (1)). Da durch Schritt 1 und 2 beide Inklusionen gezeigt sind, gilt (1) mit Gleichheit. □

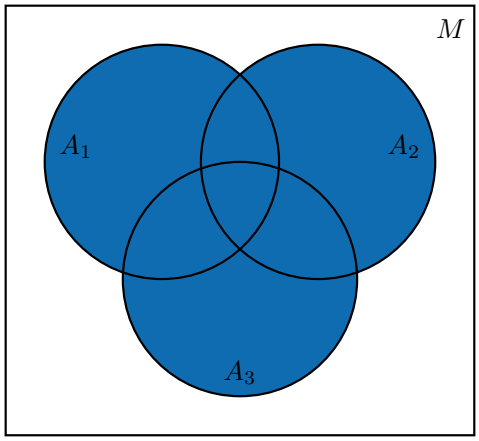
Kommentar. *In Lehrbüchern oder Vorlesungen heißt es oft einfach:* „Der Beweis ist analog“ *zu einem anderen Beweis. Das bedeutet, dass Sie, wenn sie den anderen Beweis vollständig verstanden haben, in der Lage sein sollten, diesen Beweis selbst zu machen. Die Beweisschritte und Argumente sollten also sehr ähnlich sein. Ebenso oft finden Sie auch:* „Der Beweis ist offensichtlich“*. Oder sogar:* „Der Beweis ist trivial“*. Das bedeutet, dass der Beweis mit Standardargumenten folgt, die bei den Leser*innen vorausgesetzt werden. Ob ein Beweis wirklich trivial ist oder nicht, liegt sehr im Auge der Betrachter*innen. Aber je länger Sie sich mit Mathematik beschäftigen, desto einfacher werden Ihnen die Beweise erscheinen, die Ihnen am Anfang des Studiums noch sehr schwer schienen.*

Bisweilen betrachtet man die Vereinigung bzw. den Schnitt von mehr als zwei Mengen. Dafür schaffen wir die folgende Notation, indem wir die Definition der Quantoren aus Abschnitt 4 von $n \in \mathbb{N}$ auf allgemeinere Mengen und Indizes $i \in I$ übertragen. Beachten Sie, dass für $I = \{1, 2\}$ und Mengen A_1 und A_2 die folgende Definition 5.7 mit der von Definition 5.4 übereinstimmt, d.h. $\bigcup_{i \in I} A_i = A_1 \cup A_2$ bzw. $\bigcap_{i \in I} A_i = A_1 \cap A_2$. Siehe auch Abbildung 3 für die Visualisierung in Form von Venn-Diagrammen.

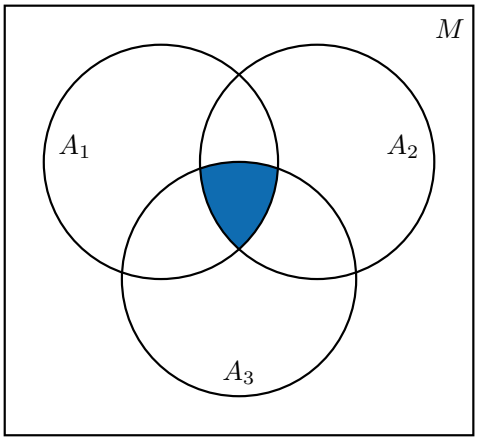
Definition 5.7. *Es sei I eine **Indexmenge**, d.h. eine Menge, deren Elemente wir nur zum Indizieren anderer Mengen oder Elemente nutzen (z.B. $I \subseteq \mathbb{N}$). Für jedes $i \in I$ sei eine Menge A_i gegeben. Dann definieren wir*

- *die **Vereinigung** $\bigcup_{i \in I} A_i := \{x \mid \exists i \in I : x \in A_i\}$,*
- *den **Schnitt** $\bigcap_{i \in I} A_i := \{x \mid \forall i \in I : x \in A_i\}$.*

Mit diesen Definitionen gilt der folgende Satz, der die Distributivgesetze von Lemma 5.6 verallgemeinert und zusätzlich die De Morgan'schen Regeln für Mengen formuliert.



$\bigcup_{i\in I} A_i$



$\bigcap_{i\in I} A_i$

ABBILDUNG 3. Venn-Diagramme für Vereinigung $\bigcup_{i\in I} A_i = A_1 \cup A_2 \cup A_3$ und Schnitt $\bigcap_{i\in I} A_i$ für $I = \{1, 2, 3\}$ und Mengen $A_i \subseteq M$ for $i \in I$.

Satz 5.8. *Es sei I eine Indexmenge. Für alle $i \in I$ sei B_i eine Menge. Sei ferner A eine Menge. Dann gelten die* ***Distributivgesetze***

$$A \cap \Big(\bigcup_{i\in I} B_i\Big) = \bigcup_{i\in I} (A \cap B_i), \tag{3}$$

$$A \cup \Big(\bigcap_{i\in I} B_i\Big) = \bigcap_{i\in I} (A \cup B_i). \tag{4}$$

Ferner gelten die ***De Morgan'schen Regeln***

$$A \backslash \Big(\bigcup_{i\in I} B_i\Big) = \bigcap_{i\in I} (A \backslash B_i), \tag{5}$$

$$A \backslash \Big(\bigcap_{i\in I} B_i\Big) = \bigcup_{i\in I} (A \backslash B_i). \tag{6}$$

Beweis. Wir beweisen jeweils beide Inklusionen in (3)–(6).

Schritt 1 (Inklusion $\subseteq$ in (3)). Sei $x \in A \cap \big(\bigcup_{i\in I} B_i\big)$. Dann ist $x \in A$, und es gibt einen Index $i_0 \in I$ mit $x \in B_{i_0}$. Also ist $x \in A \cap B_{i_0} \subseteq \bigcup_{i\in I}(A \cap B_i)$. Da x beliebig war, folgt die Inklusion $A \cap \big(\bigcup_{i\in I} B_i\big) \subseteq \bigcup_{i\in I}(A \cap B_i)$.

Schritt 2 (Inklusion $\supseteq$ in (3)). Sei $x \in \bigcup_{i\in I}(A \cap B_i)$. Dann existiert ein Index $i_0 \in I$ mit $x \in A \cap B_{i_0}$. Insbesondere gilt $x \in A$ und $x \in B_{i_0} \subseteq \bigcup_{i\in I} B_i$ und damit $x \in A \cap \big(\bigcup_{i\in I} B_i\big)$. Da x beliebig war, folgt die Inklusion $A \cap \big(\bigcup_{i\in I} B_i\big) \supseteq \bigcup_{i\in I}(A \cap B_i)$.

Schritt 3 (Inklusion $\subseteq$ in (4)). Sei $x \in A \cup \big(\bigcap_{i\in I} B_i\big)$. Also gilt $x \in A$ oder $x \in B_i$ für alle $i \in I$. Insbesondere gilt $x \in A \cup B_i$ für alle $i \in I$. Daraus folgt $x \in \bigcap_{i\in I}(A \cup B_i)$. Da x beliebig war, folgt die Inklusion $A \cup \big(\bigcap_{i\in I} B_i\big) \subseteq \bigcap_{i\in I}(A \cup B_i)$.

Schritt 4 (Inklusion $\supseteq$ in (4)). Sei $x \in \bigcap_{i\in I}(A \cup B_i)$. Also gilt $x \in A \cup B_i$ für alle $i \in I$. Insbesondere gilt also $x \in A$ oder $x \in B_i$ für alle $i \in I$. Ist $x \in A$, so folgt $x \in A \cup \big(\bigcap_{i\in I} B_i\big)$. Ist $x \notin A$, so gilt $x \in B_i$ für alle $i \in I$ und deshalb $x \in \bigcap_{i\in I} B_i \subseteq A \cup \big(\bigcap_{i\in I} B_i\big)$. Da x beliebig war, folgt die Inklusion $A \cup \big(\bigcap_{i\in I} B_i\big) \supseteq \bigcap_{i\in I}(A \cup B_i)$.

Schritt 5 (Inklusion $\subseteq$ in (5)). Sei $x \in A\backslash\big(\bigcup_{i\in I} B_i\big)$. Also ist $x \in A$, aber $x \notin \bigcup_{i\in I} B_i$. Beachte die Äquivalenz

$$y \in \bigcup_{i\in I} B_i \quad \Longleftrightarrow \quad \exists i \in I : y \in B_i.$$

Also gilt mittels Negation des Existenz-Quantors die Äquivalenz

$$x \notin \bigcup_{i\in I} B_i \quad \Longleftrightarrow \quad \forall i \in I : x \notin B_i.$$

Insbesondere gilt also $x \notin B_i$ für alle $i \in I$. Also gilt $x \in A\backslash B_i$ für alle $i \in I$ und insbesondere $x \in \bigcap_{i\in I}(A\backslash B_i)$. Da x beliebig war, folgt die Inklusion $A\backslash\big(\bigcup_{i\in I} B_i\big) \subseteq \bigcap_{i\in I}(A\backslash B_i)$.

Schritt 6 (Inklusion $\supseteq$ in (5)). Sei $x \in \bigcap_{i\in I}(A\backslash B_i)$. Also ist $x \in A\backslash B_i$ für alle $i \in I$. Insbesondere gilt $x \in A$ und $x \notin B_i$ für alle $i \in I$. Dies zeigt $x \in A$ und $x \notin \bigcup_{i\in I} B_i$, d.h. $x \in A\backslash\big(\bigcup_{i\in I} B_i\big)$. Da x beliebig war, folgt die Inklusion $A\backslash\big(\bigcup_{i\in I} B_i\big) \supseteq \bigcap_{i\in I}(A\backslash B_i)$.

Schritt 7 (Inklusion $\subseteq$ in (6)). Sei $x \in A\backslash\big(\bigcap_{i\in I} B_i\big)$. Also ist $x \in A$ und $x \notin \bigcap_{i\in I} B_i$. Beachte die Äquivalenz

$$y \in \bigcap_{i\in I} B_i \quad \Longleftrightarrow \quad \forall i \in I : y \in B_i.$$

Also gilt mittels Negation des All-Quantors die Äquivalenz

$$x \notin \bigcap_{i\in I} B_i \quad \Longleftrightarrow \quad \exists i_0 \in I : x \notin B_{i_0}.$$

Wir wählen ein $i_0 \in I$ mit $x \notin B_{i_0}$ und damit $x \in A\backslash B_{i_0} \subseteq \bigcup_{i\in I}(A\backslash B_i)$. Da x beliebig war, folgt die Inklusion $A\backslash\big(\bigcap_{i\in I} B_i\big) \subseteq \bigcup_{i\in I}(A\backslash B_i)$.

Schritt 8 (Inklusion $\supseteq$ in (6)). Sei $x \in \bigcup_{i\in I}(A\backslash B_i)$. Also existiert ein $i_0 \in I$ mit $x \in A\backslash B_{i_0}$, d.h. es gilt $x \in A$ und $x \notin B_{i_0}$. Insbesondere folgt $x \notin \bigcap_{i\in I} B_i$ und somit $x \in A\backslash\big(\bigcap_{i\in I} B_i\big)$. Da x beliebig war, folgt die Inklusion $A\backslash\big(\bigcap_{i\in I} B_i\big) \supseteq \bigcup_{i\in I}(A\backslash B_i)$. □

Als letzte Definition in diesem Abschnitt definieren wir noch die Potenzmenge einer Menge.

Definition 5.9. *Für eine Menge M bezeichnet $\mathcal{P}(M) \coloneqq \big\{A \,\big|\, A \subseteq M\big\}$ die **Potenzmenge**. Dies ist die Menge aller Teilmengen von M.*

Beispiel 5.10. *Für $M \coloneqq \{1,2,3\}$ gilt*

$$\mathcal{P}(M) = \big\{\emptyset, \{1\}, \{2\}, \{3\}, \{1,2\}, \{1,3\}, \{2,3\}, \{1,2,3\}\big\},$$

d.h. M hat 3 Elemente und $\mathcal{P}(M)$ hat bereits 8 Elemente. Beachte, dass die leere Menge $\emptyset$ und die ganze Menge M immer Elemente der Potentzmenge sind.

Im vorausgegangenen Beispiel haben wir gesehen, dass die 3-elementige Menge $M = \{1, 2, 3\}$ insgesamt $2^3 = 8$ Teilmengen hat. Dies gilt allgemein, wie wir mit Satz 5.13 zeigen werden.

Definition 5.11. *Für $n \in \mathbb{N}_0$ bezeichne $n! \coloneqq \prod_{j=1}^{n} j$ die **Faktorielle**, wobei das leere Produkt als 1 definiert sei, d.h. $0! \coloneqq 1$. Für $k \in \mathbb{N}_0$ mit $k \leq n$ sei*

$$\binom{n}{k} \coloneqq \frac{n!}{k!(n-k)!}$$

*der **Binomialkoeffizient**, sprachlich: **n über k**.*

Definition 5.12. *Eine Menge A ist eine **endliche Menge**, wenn sie entweder leer ist oder es ein $n \in \mathbb{N}$ gibt, sodass wir die Elemente von A entsprechend nummerieren können: $A = \{x_1, \ldots, x_n\} = \{x_i \mid i = 1, \ldots, n\}$ mit paarweise verschiedenen $x_j \neq x_k$ für alle $j, k = 1, \ldots, n$. In diesem Fall sagen wir auch, dass A eine **n-elementige Menge** ist und schreiben **$\#A = n$** für die **Kardinalität** von A, d.h. die **Anzahl an Elementen**. Die 0-elementige Menge sei die Menge ohne Elemente, d.h. $A = \emptyset$ und $\#\emptyset \coloneqq 0$.*

Satz 5.13. *Seien $n, k \in \mathbb{N}_0$ mit $k \leq n$. Dann hat jede n-elementige Menge A genau $\binom{n}{k}$ verschiedene k-elementige Teilmengen. Ferner hat A genau 2^n verschiedene Teilmengen, d.h. $2^n = \sum_{k=0}^{n} \binom{n}{k}$.*

Beweis. Wir beweisen beide Aussagen des Satzes mittels vollständiger Induktion nach $n \in \mathbb{N}_0$:

> Für jede Menge A mit $\#A = n \in \mathbb{N}_0$ und für alle $k = 0, \ldots, n$ erfüllen die Mengen $\mathcal{P}_k(A) \coloneqq \{B \subseteq A \mid \#B = k\}$ gerade $\#\mathcal{P}_k(A) = \binom{n}{k}$ und $\#\mathcal{P}(A) = \sum_{k=0}^{n} \#\mathcal{P}_k(A) = 2^n$.

Induktionsanfang. Für $n = 0 = k$ gilt $A = \emptyset$ und $\mathcal{P}_0(\emptyset) = \mathcal{P}(\emptyset) = \{\emptyset\}$ mit $\#\mathcal{P}_0(\emptyset) = \#\mathcal{P}(\emptyset) = 1 = \binom{0}{0}$, d.h. die Aussage ist wahr für $n = 0$.

Induktionsvoraussetzung. Sei $n \in \mathbb{N}$ und die Aussage sei wahr für alle n-elementigen Mengen.

Induktionsschritt. Sei $A = \{x_1, \ldots, x_{n+1}\}$ eine $(n+1)$-elementige Menge. Wir unterteilen die k-elementigen Teilmengen $B \in \mathcal{P}_k(A)$ in zwei Gruppen:

- $\mathcal{P}_k^-(A) \coloneqq \{B \subseteq A \mid \#B = k \wedge x_{n+1} \notin B\}$,
- $\mathcal{P}_k^+(A) \coloneqq \{B \subseteq A \mid \#B = k \wedge x_{n+1} \in B\}$.

Beachte $\mathcal{P}_k(A) = \mathcal{P}_k^-(A) \cup \mathcal{P}_k^+(A)$ und $\mathcal{P}_k^-(A) \cap \mathcal{P}_k^+(A) = \emptyset$. Daraus folgt $\#\mathcal{P}_k(A) = \#\mathcal{P}_k^-(A) + \#\mathcal{P}_k^+(A)$. Wir müssen drei Fälle unterscheiden:

Fall 1 ($k = 0$). Für $k = 0$ gilt $\mathcal{P}_0^-(A) = \{\emptyset\}$, $\mathcal{P}_0^+(A) = \emptyset$ und $\#\mathcal{P}_0(A) = 1 = \binom{n+1}{0}$.

Fall 2 ($k = n+1$). Für $k = n+1$ gilt $\#\mathcal{P}^-_{n+1}(A) = \emptyset$ and $\mathcal{P}^+_{n+1}(A) = \{A\}$, also $\#\mathcal{P}_{n+1}(A) = 1 = \binom{n+1}{n+1}$.

Fall 3 ($1 \le k \le n$). Für $1 \le k \le n$ beachte zunächst, dass $\mathcal{P}^-_k(A) = \mathcal{P}_k(A')$ für $A' := \{x_1, \dots, x_n\}$. Wir wenden die Induktionsvoraussetzung für A' an: Es folgt $\#\mathcal{P}^-_k(A) = \#\mathcal{P}_k(A') = \binom{n}{k}$. Beachte ferner, dass sich jedes $B \in \mathcal{P}^+_k(A)$ genau in der Form $B = \{x_{n+1}\} \cup B'$ schreiben lässt mit $B' \in \mathcal{P}_{k-1}(A')$. Nach Induktionsvoraussetzung folgt also $\#\mathcal{P}^+_k(A) = \#\mathcal{P}_{k-1}(A') = \binom{n}{k-1}$. Für $1 \le k \le n$ ergibt sich insgesamt

$$\begin{aligned}\#\mathcal{P}_k(A) = \binom{n}{k} + \binom{n}{k-1} &= \frac{n!}{k!(n-k)!} + \frac{n!}{(k-1)!(n-k+1)!} \\ &= \frac{n!\,(n+1-k)}{k!(n+1-k)!} + \frac{n!\,k}{k!(n+1-k)!} \\ &= \frac{n!\,(n+1)}{k!(n+1-k)!} = \binom{n+1}{k}.\end{aligned} \tag{7}$$

Damit ist $\#\mathcal{P}_k(A) = \binom{n+1}{k}$ für alle $k = 0, \dots, n+1$ gezeigt.

Abschließend müssen wir noch $\#\mathcal{P}(A)$ berechnen. Dabei verwenden wir die Identität (7) für den Binomialkoeffizienten (und einen Index-Shift in der Summe beim $\overset{!}{=}$) und erhalten

$$\begin{aligned}\#\mathcal{P}(A) = \sum_{k=0}^{n+1} \#\mathcal{P}_k(A) &= \sum_{k=0}^{n+1} \binom{n+1}{k} = \binom{n+1}{0} + \binom{n+1}{n+1} + \sum_{k=1}^{n} \binom{n+1}{k} \\ &\overset{(7)}{=} 1 + 1 + \sum_{k=1}^{n} \left[\binom{n}{k} + \binom{n}{k-1} \right] \\ &= \binom{n}{0} + \binom{n}{n} + \sum_{k=1}^{n} \binom{n}{k} + \sum_{k=1}^{n} \binom{n}{k-1} \\ &\overset{!}{=} \binom{n}{0} + \binom{n}{n} + \sum_{k=1}^{n} \binom{n}{k} + \sum_{k=0}^{n-1} \binom{n}{k} = 2 \sum_{k=0}^{n} \binom{n}{k}.\end{aligned}$$

Mit der Induktionsvoraussetzung folgt somit

$$\#\mathcal{P}(A) = 2 \sum_{k=0}^{n} \binom{n}{k} = 2 \cdot \#\mathcal{P}(A') = 2 \cdot 2^n = 2^{n+1}.$$

Damit ist der Induktionsschritt gezeigt und die Aussage des Satzes gilt für alle $n \in \mathbb{N}_0$. □

Wir beschließen den Abschnitt mit der Beobachtung, dass der Cantor'sche Begriff von Menge und Element formal nicht hinreichend präzise ist, da er innere Widersprüche enthält.

Bemerkung 5.14 (Russell'sche Antonomie (1903)). *Formal ist die Cantorsche Definition einer Menge noch „zu naiv", wie die* Russelsche Antonomie *zeigt:*

> Es sei M die Menge aller Mengen, die sich nicht selbst als Element enthalten.

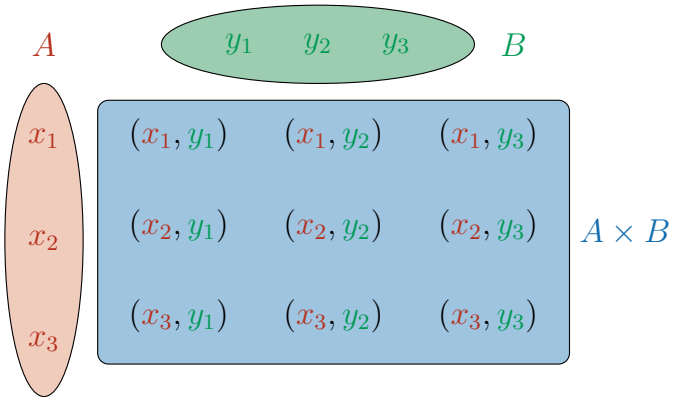


ABBILDUNG 4. Visualisierung des kartesischen Produkts $A \times B$ aus Definition 6.1 für zwei Mengen $A = \{x_1, x_2, x_3\}$ und $B = \{y_1, y_2, y_3\}$.

Diese „Definition" von M erzeugt einen Widerspruch mit der folgenden Frage:

Gilt $M \in M$?

Wenn $M \in M$, dann folgt nach Definition von M, dass $M \notin M$. Wenn $M \notin M$, dann folgt nach Definition von M, dass $M \in M$. Dieser inhärente Widerspruch der Cantor-Definition kann durch die axiomatische Mengenlehre ausgeschlossen werden, da diese die Definition der Russell-Menge nicht erlaubt.

6. Kartesisches Produkt und (Äquivalenz-) Relationen

Nach Definition einer Menge spielt die Reihenfolge bei der aufzählenden Schreibweise keine Rolle, d.h.

$$\{1, 2\} = \{2, 1\}.$$

Das ist der zentrale Unterschied zu **(geordneten) Paaren**, für die wir die runden Klammern verwenden und bei denen eben diese Reihenfolge zusätzlich beachtet wird, d.h.

$$(1, 2) \neq (2, 1).$$

Definition 6.1. *Für Mengen A und B definieren wir das **kartesische Produkt** $A \times B := \{(x, y) \mid (x \in A) \wedge (y \in B)\}$ (sprachlich auch: die **Produktmenge** oder **A Kreuz B**). Ein Element von $A \times B$ bezeichnen wir als **(geordnetes) Paar** $(x, y) \in A \times B$.*

Definition 6.2. *Seien A und B Mengen. Eine Teilmenge $R \subseteq A \times B$ heißt **Relation (zwischen A und B)**. Für $A = B$ bezeichnet man R auch als **Relation (in A)**. Für eine Relation R und $a \in A$ und $b \in B$ verwendet man oft die Schreibweise **$a\,R\,b$** anstelle von $(a, b) \in R$ und **$a \not R\, b$** anstelle von $(a, b) \notin R$.*

Beispiel 6.3. *Erste Beispiele für Relationen auf* $\mathbb{N}$*, die sie schon kennen, sind die Gleichheit* $=$*, die Ordnungsrelation* $<$ *und die Teilerrelation* $|$*:*

- $= \;:= \{(x,y) \in \mathbb{N} \times \mathbb{N} \mid x = y\}$ *(Gleichheitsrelation)*
- $< \;:= \{(x,y) \in \mathbb{N} \times \mathbb{N} \mid x < y\}$ *(Ordnungsrelation)*
- $| \;:= \{(t,x) \in \mathbb{N} \times \mathbb{N} \mid \exists x' \in \mathbb{N} : x = tx'\}$ *(Teilerrelation: t ist Teiler von x)*

Aus diesen Beispielen erklären sich auch die Schreibweisen $x = y$ *(anstelle von* $(x,y) \in =$*),* $x < y$ *(anstelle von* $(x,y) \in <$*) und* $t|x$ *(anstelle von* $(t,x) \in |$*) für diese Relationen.*

Definition 6.4. *Sei* A *eine Menge und* $\sim$ *eine Relation in* A*. Die Relation* $\sim$ *heißt*

(a) ***reflexiv****, wenn gilt* $\forall x \in A : x \sim x$*;*
(b) ***symmetrisch****, wenn gilt* $\forall x, y \in A : [x \sim y \Rightarrow y \sim x]$*;*
(c) ***transitiv****, wenn gilt* $\forall x, y, z \in A : [(x \sim y \wedge y \sim z) \Rightarrow x \sim z]$*.*

Die Relation $\sim$ *heißt* ***Äquivalenzrelation (auf A)****, wenn* $\sim$ *reflexiv, symmetrisch und transitiv ist.*

Beispiel 6.5. *Äquivalenzrelationen treten im mathematischen Alltag sehr häufig auf:*

- *Das einfachste mathematische Beispiel für eine Äquivalenzrelation ist die Gleichheit* $=$ *auf* $\mathbb{N}$*.*
- *Wenn wir die Menge der rationalen Zahlen* $\mathbb{Q} = \{z/n \mid z \in \mathbb{Z}, n \in \mathbb{N}\}$ *betrachten, so verwenden wir bei dieser Definition implizit durchs Kürzen eine Äquivalenzrelation auf* $\mathbb{Z} \times \mathbb{N}$*: Wir identifizieren beispielsweise die Brüche* $\frac{1}{3} = \frac{2}{6} = \frac{3}{9} = \ldots$*, weil diese im Sinne der Schulmathematik alle denselben Zahlenwert bezeichnen.*
- *Eine Äquivalenzrelation unseres Alltag ist, wenn wir sagen, dass zwei Menschen in Relation stehen, wenn sie im selben Jahr geboren sind.*

Beispiel 6.6. *Aber auch andere Relationen, die keine Äquivalenzrelation sind, treten oft im mathematischen Alltag auf:*

- *Die Ungleichheit* $\neq$ *auf* $\mathbb{N}$ *ist symmetrisch, aber weder reflexiv noch transitiv.*
- *Die Kleiner-Ordnung* $<$ *auf* $\mathbb{N}$ *ist transitiv, aber weder reflexiv noch symmetrisch.*
- *Die Mengen-Inklusion* $\subseteq$ *ist reflexiv und transitiv, aber nicht symmetrisch.*

Der folgende (einfache) Satz soll nur das erste Arbeiten mit Äquivalenzrelationen illustrieren: Entspricht R_1 der Äquivalenzrelation, dass zwei Personen im selben Jahr geboren sind, und R_2 der Äquivalenzrelation, dass zwei Personen gleich groß sind, so entspricht R aus dem folgenden Satz gerade der Äquivalenzrelation, dass zwei Personen im gleichen Jahr geboren sind und gleich groß sind.

Satz 6.7. *Es seien R_1, R_2 Äquivalenzrelationen auf einer Menge A. Dann ist auch $R \coloneqq R_1 \cap R_2$ eine Äquivalenzrelation auf A.*

Beweis. Jede Eigenschaft einer Äquivalenzrelation wird in einem der folgenden drei Beweisschritte gezeigt.

Schritt 1 (R_1, R_2 reflexiv $\Rightarrow$ R reflexiv). Sei $x \in A$. Aufgrund der Eigenschaften von R_1 und R_2 gelten $(x,x) \in R_1$ und $(x,x) \in R_2$, also auch $(x,x) \in R_1 \cap R_2 = R$. In üblicher Notation gilt damit $x\,R\,x$, d.h. R ist reflexiv.

Schritt 2 (R_1, R_2 symmetrisch $\Rightarrow$ R symmetrisch). Seien $x, y \in A$ mit $x\,R\,y$. Es ist $y\,R\,x$ zu zeigen. Es gilt $(x,y) \in R = R_1 \cap R_2$. Aufgrund der Eigenschaften von R_1 und R_2 folgt daraus $(y,x) \in R_1 \cap R_2 = R$. In üblicher Notation schreibt sich dies als $y\,R\,x$, d.h. R ist symmetrisch.

Schritt 3 (R_1, R_2 transitiv $\Rightarrow$ R transitiv). Seien $x, y, z \in A$ mit $x\,R\,y$ und $y\,R\,z$. Es ist $x\,R\,z$ zu zeigen. Es gilt $(x,y), (y,z) \in R = R_1 \cap R_2$. Aufgrund der Eigenschaften von R_1 und R_2 folgt daraus $(x,z) \in R_1 \cap R_2 = R$. In anderer Notation gilt also $x\,R\,z$, d.h. R ist transitiv. □

Wenn wir mittels einer Äquivalenzrelation Objekte einteilen (z.B. die Menschen nach Geburtsjahr), so partitionieren wir die Gesamtmenge (alle Menschen) in gewisse disjunkte Teilmengen (alle Menschen eines Geburtsjahres). Dieses Vorgehen wird im Folgenden formalisiert.

Definition 6.8. *Sei A eine Menge und $\sim$ eine Äquivalenzrelation auf A. Für alle $x \in A$ definieren wir die* ***Äquivalenzklasse von x bezüglich $\sim$*** *als*

$$[x]_\sim \coloneqq \{y \in A \mid x \sim y\} \subseteq A.$$

Die Menge dieser Äquivalenzklassen

$$A/\!\sim \coloneqq \{[x]_\sim \mid x \in A\} \subseteq \mathcal{P}(A)$$

bezeichnet man als ***Faktormenge von A nach $\sim$****.*

Lemma 6.9. *Sei $A \neq \emptyset$ eine Menge und $\sim$ eine Äquivalenzrelation auf A. Seien $x, y \in A$. Dann gelten die folgenden Aussagen:*

(i) $x \in [x]_\sim \neq \emptyset$.
(ii) $x \sim y \iff [x]_\sim = [y]_\sim$
(iii) $x \not\sim y \iff [x]_\sim \cap [y]_\sim = \emptyset$.

Beweis. Wir unterteilen den Beweis in sechs Schritte.

Schritt 1 ($x \in [x]_\sim$). Sei $x \in A$. Aufgrund der Reflexivität $x \sim x$ gilt $x \in [x]_\sim$ und insbesondere $[x]_\sim \neq \emptyset$. Das zeigt (i).

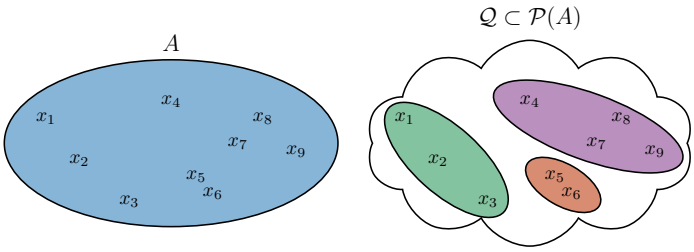


ABBILDUNG 5. Visualisierung einer Partition $\mathcal{Q} = \{Q_1, Q_2, Q_3\}$ von einer Menge $A = \{x_1, x_2, x_3, \ldots, x_9\}$ gemäß Definition 6.10.

Schritt 2 ($x \sim y \Rightarrow [x]_\sim \subseteq [y]_\sim$). Seien $x, y \in A$ mit $x \sim y$. Aufgrund der Symmetrie folgt dann auch $y \sim x$. Sei $z \in [x]_\sim$, d.h. es gilt $x \sim z$. Aufgrund der Transitivität folgt aus $y \sim x$ und $x \sim z$ auch $y \sim z$ und damit $z \in [y]_\sim$. Da $z \in [x]_\sim$ beliebig war, folgt die Inklusion $[x]_\sim \subseteq [y]_\sim$.

Schritt 3 ($x \sim y \Rightarrow [x]_\sim \supseteq [y]_\sim$). Seien $x, y \in A$ mit $x \sim y$. Aufgrund der Symmetrie folgt dann auch $y \sim x$ und Schritt 2 zeigt $[y]_\sim \subseteq [x]_\sim$.

Schritt 4 ($[x]_\sim \cap [y]_\sim \neq \emptyset \Rightarrow x \sim y$). Seien $x, y \in A$ mit $[x]_\sim \cap [y]_\sim \neq \emptyset$. Dann existiert $z \in [x]_\sim \cap [y]_\sim$, d.h. es gilt $z \in A$ mit $x \sim z$ und $y \sim z$. Aufgrund der Symmetrie gilt auch $x \sim z$ und $z \sim y$. Mit der Transitivität folgt $x \sim y$ und damit auch $[x]_\sim = [y]_\sim$ nach Schritt 2–3.

Schritt 5 ($x \sim y \Leftrightarrow [x]_\sim = [y]_\sim$). Die Kombination von Schritt 2–3 zeigt die Implikation $\Rightarrow$. Für die Implikation $\Leftarrow$ beachte, dass $[x]_\sim = [y]_\sim \neq \emptyset$ nach Schritt 1 und Schritt 4 bereits $x \sim y$ implizieren. Die zeigt (ii).

Schritt 6 ($x \not\sim y \Leftrightarrow [x]_\sim \neq [y]_\sim$). Die Äquivalenz folgt direkt durch Negation beider Seiten aus der Äquivalenz in Schritt 5.

Schritt 7 ($x \not\sim y \Leftrightarrow [x]_\sim \cap [y]_\sim = \emptyset$). Die Implikation $\Rightarrow$ ist die Kontraposition von Schritt 4 ist. Um die andere Implikation $\Leftarrow$ zu sehen, seien $x, y \in A$ mit $[x]_\sim \cap [y]_\sim = \emptyset$. Aus Schritt 1 folgt $x \in [x]_\sim \neq \emptyset$ und deshalb $[x]_\sim \neq [y]_\sim$. Aus Schritt 6 folgt $x \not\sim y$. Dies zeigt (iii). □

Definition 6.10. *Sei A eine Menge. Eine Teilmenge $\mathcal{Q} \subseteq \mathcal{P}(A)$ heißt **Partition (von A)**, wenn die folgenden drei Eigenschaften gelten:*

(a) *alle Teilmengen $Q \in \mathcal{Q}$ sind nichtleer, d.h. es gilt*

$$\forall Q \in \mathcal{Q} : Q \neq \emptyset;$$

(b) *die Teilmengen $Q \in \mathcal{Q}$ sind paarweise disjunkt, d.h. es gilt*

$$\forall Q_1, Q_2 \in \mathcal{Q} : [Q_1 \neq Q_2 \Rightarrow Q_1 \cap Q_2 = \emptyset];$$

(c) *jedes Element von A ist in einer Menge aus $\mathcal{Q}$ enthalten, d.h. $A = \bigcup_{Q \in \mathcal{Q}} Q$ bzw.*

$$\forall x \in A \, \exists Q \in \mathcal{Q} : x \in Q.$$

Der folgende Satz zeigt, dass jede Äquivalenzrelation eine Partition induziert und dass jede Partition eine Äquivalenzrelation definiert. Beide Konzepte sind also gewissermaßen äquivalent.

Satz 6.11. *Für jede Menge $A \neq \emptyset$ gelten die folgenden beiden Aussagen:*

(i) *Ist $\sim$ eine Äquivalenzrelation auf A, so ist die Faktormenge $\mathcal{Q} := A/\sim$ eine Partition von A.*

(ii) *Ist $\mathcal{Q}$ eine Partition von A, so definiert $R := \{(x,y) \mid \exists Q \in \mathcal{Q} : x,y \in Q\}$ eine Äquivalenzrelation auf A.*

Beweis. **Schritt 1 ($\mathcal{Q}$ von (i) erfüllt Definition 6.10).** Nach Lemma 6.9 gilt $x \in [x]_\sim$ für jedes $x \in A$ und damit $[x]_\sim \neq \emptyset$ für alle $x \in A$. Dies zeigt Definition 6.10(a) und (c). Zu $Q_1, Q_2 \in \mathcal{Q}$ existieren $x, y \in A$ mit $Q_1 = [x]_\sim$ und $Q_2 = [y]_\sim$. Im Fall $Q_1 \neq Q_2$ muss nach Lemma 6.9 dann $x \not\sim y$ und damit sogar $Q_1 \cap Q_2 = \emptyset$ gelten. Dies zeigt Definition 6.10(b).

Schritt 2 (R von (ii) erfüllt Definition 6.8(a)). Sei $x \in A$. Da $\mathcal{Q}$ eine Partition von A ist, existiert ein $Q \in \mathcal{Q}$ mit $x \in Q$. Es folgt $(x,x) \in R$ nach Definition von R. In üblicher Notation folgt $x\,R\,x$, d.h. R ist reflexiv.

Schritt 3 (R von (ii) erfüllt Definition 6.8(b)). Seien $x, y \in A$ mit $x\,R\,y$, d.h. $(x,y) \in R$. Nach Definition von R existiert ein $Q \in \mathcal{Q}$ mit $x, y \in Q$. Also gilt auch $(y,x) \in R$. In üblicher Notation folgt $y\,R\,x$, d.h. R ist symmetrisch.

Schritt 4 (R von (ii) erfüllt Definition 6.8(c)). Seien $x, y, z \in A$ mit $x\,R\,y$ und $y\,R\,z$, d.h. $(x,y), (y,z) \in R$. Nach Definition existieren $Q_1, Q_2 \in \mathcal{Q}$ mit $x, y \in Q_1$ und $y, z \in Q_2$. Insbesondere gilt $y \in Q_1 \cap Q_2 \neq \emptyset$. Da $\mathcal{Q}$ eine Partition von A ist, folgt $Q_1 = Q_2$ und damit $x, z \in Q_1$. Also gilt auch $(x,z) \in R$. In üblicher Notation folgt $x\,R\,z$, d.h. R ist transitiv. □

7. Funktionen

Aus der Schule kennen Sie bereits einen naiven Funktionsbegriff für $f\colon X \to Y$. Dieser wird durch die folgende Definition formalisiert.

Definition 7.1. *Seien X und Y Mengen. Eine Relation $f \subseteq X \times Y$ heißt **Funktion**, wenn Sie die folgenden beiden Eigenschaften besitzt:*

(a) $\forall x \in X\, \exists y \in Y : (x,y) \in f$, *($f$ ist überall definiert)*

(b) $\forall x \in X\, \forall y_1, y_2 \in Y : \big[(x,y_1), (x,y_2) \in f \Rightarrow y_1 = y_2\big]$. *($f$ ist wohldefiniert)*

*Die Menge X heißt **Definitionsmenge** von f, die Menge Y heißt **Zielmenge** oder **Wertevorrat** von f. Ist f eine Funktion, so schreiben wir auch $\boldsymbol{f\colon X \to Y}$ als Abbildungsvorschrift. Ferner schreiben wir $\boldsymbol{y = f(x)}$ anstelle von $(x,y) \in f$. Manchmal*

bezeichnet man in diesem Kontext die Menge $f = \{(x,y) \mid x \in X \wedge y = f(x)\} \subseteq X \times Y$ *auch als* ***Graph von*** f.

Kommentar. *Manchmal werden die Eigenschaften in Definition 7.1*(a)–(b) *als Wohldefiniertheit bezeichnet und in der Form*

$$\forall x \in X\, \exists!\, y \in Y : (x,y) \in f$$

abgekürzt (mit dem Quantor $\exists!$ *für die eindeutige Existenz): Jedem* x *ist ein eindeutiger Funktionswert* $f(x)$ *zugeordnet. Explizite Quintessenz: Um eine eindeutige Existenz zu zeigen, muss man stets* (a) *die Existenz zeigen und* (b) *die Eindeutigkeit.*

Definition 7.2. *Seien* X *und* Y *Mengen und* $f, g\colon X \to Y$ *Funktionen. Wir schreiben* $f = g$*, wenn* $f(x) = g(x)$ *für alle* $x \in X$ *gilt.*

Definition 7.3. *Seien* X*,* Y*,* Z *Mengen und* $f\colon X \to Y$ *und* $g\colon Y \to Z$ *Funktionen. Dann definiert* $(g \circ f)(x) := g\big(f(x)\big)$ *eine Funktion* $g \circ f\colon X \to Z$*. Man bezeichnet* ***$g \circ f$*** *als* ***Hintereinanderausführung*** *oder* ***Komposition von f und g****.*

Lemma 7.4 (Assoziativität der Komposition). *Für Mengen* W*,* X*,* Y*,* Z *und Funktionen* $f\colon W \to X$*,* $g\colon X \to Y$ *und* $h\colon Y \to Z$ *gilt* $h \circ g \circ f := (h \circ g) \circ f = h \circ (g \circ f)$*, sodass man die Klammern weglassen darf.*

Beweis. Für $x \in W$ gilt

$$((h \circ g) \circ f)(x) = (h \circ g)(f(x)) = h(g(f(x)) = h((g \circ f)(x)) = (h \circ (g \circ f))(x).$$

Also gilt Gleichheit $(h \circ g) \circ f = h \circ (g \circ f)$ der Funktionen. □

Definition 7.5. *Seien* X*,* Y *Mengen mit Teilmengen* $A \subseteq X$ *und* $B \subseteq Y$*. Für eine Funktion* $f\colon X \to Y$ *definieren wir das*

(a) ***Bild von A unter f*** *als* $f(A) := \{f(x) \mid x \in A\} := \{y \in Y \mid \exists x \in A : y = f(x)\}$,

(b) ***Urbild von B unter f*** *als* $f^{-1}(B) := \{x \in X \mid f(x) \in B\}$.

Die Menge $f(X)$ *bezeichnet man als* ***Bild*** *oder* ***Wertebereich von f****.*

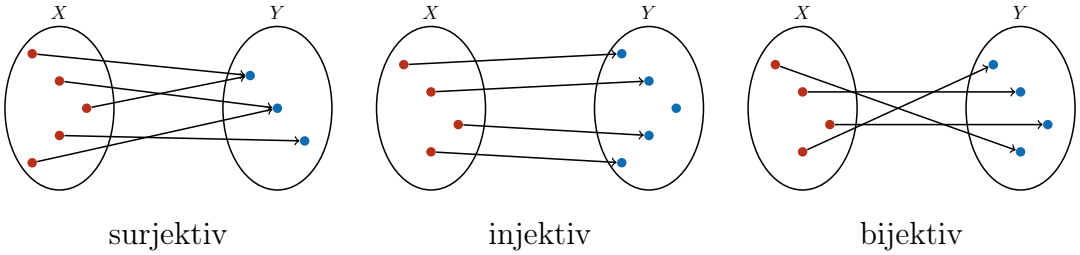
Beispiel 7.6. *Wir betrachten die Funktion* $f\colon \mathbb{Z} \to \mathbb{Z}$*,* $f(x) := x^2$*. Für* $A := \{1, -2, 2, 3\}$ *gilt dann* $B := f(A) = \{1, 4, 9\}$ *und* $f^{-1}(B) = \{-1, 1, -2, 2, -3, 3\}$*.*

Die folgende Definition wird in Abbildung 6 visualisiert. Von besonderer Bedeutung sind bijektive Funktionen $f\colon X \to Y$, da für diese eine Inverse existiert, wie wir später in Satz 7.11 sehen werden.

Definition 7.7. *Seien* X *und* Y *Mengen. Eine Funktion* $f\colon X \to Y$ *heißt*

(a) ***Surjektion*** *oder* ***surjektiv****, wenn* $f(X) = Y$ *gilt, d.h.*

$$\forall y \in Y\, \exists x \in X : y = f(x);$$



surjektiv injektiv bijektiv

ABBILDUNG 6. Visualisierungen von surjektiven, injektiven und bijektiven Funktionen $f\colon X \to Y$.

(b) ***Injektion*** *oder* ***injektiv****, wenn gilt*

$$\forall x_1, x_2 \in X : \big[f(x_1) = f(x_2) \Rightarrow x_1 = x_2\big]$$

oder (äquivalent dazu)

$$\forall x_1, x_2 \in X : \big[x_1 \neq x_2 \Rightarrow f(x_1) \neq f(x_2)\big].$$

(c) ***Bijektion*** *oder* ***bijektiv****, wenn sie injektiv und surjektiv ist, d.h.*

$$\forall y \in Y \, \exists! \, x \in X : \, y = f(x).$$

Beispiel 7.8. (i) *Es sei M die Menge aller Personen in Österreich. Jede Person in Österreich hat eine eindeutige Sozialversicherungsnummer, d.h. die zugehörige Funktion $s\colon M \to \mathbb{N}$ ist injektiv, aber nicht surjektiv.*

(ii) *Es sei M die Menge aller Personen in Österreich. Die Funktion $g\colon M \to \mathbb{N}$, die jeder Person deren (gerundete) Größe in Zentimeter zuordnet, ist weder injektiv noch surjektiv.*

(iii) *Die Funktion $q\colon \mathbb{N} \to \mathbb{N}$, die jeder Zahl ihre Quersumme zuweist (d.h. $q(a) = a_1 + a_2 + a_3 + \cdots + a_n$, wenn $a \in \mathbb{N}$ mittels Ziffern $a_j \in \{0, \ldots, 9\}$ als $a = a_1 a_2 a_3 \ldots a_n$ dargestellt ist) ist surjektiv, aber nicht injektiv.*

Bemerkung 7.9. *Es seien X und Y Mengen und $f\colon X \to Y$.*

(i) *Man kann f auch als Funktion $f\colon X \to f(X)$ auffassen. Durch diese Modifikation erhält man eine surjektive Funktion.*

(ii) *Ist $f\colon X \to Y$ injektiv, dann ist $f\colon X \to f(X)$ bijektiv.*

Eine wichtige bijektive Funktion ist die Identität.

Definition 7.10. *Für jede Menge X bezeichnet* $\mathbf{Id_X}\colon X \to X$, $\mathrm{Id}_X(x) := x$ *die* ***Identität auf X****.*

Satz 7.11 (Existenz und Eindeutigkeit der Inversen). *Seien X, Y Mengen und $f\colon X \to Y$ eine Funktion. Dann sind die folgenden beiden Aussagen äquivalent:*

(i) *f ist bijektiv*
(ii) *Es gibt eine Funktion $g\colon Y \to X$ mit $f \circ g = \mathrm{Id}_Y$ und $g \circ f = \mathrm{Id}_X$.*

*In diesem Fall ist $\boldsymbol{f^{-1}} \coloneqq g$ eindeutig und wird als **Inverse von f** bezeichnet.*

Beweis. Wir teilen den Beweis in sieben Schritte.

Schritt 1 (Definition von f^{-1}). Laut Definition gilt $f = \big\{(x,y) \,\big|\, x \in X \wedge y = f(x)\big\}$. Wir definieren die Relation

$$f^{-1} \coloneqq \big\{(y,x) \,\big|\, (x,y) \in f\big\}.$$

Es ist zu diesem Zeitpunkt noch nicht klar, dass f^{-1} eine Funktion ist.

Schritt 2 (f surjektiv $\Rightarrow$ f^{-1} überall definiert). Sei f surjektiv. Wir müssen zeigen, dass gilt

$$\forall y \in Y \exists x \in X : (y,x) \in f^{-1}.$$

Sei $y \in Y$. Da f surjektiv, existiert ein $x \in X$ mit $f(x) = y$, d.h. $(x,y) \in f$. Insbesondere folgt $(y,x) \in f^{-1}$.

Schritt 3 (f injektiv $\Rightarrow$ f^{-1} wohldefiniert). Sei f injektiv. Wir müssen zeigen, dass gilt

$$\forall y \in Y \forall x_1, x_2 \in X : \big[(y,x_1), (y,x_2) \in f^{-1} \Rightarrow x_1 = x_2\big].$$

Seien $y \in Y$ und $x_1, x_2 \in X$ mit $(y,x_1), (y,x_2) \in f^{-1}$. Dann folgt $(x_1,y), (x_2,y) \in f$, d.h. $f(x_1) = y = f(x_2)$. Da f injektiv ist, folgt $x_1 = x_2$.

Schritt 4 (f bijektiv $\Rightarrow$ $f^{-1} \circ f = \mathrm{Id}_X$, $f \circ f^{-1} = \mathrm{Id}_Y$). Sei f bijektiv. Nach Schritt 1–3 ist $f^{-1}\colon Y \to X$ eine Funktion. Für die erste Identität müssen wir zeigen, dass gilt

$$\forall x \in X : f^{-1}(f(x)) = x.$$

Sei $x \in X$ und $y \coloneqq f(x)$, d.h. $(x,y) \in f$. Dann folgt $(y,x) \in f^{-1}$, d.h. $f^{-1}(y) = x$. Insbesondere folgt $f^{-1}(f(x)) = f^{-1}(y) = x$. Die andere Gleichheit folgt analog. Mit Schritt 1–4 ist die Implikation (i) $\Rightarrow$ (ii) gezeigt.

Schritt 5 ($f \circ g = \mathrm{Id}_Y \Rightarrow$ f surjektiv). Es gelte $f \circ g = \mathrm{Id}_Y$, d.h. $f(g(y)) = y$ für alle $y \in Y$. Wir müssen zeigen, dass gilt

$$\forall y \in Y \exists x \in X : f(x) = y.$$

Sei $y \in Y$. Dann gilt $y = f(g(y))$. Definieren wir $x \coloneqq g(y)$, so folgt $f(x) = y$.

Schritt 6 ($g \circ f = \mathrm{Id}_X \Rightarrow f$ injektiv). Es gelte $g \circ f = \mathrm{Id}_X$, d.h. $g(f(x)) = x$ für alle $x \in X$. Wir müssen zeigen, dass gilt

$$\forall x_1, x_2 \in X : \big[f(x_1) = f(x_2) \Rightarrow x_1 = x_2\big].$$

Seien $x_1, x_2 \in X$ mit $f(x_1) = f(x_2)$. Dann folgt $x_1 = g(f(x_1)) = g(f(x_2)) = x_2$. Mit Schritt 5–6 ist die Implikation (ii) $\Rightarrow$ (i) gezeigt.

Schritt 7 (f^{-1} eindeutig). Sei $g\colon Y \to X$ eine Funktion mit $f \circ g = \mathrm{Id}_Y$ und $g \circ f = \mathrm{Id}_X$. Nach Schritt 5–6 ist f bijektiv. Nach Schritt 1–3 existiert also die Inverse $f^{-1}\colon Y \to X$. Mit Schritt 4 folgt dann

$$g = \mathrm{Id}_X \circ g = (f^{-1} \circ f) \circ g = f^{-1} \circ (f \circ g) = f^{-1} \circ \mathrm{Id}_Y = f^{-1}.$$

Dies beschließt den Beweis. □

Bemerkung 7.12. *Beachten Sie, dass für $f\colon X \to Y$ die Notation f^{-1} doppelt verwendet wird: Für das Urbild aus Definition 7.5 und, sofern f bijektiv ist, für die Inverse aus Satz 7.11. Tatsächlich besteht keine Verwechslungsgefahr: Das Urbild $f^{-1}(B)$ ist für Mengen $B \in Y$ definiert. Die Inverse $f^{-1}(y)$ agiert auf Elementen $y \in Y$ und ist nur definiert, wenn f bijektiv ist. In diesem Fall gilt $f^{-1}(\{y\}) = \{x\}$ für $x = f^{-1}(y)$.*

Korollar 7.13. *Seien X, Y, Z Mengen und $f\colon X \to Y$ und $g\colon Y \to Z$ bijektive Funktionen. Dann gelten die folgenden Aussagen:*

(i) *f^{-1} bijektiv mit $(f^{-1})^{-1} = f$.*
(ii) *$g \circ f$ ist bijektiv mit $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.*

Beweis. (i) Wir wenden Satz 7.11(ii) auf $F := f^{-1}$ und $G := f$ an. Es gilt $F \circ G = \mathrm{Id}_X$ und $G \circ F = \mathrm{Id}_Y$. Also ist F bijektiv mit $(f^{-1})^{-1} = F^{-1} = G = f$

(ii) Wir wenden Satz 7.11(ii) auf $F := g \circ f$ und $G := f^{-1} \circ g^{-1}$ an. Die Assoziativität der Komposition zeigt

$$F \circ G = (g \circ f) \circ (f^{-1} \circ g^{-1}) = g \circ \mathrm{Id}_Y \circ g^{-1} = g \circ g^{-1} = \mathrm{Id}_Z$$

und analog $G \circ F = \mathrm{Id}_X$. Also ist F bijektiv mit $(g \circ f)^{-1} = F^{-1} = G = f^{-1} \circ g^{-1}$. □

Definition 7.14. *Seien X und Y Mengen und $M \subseteq X$. Ist $f\colon X \to Y$ eine Funktion, so bezeichnet man die Funktion $f|_M := \{(x, y) \in f \mid x \in M\}$ als **Restriktion** oder **Einschränkung von f auf M**, d.h. $f|_M\colon M \to Y$ und $f|_M(x) = f(x)$ für alle $x \in M$. Ist $f\colon M \to Y$ eine Funktion, so bezeichnet man eine Funktion $F\colon X \to Y$ mit $F|_M = f$ als **Fortsetzung von f auf X**.*

Der folgende Satz ist auch als Schubfachprinzip bekannt: *Wir haben m Paar Socken und n Schubladen. Wenn $m > n$ ist, dann muss in mindestens einer Schublade mehr als*

ein paar Socken liegen (d.h. die Zuordnung ist nicht injektiv). Wenn $m < n$ ist, dann bleibt mindestens eine Schublade leer (d.h. die Zuordnung ist nicht surjektiv).

Satz 7.15 (Schubfachprinzip). *Seien $m, n \in \mathbb{N}$ und $f\colon \{1, \dots, m\} \to \{1, \dots, n\}$. Dann gelten die folgenden Aussagen:*

(i) *Ist f injektiv, so folgt $m \leq n$.*
(ii) *Ist f surjektiv, so folgt $m \geq n$.*
(iii) *Ist f bijektiv, so folgt $m = n$.*

Insbesondere kann f nicht bijektiv sein für $m \neq n$.

***Beweis von Satz 7.15*(i).** Der Beweis erfolgt in drei Schritten. Zur Abkürzung der Notation definieren wir $M_n \coloneqq \{1, \dots, n\}$ für alle $n \in \mathbb{N}$.

Schritt 1 ($f\colon M_{n+1} \to M_n$ ist nicht injektiv). Wir beweisen mittels vollständiger Induktion nach n, dass jede Funktion $f : M_{n+1} \to M_n$ nicht injektiv ist (d.h. kein solches f ist injektiv).

Induktionsbehauptung $A(n)$: $\forall f\colon M_{n+1} \to M_n : f$ nicht injektiv.

Induktionsanfang $n = 1$. Für jedes $f\colon \{1, 2\} \to \{1\}$ gilt $f(1) = 1 = f(2)$, d.h. f ist nicht injektiv.

Induktionsvoraussetzung. Sei $n \in \mathbb{N}$. Es gelte $A(n)$, d.h.

$$\forall g\colon M_{n+1} \to M_n : g \text{ nicht injektiv.}$$

Induktionsschritt. Wir müssen zeigen, dass $A(n+1)$ gilt. Wir machen einen indirekten Beweis und nehmen an, dass $A(n+1)$ falsch ist. Dann existiert eine injektive Funktion $f\colon M_{n+2} \to M_{n+1}$. Auf M_{n+1} betrachten wir für $a, b \in M_{n+1}$ die Funktion

$$\sigma_{a,b}\colon M_{n+1} \to M_{n+1}, \quad \sigma_{a,b}(x) \coloneqq \begin{cases} x & \text{für } x \notin \{a, b\}, \\ a & \text{für } x = b, \\ b & \text{für } x = a. \end{cases}$$

Dann ist $\sigma_{a,b}$ wohldefiniert und bijektiv, denn es gilt $\sigma_{a,b} \circ \sigma_{a,b} = \mathrm{Id}_{M_{n+1}}$. Also ist

$$g \coloneqq \sigma_{n+1,f(n+2)} \circ f\colon M_{n+2} \to M_{n+1}$$

injektiv als Komposition einer Bijektion und einer Injektion. Es gilt

$$g(n+2) = \sigma_{n+1,f(n+2)}(f(n+2)) = n+1.$$

Da g injektiv ist, folgt für alle $x \in M_{n+2} \backslash \{n+2\} = M_{n+1}$, dass $g(x) \in M_{n+1} \backslash \{n+1\} = M_n$. Also ist $g(M_{n+1}) \subseteq M_n$, d.h. $g|_{M_{n+1}}\colon M_{n+1} \to M_n$ ist injektiv. Dies steht aber im Widerspruch zur Induktionsvoraussetzung. Also ist die Annahme falsch und Schritt 1 damit bewiesen.

Schritt 2 ($m > n \implies f\colon M_m \to M_n$ nicht injektiv). Seien $m > n$ und $f\colon M_m \to M_n$. Nach Schritt 1 ist die Restriktion $f|_{M_{n+1}}\colon M_{n+1} \to M_n$ nicht injektiv. Also ist auch $f\colon M_m \to M_n$ nicht injektiv.

Schritt 3. Die Kontraposition von Schritt 2 zeigt, dass Injektivität von $f\colon M_m \to M_n$ impliziert, dass $m \leq n$. □

***Beweis von Satz 7.15*(ii).** Der Beweis erfolgt wieder in drei Schritten und mit derselben Notation und demselben Vorgehen wie zuvor.

Schritt 1 ($f\colon M_n \to M_{n+1}$ ist nicht surjektiv). Wir beweisen mittels Induktion nach n, dass jede Funktion $f : M_n \to M_{n+1}$ nicht surjektiv ist, d.h.

Induktionsbehauptung $A(n)$: $\forall f\colon M_{n+1} \to M_n : f$ nicht surjektiv.

Induktionsanfang $n = 1$. Für jedes $f\colon \{1\} \to \{1, 2\}$ gilt offensichtlich, dass f nicht surjektiv ist, denn entweder gilt $f(1) = 1$ oder $f(1) = 2$.

Induktionsvoraussetzung. Sei $n \in \mathbb{N}$. Es gelte $A(n)$, d.h.

$$\forall g\colon M_{n+1} \to M_n : g \text{ nicht surjektiv.}$$

Induktionsschritt. Wir müssen zeigen, dass $A(n+1)$ gilt. Wir machen einen indirekten Beweis und nehmen an, dass $A(n+1)$ falsch ist. Dann existiert eine surjektive Funktion $f\colon M_{n+1} \to M_{n+2}$. Dann existiert ein $k \in M_{n+1}$ mit $f(k) = n + 2$. Da $\sigma_{k,n+1}\colon M_{n+1} \to M_{n+1}$ bijektiv ist, ist

$$g \coloneqq f \circ \sigma_{k,n+1}\colon M_{n+1} \to M_{n+2}$$

surjektiv und es gilt $g(n+1) = f(\sigma_{k,n+1}(n+1)) = f(k) = n + 2$. Insbesondere folgt $g(M_n) \supseteq M_{n+1}$. Wir definieren die modifizierte Funktion

$$\widetilde{g}\colon M_n \to M_{n+1}, \quad \widetilde{g}(x) \coloneqq \begin{cases} g(x), & \text{falls } g(x) \in M_{n+1}, \\ n+1, & \text{sonst.} \end{cases}$$

Da wir die Funktion g nur dort modifizieren, wo $g(x) \notin M_{n+1}$ gilt, folgt aus $g(M_n) \supseteq M_{n+1}$, dass $\widetilde{g}(M_n) = M_{n+1}$. Also ist $\widetilde{g}\colon M_n \to M_{n+1}$ surjektiv. Dies steht aber im Widerspruch zur Induktionsvoraussetzung. Also ist die Annahme falsch und Schritt 1 damit bewiesen.

Schritt 2 ($m < n \implies f\colon M_m \to M_n$ nicht surjektiv). Seien $1 \leq m < n$ und $f\colon M_m \to M_n$. Dann gilt $M_m \subseteq M_{n-1}$. Wir definieren eine Fortsetzung

$$F\colon M_{n-1} \to M_n, \quad F(x) \coloneqq \begin{cases} f(x) & \text{für } x \in M_m, \\ f(1) & \text{für } x \in M_{n-1} \backslash M_m. \end{cases}$$

Nach Schritt 1 ist die Fortsetzung F nicht surjektiv. Also ist auch f nicht surjektiv.

Schritt 3. Die Kontraposition von Schritt 2 zeigt, dass Surjektivität von $f\colon M_m \to M_n$ impliziert, dass $m \geq n$. □

***Beweis von Satz 7.15*(iii)**. Der Beweis folgt unmittelbar aus (i) und (ii). □

Nach Definition 5.12 ist eine Menge $X \neq \emptyset$ endlich, wenn wir die Elemente $X = \{x_1, \dots, x_n\}$ nummerieren können. Formal entspricht eine solche Nummerierung einer Bijektion $\phi\colon \{1, \dots, n\} \to X$. Das folgende Korollar zeigt, dass die Kardinalität $n = \#X$ tatsächlich eindeutig definiert ist.

Korollar 7.16. *Ist X eine Menge und $\phi\colon \{1, \dots, n\} \to X$ eine Bijektion, so ist die Menge endlich und die Kardinalität $n = \#X$ eindeutig festgelegt, d.h. es kann keine Bijektion $\psi\colon \{1, \dots, m\} \to X$ mit $m \neq n$ geben.*

Beweis. Sind $\phi\colon \{1, \dots, n\} \to X$ und $\psi\colon \{1, \dots, m\} \to X$ Bijektionen, so ist die Komposition $\phi^{-1} \circ \psi\colon \{1, \dots, m\} \to \{1, \dots, n\}$ eine Bijektion. Satz 7.15 garantiert $m = n$. □

Endlichkeit ist eine starke Eigenschaft von Mengen, wie Ihnen der folgende Satz illustrieren soll.

Satz 7.17. *Seien X und Y endliche Mengen mit $\#X = \#Y$. Dann sind für $f\colon X \to Y$ die folgenden Aussagen paarweise äquivalent:*

(i) *f ist injektiv.*
(ii) *f ist surjektiv.*
(iii) *f ist bijektiv.*

Beweis. Aufgrund der Definition der Begriffe ist nur die Äquivalenz [(i) $\Leftrightarrow$ (ii)] zu zeigen. Sei $n := \#X = \#Y \in \mathbb{N}_0$. Für $k \in \mathbb{N}$ betrachten wir wieder $M_k := \{1, \dots, k\}$ und gliedern den Beweis in drei Schritte.

Schritt 1 (o.B.d.A. $X = Y = M_n$ und $n \geq 2$). Für $n = 0$ gilt $X = Y = \emptyset$ und damit ist nichts zu zeigen (denn alle Aussagen starten mit einem Allquantor). Für $n = 1$ gilt $X = \{x\}$, $Y = \{y\}$ und $f(x) = y$. Also ist f jedenfalls bijektiv. Ohne Beschränkung der Allgemeinheit gilt also im Folgenden $n \in \mathbb{N}$ mit $n \geq 2$. Nach Voraussetzung existieren Bijektionen $\phi\colon M_n \to X$ und $\psi\colon M_n \to Y$. Betrachtet man eine Funktion $F\colon X \to Y$, so kann man auch die Komposition

$$f := \psi^{-1} \circ F \circ \phi\colon M_n \to M_n$$

betrachten. Da ψ^{-1} und ϕ bijektiv sind, gelten die folgenden Äquivalenzen:

$$f \text{ injektiv} \iff F \text{ injektiv};$$
$$f \text{ surjektiv} \iff F \text{ surjektiv};$$
$$f \text{ bijektiv} \iff F \text{ bijektiv}.$$

Also reicht es, die behaupteten Äquivalenzen im Spezialfall $X = Y = M_n$ zu zeigen.

Schritt 2 ($f\colon M_n \to M_n$ injektiv $\Rightarrow$ f surjektiv). Wir zeigen die Kontraposition

$$f\colon M_n \to M_n \text{ nicht surjektiv} \quad \Rightarrow \quad f \text{ nicht injektiv}$$

und setzen deshalb voraus, dass $f\colon M_n \to M_n$ nicht surjektiv ist. Es existiert also ein $k \in M_n$ mit $k \in M_n \backslash f(M_n)$. Wir betrachten die Vertauschung $\sigma_{k,n}\colon M_n \to M_n$ aus dem Beweis von Satz 7.15. Wir definieren

$$g \coloneqq \sigma_{k,n} \circ f\colon M_n \to M_n.$$

Da $f(x) \neq k$ für alle $x \in M_n$, gilt $g(x) \neq n$ für alle $x \in M_n$. Also folgt $g(M_n) \subseteq M_n \backslash \{n\} = M_{n-1}$. Nach Satz 7.15 ist die Funktion

$$\widetilde{g}\colon M_n \to M_{n-1}, \quad \widetilde{g}(x) \coloneqq g(x)$$

nicht injektiv. Also ist auch $g = \sigma_{k,n} \circ f$ nicht injektiv. Da $\sigma_{k,n}$ bijektiv ist, ist also f nicht injektiv.

Schritt 3 ($f\colon M_n \to M_n$ surjektiv $\Rightarrow$ f injektiv). Wir zeigen die Kontraposition

$$f\colon M_n \to M_n \text{ nicht injektiv} \quad \Rightarrow \quad f \text{ nicht surjektiv}$$

und setzen deshalb voraus, dass $f\colon M_n \to M_n$ nicht injektiv ist. Es existieren also $j, k \in M_n$ mit $f(j) = f(k)$. Ohne Beschränkung der Allgemeinheit gilt $j < k$. Mit der Vertauschung $\sigma_{k,n}\colon M_n \to M_n$ aus dem Beweis von Satz 7.15 definieren wir

$$g \coloneqq f \circ \sigma_{k,n}\colon M_n \to M_n.$$

Dann gilt $g(j) = f(j) = f(k) = g(n)$. Mit der Restriktion

$$g|_{M_{n-1}}\colon M_{n-1} \to M_n$$

folgt dann insgesamt $f(M_n) = g(M_n) = g|_{M_{n-1}}(M_{n-1})$. Aufgrund von Satz 7.15 ist $g|_{M_{n-1}}$ nicht surjektiv und deshalb $g|_{M_{n-1}}(M_{n-1}) \subsetneq M_n$. Insbesondere ist auch f nicht surjektiv. □

Kommentar. *Die Phrase „**Ohne Beschränkung der Allgemeinheit**“, liebevoll abgekürzt als **o.B.d.A.**, findet sich oft in mathematischen Texten und Präsentationen. Meist wird nicht weiter erklärt, warum man das darauf Folgende dann zusätzlich voraussetzen darf. Formal ist meist eine Fallunterscheidung nötig (z.B. $n \in \{0, 1\}$ oder $n \geq 2$ wie in Schritt 1 im Beweis von Satz 7.17) oder es braucht ein Argument, warum es reicht, den Spezialfall statt des allgemeinen Falls zu betrachten (siehe ebenfalls Schritt 1 im Beweis von Satz 7.17). Die Vortragenden bzw. Autor*innen gehen dann meist davon aus, dass den Leser*innen und Hörer*innen das „Standardargument eh klar“ ist. Wenn Sie also in Ihren Vorlesungen oder Skripten ein* o.B.d.A. *sehen, dann sollten Sie (später und in aller Ruhe) explizit darüber nachdenken!*

Häufig kommen Funktionen in Zusammenhang mit zusätzlicher mathematischer Struktur vor. Beispielhaft betrachten wir hier den Begriff der *Gruppe*.

Definition 7.18. *Ein Tripel $(G, *, e)$ heißt **Gruppe**, wenn die folgenden Eigenschaften erfüllt sind:*

(a) $G \neq \emptyset$ *ist eine Menge mit* $e \in G$*;*

(b) $*\colon G \times G \to G$ *ist eine Funktion mit den folgenden Eingeschaften:*

(b_1) $\forall a, b, c \in G : (a * b) * c = a * (b * c)$ *(**Assoziativität**)*

(b_2) $\forall a \in G : a * e = a = e * a$ *(**neutrales Element**)*

(b_3) $\forall a \in G \, \exists a^{-1} \in G : a * a^{-1} = e = a^{-1} * a$ *(**inverse Elemente**)*

Lemma 7.19. *Es sei $(G, *, e)$ eine Gruppe. Dann gelten die folgenden Aussagen:*

(i) *Das neutrale Element e ist eindeutig, d.h. nur e erfüllt Definition 7.18(b_2).*

(ii) *Für jedes $a \in G$ ist das inverse Element a^{-1} in Definition 7.18(b_3) eindeutig.*

Insbesondere gilt $e^{-1} = e$.

Beweis. Sei $E \in G$ ein Element, das Definition 7.18(b_2) erfüllt. Dann folgt

$$E = E * e = e,$$

d.h. das neutrale Element ist eindeutig. Seien $a, b \in G$ mit $a * b = e = b * a$. Dann folgt

$$a^{-1} = a^{-1} * e = a^{-1} * (a * b) = (a^{-1} * a) * b = e * b = b,$$

d.h. das inverse Element zu a ist eindeutig. □

Beispiel 7.20. *Gruppen zählen zu den wichtigsten mathematischen Strukturen der Algebra. Sie kennen auch schon zahlreiche Beispiele:*

(i) $\mathbb{Z}$ *mit der Addition (und $a^{-1} := -a$) bildet die Gruppe $(\mathbb{Z}, +, 0)$.*

(ii) $\mathbb{K} \in \{\mathbb{Q}, \mathbb{R}, \mathbb{C}\}$ *mit der Addition bildet die Gruppe $(\mathbb{K}, +, 0)$.*

(iii) $\mathbb{K} \in \{\mathbb{Q}, \mathbb{R}, \mathbb{C}\}$ *mit der Multiplikation bildet die Gruppe $(\mathbb{K} \setminus \{0\}, \cdot, 1)$.*

(iv) *Ist X eine Menge, so bildet $S_X := \{f \mid f\colon X \to X \text{ Bijektion}\}$ mit der Komposition die Gruppe $(S_X, \circ, \mathrm{Id}_X)$, die als **symmetrische Gruppe** bzw. **Permutationsgruppe** bezeichnet wird.*

Kommentar. *Oft schreibt man nur* „Sei G eine Gruppe." *anstelle von* „Sei $(G, *, e)$ eine Gruppe." *In diesem Fall verwendet man in Anlehnung an $(\mathbb{K} \setminus \{0\}, \cdot, 1)$ in der Regel die Multiplikation $\cdot$ (anstelle von $*$) als Notation für die assoziative Verknüpfung $G \times G \to G$ und 1 (anstelle von e) als Notation für das neutrale Element. Wichtig ist, dass dies nur Notation ist und nichts mit der Multiplikation in $\mathbb{K} \setminus \{0\}$ zu tun hat.*

8. Kardinalität und Abzählbarkeit

Eine Menge A ist **endlich**, wenn sie entweder leer ist (mit $\#A := 0$) oder es ein $n \in \mathbb{N}$ und eine Bijektion $\phi\colon \{1, \ldots, n\} \to A$ gibt (mit $\#A := n$). Diese Definition können wir nun auf *abzählbare Mengen* erweitern.

Definition 8.1. *Eine Menge A ist **abzählbar** bzw. **abzählbar unendlich**, wenn es eine Bijektion $\phi\colon \mathbb{N} \to A$ gibt. Eine Menge A ist **höchstens abzählbar**, wenn sie entweder endlich oder abzählbar ist. Eine Menge A ist **überabzählbar** bzw. **überabzählbar unendlich**, wenn sie nicht höchstens abzählbar ist.*

Lemma 8.2. *Seien A, B Mengen mit $A \subseteq B$. Ist B endlich, so ist auch A endlich.*

Beweis. Wir beweisen die Aussage mittels vollständiger Induktion nach $n = \#B$. Wir behandeln den Fall $B = \emptyset$ separat. Ist $B = \emptyset$, so ist auch $A = \emptyset$ und damit endlich.

Induktionsanfang $n = 1$. Ist $n = 1$, so ist $B = \{b\}$. Dann ist entweder $A = \emptyset$ oder $A = \{b\}$. In beiden Fällen ist A endlich.

Induktionsvoraussetzung. Sei $n \in \mathbb{N}$. Es gelte die Aussage für alle Mengen B mit $\#B = n$.

Induktionsschritt. Sei B eine Menge mit $\#B = n+1$. Dann gibt es eine Bijektion $\phi\colon \{1, \dots, n+1\} \to B$. Ohne Beschränkung der Allgemeinheit gilt $A \subsetneq B$ (da für $A = B$ nichts zu zeigen ist). Also gibt es ein $b \in B \setminus A$. Definiere $B' \coloneqq B \setminus \{b\}$. Da ϕ bijektiv ist, gibt es ein $k \in \{1, \dots, n+1\}$ mit $\phi(k) = b$. Wir betrachten die bijektive Vertauschung $\sigma_{n+1,k} : M_{n+1} \to M_{n+1}$ aus dem Beweis von Satz 7.15 und definieren

$$\psi \coloneqq \phi \circ \sigma_{n+1,k}\colon M_{n+1} \to B.$$

Dann ist ψ eine Bijektion mit $\psi(n+1) = \phi(k) = b$. Insbesondere ist $\psi|_{M_n}\colon M_n \to B'$ eine Bijektion. Da $A \subseteq B'$, folgt aus der Induktionsvoraussetzung, dass A endlich ist. □

Lemma 8.3. *Es sei A eine Menge. Ferner sei $\psi\colon \mathbb{N} \to A$ surjektiv. Dann ist A höchstens abzählbar.*

Beweis. Wir müssen zeigen, dass A endlich oder abzählbar unendlich ist. Ohne Beschränkung der Allgemeinheit ist A nicht endlich. Also müssen wir zeigen, dass A abzählbar unendlich ist. Dazu müssen wir eine bijektive Funktion $\phi_A\colon \mathbb{N} \to A$ konstruieren.

Da ψ nicht injektiv sein muss, kann es Elemente $a \in A$ geben, deren Urbild $\psi^{-1}(\{a\})$ mehr als ein Element enthält. Dies müssen wir bei der Definition von ϕ_A vermeiden. Wir definieren die Funktion ϕ_A induktiv für $n \in \mathbb{N}$:

- $\phi_A(1) \coloneqq \psi(1)$.

Sind $\phi_A(1), \dots, \phi_A(n)$ bereits definiert, so definieren wir zunächst

- $\chi(n+1) \coloneqq \min\left\{k \in \mathbb{N} \,\middle|\, \psi(k) \notin \{\phi_A(1), \dots, \phi_A(n)\}\right\}$.

Da A nicht endlich und $\psi\colon \mathbb{N} \to A$ surjektiv ist, ist $\chi(n+1)$ wohldefiniert. Wir definieren

- $\phi_A(n+1) \coloneqq \psi(\chi(n+1))$.

Wir müssen noch zeigen, dass ϕ_A bijektiv ist.

Schritt 1 (ϕ_A ist injektiv). Seien $m, n \in \mathbb{N}$ mit $\phi_A(n) = \phi_A(m)$. Ohne Beschränkung der Allgemeinheit gilt $n \leq m$. Nach Definition von ϕ_A gilt

$$\phi_A(n) = \phi_A(m) \notin \{\phi_A(1), \dots, \phi_A(m-1)\}.$$

Also muss $n > m - 1$ gelten und damit $n = m$. Dies zeigt die Injektivität von ϕ_A.

Schritt 2. Wir zeigen mittels vollständiger Induktion, dass

$$\{\psi(1), \dots, \psi(n)\} \subseteq \{\phi_A(1), \dots, \phi_A(n)\} \quad \text{für alle } n \in \mathbb{N}.$$

Induktionsanfang $n = 1$. Es gilt $\{\psi(1)\} = \{\phi_A(1)\}$.

Induktionsvoraussetzung. Sei $n \in \mathbb{N}$. Es gelte $\{\psi(1), \dots, \psi(n)\} \subseteq \{\phi_A(1), \dots, \phi_A(n)\}$.

Induktionsschritt. Wir müssen zeigen, dass

$$\{\psi(1), \dots, \psi(n+1)\} \subseteq \{\phi_A(1), \dots, \phi_A(n+1)\}.$$

Nach Induktionsvoraussetzung reicht es zu zeigen, dass $\psi(n+1) \in \{\phi_A(1), \dots, \phi_A(n+1)\}$ gilt. Ohne Beschränkung der Allgemeinheit gilt $\psi(n+1) \notin \{\phi_A(1), \dots, \phi_A(n)\}$. Aus der Definition von ϕ_A folgt dann aber sofort $\phi_A(k) = \psi(k)$ für alle $k = 1, \dots, n$ und insbesondere $\phi_A(n+1) = \psi(n+1)$. Damit ist der Induktionsschritt gezeigt.

Schritt 2 (ϕ_A ist surjektiv). Sei nun $a \in A$. Da ψ surjektiv ist, gibt es ein $n \in \mathbb{N}$ mit $a = \psi(n) \in \{\phi_A(1), \dots, \phi_A(n)\}$. Also existiert ein $k \leq n$ mit $a = \phi_A(k)$. Damit ist ϕ_A surjektiv. □

Satz 8.4. *Die Menge $\mathbb{Z} = \{0, \pm 1, \pm 2, \pm 3, \dots\}$ der ganzen Zahlen ist abzählbar, d.h. es gibt eine Bijektion $\phi_{\mathbb{Z}} \colon \mathbb{N} \to \mathbb{Z}$.*

Beweis. Wir betrachten die Abbildungen

$$\phi_{\mathbb{Z}} \colon \mathbb{N} \to \mathbb{Z}, \quad \phi_{\mathbb{Z}}(n) \coloneqq \begin{cases} -(n-1)/2, & \text{falls } n \text{ ungerade,} \\ n/2, & \text{falls } n \text{ gerade,} \end{cases}$$

$$\psi_{\mathbb{Z}} \colon \mathbb{Z} \to \mathbb{N}, \quad \psi_{\mathbb{Z}}(z) \coloneqq \begin{cases} 2\,|z| + 1, & \text{falls } z \leq 0, \\ 2z, & \text{falls } z > 0. \end{cases}$$

Wir können leicht nachrechnen, dass

$$\psi_{\mathbb{Z}}\big(\phi_{\mathbb{Z}}(n)\big) = n \quad \text{und} \quad \phi_{\mathbb{Z}}\big(\psi_{\mathbb{Z}}(z)\big) = z \quad \text{für alle } n \in \mathbb{N} \text{ und alle } z \in \mathbb{Z}$$

gelten, d.h. es gilt $\phi_{\mathbb{Z}} \circ \psi_{\mathbb{Z}} = \mathrm{Id}_{\mathbb{Z}}$ und $\psi_{\mathbb{Z}} \circ \phi_{\mathbb{Z}} = \mathrm{Id}_{\mathbb{N}}$. Nach Satz 7.11 ist $\phi_{\mathbb{Z}}$ bijektiv (mit $\phi_{\mathbb{Z}}^{-1} = \psi_{\mathbb{Z}}$) und $\mathbb{Z}$ damit abzählbar. □

Satz 8.5. *Das kartesische Produkt $\mathbb{N} \times \mathbb{N}$ ist abzählbar, d.h. es gibt eine Bijektion $\phi_{\mathbb{N}\times\mathbb{N}} \colon \mathbb{N} \to \mathbb{N} \times \mathbb{N}$.*

Beweis. Wir teilen den Beweis in fünf Schritte, in denen wir $\phi_{\mathbb{N}\times\mathbb{N}}$ explizit konstruieren.

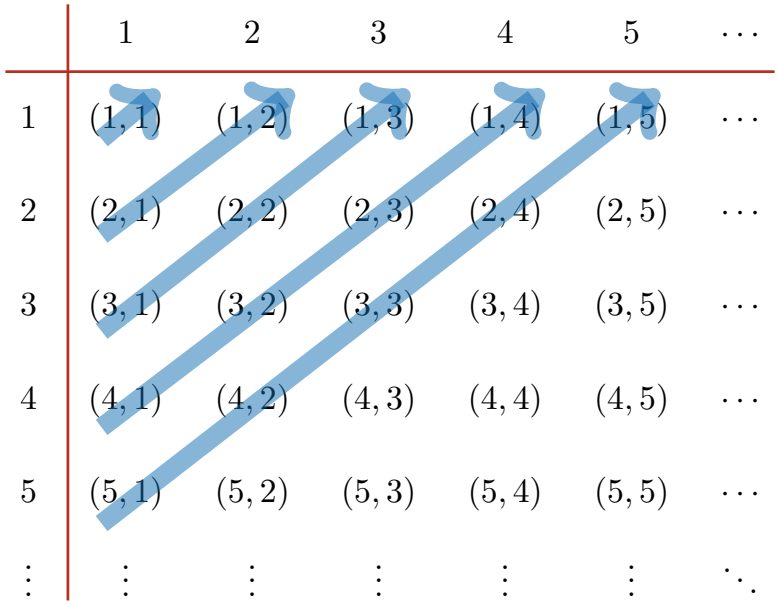


ABBILDUNG 7. Visualisierung der Bijektion $\phi_{\mathbb{N}\times\mathbb{N}}\colon \mathbb{N}\times\mathbb{N}\to\mathbb{N}$ aus dem Beweis von Satz 8.5, wobei j vertikal und k horizontal aufgetragen ist.

Schritt 1 (Konstruktion von $\psi_{\mathbb{N}\times\mathbb{N}}\colon \mathbb{N}\to\mathbb{N}\times\mathbb{N}$). Wir zählen $\mathbb{N}\times\mathbb{N}$ über seine Diagonalen ab, siehe Abbildung 7:

- In der ersten Diagonale gibt es nur das Paar $(1,1)$ mit $1+1=2$.
- In der zweiten Diagonale gibt es nur die Paare $(2,1)$ und $(1,2)$ mit $1+2=3$.
- In der dritte Diagonale gibt es nur die Paare $(3,1)$, $(2,2)$ und $(1,3)$ mit $1+3=4=2+2$.
- etc.

Auf der ℓ-ten Diagonale von $\mathbb{N}\times\mathbb{N}$ stehen insgesamt ℓ Paare $(j,k)\in\mathbb{N}\times\mathbb{N}$ mit $j+k=\ell+1$. Bevor man in die ℓ-te Diagonale kommt, gehen also $\ell-1$ Diagonalen mit $\sum_{i=1}^{\ell-1} i = \frac{(\ell-1)\ell}{2}$ Paaren voraus. In der ℓ-ten Diagonale können wir die Paare $(j,k)\in\mathbb{N}\times\mathbb{N}$ mit $j+k=\ell+1$ mittels dem zweiten Index k abzählen. Insgesamt erhalten wir die Abbildung

$$\psi_{\mathbb{N}\times\mathbb{N}}\colon \mathbb{N}\times\mathbb{N}\to\mathbb{N},\quad \psi_{\mathbb{N}\times\mathbb{N}}(j,k) \coloneqq \frac{(j+k-2)(j+k-1)}{2}+k$$

Damit gilt $\psi_{\mathbb{N}\times\mathbb{N}}(1,1)=1$, $\psi_{\mathbb{N}\times\mathbb{N}}(2,1)=2$, $\psi_{\mathbb{N}\times\mathbb{N}}(1,2)=3$, $\psi_{\mathbb{N}\times\mathbb{N}}(3,1)=4$, $\psi_{\mathbb{N}\times\mathbb{N}}(2,2)=5$, $\psi_{\mathbb{N}\times\mathbb{N}}(1,3)=6$, etc.

Schritt 2 (Konstruktion von $\phi_{\mathbb{N}\times\mathbb{N}}\colon \mathbb{N}\times\mathbb{N}\to\mathbb{N}$). Zu $n\in\mathbb{N}$ existiert ein (eindeutiges) maximales $\ell\in\mathbb{N}$ mit $\frac{(\ell-1)\ell}{2}<n$. Definiere $k\coloneqq n-\frac{(\ell-1)\ell}{2}\in\mathbb{N}$. Mittels indirektem Beweis zeigen wir $k\le\ell$. Dazu machen wir die Annahme $k>\ell$, d.h. es existiert $i\in\mathbb{N}$ mit $\ell+i=k=n-\frac{(\ell-1)\ell}{2}$. Daraus folgt

$$n>n-i=\frac{(\ell-1)\ell}{2}+\ell=\frac{\ell^2+\ell}{2}=\frac{\ell(\ell+1)}{2}.$$

Dies steht aber im Widerspruch zur Maximalität von ℓ (denn $\ell+1$ erfüllt dieselbe Bedingung). Dies zeigt $k \leq \ell$ und erlaubt die Definition von $j := \ell - k + 1 \in \mathbb{N}$. Mit dieser Konstruktion erhalten wir eine Funktion

$$\phi_{\mathbb{N}\times\mathbb{N}} \colon \mathbb{N} \times \mathbb{N} \to \mathbb{N}, \quad \phi_{\mathbb{N}\times\mathbb{N}}(n) := (j,k)$$

Schritt 3 ($\psi_{\mathbb{N}\times\mathbb{N}} \circ \phi_{\mathbb{N}\times\mathbb{N}} = \mathrm{Id}_{\mathbb{N}}$). Sei $n \in \mathbb{N}$. Nach Konstruktion folgt aus $\phi_{\mathbb{N}\times\mathbb{N}}(n) = (j,k)$, dass $\ell = j + k - 1$ und $\frac{(\ell-1)\ell}{2} + k = n$. Dies zeigt

$$\psi_{\mathbb{N}\times N}(j,k) = \frac{(j+k-2)(j+k-1)}{2} + k = \frac{(\ell-1)\ell}{2} + k = n,$$

also $\psi_{\mathbb{N}\times N}\big(\phi_{\mathbb{N}\times\mathbb{N}}(n)\big) = n$.

Schritt 4 ($\phi_{\mathbb{N}\times\mathbb{N}} \circ \psi_{\mathbb{N}\times\mathbb{N}} = \mathrm{Id}_{\mathbb{N}\times\mathbb{N}}$). Seien $j,k \in \mathbb{N}$. Dann gilt

$$\psi_{\mathbb{N}\times N}(j,k) = \frac{(j+k-2)(j+k-1)}{2} + k =: n.$$

Offensichtlich erfüllt $\widetilde{\ell} := j + k - 1$ damit $\frac{(\widetilde{\ell}-1)\widetilde{\ell}}{2} < \frac{(\widetilde{\ell}-1)\widetilde{\ell}}{2} + k = n$. Ferner gilt

$$\begin{aligned}\frac{\widetilde{\ell}(\widetilde{\ell}+1)}{2} = \sum_{i=1}^{j+k-1} i = (j+k-1) + \sum_{i=1}^{j+k-2} i &= (j+k-1) + \frac{(j+k-2)(j+k-1)}{2} \\ &= (j+k-1) + (n-k) = n + j - 1 \geq n,\end{aligned}$$

d.h. $\widetilde{\ell}$ ist maximal mit $\frac{(\widetilde{\ell}-1)\widetilde{\ell}}{2} < n$. Es folgt $\phi_{\mathbb{N}\times\mathbb{N}}(n) = (\widetilde{j},\widetilde{k})$ mit

$$\begin{aligned}\widetilde{k} &= n - \frac{(\widetilde{\ell}-1)\widetilde{\ell}}{2} = k, \\ \widetilde{j} &= \widetilde{\ell} - \widetilde{k} + 1 = (j+k-1) - k + 1 = j.\end{aligned}$$

Dies zeigt $\phi_{\mathbb{N}\times\mathbb{N}}\big(\psi_{\mathbb{N}\times\mathbb{N}}(j,k)\big) = (j,k)$.

Schritt 5. Nach Satz 7.11 ist $\phi_{\mathbb{N}\times\mathbb{N}}$ bijektiv (mit $\phi^{-1}_{\mathbb{N}\times\mathbb{N}} = \psi_{\mathbb{N}\times\mathbb{N}}$) und $\mathbb{N}\times\mathbb{N}$ damit abzählbar. □

Korollar 8.6. *Die Menge $\mathbb{Q}$ der rationalen Zahlen ist abzählbar.*

Beweis. Für jede Zahl $x \in \mathbb{Q}$ existieren Zähler $z \in \mathbb{Z}$ und Nenner $n \in \mathbb{N}$ mit $x = z/n$. Sei $\phi_{\mathbb{N}\times\mathbb{N}} \colon \mathbb{N} \to \mathbb{N}\times\mathbb{N}$ die Bijektion von Satz 8.5. Sei $\phi_{\mathbb{Z}} \colon \mathbb{N} \to \mathbb{Z}$ die Bijektion von Satz 8.4. Dann definieren wir die Abbildung

$$\phi_{\mathbb{Q}} \colon \mathbb{N} \to \mathbb{Q} \quad \text{vermöge} \quad \phi_{\mathbb{Q}}(n) := \phi_{\mathbb{Z}}(j)/k \text{ und } (j,k) = \phi_{\mathbb{N}\times\mathbb{N}}(n).$$

Dann ist $\phi_{\mathbb{Q}}$ surjektiv. Aus Lemma 8.3 folgt, dass $\mathbb{Q}$ höchstens abzählbar ist. Da $\mathbb{N} \subseteq \mathbb{Q}$, kann $\mathbb{Q}$ nach der Kontraposition von Lemma 8.2 nicht endlich sein. Also ist $\mathbb{Q}$ abzählbar unendlich. □

Korollar 8.7. *Die abzählbare Vereinigung $A := \bigcup_{j\in\mathbb{N}} A_j$ abzählbar unendlicher Mengen A_j ist abzählbar unendlich.*

Beweis. Für $j \in \mathbb{N}$ sei $\phi_j \colon \mathbb{N} \to A_j$ eine Bijektion. Dann ist $\phi \colon \mathbb{N}\times\mathbb{N} \to A$, $\phi(j,k) \coloneqq \phi_j(k)$ surjektiv. In Verbindung mit der Bijektion $\phi_{\mathbb{N}\times\mathbb{N}}$ von Satz 8.5 gibt es damit eine Surjektion $\phi_A \coloneqq \phi \circ \phi_{\mathbb{N}\times\mathbb{N}} \colon \mathbb{N} \to A$. Aus Lemma 8.3 folgt, dass A höchstens abzählbar ist. Da $A_1 \subseteq A$, kann A nach der Kontraposition von Lemma 8.2 nicht endlich sein. Also ist A abzählbar unendlich. □

Satz 8.8 (Cantor'sches Diagonalverfahren). *$\mathbb{R}$ ist überabzählbar.*

Beweis. Wir betrachten das Intervall $[0,1] \coloneqq \{x \in \mathbb{R} \mid 0 \leq x \leq 1\}$. Im Vorgriff auf den späteren Beweis verwenden wir die Dezimaldarstellung von Zahlen $x \in [0,1]$: Für jedes $x \in [0,1]$ gibt es Ziffern $a_k \in \{0,1,\dots,9\}$ für alle $k \in \mathbb{N}$, sodass sich x in der Form

$$x = 0.a_1a_2a_3a_4\dots$$

schreiben lässt – wobei die a_k in dieser Darstellung als dezimale Ziffern und nicht als Produkt der Ziffern verstanden werden. Sei $\psi \colon \mathbb{N} \to [0,1]$ eine Aufzählung von Zahlen in $[0,1]$. Wir stellen alle Zahlen $\psi(j)$ mittels ihrer Ziffern $a_{jk} \in \{0,1,\dots,9\}$ dar:

$$\begin{aligned}\psi(1) &= 0.a_{11}a_{12}a_{13}a_{14}\dots\\ \psi(2) &= 0.a_{21}a_{22}a_{23}a_{24}\dots\\ \psi(3) &= 0.a_{31}a_{32}a_{33}a_{34}\dots\\ &\text{etc.}\end{aligned}$$

Wir definieren die Zahl

$$y \coloneqq 0.b_1b_2b_3b_4\dots \quad \text{mit den Ziffern} \quad b_k \coloneqq \begin{cases} 4, & \text{falls } a_{kk} = 5,\\ 5, & \text{falls } a_{kk} \neq 5.\end{cases}$$

Dann gilt $y \neq \psi(j)$ für alle $j \in \mathbb{N}$, da für die k-ten Ziffern von y gemäß Definition $b_k \neq a_{kk}$ gilt. Also kann ψ nicht surjektiv sein. Es gibt also keine Surjektion $\psi \colon \mathbb{N} \to [0,1]$ und insbesondere keine Bijektion $\mathbb{N} \to \mathbb{R}$. Also muss $\mathbb{R}$ überabzählbar sein. □

Satz 8.9. *Sei A eine Menge und $\phi \colon A \to \mathcal{P}(A)$. Dann ist ϕ nicht surjektiv. Insbesondere ist $\mathcal{P}(\mathbb{N})$ nicht abzählbar.*

Beweis. Wir adaptieren das Cantor'sche Diagonalverfahren aus dem Beweis von Satz 8.8. Sei $\phi \colon A \to \mathcal{P}(A)$. Um zu zeigen, dass ϕ nicht surjektiv sein kann, betrachten wir die Menge $Y \coloneqq \{x \in A \mid x \notin \phi(x)\}$. Wir zeigen $Y \notin \phi(A)$. Dazu argumentieren wir indirekt und nehmen $Y \in \phi(A)$ an. Dann gibt es ein $y \in A$ mit $\phi(y) = Y$. Wir machen eine Fallunterscheidung:

Fall 1 ($y \in Y$). Falls $y \in Y$, so erhalten wir aus der Definition von Y den Widerspruch $y \notin \phi(y) = Y$.

Fall 1 ($y \notin Y$). Falls $y \notin Y$, so erhalten wir aus der Definition von Y den Widerspruch $y \in \phi(y) = Y$.

Da beide Fälle auf einen Widerspruch führen, ist unsere Annahme falsch, d.h. es gilt $Y \notin \phi(A)$. Insbesondere ist jedes $\phi\colon A \to \mathcal{P}(A)$ nicht surjektiv. □

Bemerkung 8.10. *Für eine endliche Menge A folgt der Beweis von Satz 8.9 auch aus Satz 5.13. Vollständige Induktion zeigt, dass $n < 2^n$ für alle $n \in \mathbb{N}_0$ gilt. Mit $n := \#A$ und Satz 5.13 folgt $\#\mathcal{P}(A) = 2^n > n = \#A$. Nach dem Schubfachprinzip von Satz 7.15 kann es keine surjektive Abbildung $\phi\colon A \to \mathcal{P}(A)$ geben.*

Bemerkung 8.11. *Man kann zeigen, dass eine Bijektion $\phi\colon \mathbb{R} \to \mathcal{P}(\mathbb{N})$ existiert, d.h. $\mathcal{P}(\mathbb{N})$ ist nicht nur überabzählbar, sondern „genauso überabzählbar" wie $\mathbb{R}$.*

Kommentar. *Mit den Techniken dieses Abschnitts haben Sie auch vollständiges Verständnis von Hilberts Hotel: Wenn ein Hotel nur endlich viele Zimmer hat, die alle voll belegt sind, dann ist kein Platz mehr für einen weiteren Gast. Wenn ein Hotel aber abzählbar viele Zimmer hat, so ist immer Platz für abzählbar-viele zusätzliche Gäste, auch wenn alle Zimmer bereits belegt sind.*

9. Die natürlichen Zahlen

In den vergangenen Abschnitten haben wir die natürlichen Zahlen $\mathbb{N} = \{1, 2, 3, \dots\}$ und ihre schulmathematischen Eigenschaften vorausgesetzt und auf vielfältige Weise genutzt (z.B. zur Definition von höchstens abzählbaren Mengen). Um unserem Vorgehen eine formale Grundlage zu geben, müssen wir noch zeigen, dass $\mathbb{N}$ gewissermaßen eindeutig ist, sodass die Verwendung einer „anderen Menge natürlicher Zahlen" auf dieselben Definitionen und Ergebnisse führt.

Formal folgt die Existenz von $\mathbb{N}$ aus den Axiomen der Mengenlehre. Die sogenannte **John-von-Neumann-Konstruktion** konstruiert $\mathbb{N}_0 = \{0, 1, 2, 3, \dots\}$ auf folgende Weise

$$\begin{aligned} 0 &:= \emptyset, \\ 1 &:= \{0\} &&= \{\,\emptyset\,\}, \\ 2 &:= \{0, 1\} &&= \{\,\emptyset, \{\emptyset\}\,\}, \\ 3 &:= \{0, 1, 2\} &&= \{\,\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\,\}, \quad \text{etc,} \end{aligned}$$

d.h. der Nachfolger von n ist definiert als $(n{+}1) := n \cup \{n\}$. Dabei ist wichtig zu bemerken, dass n und $n + 1$ Mengen sind mit $n \subsetneq n + 1$ und dass die Definition des Nachfolgers lediglich auf der Mengenvereinigung basiert. Natürlich kann dieses Vorgehen nicht nur zur Konstruktion von $\mathbb{N}_0$, sondern auch zur Konstruktion von $\mathbb{N}$ herangezogen werden.

Die folgende Definition präzisiert die Eigenschaften der John-von-Neumann-Konstruktion.

Definition 9.1. *Eine Menge $N \neq \emptyset$, genauer ein Tripel $(N, 1, (\cdot)')$, heißt **natürliche Zahlen**, wenn es eine Nachfolgerabbildung $(\cdot)' \colon N \to N$ und ein ausgezeichnetes „erstes Element“ $1 \in N$ gibt, sodass die folgenden **Peano-Axiome** gelten:*

(N1) *Die Abbildung $(\cdot)'$ ist injektiv,*
(N2) $\forall n \in N : n' \neq 1$, *(1 ist kein Nachfolger)*
(N3) $\forall M \subseteq N : \big[\big(1 \in M \wedge (\forall n \in M : n' \in M)\big) \Rightarrow M = N\big]$. *(Induktionsprinzip)*

Bemerkung 9.2. *Wir wissen, dass die aus der Schule bekannten natürlichen Zahlen $\mathbb{N}$ die Peano-Axiome (N1)–(N3) erfüllen mit $n' := n + 1$ für $n \in \mathbb{N}$, denn $\mathbb{N}$ erfüllt laut Satz 4.3 das Induktionsprinzip. Wir wollen in diesem Abschnitt zunächst zeigen, dass jede Menge N mit (N1)–(N3) defacto mit $\mathbb{N}$ übereinstimmt (d.h. $\mathbb{N}$ ist eindeutig); siehe Korollar 9.4. Ferner werden wir zeigen, dass die Peano-Axiome (N1)–(N3) insbesondere ausreichen, um Addition, Multiplikation und Ordnung auf N zu definieren, sodass sich N wie $\mathbb{N}$ verhält.*

Der folgende Rekursionssatz ist das zentrale mathematische Argument in diesem Abschnitt.

Satz 9.3 (Rekursionssatz). *Es sei N eine Menge natürlicher Zahlen gemäß Definition 9.1. Es sei $A \neq \emptyset$ eine Menge, $a \in A$ und $g \colon A \to A$ eine Funktion, die sogenannte **Rekursionsfunktion**. Dann existiert eine eindeutige Funktion $\phi \colon N \to A$ mit den folgenden beiden Eigenschaften:*

(a) $\phi(1) = a$,
(b) $\forall n \in N : \phi(n') = g(\phi(n))$.

Bevor wir Satz 9.3 beweisen, zeigen wir, wie daraus die Eindeutigkeit von $\mathbb{N}$ folgt. Beachten Sie, dass die behauptete Funktion $\phi \colon N \to \widetilde{N}$ im folgenden Korollar nicht nur eine Bijektion ist, sondern auch die Struktur erhält (konkret das ausgezeichnete Element und die Nachfolgerabbildung).

Korollar 9.4 (Eindeutigkeit von $\mathbb{N}$). *Seien N, $\widetilde{N}$ zwei Mengen natürlicher Zahlen gemäß Definition 9.1. Dann existiert eine eindeutige Bijektion $\phi \colon N \to \widetilde{N}$ mit*

(i) $\phi(1) = \widetilde{1}$,
(ii) $\forall n \in N : \phi(n') = \phi(n)'$,

wobei $1 \in N$ und $\widetilde{1} \in \widetilde{N}$ die ausgezeichneten Elemente seien. Beachte gegebenenfalls, dass in (ii) n' der Nachfolger in N ist, während $\phi(n)'$ der Nachfolger in $\widetilde{N}$ ist.

Beweis von Korollar 9.4. Im Folgenden wenden wir den Rekursionssatz viermal an:

Schritt 1 (Kandidat für $\phi \colon N \to \widetilde{N}$). Wir wenden den Rekursionssatz an für N, $A = \widetilde{N}$, $a = \widetilde{1}$ und $g(\widetilde{n}) := \widetilde{n}'$. Dann existiert eine eindeutige Funktion $\phi \colon N \to \widetilde{N}$ mit

$$\phi(1) = \widetilde{1} \quad \text{und} \quad \forall n \in N : \phi(n') = \phi(n)'$$

Beachte, dass dieses ϕ der einzige Kandidat für die behauptete Bijektion ist.

Schritt 2 (Kandidat für Inverse von ϕ). Wir wenden den Rekursionssatz an für $\widetilde{N}$, $A = N$, $a = 1$ und $g(n) \coloneqq n'$. Dann existiert eine eindeutige Funktion $\psi\colon \widetilde{N} \to N$ mit

$$\psi(\widetilde{1}) = 1 \quad \text{und} \quad \forall \widetilde{n} \in \widetilde{N} : \psi(\widetilde{n}') = \psi(\widetilde{n})'$$

Schritt 3 ($\psi \circ \phi = \mathrm{Id}_N$). Die Komposition $\psi \circ \phi\colon N \to N$ hat die folgenden Eigenschaften:

(a) $(\psi \circ \phi)(1) = \psi(\phi(1)) = \psi(\widetilde{1}) = 1$,

(b) $\forall n \in N : (\psi \circ \phi)(n') = \psi(\phi(n')) = \psi(\phi(n)') = \psi(\phi(n))' = [(\psi \circ \phi)(n)]'$.

Wir wenden den Rekursionssatz an für N, $A = N$, $a = 1$ und $g(n) \coloneqq n'$: Da auch Id_N die Eigenschaften (a)–(b) hat, folgt aus der bewiesenen Eindeutigkeit im Rekursionssatz, dass $\psi \circ \phi = \mathrm{Id}_N$.

Schritt 4 ($\phi \circ \psi = \mathrm{Id}_{\widetilde{N}}$). Die Identität $\phi \circ \psi = \mathrm{Id}_{\widetilde{N}}$ folgt wie in Schritt 3, wenn wir den Rekursionssatz für $\widetilde{N}$, $A = \widetilde{N}$, $a = \widetilde{1}$ und $g(\widetilde{n}) \coloneqq \widetilde{n}'$ anwenden.

Schritt 5. Aus Schritt 1 folgt die Existenz von ϕ. Mit Satz 7.11 folgt aus Schritt 3–4, dass ϕ bijektiv ist mit $\phi^{-1} = \psi$. □

Beweis vom Rekursionssatz 9.3. Nach Definition 7.1 ist jede Funktion eine Relation. Aus diesem Grund betrachten wir die Menge aller Relationen $R \subseteq N \times A$, die die Eigenschaften (a)–(b) der zu konstruierenden Funktion $\phi\colon N \to A$ besitzen:

$$\mathcal{R} \coloneqq \big\{ R \subseteq N \times A \,\big|\, (1, a) \in R \wedge [\forall (n, b) \in R : (n', g(b)) \in R] \big\}.$$

Beachte, dass $\mathcal{R} \neq \emptyset$, da $N \times A \in \mathcal{R}$ für das vollständige kartesische Produkt $N \times A$.

Schritt 1 (Konstruktion von ϕ). Damit eine Relation eine Funktion ist, muss jedem $n \in N$ genau ein Funktionswert zugeordnet werden; vgl. Definition 7.1. Die Relation darf also gewissermaßen keine überflüssigen Beziehungen definieren (bzw. keine unnötigen Paare enthalten). Aus diesem Grund definieren wir ϕ als „kleinste Relation“ in $\mathcal{R}$, d.h.

$$\phi \coloneqq \bigcap_{R \in \mathcal{R}} R.$$

Da $(1, a) \in R$ für alle $R \in \mathcal{R}$, gilt nach Definition des Schnitts $(1, a) \in \phi$. Sei $(n, b) \in \phi$. Dann gilt für alle $R \in \mathcal{R}$, dass $(n, b) \in R$ und damit nach Definition von $\mathcal{R}$ auch $(n', g(b)) \in R$. Nach Definition des Schnitts folgt also $(n', g(b)) \in \phi$. Damit haben wir $\phi \in \mathcal{R}$ gezeigt. Also erfüllt die *Relation* ϕ die Eigenschaften (a)–(b), wenn wir zeigen, dass ϕ eine Funktion ist.

Schritt 2 (ϕ ist eine Funktion). Laut Definition 7.1 müssen wir zeigen, dass gilt

$$\forall n \in N \exists! \, b \in A : (n, b) \in \phi.$$

Wir zeigen dies mit Hilfe des Induktionsprinzips (N3). Wir definieren

$$M \coloneqq \big\{ n \in N \,\big|\, \exists! \, b \in A : (n, b) \in \phi \big\}.$$

Um $M = N$ zu zeigen, müssen wir gemäß (N3) zeigen, dass $1 \in M$ und $[\forall n \in M : n' \in M]$ gelten.

Schritt 2a ($1 \in M$). Wir haben in Schritt 1 bereits gezeigt, dass $(1, a) \in \phi$ gilt. Also müssen wir nur noch die Eindeutigkeit von a zeigen. Wir machen einen indirekten Beweis und nehmen an, dass a nicht eindeutig ist, d.h. es existiert ein $b \in A$ mit $b \neq a$ und $(1, b) \in \phi$. Wir betrachten $\phi \backslash \{(1, b)\}$ und zeigen nun $\phi \backslash \{(1, b)\} \in \mathcal{R}$: Wegen $a \neq b$ gilt $(1, a) \in \phi \backslash \{(1, b)\}$. Gemäß (N2) gilt $1 \neq n'$ für alle $n \in N$. Deshalb gilt für alle $(n, b) \in \phi \backslash \{(1, b)\}$ weiterhin $(n', g(b)) \in \phi \backslash \{(1, b)\}$. Also folgt $\phi \backslash \{(1, b)\} \in \mathcal{R}$ gemäß Definition von $\mathcal{R}$. Dies liefert aber den Widerspruch

$$(1, b) \in \phi = \bigcap_{R \in \mathcal{R}} R \subseteq \phi \backslash \{(1, b)\}.$$

Also war die Annahme falsch, d.h. aus $(1, b) \in \phi$ folgt $a = b$. Also gilt $1 \in M$.

Schritt 2b ($\forall n \in M : n' \in M$). Sei $n \in M$. Nach Definition von M existiert ein eindeutiges $b \in A$ mit $(n, b) \in \phi$. Wegen $\phi \in \mathcal{R}$ folgt $(n', g(b)) \in \phi$. Also müssen wir nur noch die Eindeutigkeit von $g(b)$ zeigen. Wir machen einen indirekten Beweis und nehmen an, dass $g(b)$ nicht eindeutig ist, d.h. es existiert ein $c \in A$ mit $c \neq g(b)$ und $(n', c) \in \phi$. Wir betrachten $\phi \backslash \{(n', c)\}$ und zeigen nun $\phi \backslash \{(n', c)\} \in \mathcal{R}$: Wegen $1 \neq n'$ nach (N2) gilt $(1, a) \in \phi \backslash \{(n', c)\}$. Sei $(k, d) \in \phi \backslash \{(n', c)\}$ und damit insbesondere $(k', g(d)) \in \phi$. Wir müssen zeigen, dass $(k', g(d)) \in \phi \backslash \{(n', c)\}$. Dazu machen wir eine Fallunterscheidung:

Fall 1 ($k' \neq n'$). Aus $k' \neq n'$ folgt $(k', g(d)) \neq (n', c)$ und deshalb $(k', g(d)) \in \phi \backslash \{(n', c)\}$.

Fall 2 ($k' = n'$). Aus $k' = n'$ und der Injektivität von $(\cdot)'$ gemäß (N1) folgt $k = n \in M$. Gemäß der Definition von M folgt also $(k, d) = (n, b)$ und damit $(k', g(d)) = (n', g(b)) \neq (n', c)$. Also folgt auch in diesem Fall $(k', g(d)) \in \phi \backslash \{(n', c)\}$.

Insgesamt haben wir damit $\phi \backslash \{(n', c)\} \in \mathcal{R}$ gezeigt und wie in Schritt 2a folgt der Widerspruch

$$(n', c) \in \phi = \bigcap_{R \in \mathcal{R}} R \subseteq \phi \backslash \{(n', c)\}.$$

Also war die Annahme falsch, d.h. aus $(n', c) \in \phi$ folgt $c = g(b)$. Insgesamt folgt also $n' \in M$. Mit Hilfe von (N3) erhalten wir $M = N$, d.h. die Relation ϕ definiert tatsächlich eine Funktion $\phi \colon N \to A$.

Schritt 3 (Eindeutigkeit von ϕ). Ist $\psi \colon N \to A$ eine weitere Funktion mit den Eigenschaften (a)–(b), so folgt $\psi \in \mathcal{R}$ und damit $\phi \subseteq \psi \subseteq N \times A$ im Sinne von Relationen. Also folgt für alle $n \in N$, dass $(n, \phi(n)) \in \psi$. Da ψ eine Funktion ist, folgt aus der Wohldefiniertheit, dass $\psi(n) = \phi(n)$ für alle $n \in N$; vgl. Definition 7.1. Damit ist die Eindeutigkeit von ϕ gezeigt. □

Definition 9.5 (Definition der Addition auf N). *Sei N eine Menge natürlicher Zahlen. Zu $m \in N$ wähle $A = N$, $a = m'$ und $g(n) := n'$. Laut Rekursionssatz 9.3 existiert dann eine eindeutige Funktion $+_m := \phi\colon N \to A$ mit*

(a) $+_m(1) = m'$, *(d.h. $m + 1 = m'$)*

(b) $\forall n \in N : +_m(n') = [+_m(n)]'$. *(d.h. $m + (n + 1) = (m + n) + 1$)*

Wir definieren die Verknüpfung $+\colon N \times N \to N$ durch $+(m, n) := m + n := +_m(n)$.

Satz 9.6 (Eigenschaften der Addition). *Sei N eine Menge natürlicher Zahlen. Dann erfüllt die Verknüpfung $+$ aus Definition 9.5 die folgenden Eingeschaften:*

(i) $\forall n \in N : +_1(n) = n'$, *(d.h. wir schreiben später $n + 1$ statt n')*

(ii) $\forall m, n \in N : m + n = n + m$, *(**Kommutativität** von $+$)*

(iii) $\forall k, m, n \in N : k + (m + n) = (k + m) + n$. *(**Assoziativität** von $+$)*

Beweis. **Schritt 1 ($\forall n \in N : +_1(n) = n'$).** Wir zeigen die Behauptung durch vollständige Induktion nach n.

Induktionsanfang. Nach Definition 9.5 gilt $+_1(1) \overset{\text{(a)}}{=} 1'$. Dies zeigt den Induktionsanfang $n = 1$.

Induktionsvoraussetzung. Sei $n \in \mathbb{N}$. Es gelte $+_1(n) = n'$.

Induktionsschritt. Mit der Induktionsvoraussetzung (IV) gilt

$$+_1(n') \overset{\text{(b)}}{=} [+_1(n)]' \overset{\text{IV}}{=} [n']'.$$

Damit ist der Induktionsschritt gezeigt und Schritt 1 damit bewiesen. Dies zeigt (i).

Schritt 2 ($\forall m, n \in N : +_m(n) = +_n(m)$). Wir machen eine geschachtelte Induktion. Die äußere Induktion ist eine vollständige Induktion über m, die innere Induktion eine vollständige Induktion über n.

Induktionsbehauptung. Es gilt $\forall m \in N : \big[\forall n \in N : +_m(n) = +_n(m)\big]$.

Induktionsanfang. Für $m = 1$ ist zu zeigen, dass gilt $[\forall n \in N : +_1(n) = +_n(1)]$. Sei $n \in N$. Mit (i) bzw. Schritt 1 gilt

$$+_1(n) \overset{\text{(i)}}{=} n' \overset{\text{(a)}}{=} +_n(1).$$

Damit ist der Induktionsanfang gezeigt.

Induktionsvoraussetzung. Sei $m \in N$. Es gelte $[\forall n \in N : +_m(n) = +_n(m)]$. $(*)$

Induktionsschritt. Wir müssen zeigen, dass gilt $[\forall n \in N : +_{m'}(n) = +_n(m')]$. Wir beweisen dies mittels vollständiger Induktion nach n.

(Innerer) Induktionsanfang. Für $n = 1$ gilt gemäß (i) bzw. Schritt 1

$$+_{m'}(1) \overset{\text{(a)}}{=} [m']' \overset{\text{(i)}}{=} +_1(m').$$

Damit ist der Induktionsanfang gezeigt.

(Innere) Induktionsvoraussetzung. Sei $n \in N$. Es gelte $+_{m'}(n) = +_n(m')$. $(**)$

(Innerer) Induktionsschritt. Wir müssen zeigen, dass gilt $+_{m'}(n') = +_{n'}(m')$. Tatsächlich gilt

$$+_{m'}(n') \overset{\text{(b)}}{=} [+_{m'}(n)]' \overset{(**)}{=} [+_n(m')]' \overset{\text{(b)}}{=} [(+_n(m))']' \overset{(*)}{=} [(+_m(n))']' \overset{\text{(b)}}{=} [+_m(n')]' \overset{(*)}{=} [+_{n'}(m)]' \overset{\text{(b)}}{=} +_{n'}(m').$$

Damit ist der innere Induktionsschritt gezeigt und die innere Induktion erfolgreich abgeschlossen. Da die innere Induktionsbehauptung gerade der (äußere) Induktionsschritt war, ist der (äußere) Induktionsschritt gezeigt und die (äußere) Induktion erfolgreich abgeschlossen. Damit ist Schritt 2 bewiesen. Aus Schritt 2 folgt die Kommutativität (ii) gemäß Definition der Verknüpfung $+$ in Definition 9.5.

Schritt 3 (Beweis von (iii)). Wir machen eine vollständige Induktion nach k.

Induktionsbehauptung. Es gilt $\forall k \in N : \big[\forall m, n \in N : k+(m+n) = (k+m)+n\big]$.

Induktionsanfang. Sei $k = 1$. Seien $m, n \in N$. Mit (i) und (ii) gilt dann

$$1 + (m + n) = +_n(m) + 1 \overset{\text{(b)}}{=} +_n(m') = n + (m + 1) = (1 + m) + n.$$

Damit ist der Induktionsanfang gezeigt.

Induktionsvoraussetzung. Sei $k \in N$. Es gelte

$$\forall m, n \in N : k + (m + n) = (k + m) + n.$$

Induktionsschritt. Seien $m, n \in N$. Dann ist $(k + 1) + (m + n) = ((k + 1) + m) + n$ zu zeigen. Mit zweifacher Anwendung der Induktionsvoraussetzung (IV) und unter Verwendung von (i) und (ii) folgt

$$\begin{aligned}(k + 1) + (m + n) &= +_{m+n}(k + 1) \overset{\text{(b)}}{=} +_{m+n}(k) + 1 = (k + (m + n)) + 1 \\ &\overset{\text{IV}}{=} ((k + m) + n) + 1 = +_n(k + m) + 1 \overset{\text{(b)}}{=} +_n((k + m) + 1) \overset{\text{IV}}{=} +_n((k + 1) + m) \\ &= ((k + 1) + m) + n.\end{aligned}$$

Damit ist der Induktionsschritt gezeigt und der Beweis von (iii) abgeschlossen. □

Definition 9.7 (Definition der Multiplikation auf N). *Sei N eine Menge natürlicher Zahlen. Sei $+$ die Verknüpfung aus Definition 9.5. Zu $m \in N$ wähle $A = N$, $a = m$ und $g(n) := m + n$. Laut Rekursionssatz 9.3 existiert dann eine eindeutige Funktion $*_m := \phi\colon N \to A$ mit*

(a) $*_m(1) = m$, *(d.h. $m \cdot 1 = m$)*

(b) $\forall n \in N : *_m(n + 1) = m + *_m(n)$. *(d.h. $m(n + 1) = m + mn$)*

Wir definieren die Verknüpfung $\cdot\colon N \times N \to N$ durch $\cdot(m, n) := m \cdot n := mn := *_m(n)$.

Analog zum Beweis von Satz 9.6 zeigt man mittels (geschachtelter) vollständiger Induktion den folgenden Satz.

Satz 9.8 (Eigenschaften der Multiplikation). *Sei N eine Menge natürlicher Zahlen. Sei $+$ die Verknüpfung aus Definition 9.5. Dann erfüllt die Verknüpfung $\cdot$ aus Definition 9.7 die folgenden Eingeschaften:*

(i) $\forall n \in N : n \cdot 1 = n = 1 \cdot n$, *(Existenz des neutralen Elements)*
(ii) $\forall m, n \in N : m \cdot n = n \cdot m$, *(**Kommutativität** von $\cdot$)*
(iii) $\forall k, m, n \in N : k \cdot (m \cdot n) = (k \cdot m) \cdot n$. *(**Assoziativität** von $\cdot$)*
(iv) $\forall k, m, n \in N : k \cdot (m + n) = k \cdot m + k \cdot n$. *(**Distributivität** von $\cdot$ und $+$)*

Aus der Injektivität (N1) bekommt man die Injektivität von $+_m$ und $*_m$ für alle $m \in N$. Der Beweis folgt wieder analog zum Beweis von Satz 9.6 mittels vollständiger Induktion.

Satz 9.9 (Kürzungsregeln). *Sei N eine Menge natürlicher Zahlen. Sei $m \in N$. Dann sind die Abbildungen $+_m \colon N \to N$ aus Definition 9.5 und $*_m \colon N \to N$ aus Definition 9.7 injektiv mit $m \notin +_m(N)$. Insbesondere gelten die folgenden beiden Aussagen für die Verknüpfungen $+$ und $\cdot$ aus Definition 9.5 und Definition 9.7:*

(i) $\forall k, m, n \in N : (m = n \Leftrightarrow k + m = k + n)$.
(ii) $\forall k, m, n \in N : (m = n \Leftrightarrow k \cdot m = k \cdot n)$.

Abschließend definieren wir mit Hilfe der Addition die Ordnung $<$ auf N.

Definition 9.10. *Sei N eine Menge natürlicher Zahlen. Sei $+$ die Verknüpfung aus Definition 9.5. Für $m, n \in N$ schreiben wir $m < n$ sowie $n > m$, wenn gilt $\exists k \in N : m + k = n$. Dies definiert die Relation $<$ auf N. Ferner schreiben wir $m \leq n$ sowie $n \geq m$, wenn $m < n$ oder $m = n$ gelten.*

Auch der folgende Satz wird mit vollständiger Induktion bewiesen und definiert insbesondere die Subtraktion auf N.

Satz 9.11 (Eigenschaften der Ordnung). *Sei N eine Menge natürlicher Zahlen. Seien $+$ und $\cdot$ die Verknüpfungen aus Definition 9.5 und Definition 9.7 Dann gelten die folgenden Aussagen für die Ordnung aus Definition 9.10:*

(i) $\forall n \in N : 1 \leq n$, *(Existenz eines kleinsten Elements)*
(ii) $\forall m, n \in N : (m < n \Rightarrow m \neq n)$,
(iii) $\forall m, n \in N : (m < n) \vee (m = n) \vee (m > n)$ *(totale Ordnung)*
(iv) $\forall m, n \in N : [(m \leq n) \wedge (m \geq n)] \Rightarrow (m = n)$
(v) $\forall k, m, n \in N : (m < n \Leftrightarrow k + m < k + n)$, *(Kürzungsregel $+$)*
(vi) $\forall k, m, n \in N : (m < n \Leftrightarrow km < kn)$, *(Kürzungsregel $\cdot$)*
(vii) $\forall m, n \in N, m < n \, \exists! n - m := k \in N : m + k = n$. *(Definition von $-$)*

Abschließend wollen wir noch den folgenden Satz zeigen, weil dieser in in der Tat das zentrale Argument war, um für die aus der Schule bekannten natürlichen Zahlen $\mathbb{N}$ das Induktionsprinzip zu beweisen; siehe Satz 4.3 und dessen Beweis.

Satz 9.12 (Eindeutige Existenz minimaler Elemente). *Sei N eine Menge natürlicher Zahlen und $\emptyset \neq A \subseteq N$. Dann existiert ein eindeutiges Element* $\min(A) \coloneqq a \in A$ *mit $a \leq n$ für alle $n \in A$.*

Beweis. Wir machen einen indirekten Beweis und nehmen an, dass es kein solches Element $a \in A$ gibt. Dann definieren wir $M \coloneqq \{m \in N \mid \forall n \in A : m < n\}$. Wir zeigen, dass die Menge $M \subseteq N$ das Induktionsprinzip (N3) erfüllt:

Zunächst gilt $1 \in M$, da ansonsten $1 \in A$ und $1 =: a \leq n$ für alle $n \in A$. Sei nun $m \in M$. Dann gilt $m < n$ und damit $m + 1 \leq n$ für alle $n \in A$. Es folgt $m + 1 \in M$, da ansonsten $m + 1 \in A$ und $m + 1 =: a \leq n$ für alle $n \in A$.

Damit sind die Voraussetzungen von (N3) gezeigt und es folgt $M = N$. Wegen $A \neq \emptyset$, existiert mindestens ein $n \in A$. Aus $n \in A \subseteq N = M$ erhalten wir $n < n$ und deshalb mit Satz 9.11(ii) einen Widerspruch. Also war unsere Annahme falsch. Damit haben wir die Existenz eines minimalen Elementes $\min(A) \coloneqq a \in A$ bewiesen. Sei $b \in A$ ein weiteres minimales Element. Dann folgen aus $a, b \in A$ und der Minimalitätseigenschaft die Abschätzungen $b \leq a$ und $a \leq b$. Mit Satz 9.11(iv) folgt die Gleichheit $b = a$, d.h. das minimale Element ist eindeutig. □

Bemerkung 9.13. *Von nun an können, werden und sollen wir wieder $\mathbb{N}$ schreiben für die aus der Schule bekannten natürlichen Zahlen. Ferner können und werden wir die Arithmetik und die Ordnung mit ihren bekannten Rechenregeln verwenden.*