Was ist eigentlich Mathematik?

Vorkurs Mathematik, ETH Zürich

Hrvoje Krizic

2025

Vorwort

Dieses Skript behandelt die Methoden mathematischer Beweisführung, einschliesslich direkter Beweise, Widerspruchsbeweise, Induktion und Kontraposition. Die dargelegten Erläuterungen und Beispiele sollen den Übergang von der Gymnasium-Mathematik zur anspruchsvolleren Universitätsmathematik erleichtern. Als ergänzendes Material begleitet es die beiden Mathematik-Vorlesungen während der Vorkurswoche an der ETH Zürich im September 2025. Ein grosser Dank geht an Stefan Zentarra, der einen Grossteil des ersten Kapitels verfasst hat.

Version vom 10. August 2025

1

Grundlagen

1.1 Mengen

Bevor wir mit der „richtigen“ Einführung beginnen, müssen wir den Begriff der Menge kennenlernen und einige Notationen definieren. All diese Definitionen werden wir in den weiteren Kapitel verwenden (vor allem dann im Kapitel über Relationen).
Unter einer **Menge** verstehen wir in der Mathematik eine Sammlung an Elementen, welche etwa Zahlen oder Funktionen sein können. Die am häufigsten benutzten Mengen sind die sogenannten **Zahlenmengen**:

$$\begin{aligned}
&\mathbb{N} := \{(0,)1, 2, 3, ...\} \\
&\mathbb{Z} := \{..., -2, -1, 0, 1, 2, ...\} \\
&\mathbb{Q} := \{..., -\frac{5}{2}, ..., -\frac{1}{6}, ..., 0, ..., \frac{1}{4}, ...\} \\
&\mathbb{R} := \{..., -\sqrt{2}, ..., -\frac{1}{2}, ..., e, ..., \pi, ...\}
\end{aligned}$$

Später werden wir noch die komplexen Zahlen $\mathbb{C}$ einführen. Jede natürliche Zahl ist auch eine ganze Zahl, und jede ganze Zahl ist eine rationale. Wir schreiben

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

wobei wir (für zwei Mengen A und B) $A \subset B$ schreiben, falls jedes Element aus A auch in B enthalten ist. A ist eine sogenannte **Teilmenge** von B. Ist ein Element x in einer Menge A enthalten, so schreiben wir $x \in A$. Mengen lassen sich auch durch Eigenschaften beschreiben. Wollen wir die Menge A als die Menge definieren, welche alle geraden Zahlen enthält, so schreiben wir

$$A = \{x \in \mathbb{Z} \mid x \text{ gerade}\},$$

oder aber auch

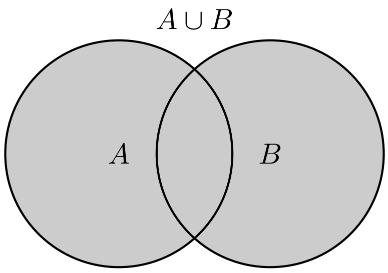
$$A = \{2k, k \in \mathbb{Z}\}.$$

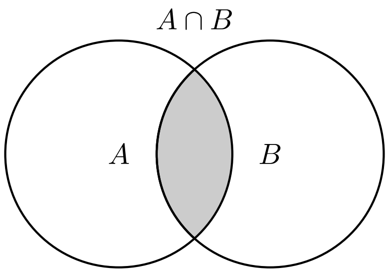
Wir führen nun noch zwei weitere Begriffe ein:

1. Eine **Vereinigung** von zwei Mengen A und B bezeichnet die Menge, welche alle Elemente aus A und alle Elemente aus B enthält. Wir schreiben $A \cup B$. Beispielsweise ist $\{3, 4, 5\} \cup \{-2, -1, 0, 1\} = \{-2, -1, 0, 1, 3, 4, 5\}$.

2. Der **Durchschnitt** zweier Mengen ist die Menge, welche nur die Elemente enthält, die in beiden Mengen vorkommen. Wir schreiben $A \cap B$. Ein Beispiel ist $\{1,3,5,7\} \cap \{1,2,3\} = \{1,3\}$.

Die beiden Begriffe lassen sich mit sogenannten Venn-Diagrammen leicht visualisieren.





Die Menge ohne Elemente (**leere Menge**) bezeichnen wir mit $\emptyset$ oder $\{\}$. Sind nun $X_1, X_2, ..., X_n$ Mengen, so definieren wir das **direkte Produkt** dieser n Mengen als

$$X_1 \times X_2 \times ... \times X_n := \{(x_1, ..., x_n) \,|\, x_i \in X_i\}$$

Das direkte Produkt von n Mengen ist also die Menge aller (geordneten) n-Tupel bestehend aus diesen Mengen. Sei beispielsweise $X = \{1,2\}$ und $Y = \{3,4\}$. Dann ist

$$X \times Y = \{(1,3),(1,4),(2,3),(2,4)\}.$$

Im Anhang sind noch weitere wichtige mathematische Symbole aufgelistet, welche wir im Verlauf dieses Skriptes antreffen werden.

1.2 Eine Einführung: Nullstellen von Polynomen

Betrachte die Funktion

$$f(x) = x^2 - x - 6\,. \tag{1.1}$$

Diese Funktion ist ein Polynom zweiten Grades[1] und damit eine typische Funktion aus der Schulzeit. Eine typische Fragestellung aus der Schulzeit wäre zum Beispiel die nach den Null-

[1]Polynome sind Funktionen der Form

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x^1 + a_0 = \sum_{i=0}^{n} a_i x^i\,, \tag{1.2}$$

wobei $a_n \neq 0$. Das Summenzeichen $\sum$ ist eine Abkürzung der linken Summe über $n+1$ Terme. Wir nennen dann n den Grad des Polynoms $f(x)$. Es ist der grösste auftauchende Exponent der Variable x.

stellen dieses Polynoms, also die Lösungen der Gleichung

$$0 = x^2 - x - 6\,. \tag{1.3}$$

Beispiel. Berechnung der Nullstellen von $f(x) = x^2 - x - 6$:
Wir nutzen die bekannte „Mitternachtsformel", die besagt, dass die Lösungen einer quadratischen Gleichung $0 = ax^2 + bx + c$ durch

$$x_{1,2} = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a} \tag{1.4}$$

gegeben sind. Hier erhalten wir

$$x_1 = \frac{-(-1) + \sqrt{(-1)^2 - 4 \cdot 1 \cdot (-6)}}{2 \cdot 1} = \frac{1 + \sqrt{25}}{2} = 3\,, \tag{1.5}$$

$$x_2 = \frac{-(-1) - \sqrt{(-1)^2 - 4 \cdot 1 \cdot (-6)}}{2 \cdot 1} = \frac{1 - \sqrt{25}}{2} = -2\,. \tag{1.6}$$

Demnach sind die Nullstellen von $f(x)$ gerade bei $x_1 = 3$ und $x_2 = -2$.

Wir sehen: diese Fragestellung fordert eine Berechnung. Wir erhalten die explizite Antwort für ein spezifisches Problem.

Die Herangehensweise der Mathematik in der Universität ist eine vollkommen andere. Wir sind nur selten an der expliziten Lösung eines spezifischen mathematischen Problems interessiert. Stattdessen sind allgemeinere Fragen und Aussagen für uns relevant.

Beispiel. Mathematische Fragen zu Nullstellen von Polynomen:

- Wie viele Nullstellen hat ein Polynom von Grad n?
- Gibt es ein Kriterium, wann Polynome keine Nullstellen haben?
- Funktioniert die „Mitternachtsformel" immer? Warum?
- Gibt es Lösungsformeln auch für höhere Grade?
- Wie kann man Nullstellen numerisch optimal approximieren?
- ...

Diese Fragen sind wesentlich interessanter, da sie nicht nur Informationen über ein spezielles Polynom liefern. Stattdessen betrachten wir Eigenschaften, die alle Polynome erfüllen. Insbesondere können wir die Antworten zu diesen Fragen (sofern wir sie finden können) auf jedes spezielle Polynom anwenden.

Der Preis der Allgemeinheit ist allerdings, dass die Fragen, denen wir hier nachgehen, um ein Vielfaches komplizierter sind. Antworten auf manche, der oben genannten Fragen erfordern mehrere Semester Mathematikstudium und sind teils das Ergebnis von Jahrhunderte langer Forschung.

Aber nicht nur die Fragestellungen der Mathematik an der Universität sind anders zu denen aus der Schule. Auch die Methodiken - und damit die Form der Antworten - sind anders. Da die Fragestellungen sehr viel allgemeiner sind, müssen dies die Antworten auf diese Fragen ebenfalls sein. Explizite Berechnungen sind daher üblicherweise nicht ausreichend. An deren Stelle tritt das Konzept des **mathematischen Beweises**: Eine Kette logischer Schlussfolgerungen, die eine mathematische Behauptung begründet.

Betrachten wir als Beispiel die erste Frage in der obigen Liste: „Wie viele Nullstellen hat ein Polynom von Grad n?“ Eine teilweise Antwort auf diese Frage liefert die folgende mathematische Behauptung. Wir nennen eine solche Behauptung, deren Korrektheit nachgewiesen ist, einen **mathematischen Satz**.

Satz. Ein Polynom vom Grad $n \in \mathbb{N}$ hat maximal n Nullstellen.

Beweis. Wird in den Übungsaufgaben am Dienstag bewiesen. □

Üblicherweise werden wir die Korrektheit eines Satzes immer direkt auch mittels eines mathematischen Beweises nachweisen. Hier verschieben wir das ausnahmsweise, da wir zunächst Beweismethoden erlernen müssen.

Mithilfe des obigen Satzes können wir nun die Frage nach den Nullstellen von $f(x) = x^2 - x - 6$ im Stile der Universität beantworten:

Satz. Zeige, dass $x_1 = 3$ und $x_2 = -2$ die einzigen Nullstellen von $f(x) = x^2 - x - 6$ sind.

Beweis. Wir prüfen nach mit direktem Einsetzen der vermeintlichen Nullstellen:

$$f(-3) = 3^2 - 3 - 6 = 0\,, \tag{1.7}$$
$$f(2) = (-2)^2 - (-2) - 6 = 0\,. \tag{1.8}$$

Demnach sind x_1 und x_2 Nullstellen von $f(x)$. Dass diese auch die einzigen Nullstellen von $f(x)$ sind, folgt aus vorherigem Satz, denn $f(x)$ ist ein Polynom vom Grad 2 und hat demnach maximal 2 Nullstellen. □

1.3 Mathematische Aussagen

Nicht jede sprachliche Aussage eignet sich als mathematische Behauptung. Einer mathematischen Behauptung muss ein eindeutiger Wahrheitswert - entweder wahr oder falsch - zugewiesen werden können. Zudem muss die Aussage in sich selbst widerspruchsfrei sein. Wir definieren also:

Definition. Eine **Aussage** im mathematischen Sinn ist eine Feststellung, deren Wahrheitsgehalt stets mit „wahr" oder „falsch" angegeben werden kann.

Beispiel.

Aussage	mathematische Behauptung?	Begründung
„$\sin(x)$ ist eine interessante Funktion."	$\times$	„interessant" ist subjektiv
„Die Ableitung von $\sin(x)$ ist $\cos(x)$."	$\checkmark$	Aussage ist wahr
„Die Menge aller Mengen die sich nicht selbst enthalten, enthält sich selbst."	$\times$	widersprüchlich[2]
„Hoffentlich ist 17 eine Primzahl."	$\times$	unspezifisch
„Es ist $\int_0^1 x^2 \,\mathrm{d}x = 1$."	$\checkmark$	Aussage ist falsch
„Es gibt unendlich viele Paare von Primzahlen mit Differenz von zwei."	$\checkmark$	Wahrheitswert derzeit unbekannt, aber eindeutig

Man beachte, dass auch falsche oder unbewiesene Aussagen als mathematische Behauptungen dienen können. Wichtig ist eben nur, dass diese entweder eindeutig wahr oder eindeutig falsch sind. Unabdingbar dafür ist es, dass die verwendeten Begriffe eindeutig definiert sind. Daher ist es ein wichtiger Teil der Mathematik, mathematische Konzepte und Objekte eindeutig zu definieren. Oftmals ist die Struktur einer Mathematikvorlesung Definition - Satz - Beweis. Dabei wird in der Definition ein neuer mathematischer Begriff eingeführt, im Satz eine damit verbundene Eigenschaft behauptet und die Richtigkeit dieser Aussage dann im folgenden Beweis nachgewiesen. Wir haben weiter oben (beispielsweise in Fussnote 1) bereits ein Beispiel für eine formelle Definition gesehen. Ein anderes Beispiel ist folgende Definition:

Definition. Sei $n \in \mathbb{N}$ eine natürliche Zahl[3]. n heisst **gerade**, falls es ein $k \in \mathbb{N}$ gibt mit $n = 2k$. Eine natürliche Zahl $n \in \mathbb{N}$ heisst **ungerade**, falls $(n + 1)$ gerade ist.[4]

Es sei angemerkt, dass man auf fast identische Weise Teilbarkeit durch Zahlen $m > 2$ definieren kann. Nämlich ist $n \in \mathbb{N}$ durch $m \in \mathbb{N}$ teilbar, falls es ein $k \in \mathbb{N}$ gibt, sodass $n = mk$. Beachte, dass sich für $m = 2$ obige Definition ergibt.

[2]Der Unvollständigkeitssatz von Gödel suggeriert, dass solche widersprüchlichen Aussagen Teil der Mathematik sein können. Wir möchten uns hier aber auf binäre Logik beschränken, die nur die Wahrheitswerte wahr und falsch kennt.

[3]Ist A eine Menge, so bezeichnet $a \in A$, dass a ein Element der Menge A ist. Siehe hierzu den Anhang A.

[4]Dies impliziert direkt, dass für ungerade Zahlen $n \in \mathbb{N}$ ein $\tilde{k} \in \mathbb{N}$ existiert, sodass $n = 2\tilde{k} + 1$.

Bevor wir zum wichtigen Thema des Beweises kommen, ist es an dieser Stelle hilfreich, ein paar Begriffe aus der Aussagenlogik zu besprechen. Die Aussagenlogik ist Teil der Disziplin der formalen Logik, die sich mit der Formalisierung von logischen Folgerungen beschäftigt. Wir beginnen mit folgender Definition:

Definition. Sei A eine mathematische Aussage. Dann bezeichnen wir mit $\neg A$ die Verneinung dieser Aussage. Ist A wahr, so ist $\neg A$ falsch und umgekehrt.

Wir können den Zusammenhang zwischen den Aussagen A und $\neg A$ auch in einer sogenannten **Wahrheitstafel** darstellen (siehe rechts). Wir schreiben w für „wahr" und f für „falsch". Dabei wird der Wahrheitswert von $\neg A$ für alle möglichen Wahrheitswerte von A beschrieben. Dies definiert den Operator $\neg$ eindeutig.

A	$\neg A$
w	f
f	w

Es gibt vier weitere wichtige logische Operatoren, die wir in der Mathematik oft verwenden. Diese sind zweiwertige Operatoren, also verknüpfen zwei mathematische Aussagen.

Definition. Seien A und B mathematische Aussagen. Wir definieren die Operatoren „oder" ($\vee$), „und" ($\wedge$), „impliziert" ($\Rightarrow$) und „ist äquivalent zu" ($\Leftrightarrow$) mittels folgender Wahrheitstafel:

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

Von besonderer Bedeutung ist dabei die Implikation $A \Rightarrow B$. Sie besagt, dass wenn eine Aussage A wahr ist, dass dann B ebenfalls wahr sein muss. Falls A falsch ist, kann B entweder wahr oder falsch sein. Viele mathematische Sätze haben die Struktur „Voraussetzung $\Rightarrow$ Aussage", also besagen, dass eine Aussage unter bestimmten Voraussetzungen gilt. Man beachte, dass die Aussage auch dann wahr sein kann, wenn die Voraussetzungen nicht erfüllt sind. Ein Beispiel ist folgender Satz:

Satz. Ist eine natürliche Zahl $n \in \mathbb{N}$ gerade, so ist auch deren Quadrat n^2 gerade.

Beweis. Um nachzuweisen, dass die Aussage des Satzes korrekt ist, müssen wir zeigen, dass die Aussage $A \Rightarrow B$ immer wahr ist (dabei ist im konkreten Fall $A =$ „n ist gerade" und

$B =$ „n^2 ist gerade“). Gemäss der Wahrheitstafel in der vorherigen Definition ist aber $A \Rightarrow B$ ohnehin nur dann falsch, wenn A wahr und B falsch ist. Dieser Fall ist genau der, der unserer naiven Vorstellung von „Implikation“ widersprechen würde.[5] Denn wenn A wahr ist und A auch B impliziert, so muss dann B wahr sein. Daher ist lediglich nachzuweisen, dass wenn A wahr ist, dann auch B wahr ist.

Nehmen wir also an, dass A wahr ist, also dass n eine gerade natürliche Zahl ist. Demnach ist also definitionsgemäss $n = 2k$ für ein $k \in \mathbb{N}$. Dann ist aber $n^2 = (2k)^2 = 2\,(2k^2) = 2\ell$ (mit $\ell = (2k^2)$) ebenfalls gerade. Daher ist B ebenfalls wahr. $\square$

1.4 Direkte Beweise

Im vorherigen Beweis haben wir einen sogenannten **direkten Beweis** durchgeführt. Wir haben angenommen, dass die Voraussetzung $A =$ „n ist gerade“ wahr ist, und nachgewiesen, dass dann die Folgerung $B =$ „n^2 ist gerade“ ebenfalls wahr ist. Wir werden im nächsten Kapitel noch andere Beweismethoden kennenlernen. Diese beruhen darauf, dass man $A \Rightarrow B$ in eine logisch äquivalente Aussage umformt und dann diese Aussage beweist. Eine solche Umformung macht manchmal einen Beweis um ein Vielfaches einfacher, gelegentlich sogar erst möglich.

Direkte Beweise bestehen üblicherweise aus einer Kette von logischen Implikationen. Es gilt nämlich Folgendes:

Satz. Die Aussage $((A \Rightarrow C) \wedge (C \Rightarrow B)) \Rightarrow (A \Rightarrow B)$ ist wahr für alle Aussagen A, B und C.

Beweis. Wir führen den Beweis mittels einer Wahrheitstafel durch:

[5] In der Tat, man kann mittels einer Wahrheitstafel nachweisen, dass $A \Rightarrow B$ äquivalent zu $(\neg A) \vee B$ ist. Dass die Implikation definitionsgemäss immer wahr ist, wenn A falsch ist, entspricht ebenfalls unserem Sprachgebrauch. Dazu ein anschauliches Beispiel: „Wenn es regnet (A), ist die Strasse nass (B).“ Diese Implikation $A \Rightarrow B$ ist wahr. Wenn es aber nun nicht regnet ($\neg A$), kann die Strasse entweder nass sein (B) oder eben nicht ($\neg B$). Vielleicht hat es ja früher geregnet oder es gab ein Leck in einer Wasserleitung. Die Implikation ist trotzdem wahr, auch wenn A falsch ist. Dies wird häufig zusammengefasst als „Aus einer falschen Aussage kann man alles folgern.“ Nämlich ist die Implikation $\mathsf{f} \Rightarrow C$ für jede beliebige Aussage C wahr. Ein Beispiel: „Wenn 4 eine Primzahl ist, dann ist 3 gerade.“ ist eine wahre Aussage. Aber 4 ist eben keine Primzahl, daher kommt diese Implikation nie zur Anwendung.

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

Die zu betrachtende Aussage ist, dass die Aussage in der rechten Spalte die Aussage in der vierten Spalte impliziert. Das heisst, in Fällen, in denen die Aussage in der rechten Spalte wahr ist, muss auch die Aussage in der vierten Spalte wahr sein. Dies ist in der Tat der Fall, daher ist $((A \Rightarrow C) \wedge (C \Rightarrow B)) \Rightarrow (A \Rightarrow B)$ immer wahr. $\square$

Wir schreiben auch kurz $A \Rightarrow C \Rightarrow B$ für $((A \Rightarrow C) \wedge (C \Rightarrow B))$. Diese Kette kann natürlich auch beliebig verlängert werden, indem man diesen Satz iterativ anwendet. Idealerweise besteht ein direkter Beweis dann aus einer Vielzahl sehr einfacher Implikationen, von der jede ohne weitere Erläuterung „offensichtlich" wahr ist. Zusammengenommen ergeben diese Implikationen dann aber eine gegebenenfalls sehr komplizierte Implikation. Ein Beispiel:

Satz. Ist $n \in \mathbb{N}$ gerade, so ist $(n^2+1)^2$ ungerade.

Beweis. Wir haben bereits bewiesen, dass für gerade natürliche Zahlen n auch deren Quadrat n^2 gerade ist. Ist n^2 gerade, so ist aber n^2+1 ungerade. Ist nämlich $n^2 = 2k$, so ist $n^2+1 = 2k+1$. Folglich kann n^2+1 nicht als 2ℓ mit $\ell \in \mathbb{N}$ geschrieben werden, denn Division von n^2+1 durch 2 ergibt Rest 1.
Wir nutzen nun, dass $n^2+1 = 2k+1$ mit $k \in \mathbb{N}$ wie wir gerade gezeigt haben. Dann ist $(n^2+1)^2 = (2k+1)^2 = 4k^2+4k+1$. Division dieser Zahl durch 2 ergibt Rest 1, was, wie zuvor, zeigt, dass diese Zahl ungerade ist. Damit ist die Aussage bewiesen. $\square$

Man beachte, dass wir im Beweis die Aussage „n ist gerade" und „n^2 ist gerade" jeweils nur im darauffolgenden Schritt verwendet haben. In der Praxis sind die Argumente und logische Schlussfolgerungen in Beweisen oftmals natürlich etwas komplizierter. Die Kette logischer Folgerungen kann zum Beispiel verzweigt sein. Eventuell müssen aus einer Aussage mehrere Folgerungen gezogen werden, die dann kombiniert die gewünschte Aussage ergeben. Um beispielsweise zu zeigen, dass für $n \in \mathbb{N}$ gerade, auch n^2+n^3 eine gerade Zahl ist, könnte man erst zeigen, dass dann n^2 und n^3 gerade sind. Anschliessend weist man nach, dass die Summe zweier gerader Zahlen gerade ist und die Aussage folgt.

In anderen Beweisen müssen verschiedene Fälle unterschieden werden. Eine solche **Fallunterscheidung** ist zum Beispiel in folgendem Satz hilfreich:

Satz. Für alle natürlichen Zahlen $n \in \mathbb{N}$ ist $\frac{n(n+1)}{2} \in \mathbb{N}$.

Beweis. Wir betrachten zwei Fälle:

1. n ist gerade: Ist n gerade, so gilt $n = 2k$ für ein $k \in \mathbb{N}$ per Definition. Daher ist dann $\frac{n(n+1)}{2} = \frac{2k(n+1)}{2} = k(n+1)$ eine natürliche Zahl.
2. n ist ungerade: In diesem Fall verwenden wir, dass falls n ungerade ist, dann ist $(n+1)$ gerade. Ist n nämlich ungerade, so gibt es kein k sodass $n = 2k$. Demnach ergibt Division von n durch 2 Rest 1, also $n = 2\ell + 1$ für ein $\ell \in \mathbb{N}$. Dann ist aber $n + 1 = 2\ell + 2 = 2\underbrace{(\ell + 1)}_{=m\in\mathbb{N}}$ gerade. Folglich ist $\frac{n(n+1)}{2} = \frac{n(2m)}{2} = nm \in \mathbb{N}$.

In beiden Fällen ist die Aussage $\frac{n(n+1)}{2} \in \mathbb{N}$ wahr, und da alle natürlichen Zahlen entweder gerade oder ungerade sind, gilt diese Aussage also für alle $n \in \mathbb{N}$. $\square$

Eine Art von Fallunterscheidung ist es zu zeigen, dass zwei Aussagen äquivalent ($\Longleftrightarrow$) sind. Wir zeigen in diesem Fall fast immer die beiden Richtungen $A \Longrightarrow B$ und $B \Longrightarrow A$ separat.[6] Wir machen ein Beispiel:

Satz. Sei $a \in \mathbb{N}$ durch $p \in \mathbb{N}$ teilbar. Dann gilt für $b \in \mathbb{N}$:

$$a + b \text{ teilbar durch } p \iff b \text{ teilbar durch } p.$$

Beweis. Die Aussage $A \Longleftrightarrow B$ ist äquivalent zur Aussage $(A \Longrightarrow B) \wedge (B \Longrightarrow A)$. Wir beweisen also die beiden Richtungen separat. Die Voraussetzung gilt für beide Richtungen: es existiert also ein $m \in \mathbb{N}$ sodass $a = m \cdot p$.

1. $A \Longrightarrow B$: Wir nehmen an, dass $a + b$ durch p teilbar ist. Dann muss ein $r \in \mathbb{N}$ mit

[6] Diese Art von Fallunterscheidung gibt es auch bei der Äquivalenz von zwei Mengen oder Funktionen. Als Beispiel: wir möchten zeigen, dass $A = B$, wobei A und B zwei Mengen sind. Wir zeigen dann zuerst, dass A eine Teilmenge von B ist (also $A \subseteq B$) und dann, dass B eine Teilmenge von A ist ($B \subseteq A$). Sind beide Mengen jeweils Teilmengen von der anderen Menge, dann muss $A = B$ gelten. Wieso machen wir das so? Ganz einfach: um zu zeigen, dass A eine Teilmenge ist von B können wir einfach ein beliebiges Element von A wählen und zeigen, dass dieses Element (unabhängig von der Wahl aus A) auch in B enthalten sein muss.

$r > m$ existieren[7], sodass $a+b = r \cdot p$. Wir verwenden die Voraussetzung und schreiben

$$\begin{aligned} a+b = r \cdot p \implies b &= r \cdot p - a \\ &= r \cdot p - m \cdot p \\ &= (r-m) \cdot p \end{aligned}$$

Wir definieren $n := r - m \in \mathbb{N}$ und erhalten somit $b = n \cdot p$ durch p teilbar.

2. $B \implies A$: Wir nehmen nun an, dass b durch p teilbar ist und somit existiert ein $n \in \mathbb{N}$ sodass $b = n \cdot p$. Es gilt

$$a + b = m \cdot p + n \cdot p = (m+n) \cdot p$$

und da $(m+n) \in \mathbb{N}$ ist $a+b$ auch durch p teilbar.

Aus dem Beweis der beiden Richtungen folgt die Äquivalenz. $\square$

[7]Wir nehmen im gesamten Beweis/Satz an, dass $\mathbb{N} := \mathbb{N} \setminus \{0\}$. Die Aussage folgt also aus $b > 0$ und somit $a + b > a$

2

Beweismethoden

2.1 Kontraposition

In der Mathematik möchten wir häufig Aussagen der Form

$$A \implies B \tag{2.1}$$

beweisen. Wir können diese Aussage mit einem direkten Beweis zeigen. Eine andere Möglichkeit wäre es, die folgende Implikation zu betrachten:

$$\neg B \implies \neg A. \tag{2.2}$$

Wir nennen dies eine **Kontraposition**. Es lässt sich mit Aussagenlogik[8] zeigen, dass diese Aussage äquivalent ist zur Aussage $A \implies B$. Wenn man also die Kontraposition 2.2 bewiesen hat, so hat man auch die Implikation 2.1 selber bewiesen. Ein Beispiel bieten die Aussagen „die Studierenden sind alle älter als 20“ (Aussage A) und „alle Studierenden sind volljährig“ (Aussage B). Man beachte, dass hier nur $A \implies B$ gilt, aber nicht unbedingt $B \implies A$, da man mit 18 und 19 auch volljährig ist. Die Kontraposition zu dieser Aussage ist dann $\neg B \implies \neg A$, also dass die Aussage „nicht alle Studierenden sind volljährig“ die Aussage „es gibt Studierende, die jünger sind als 20“ impliziert. Die Aussagen sind äquivalent. Wir fassen zusammen:

Methode. Beweis durch Kontraposition, dass $A \implies B$ gilt.

1. Man negiert die Aussagen A und B und erhält somit $\neg A$ und $\neg B$.
2. Mithilfe einer anderen Beweismethode (meist ein direkter Beweis) soll nun gezeigt werden, dass $\neg B \implies \neg A$ gilt.

[8] $A \implies B$ ist äquivalent zur Aussage $\neg A \vee B$. Damit ist $\neg B \implies \neg A$ in Aussagenlogik $\neg(\neg B) \vee \neg A$. Dies entspricht aber genau $B \vee \neg A$ und somit sind die zwei Implikationen äquivalent.

Wir beweisen nun einen mathematischen Satz:

Beispiel. Man beweise folgenden Satz:

Für alle natürlichen Zahlen $n \in \mathbb{N}$ gilt: ist n^2 gerade, dann ist n gerade.

Beweis. Der Satz hat die Form einer Implikation $A \implies B$ mit

$$\underbrace{n^2 \text{ ist gerade}}_{=A} \implies \underbrace{n \text{ ist gerade}}_{=B}. \tag{2.3}$$

Wir beweisen diesen Satz durch Kontraposition. Dazu müssen wir die Aussagen A und B negieren und die Richtung der Implikation wechseln. Die Negation der Aussagen sind

$$\neg A = \neg(n^2 \text{ ist gerade}) = n^2 \text{ ist ungerade}$$
$$\neg B = \neg(n \text{ ist gerade}) = n \text{ ist ungerade}$$

und somit erhalten wir die Kontraposition $\neg B \implies \neg A$, beziehungsweise

$$n \text{ ist ungerade} \implies n^2 \text{ ist ungerade.} \tag{2.4}$$

Diese Aussage kann dann mit einem direkten Beweis bewiesen werden. Sei also n eine ungerade Zahl. Dann existiert ein $k \in \mathbb{N}$, sodass $n = 2k + 1$. Damit ist

$$n^2 = (2k+1)^2 = 4k^2 + 4k + 1 = 2 \cdot \underbrace{(2k^2 + 2k)}_{=:m} + 1 = 2m + 1, \tag{2.5}$$

wobei wir bemerken müssen, dass $m := 2k^2 + 2k \in \mathbb{N}$ eine natürliche Zahl ist, da $k \in \mathbb{N}$ gilt. Es folgt die Kontraposition und damit die Aussage. □

Wir bemerken hier, dass der direkte Beweis dieser simplen Aussage gar nicht so einfach ist. Beim direkten Beweis beginnen wir bei n^2 und möchten dann etwas für n schlussfolgern. Es ist deutlich einfacher Information von n zu verwenden, um daraus eine Information von n^2 zu gewinnen, als umgekehrt. Nun ein etwas schwierigeres Beispiel:

Beispiel. Beweise folgenden Satz:

Sei $x, y \in \mathbb{R}$. Wenn $y^3 + yx^2 \leq x^3 + xy^2$, dann gilt $y \leq x$.

Bemerkung: Dieser Satz lässt sich auch direkt beweisen (Siehe dazu das Aufgabenblatt vom Montag).

Beweis. Beweis durch Kontraposition: Wir nehmen an, dass $y > x$. Dann gilt $y - x > 0$. Wir multiplizieren beide Seiten mit $x^2 + y^2$ (offensichtlich positiv):

$$\begin{aligned} (y-x)(x^2+y^2) &> 0 \\ yx^2 + y^3 - x^3 - xy^2 &> 0 \\ y^3 + yx^2 &> x^3 + xy^2. \end{aligned} \tag{2.6}$$

Somit gilt $y^3 + yx^2 > x^3 + xy^2$ und $y^3 + yx^2 \leq x^3 + xy^2$ ist nicht wahr. □

2.2 Widerspruchsbeweis

Wir haben im letzten Abschnitt gezeigt, dass $A \implies B$ äquivalent ist zur Aussage $\neg B \implies \neg A$. Es gibt auch noch eine weitere Aussage welche äquivalent ist: $\neg(A \wedge \neg B)$[9]. Das $\wedge$ in der Aussagenlogik ist das „und" in der deutschen Sprache. Was bedeutet nun diese Aussage genau? Man nimmt an, dass die Aussage A richtig ist und man nimmt an, dass die Aussage B falsch ist. Wenn wir nun zeigen können, dass diese beiden Annahmen durch logisches Schlussfolgern zu einem **Widerspruch** führen, so ist die Implikation $A \implies B$ bewiesen. Zusammengefasst können wir also folgendes tun:

Methode. Widerspruchsbeweis von $A \implies B$

1. Man negiert zunächst die Aussage B und erhält $\neg B$.
2. Wir nehmen nun an, dass $\neg B$ und A beide wahr sind und führen dies durch logisches Schlussfolgern zu einem Widerspruch.

Man beachte, dass die Implikation nur eine Art von mathematischen Sätzen ist. Wir werden aber Beispiele sehen, wo wir einfach nur eine Aussage A beweisen müssen. Dazu nehmen wir $\neg A$ an und führen dies zu einem Widerspruch. Trotzdem: es lassen sich sehr viele mathematische Sätze in die Form $A \implies B$ bringen.

Beispiel. Seien m und n natürliche Zahlen und sei $m \cdot n$ ungerade. Beweise, dass dann sowohl m als auch n ungerade sind.

Beweis. Wir beweisen die Implikation per Widerspruch. Sei also $m \cdot n$ ungerade und o.B.d.A.[10]

[9] Für Implikationen lässt es sich zeigen (siehe dazu die „De Morganschen Gesetze" weiter unten), dass $\neg A \vee B$ äquivalent ist zu $\neg(A \wedge \neg B)$. Ohne dies wirklich zu beweisen, können wir dies auch logisch schlussfolgern, denn wenn nicht A und $\neg B$ gleichzeitig gelten, dann ist entweder A falsch oder B wahr.

[10] o.B.d.A: ohne Beschränkung der Allgemeinheit. Da das Problem in n und m symmetrisch ist, könnten wir auch n als gerade annehmen. Der Beweis wäre aber genau gleich. Daher dürfen wir o.B.d.A. schreiben und ersparen uns das wiederholen des Beweises.

m gerade ($\neg B$). Dann können wir $m = 2 \cdot k$ mit $k \in \mathbb{Z}$ schreiben. Somit gilt $m \cdot n = 2k \cdot n = 2 \cdot (k \cdot n)$ und somit ist $m \cdot n$ gerade. Ein Widerspruch zu unserer Annahme. □

Wir schon vorhin erwähnt, können wir bei einem Satz der keine Implikation ist, die Negation zu einem Widerspruch führen. Eines der berühmtesten Beispiele eines Widerspruchsbeweises ist der folgende Satz über Primzahlen.

Beispiel. Man beweise folgenden Satz:

Es existieren unendlich viele Primzahlen.

Beweis. Bevor wir den Widerspruchsbeweis durchführen, möchten wir kurz die Definition der Primzahlen wiederholen:

Definition. Eine Primzahl p ist eine natürliche Zahl, die genau zwei Teiler hat.

Wir beweisen nun per Widerspruch, dass unendlich viele dieser Primzahlen existieren. Angenommen, es gibt also nur endlich viele Primzahlen; sei N die Anzahl dieser Primzahlen. Wir können dann, weil wir die Menge an Primzahlen als endlich angenommen haben, eine aufsteigende vollständige Liste unserer Primzahlen machen: $p_1 = 2$, $p_2 = 3$, $p_3 = 5 ...$, bis p_N. Wir bilden nun das Produkt[11] dieser Primzahlen:

$$P := \prod_{k=1}^{N} p_k = p_1 \cdot p_2 \cdot p_3 \cdot ... \cdot p_{N-1} \cdot p_N. \tag{2.7}$$

Offensichtlich ist P durch jede unserer Primzahlen teilbar. Dann ist die Zahl $P+1$ durch keine Primzahl teilbar, da die 1 nur durch sich selber und damit durch keine Primzahl teilbar ist[12]. Also muss $P+1$ prim sein. Da ausserdem $P+1 > p_N$ gilt, erhalten wir einen Widerspruch, da wir angenommen haben, dass unsere geordnete Liste vollständig ist. □

Der Satz wird auch „Satz von Euklid“ genannt, da dieser den Satz im dritten Jahrhundert v. Chr. als Erster bewiesen hat. Da damals das Konzept der „Unendlichkeit“ noch nicht bekannt war, formulierte Euklid den Satz wie folgt: „Es gibt mehr Primzahlen als jede vorgelegte Anzahl von Primzahlen“.

Beispiel. Jule hat zehn Karten, die durchnummeriert sind von 1 bis 10. Sie wählt nun 6 Karten aus. Beweise, dass zwei der 6 gezogenen Karten zusammenaddiert 11 ergeben.

[11] Zur Abkürzung des Produktes von n Faktoren verwendet man das griechische Symbol Π („Pi“), ähnlich wie bei einer Summe von n Faktoren das griechische Symbol Σ („Sigma“) gebraucht wird

[12] Siehe hierzu den letzten Satz aus dem ersten Kapitel.

Beweis. Wir beweisen die Aussage mit einem Widerspruchsbeweis. Wir nehmen also an, dass die Karten paarweise summiert nie 11 ergeben. Die 10 zur Verfügung stehenden Karten lassen sich in 5 Mengen[13] unterteilen:

$$\{1, 10\},\ \{2, 9\},\ \{3, 8\},\ \{4, 7\} \text{ und } \{5, 6\}. \tag{2.8}$$

In jeder dieser Mengen befinden sich zwei Zahlen, welche zusammenaddiert 11 ergeben. Da wir nun 6 Karten ziehen und kein Pärchen entstehen darf, dessen Summe 11 ergibt, müssen wir alle 6 aus verschiedenen Mengen ziehen. Da wir aber nur 5 Mengen haben ist dies unmöglich und somit ein Widerspruch zur Aussage, dass zwei Zahlen nie zusammenaddiert 11 ergeben. □

Das Prinzip, einen Widerspruch zu finden indem man m Objekte (in unserem Fall die Karten) auf n Mengen ($n < m$) zu verteilen versucht, nennt sich das **Schubfachprinzip**:

Satz. Seien m verschiedene Objekte in n disjunkte[14] Kategorien eingeteilt. Wenn $m > n$ ist, so gibt es mindestens eine Kategorie, die mindestens zwei Objekte enthält.

Ein Beispiel: In Zürich leben mindestens zwei Personen, die die gleiche Anzahl Haare haben. Der Beweis dafür folgt aus dem Schubfachprinzip: in Zürich leben ungefähr 400'000 Menschen, während wir auf dem Kopf zwischen 100'000 und 200'000 Haare haben. Unsere Kategorien sind also die Anzahl Haare und unsere Objekte sind die Menschen.

Beispiel. Mara stellt fest, dass immer, wenn sie 7 ganze Zahlen auswählt, es in ihrer Sammlung immer ein Tripel von Zahlen a, b und c gibt, bei denen alle Zahlen voneinander um ein Vielfaches von 3 abweichen. Man beweise Maras Vermutung.

Beweis. Es gibt nur 3 mögliche Reste, wenn man eine ganze Zahl durch 3 teilt, nämlich 0, 1 oder 2. Egal welche 7 Zahlen Mara wählt, haben sie jeweils einen dieser 3 Reste. Daher müssen nach dem Schubfachprinzip mindestens 3 Zahlen mit demselben Rest ausgewählt worden sein. Wenn zwei Zahlen beim Teilen durch 3 den gleichen Rest haben, ist ihre Differenz durch 3 teilbar. □

[13] Cantor definierte 1895 den Begriff der „Menge“ wie folgt: „Unter einer Menge verstehen wir jede Zusammenfassung M von bestimmten wohlunterschiedenen Objekten [...]“. Wir schreiben eine (endliche) Menge durch eine konkrete Auflistung ihrer Elemente in geschweiften Klammern ($M = \{x_1, x_2, ..., x_n\}$ zum Beispiel).

[14] disjunkt: keine gemeinsamen Elemente.

2.3 Induktion

Dieser Abschnitt führt eine äusserst effektive Beweistechnik ein, die **vollständige Induktion**[15] genannt wird (kurz: Induktion). Um die Diskussion zu motivieren, wollen wir zunächst die Arten von Aussagen untersuchen, die mithilfe der Induktion bewiesen werden. Wir betrachten folgende Aussage:

Die Summe der ersten n ungeraden natürlichen Zahlen ist n^2.

Um dies zu überprüfen können wir zunächst ein paar Werte für n einsetzen. Wir benennen dabei die Summe der ersten n ungeraden Zahlen $A(n)$:

$$\begin{aligned} A(1) &= 1 = 1 \\ A(2) &= 1+3 = 4 \\ A(3) &= 1+3+5 = 9 \\ A(4) &= 1+3+5+7 = 16 \\ &\vdots \\ A(n) &= 1+3+\ldots+(2n-1) = n^2 \text{ (?)} \\ &\vdots \end{aligned} \tag{2.9}$$

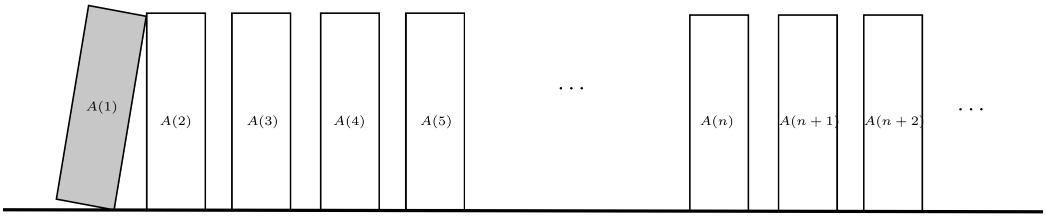
Auch wenn wir die ersten vier überprüft haben, wissen wir immer noch nicht, ob $A(n) = n^2$ für jedes n gilt. Vollständige Induktion ist darauf ausgelegt, genau diese Art von Frage zu beantworten. Die Methode ist wirklich ziemlich einfach. Um sie sich vorzustellen, kann man sich die Aussagen als Dominosteine denken, die in einer Reihe aufgestellt sind. Man stellt sich nun vor, man könne die erste Aussage $A(1)$ beweisen, und symbolisiert dies als Umstossen des Dominosteins $A(1)$. Zusätzlich stellt man sich vor, dass man beweisen kann, dass wenn eine Aussage $A(n)$ wahr ist, die nächste Aussage $A(n+1)$ ebenfalls wahr sein muss (umfallen muss). Dann fällt $A(1)$ um (weil man die Aussage $A(1)$ explizit beweist) und stösst $A(2)$ um. Als Nächstes fällt $A(2)$ um und stösst $A(3)$ um, dann stösst $A(3)$ $A(4)$ um und so weiter. Die Schlussfolgerung ist, dass alle Aussagen umgestossen werden (als wahr bewiesen werden). Wir fassen das in der folgenden Grafik zusammen:

[15] Das Beweisverfahren wurde 1838 von Augustus De Morgan erstmals als Induktion bezeichnet. Augustus De Morgan ist vor allem bekannt für seine De-Morgansche Regeln:

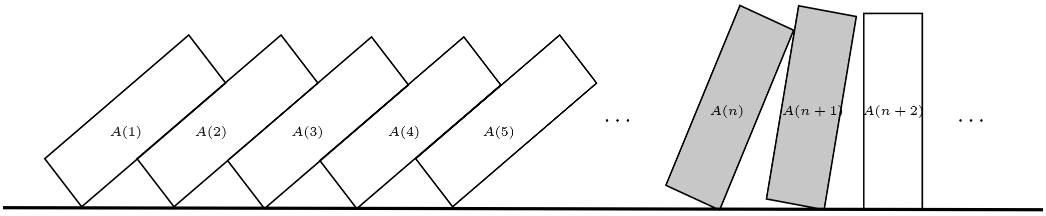
$$\begin{aligned} \neg(A \wedge B) &\iff (\neg A \vee \neg B) \\ \neg(A \vee B) &\iff (\neg A \wedge \neg B). \end{aligned}$$

1888 schrieb Richard Dedekind in seiner Schrift „Was sind und was sollen die Zahlen?“ vom Beweis der vollständige Induktion. „vollständig“, um die Beweismethode nicht mit der philosophischen Induktion zu verwechseln. Während die philosophische Induktion kein exaktes Schlussverfahren ist, soll die „vollständige“ Induktion ein logisches und exaktes Beweisverfahren sein.

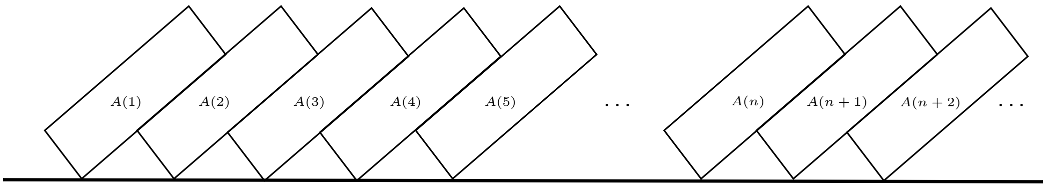
Induktionsanfang



Induktionsschritt



Die Aussage ist für alle n wahr



Wieso das ganze funktioniert, können wir auch anhand eines Bücherregals einsehen. Es seien dazu folgende zwei Eigenschaften bekannt:

1. Das erste Buch, ganz links im Bücherregal, hat einen roten Umschlag.
2. Jedes Buch, das direkt rechts von einem Buch mit rotem Umschlag steht, hat ebenfalls einen roten Umschlag.

Welche Farbe hat der Umschlag des zehn-tausendsten Buches in diesem Regal? Klar, rot! Denn wenn das erste Buch rot ist, dann ist das zweite ebenfalls rot wegen der zweiten Bedingung. Und so weiter. Ohne jedes Buch zu überprüfen, weisst du anhand dieser zwei Eigenschaften, dass der Umschlag alles Bücher rot ist. Das ist mathematische Induktion.

Methode. Vollständige Induktion für eine Aussage $A(n)$ für alle $n \geq n_0$.

1. Man beweist die Aussage für $n = n_0$ (also den kleinstmöglichen Wert von n, meist $n_0 = 1$).
2. Wir nehmen nun an, dass ein beliebiges k existiert, welches die Aussage erfüllt. $A(k)$ ist also richtig. Es soll nun gezeigt werden, dass $A(k + 1)$ ebenfalls richtig ist.

Der erste Schritt wird häufig **Induktionsanfang** genannt, während der zweite Schritt der **Induktionsschritt** ist. [16]

Beispiel. Man beweise, dass die Summe der ersten n ungeraden natürlichen Zahlen n^2 ist.

Beweis. Wir beweisen die Aussage mithilfe der vollständigen Induktion.

1. $A(1) = 1 = 1^2$ ist offensichtlich wahr.
2. Wir müssen nun $A(k) \implies A(k+1)$ für ein beliebiges $k \geq 1$ zeigen. Es gilt also zu zeigen, dass aus $1+3+5+...+(2k-1) = k^2$ dann $1+3+5+...+(2(k+1)-1) = (k+1)^2$ folgt. Dies kann direkt bewiesen werden, denn

$$\begin{aligned} &1+3+5+7+\ldots\ldots\ldots\ldots+(2(k+1)-1) = \\ &\underbrace{1+3+5+7+\ldots+(2k-1)}_{A(k)}+(2(k+1)-1). \end{aligned} \tag{2.10}$$

Nun kann die Annahme $A(k) = k^2$ eingesetzt werden und wir erhalten:

$$= k^2 + (2(k+1)-1) = k^2 + 2k + 1 = (k+1)^2. \tag{2.11}$$

Damit ist der Beweis von $A(k) \implies A(k+1)$ abgeschlossen. Der Satz folgt per Induktion.

□

Beispiel. Wir beweisen die Bernoulli-Ungleichung: Sei $n \in \mathbb{N}$, dann gilt für alle $x \in \mathbb{R}$ mit $x > -1$:

$$(1+x)^n \geq 1 + nx. \tag{2.12}$$

Beweis. Wir beweisen die Aussage mithilfe der vollständigen Induktion.

1. Für $n = 1$ erhalten wir $(1+x)^1 \geq 1 + 1 \cdot x$ und somit wahr, da beide Seiten gleich $1+x$ sind.

[16] In der Mathematik gibt es neben der vollständigen Induktion auch die **starke** Induktion. Der Unterschied liegt vor allem im Induktionsschritt. Anstelle davon anzunehmen, dass $A(k)$ wahr ist und zu zeigen, dass dies $A(k+1)$ impliziert, nehmen wir an, dass **alle** Aussagen $A(1), A(2), ..., A(k)$ wahr sind und zeigen, dass dies $A(k+1)$ impliziert. Man beachte hierbei, dass es je nach Aussage notwendig ist, nicht nur den Induktionsanfang für den kleinsten Wert, sondern für mehrere Werte zu überprüfen. Dies gilt vor allem bei rekursiven Folgen (viele Eigenschaften von Fibonacci-Zahlen lassen sich induktiv beweisen. Da diese aber jeweils durch zwei kleinere Werte bestimmt sind, müssen wir die ersten zwei Werte im Induktionsanfang überprüfen). Da dies den Rahmen dieses Skriptes sprengt, werden wir nicht weiter darauf eingehen.

2. Wir nehmen nun an, dass die Bernoulli-Ungleichung für ein beliebiges $n = k$ gilt. Es gilt dann zu zeigen, dass

$$(1+x)^k \geq 1 + kx \implies (1+x)^{k+1} \geq 1 + (k+1)x. \tag{2.13}$$

Es gilt

$$\begin{aligned}
(1+x)^{k+1} &= (1+x)^k(1+x) \\
&\geq \underbrace{(1+kx)}_{\text{Annahme}}(1+x) \\
&= 1 + x + kx + kx^2 \\
&= 1 + (k+1)x + kx^2 \\
&\geq 1 + (k+1)x,
\end{aligned} \tag{2.14}$$

wobei wir im letzten Schritt ausgenutzt haben, dass $kx^2 \geq 0$ für $k \in \mathbb{N}$ und $x \in \mathbb{R}$. Die Implikation folgt und somit auch der Satz durch vollständige Induktion.

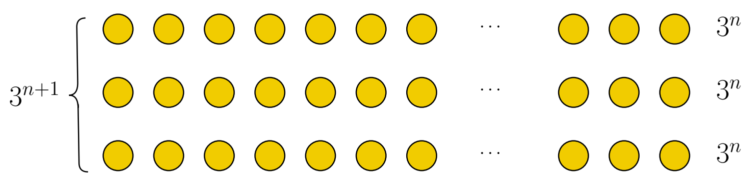
□

Beispiel. Wir haben eine Sammlung von 3^n Münzen und eine Waage. Alle Münzen, bis auf eine, sind echt. Eine von ihnen wiegt aber mehr als die anderen. Beweise, dass man immer herausfinden kann, welche Münze gefälscht ist, indem man nur n Wägungen auf der Waage macht.

Beweis. Wir beweisen die Aussage per Induktion.

1. Für $n = 1$ haben wir $3^1 = 3$ Münzen. Wir sollen nun zeigen, dass wir exakt eine Wägung brauchen um herauszufinden, welche der drei Münzen gefälscht ist. Wir machen dazu eine Fallunterscheidung und wiegen jeweils zwei Münzen. Sei dabei x_1 die gefälschte Münze und x_2 respektive x_3 gleich schwer:
   (a) Eine der zwei Münzen, welche wir wiegen, ist x_1. Dann ist der Fall klar, denn die Waage wird sich auf die Seite von x_1 neigen.
   (b) Keine der zwei Münzen ist x_1. In diesem Fall wird die Waage im Gleichgewicht stehen. Dies muss aber bedeuten, dass beide gleich schwer sind und somit x_1 nicht unter den beiden Münzen ist. Also ist x_1 die dritte Münze, die wir nicht gewogen haben.

2. Nun zum Induktionsschritt. Wir nehmen an, dass wir für 3^n Münzen genau n Mal wiegen müssen. Zu zeigen gilt, dass wir 3^{n+1} Münzen insgesamt $n+1$ Mal wiegen müssen. Die 3^{n+1} Münzen lassen sich in 3 Mengen à je 3^n Münzen aufteilen.



Wenn wir diese drei Mengen gleich wiegen, wie die drei Münzen im Induktionsanfang, so wissen wir, in welcher der Mengen die Münze liegt. Dies entspricht genau einer Wägung. Nach dieser einen Wägung müssen wir also nur noch 3^n Münzen untersuchen. Aus der Annahme wissen wir aber, dass für die 3^n Münzen genau n Wägungen benötigt werden. Somit brauchen wir insgesamt $n + 1$ Wägungen für 3^{n+1} Münzen. Die Aussage folgt per Induktion.

$\square$

3

Über Mengen und Relationen

3.1 Relationen

Ähnliche Beziehungen wie für natürliche Zahlen etwa, die man nach ihrer Grösse ordnen kann, gibt es auch zwischen allgemeineren mathematischen Objekten, wie etwa Aussagen, Mengen, Abbildungen und so weiter. Zum Beispiel können zwei Aussagen zueinander äquivalent sein (wie wir es im ersten Kapitel gesehen haben) oder eine Menge kann in einer anderen enthalten sein. In diesem Kapitel wollen wir das Konzept der Relation zwischen mathematischen Objekten in seiner verallgemeinerten Form diskutieren und etwas präziser darstellen.

Definition. Seien X und Y Mengen. Eine **Relation** auf $X \times Y$ ist eine Teilmenge $\mathcal{R} \subseteq X \times Y$.

Wir schreiben $x\mathcal{R}y$ falls $(x, y) \in \mathcal{R}$ und ersetzen $\mathcal{R}$ oft durch Symbole wie $<, \ll, \leq, \simeq, \sim$. Sei beispielsweise $X = \{1, 5, 13\}$ und $Y = \{3, 4, 9\}$. Dann kann eine Relation beispielsweise

$$\mathcal{R} = \{(1, 3), (1, 4), (1, 9), (5, 9)\}$$

sein. In diesem Fall würden wir vermutlich eher $<$ als Symbol für $\mathcal{R}$ verwenden. Aber auch

$$\mathcal{R} = \{(5, 4), (1, 9), (13, 3)\}$$

ist eine Relation, auch wenn wir dieser kein uns bekanntes Symbol zuweisen könnten.

3.2 Äquivalenzrelationen

Die folgende Definition beschreibt eine wichtige Klasse von Relationen:

Definition. Eine Relation $\sim$ auf $X \times X$[17] ist eine **Äquivalenzrelation**, falls folgende drei Eigenschaften erfüllt sind:

[17] Wir sagen meist nur „eine Äquivalenzrelation auf X“, da das direkte Produkt aus zwei gleichen Mengen genommen wird.

- Reflexivität: $\forall x \in X$: $x \sim x$
- Symmetrie: $\forall x, y \in X$: $x \sim y \implies y \sim x$.
- Transitivität: $\forall x, y, z \in X$: $(x \sim y) \wedge (y \sim z) \implies x \sim z$

Beispiel. Beweise, dass „=“ auf einer beliebigen Menge X eine Äquivalenzrelation definiert.

Lösung. Die Relation lautet in diesem Fall

$$x \sim y \iff x = y.$$

Wir müssen einfach die drei Eigenschaften der Definition einer Äquivalenzrelation überprüfen. Es seien also $x, y, z \in X$ drei gegebene Elemente aus X. Dann gilt

- Reflexivität: Offenbar ist $x = x$ für alle $x \in X$ erfüllt.
- Symmetrie: Ist $x = y$ so ist auch $y = x$, also ist Symmetrie erfüllt.
- Transitivität: Aus $x = y$ und $y = z$ folgt $x = y = z$, also $x = z$.

Das war wohl das intuitivste Beispiel einer Äquivalenzrelation. Ein weiteres schönes Beispiel einer Äquivalenzrelation ist es, X als Menge der Geraden in einer Ebene zu definieren. Wir definieren dann die Äquivalenzrelation für die Geraden $G_1, G_2 \in X$ wie folgt:

$$G_1 \sim G_2 \iff G_1 \text{ und } G_2 \text{ sind parallel.}$$

Dies definiert eine Äquivalenzrelation (wir überlassen den Beweis dem Leser).

Beispiel. Sei X die Menge aller Studierenden in einem Vorlesungssaal. Mann soll nun zeigen, dass für zwei beliebige Studierende $x, y \in X$

$$x \sim y \iff x \text{ hat das gleiche Alter wie } y$$

eine Äquivalenzrelation ist.

Lösung. Wir zeigen die drei Eigenschaften einer Äquivalenzrelation anhand der Studierenden $x, y, z \in X$:

- Reflexivität: Jede*r Studierende hat zwangsläufig das gleiche Alter wie er/sie selbst.
- Symmetrie: Wenn x das gleiche Alter hat wie y, dann muss auch y das gleiche Alter haben wie x. Die Symmetrie ist somit erfüllt.
- Transitivität: Wenn x das gleiche Alter hat wie y und y das gleiche Alter hat wie z, dann muss auch x zwangsläufig das gleiche Alter haben wie z.

Ein sehr wichtiges Beispiel einer Äquivalenzrelation ist das Folgende:

Beispiel. Seien $n, m \in \mathbb{Z}$ und $p \in \mathbb{N}$. Wir setzen $n \sim m \iff n = m \mod p$. Man soll zeigen, dass $\sim$ eine Äquivalenzrelation auf $\mathbb{Z}$ definiert.

Wir gehen genau wie im vorigen Beispiel vor und überprüfen die drei Eigenschaften der Definition einer Äquivalenzrelation. Erinnerung:

$$n = m \mod p \iff \exists k \in \mathbb{Z} : n = m + kp$$

Seien also $n, m, r \in \mathbb{Z}$ gegeben. Dann gilt

- Reflexivität: Es gilt $m \sim m$, weil $m = m + 0 \cdot p$ (wähle $k = 0$).
- Symmetrie: Ist $m \sim n$, so gilt $m = n + kp$ für ein $k \in \mathbb{Z} \implies n = m - kp = m + \tilde{k}p$, also $n \sim m$ (mit der Wahl $\tilde{k} = -k$). Die Symmetrie ist somit erfüllt.
- Transitivität: Falls $n \sim r$ und $r \sim m$, so gilt $n = r + kp$ und $r = m + \tilde{k}p$ für $k, \tilde{k} \in \mathbb{Z}$. Das impliziert $n = r+kp = m+\tilde{k}p+kp = m+(k+\tilde{k})p$, wobei offensichtlich $(k+\tilde{k}) \in \mathbb{Z}$ gilt. Damit ist auch $n \sim m$ und somit die Transitivität auch erfüllt.

3.2.1 Äquivalenzklassen

Sei nun $\sim$ eine Äquivalenzrelation auf einer Menge X.

Definition. Für $x \in X$ wird die Menge

$$[x]_\sim = \{y \in X \mid y \sim x\}$$

die **Äquivalenzklasse** von x genannt. Ein Element $x \in X$ wird auch **Repräsentant** seiner Äquivalenzklasse genannt.

Anschaulich gesprochen, können wir die Elemente aus X in Töpfe unterteilen. Alle Elemente, die in einem Topf sind, sollen hierbei äquivalent sein zu allen anderen Elementen im Topf. Für jeden Topf können wir dann einen Repräsentanten wählen, der den Topf „vertritt“. Wir zeigen nun noch, dass folgende Aussagen äquivalent sind:

$$x \sim y \iff [x]_\sim = [y]_\sim$$

Beweis. Wir beweisen zunächst $x \sim y \implies [x]_\sim = [y]_\sim$: Sei $z \in [x]_\sim$. Dann ist $z \sim x \sim y$ und also $z \sim y$ und somit $z \in [y]_\sim$ wegen der Transitivität. Durch Vertauschen von x und y folgt die andere Inklusion analog: Sei also $z \in [y]_\sim$. Dann muss wegen $z \sim y \sim x$ (die letzte Äquivalenz folgt aus der Symmetrie) auch $z \sim x$ gelten (wegen der Transitivität). Es ist also

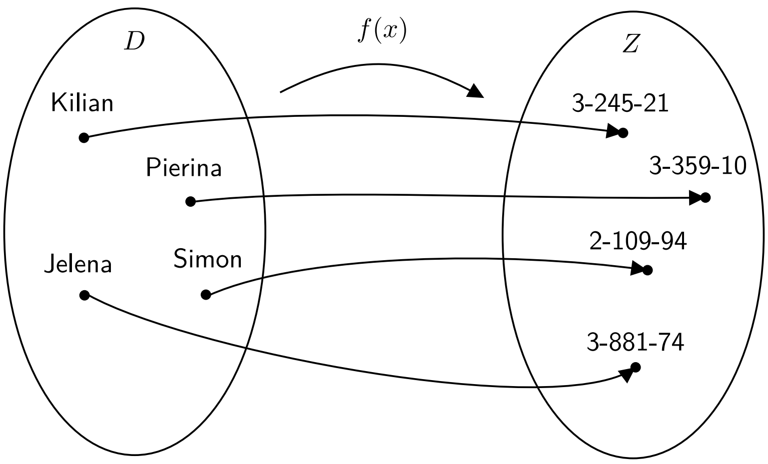
$z \in [x]_\sim$ und somit haben wir $[x]_\sim = [y]_\sim$ gezeigt[18]. Wir beweisen nun die andere Richtung „ $\Longleftarrow$ “. Sei also $[x]_\sim = [y]_\sim$. Da beide Mengen gleich sind, gilt für ein $z \in X$ somit $z \in [x]_\sim$ und $z \in [y]_\sim$, beziehungsweise $z \sim x$ und $z \sim y$. Aus Symmetrie und Transitivität folgt dann $x \sim y$. □

3.3 Mächtigkeit

Wir kommen nun zu einer etwas abstrakteren Äquivalenzrelation. Bevor wir das machen, definieren wir, was eine Bijektion ist:

Definition. Sei eine Funktion $f : X \to Y$ gegeben. Die Funktion f ist eine **Bijektion**, falls *für alle* $y \in Y$ *genau* ein $x \in X$ existiert mit $f(x) = y$.

Wir veranschaulichen das in der folgenden Abbildung. Dabei ordnet die Funktion f jeder Studentin und jedem Studenten ihre/seine Immatrikulationsnummer zu:



Jeder Punkt in der Zielmenge (Y) wird also bei einer Bijektion genau einmal getroffen. Wir besprechen nun wie angekündigt einen fundamentalen Begriff der Mengenlehre, den man sich intuitiv auch als Grössenvergleich vorstellen sollte:

Definition. Zwei Mengen X und Y sind **gleichmächtig**, falls eine Bijektion $f : X \to Y$ existiert.

Wir können dies auch als Äquivalenzrelation schreiben:

$$X \sim Y \iff \exists f : X \to Y \text{ bijektiv}.$$

Dabei ist die Äquivalenzrelation auf einer Menge aller Mengen zu betrachten. Der Beweis, dass dies eine Äquivalenzrelation ist, überlassen wir dem Leser. Viel mehr interessieren uns nun

[18]Wir haben dies schon im ersten Kapitel kurz erwähnt. Die Gleichheit zweier Mengen A und B lässt sich häufig so beweisen, dass man $A \subseteq B$ und $B \subseteq A$ separat beweist. A ist beispielsweise nämlich genau dann eine Teilmenge von B, wenn man zeigen kann, dass unabhängig von der Wahl $x \in A$ auch $x \in B$ gelten muss.

die Äquivalenzklassen. Wir schreiben nun anstelle von $[X]_\sim$ einfach nur $|X|$. Gleichmächtig bedeutet intuitiv so viel wie „gleich viele Elemente". Hat also Y „gleich viele Elemente" wie X, so haben wir $X \sim Y$ und aus dem Satz vom vorherigen Abschnitt $|X| = |Y|$.

Beispiel. Man zeige, dass $|\mathbb{N}| = |2\mathbb{N}|$.

Lösung. Die Abbildung $f : \mathbb{N} \to 2\mathbb{N}, n \mapsto 2n$ bildet eine Bijektion. Somit gilt $\mathbb{N} \sim 2\mathbb{N}$ und folglich $|\mathbb{N}| = |2\mathbb{N}|$.

Beispiel. Man zeige, dass $|\mathbb{N}| = |\mathbb{Z}|$.

Lösung. Wir skizzieren den Beweis und definieren die Abbildung

$$f(n) = \begin{cases} \frac{n}{2} & n \text{ gerade} \\ -\frac{n-1}{2} & n \text{ ungerade} \end{cases}$$

Die ersten Elemente wären also

$$\begin{aligned} f(1) &= 0 \\ f(2) &= 1 \\ f(3) &= -1 \\ f(4) &= 2 \\ f(5) &= -2 \\ f(6) &= 3 \\ &\vdots \end{aligned}$$

Wir sehen also, dass alle Elemente aus $\mathbb{Z}$ genau einmal getroffen werden. f bildet also eine Bijektion $f : \mathbb{N} \to \mathbb{Z}$ und somit gilt wieder mit dem gleichen Argument wie vorhin $|\mathbb{N}| = |\mathbb{Z}|$.

3.3.1 Hilberts Hotel

Stellen wir uns nun das grösste Hotel überhaupt vor, das Hotel Unendlichkeit, in dem es eine unendliche Anzahl Zimmer gibt, die allesamt belegt sind. Nehmen wir an, ein Gast, der an der Rezeption nach einem Zimmer fragt, wird vom Portier die freundliche Antwort erhalten: „Tut mir leid, wir sind eigentlich voll besetzt, aber wir können Ihnen ohne weiteres ein Zimmer geben". Doch was wird der Portier unternehmen können, um den neuen Gast unterzubringen? In das letzte Zimmer kann der Portier den neu angekommenen Gast nicht ziehen lassen, da es im Hotel Unendlichkeit kein letztes Zimmer gibt. Weiterhin sind alle Zimmer - wir erinnern uns an die Aussage des Portiers - belegt. Um dennoch ein Zimmer für den einzelnen Gast zur Verfügung stellen zu können, sagt Hilbert dem Portier er soll einen Umzug aller Gäste in deren jeweilige Nebenzimmer veranlassen.

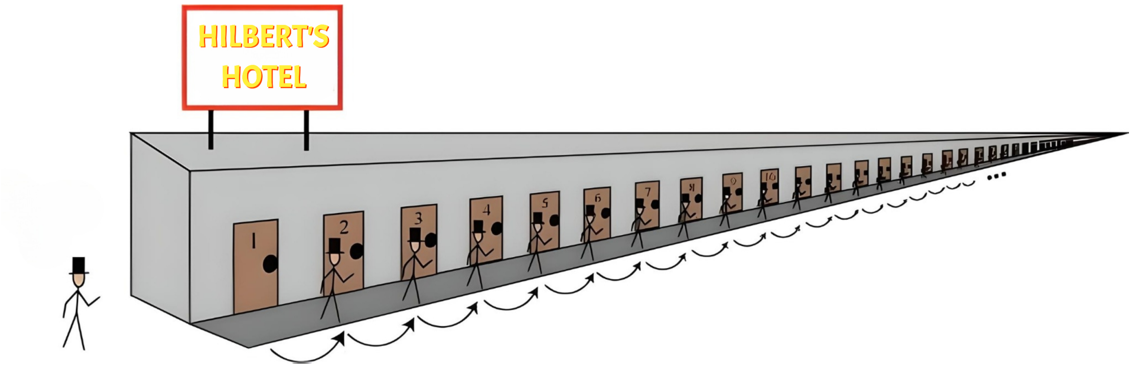


Abbildung 3.1: Auch wenn Hilberts Hotel ausgelastet ist, kann ein weiterer Gast ein Zimmer erhalten, wenn alle Gäste zum nächsten Zimmer $n+1$ wechseln.

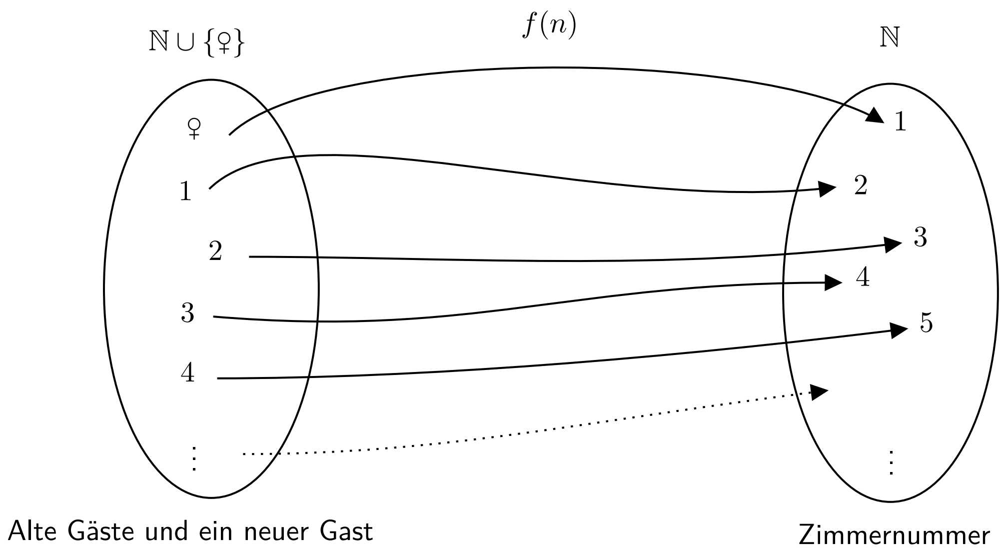
Der Portier verlegt also den Gast von Zimmer 1 in Zimmer 2, den von Zimmer 2 in Zimmer 3 und so weiter. Folglich kann der neue Gast in das gerade frei gewordene Zimmer 1 einziehen. Wir formulieren dies nun mathematisch. Bevor der neue Gast ein Zimmer haben möchte, haben wir eine Bijektion

$$\begin{aligned} f : \mathbb{N}_{\text{Gäste}} &\to \mathbb{N}_{\text{Zimmer}}, \\ n &\mapsto n \end{aligned}$$

welche jedem Gast ein Zimmer zuweisen kann. Nun kommt ein neuer Gast und möchte ein Zimmer haben. Wir suchen also eine Bijektion $f : \mathbb{N}_{\text{Gäste}} \cup \{♀\} \to \mathbb{N}_{\text{Zimmer}}$. Diese finden wir (mit der Idee von vorhin)

$$\begin{aligned} f : \mathbb{N}_{\text{Gäste}} \cup \{♀\} &\to \mathbb{N}_{\text{Zimmer}}, \\ n &\mapsto \begin{cases} 1 & n = ♀ \\ n+1 & n \neq ♀ \end{cases} \end{aligned}$$

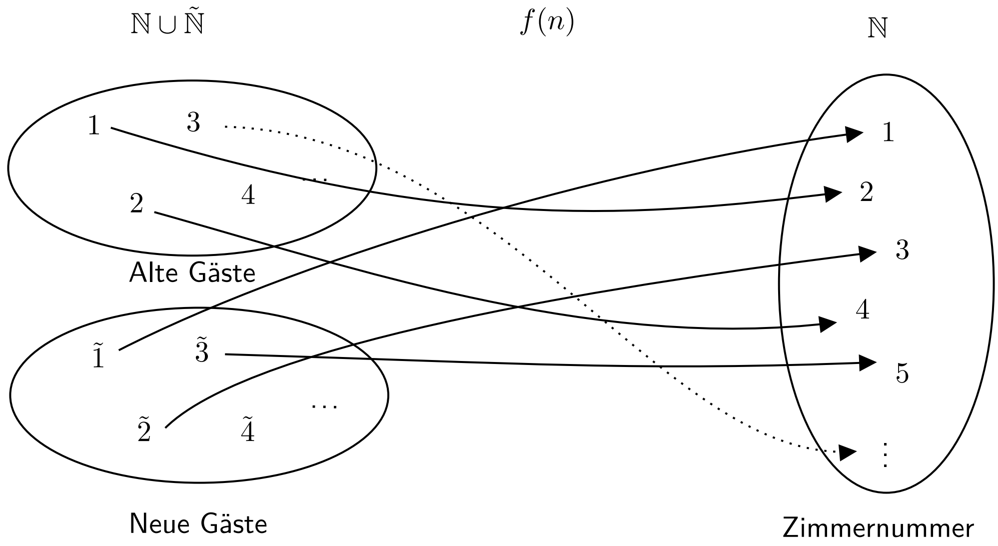
Das ist in der folgenden Abbildung dargestellt:



Was geschieht nun aber, wenn nicht nur ein Gast neu ins Hotel kommt, sondern ein unendlich langer Bus (dessen Sitzplätze mit Nummern beschriftet sind) mit unendlich vielen neuen Gästen. Hier suchen wir eine Bijektion $f : \mathbb{N}_{\text{alte Gäste}} \cup \tilde{\mathbb{N}}_{\text{neue Gäste}} \to \mathbb{N}_{\text{Zimmer}}$. In diesem Fall können wir folgende Bijektion wählen:

$$f : \mathbb{N}_{\text{alte Gäste}} \cup \tilde{\mathbb{N}}_{\text{neue Gäste}} \to \mathbb{N}_{\text{Zimmer}}$$
$$n \mapsto \begin{cases} 2n-1 & n \text{ ist ein neuer Gast} \\ 2n & n \text{ ist ein alter Gast} \end{cases}$$

Diese Abbildung sieht wie folgt aus:



Intuitiv bedeutet die Bijektion, dass wir die alten Gäste in die Zimmer $2n$ schicken können und jeden neuen Gast in die übrig gebliebenen ungeraden Zimmer. Wir sehen also: in der Sprache der Mathematik haben die Mengen aller geraden Zahlen und die Menge aller natürlicher Zahlen tatsächlich „gleich viele Elemente“.

3.4 Unendlich ist nicht gleich unendlich?

Mengen, die gleichmächtig sind zu den natürlichen Zahlen, nennen wir **abzählbar unendlich**. Ein Beispiel einer Menge, die unendlich, aber nicht abzählbar unendlich ist[19], wäre die Menge der reellen Zahlen $\mathbb{R}$. Das lässt sich ganz einfach zeigen. Wir beschränken uns einfachheitshalber auf die reellen Zahlen zwischen 0 und 1 und beweisen die Überabzählbarkeit per Widerspruch. Sei also eine Auflistung aller reellen Zahlen gegeben. Beispielsweise

1. Zahl: $0.5148309752971...$
2. Zahl: $0.4354354354354...$
3. Zahl: $0.1415926540308...$
4. Zahl: $0.9819025736626...$
5. Zahl: $0.6392347543742...$

usw. ....

[19]Wir nennen diese Mengen **überabzählbar** unendlich.

Auch wenn die Liste eben abzählbar unendlich ist, lässt sich zeigen, dass die Liste niemals vollständig sein kann. Denn wenn wir die erste Nachkommastelle der ersten Zahl nehmen und um 1 erhöhen, dann die zweite Nachkommastelle der zweiten Zahl nehmen und diese ebenfalls um 1 erhöhen etc. dann entsteht eine neue Zahl, die so nicht in der Liste sein kann, da sich jede Zahl mindestens in einer Nachkommastelle um 1 unterscheidet:

1. Zahl: $0.5148309752971...$
2. Zahl: $0.4354354354354...$
3. Zahl: $0.1415926540308...$
4. Zahl: $0.9819025736626...$
5. Zahl: $0.6392347543742...$

usw. ....

neue Zahl: $0.64204..................$

Wir sehen also, dass es keine Auflistung aller reellen Zahlen zwischen 0 und 1 geben kann und mit demselben Argument auch keine Auflistung aller reellen Zahlen.

Anhang A

Mengen

Name	Zeichen	Beispiel
Natürliche Zahlen	$\mathbb{N}$	$\mathbb{N} = \{1, 2, ...\}$ (manchmal auch inklusive 0)
Ganze Zahlen	$\mathbb{Z}$	$\mathbb{Z} = \{..., -2, -1, 0, 1, 2, ...\}$
Rationale Zahlen	$\mathbb{Q}$	$\mathbb{Q} = \{..., \frac{1}{2}, ...1, ..., \frac{9}{8}, ...\}$
Reelle Zahlen	$\mathbb{R}$	$\mathbb{R} = \{..., 1, ..., \frac{3}{2}, ..., e, ..., \pi, ...\}$
Komplexe Zahlen	$\mathbb{C}$	$\mathbb{C} = \{..., 1, ..., \pi, ..., i, .., 3i, ..., \frac{2i}{5}, ...\}$
Element von	$\in$	$x \in \mathbb{R}$ („x ist eine reelle Zahl“)
leere Menge	$\emptyset$	$\emptyset = \{\}$ (alternative Schreibweise)
Differenz Mengen	$\setminus$	$\mathbb{Z} \setminus \mathbb{N}$ (alle Zahlen $x \leq 0$)
Schnittmenge	$\cap$	$\{2, 3, 4\} \cap \{1, 3, 4, 5\} = \{3, 4\}$
Vereinigung	$\cup$	$\{2, 3, 4\} \cup \{1, 3, 4, 5\} = \{1, 2, 3, 4, 5\}$
Teilmenge	$\subset$	$\mathbb{R} \subset \mathbb{C}$ (alle reellen Zahlen sind auch komplex)

Anhang B

Aussagenlogik

Name	Zeichen	Beispiel
für alle	$\forall$	$\forall\, x \in \mathbb{R} : x^2 \geq 0$
		(alle Quadrate reeller Zahlen sind positiv)
es existiert	$\exists$	$\exists\, x \in \mathbb{R} : x^2 = 2$
		(es existiert mindestens eine reelle Zahl, deren Quadrat 2 ist)
es existiert genau ein	$\exists!$	$\exists!\, x \in \mathbb{R} : x^3 = 2$
		(es existiert genau eine kubische Wurzel aus 2)
Verneinung	$\neg$	sei $A =$„es regnet“; dann ist $\neg A =$„es regnet nicht“
und	$\wedge$	$x \in \mathbb{R} \wedge y \in \mathbb{R}$
		(x und y sind reell)
oder	$\vee$	$x \in \mathbb{R} \vee y \in \mathbb{R}$
		(x ist reell oder y ist reell oder beide sind reell*)
impliziert	$\Longrightarrow$	$x \in \mathbb{R} \implies x \in \mathbb{C}$
		(wenn x reell ist, so ist x auch komplex)
wird impliziert von	$\Longleftarrow$	$x \in \mathbb{C} \impliedby x \in \mathbb{R}$
		(Umkehrung der vorherigen Aussage)
Äquivalenz	$\Longleftrightarrow$	$x \in \mathbb{N} \iff (x \in \mathbb{Z} \wedge x > 0)$

*Das „oder“ in der Logik entspricht also nicht dem „entweder, ... oder“ in der deutschen Sprache (was ausschliessen würde, dass beide richtig sind). $A \vee B$ ist also auch wahr, wenn A und B beide wahr sind.