Mengen, Abbildungen, Verknüpfungen, Beweise

R. Busam SS 1998

Inhaltsverzeichnis

Die Mengenlehre ist eine *eigenständige mathematische Disziplin.* Ihre Begriffsbildungen und Sprechweisen haben jedoch Eingang in die meisten mathematischen Betrachtungen gefunden. Es hat sich gezeigt, daß die Mengenlehre für praktisch alle mathematischen Theorien ein *begriffliches Gerüst* zu liefern vermag. Wir können daher die Mengenlehre als Hilfsmittel benutzen, um mathematische Sachverhalte zu formulieren. In der Entwicklung des Mengenbegriffs sind Schwierigkeiten aufgetreten, die zum Teil heute noch anstehen. Wer über Mengenlehre als mathematische Theorie mehr wissen will, sei auf die einschlägigen Vorlesungen verwiesen (diese zu hören hat aber erst dann Sinn, wenn man ein bestimmtes mathematisches Basiswissen besitzt) oder auf einschlägige Literatur wie z.B. *Ebbinghaus, H.-D.: Einführung in die Mengenlehre; Spektrum-Verlag. 3. Aufl. 1994* oder *Friedrichsdorf, U., Prestel, A.: Mengenlehre für Mathematiker, Vieweg, 1985.*
Auf den folgenden Seiten soll für diejenigen, die noch nicht im genügenden Maße mit den Sprechweisen der Mengenlehre vertraut sind, eine kurze Einführung mit Beispielen aus verschiedenen

Zweigen der Mathematik gegeben werden. Wir gehen dabei völlig naiv vor. Wir benutzen die Umgangssprache.

§1. Mengen

§1.1. Die Begriffe „Menge“ und „Element“

Georg Cantor (1845-1918), der als Begründer der Mengenlehre gilt, gab 1895 folgende Erklärung für den Begriff „Menge“:

„Unter einer Menge verstehen wir jede Zusammenfassung von bestimmten wohlunterschiedenen Objekten unserer Anschauung oder unseres Denkens zu einem Ganzen.“

Beachten Sie, daß dies keine mathematisch exakte Definition ist, da der zu definierende Begriff „Menge“, durch die nicht definierte Umschreibung „Zusammenfassung ... zu einem Ganzen“ erklärt wird. Daß diese „Definition“ problematisch ist, hat man schon sehr früh erkannt.
Dennoch wollen wir uns — mit Cantor — auf den Standpunkt stellen, daß eine Menge definiert ist, wenn feststeht, welche Objekte zu ihr gehören.
Die Objekte einer Menge bezeichnen wir als ihre *Elemente*. Mengen werden oft (aber nicht immer!) mit großen lateinischen Buchstaben bezeichnet, die Elemente häufig mit kleinen lateinischen Buchstaben.

Ist a ein Element der Menge M, so schreibt man $a \in M$ (*Sprechweise*: a ist Element der Menge M; oder: a ist enthalten in M). Gehört a nicht zu M, so schreibt man $a \notin M$.

Beispiele:

- Die Menge der natürlichen Zahlen ohne Null; Standardbezeichnung $\mathbb{N}$. Beachte: Andere Autoren verstehen unter $\mathbb{N}$ die Menge der natürlichen Zahlen einschließlich Null.
- Die Menge der rationalen Zahlen; Standardbezeichnung $\mathbb{Q}$.
- Die Menge der reellen Zahlen; Standardbezeichnung $\mathbb{R}$.
- Die Menge der Lösungen der quadratischen Gleichung $x^2 + px + q = 0$; p, q reelle Zahlen.
- Die Menge aller rechtwinkligen Dreiecke.
- Die Menge aller (natürlichen) Teiler der Zahl 60.
- Die Menge der Hörer der Vorlesung „Analysis 1“ an der Universität Heidelberg im Sommersemester 1998.

Es gibt verschiedene Möglichkeiten, Mengen anzugeben:

1. Am einfachsten dadurch, daß man alle Elemente *explizit* nennt (aufzählt). Diese werden dann in eine geschweifte Klammer gesetzt: z.B. ist $\{1, 2, 3, 4, 5, 6\}$ die Menge, welche die 6 Elemente $1, 2, 3, 4, 5, 6$ enthält. Auf die Reihenfolge kommt es dabei nicht an, also ist z.B. $\{1, 2, 3, 4, 5, 6\} = \{6, 5, 4, 3, 2, 1\} = \{3, 4, 5, 6, 1, 2\}$, ferner kann ein Element mehrfach aufgelistet sein: $\{1, 2, 3, 4\} = \{1, 2, 2, 3, 4\}$. Diese *aufzählende Schreibweise* bietet sich insbesondere bei *endlichen Mengen* an. Dieser Begriff wird später präzisiert.
2. $\mathbb{N} := \{1, 2, 3, 4, 5, \dots\}$ ist die Menge der natürlichen Zahlen (ohne Null).
$\mathbb{N}_0 = \{0, 1, 2, 3, 4, 5, \dots\}$ die Menge der natürlichen Zahlen (mit Null),
$\mathbb{Z} := \{0, +1, -1, +2, -2, +3, -3, \dots\}$ die Menge der ganzen Zahlen. Über die Bedeutung von „ ... “ muß man sich dabei im klaren sein. In der Menge {3,5, ... } ist zunächst nicht klar, was die Pünktchen bedeuten. Schließlich sei $\mathbb{Q}$ die Menge der rationalen Zahlen und $\mathbb{R}$ die Menge der reellen Zahlen. Es gilt z.B.:
$$2 \in \mathbb{N}, \quad -2 \notin \mathbb{N}, \quad 0 \notin \mathbb{N}, \quad 0 \in \mathbb{N}_0, \quad -2 \in \mathbb{Z}, \quad \sqrt{2} \notin \mathbb{Q}, \quad \sqrt{2} \in \mathbb{R}.$$
3. Oft beschreibt man Mengen verbal (wie eben). Ein zweites Beispiel ist
$$G = \{2, 4, 6, 8, \dots\} = \text{Menge der geraden natürlichen Zahlen.}$$

4. Oft beschreibt man Mengen dadurch, daß man alle Objekte (einer Menge) mit bestimmten Eigenschaften zu einer neuen zusammenfaßt: z.B. $\{x;\ x \in \mathbb{N},\ x \text{ ist durch 2 teilbar }\}$ ist die Menge G der geraden natürlichen Zahlen:

   - $\{x;\ x \in \mathbb{N},\ x \text{ ist durch 2 teilbar}\} = G$
   - $\{x;\ x \in \mathbb{R},\ x^2 = 1\} = \{-1, 1\}$
   - $\{x;\ x \in \mathbb{N},\ x \text{ ist Primzahl und Teiler von } 1001\} = \{7, 11, 13\}$
   - $F = \{p;\ p \text{ ist Primzahl der Gestalt } p = 2^{2^n} + 1 \text{ mit } n \in \mathbb{N}\}$. Eine Primzahl dieser Gestalt heißt FERMATsche Primzahl. Für $n = 0, 1, 2, 3, 4$ erhält man die Primzahlen $3, 5, 17, 257, 65537$, Für $n = 5$ hat schon Euler (1707–1783) gezeigt, daß gilt: $2^{2^5} + 1 = 641 \cdot 6.700.417$. Für jedes $n \in \mathbb{N}$ läßt sich grundsätzlich entscheiden, ob $2^{2^n} + 1$ eine Primzahl ist oder nicht. Die *praktische Entscheidung* scheitert jedoch sehr schnell an der Größe der Zahl $2^{2^n} + 1$ und der Leistungsfähigkeit der Computer. Wir stellen uns dennoch auf den Standpunkt, daß durch obiges F eine Menge definiert ist. Sie werden sehr schnell berühmt werden, wenn sie beweisen $F = \{3, 5, 17, 257, 65537\}$, d.h. außer den bekannten 5 gibt es keine weiteren Fermatschen Primzahlen.
   - Fermat behauptete 1637 einen Beweis dafür zu haben, daß für jede Primzahl $p > 2$ die Gleichung

     $$x^p + y^p = z^p \tag{F_p}$$

     keine Lösung mit $x, y, z \in \mathbb{N}$ besitzt. Man nannte dies die Fermatsche Vermutung. Ein Beweis der Formel ist nicht überliefert. Man setzt

     $$M = \{p;\ p > 2 \text{ Primzahl, für welche die Fermatsche Vermutung } \textit{falsch} \text{ ist}\}.$$

     1994/95 wurde nach Vorarbeiten vieler anderer Mathematiker von Wiles und Taylor gezeigt, daß M kein Element enthält.
     Schreibweise: $M = \emptyset$, d.h. (F_p) ist für alle $p > 2$ richtig. Die Fermatsche Vermutung ist daher zum Fermatschen Theorem geworden (FLT).

   Allgemein schreiben wir für die Menge, die kein Element enthält (die sogenannte *leere* Menge) das Symbol $\emptyset$. Für alle Objekte a gilt also $a \notin \emptyset$.

   Ist $M_1 = \{x;\ x \text{ Primzahl und Teiler von } 1001\}$ und $M_2 = \{7, 11, 13\}$, dann enthalten M_1 und M_2 dieselben Elemente, denn die Primzahlen, welche 1001 teilen sind gerade 7, 11 und 13. Wir schreiben $M_1 = M_2$ und definieren allgemein:

   Def.: Zwei Mengen M und N sind *gleich*, wenn sie dieselben Elemente enthalten. Genauer: $M = N$ bedeutet, daß jedes Element $a \in M$ auch Element von N ist, und umgekehrt jedes Element $b \in N$ auch Element von M ist.

   Wenn man die Gleichheit zweier Mengen M und N nachweisen will, muß man also zeigen: Wenn $a \in M$ gilt, so gilt auch $a \in N$, und wenn $b \in N$ gilt, so gilt auch $b \in M$.

   Kurzschreibweise hierfür: $a \in M \Rightarrow a \in \mathbb{N}$ und $b \in \mathbb{N} \Rightarrow b \in M$, oder noch kürzer: $a \in M \Longleftrightarrow a \in N$.

   Beispiel: Sei $M := \{x \in \mathbb{R};\ x^2 - 4x + 3 = 0\}$, also die Lösungsmenge der quadratischen Gleichung $x^2 - 4x + 3 = 0$ in $\mathbb{R}$. Mit der bekannten Lösungsformel $x_{1/2} = 2 \pm \sqrt{4 - 3}$ ergeben sich $x_1 = 1$ und $x_2 = 3$ als Lösungen. Für $N := \{1, 3\}$ gilt also $M = N$.

5. $M_1 = \{p \in \mathbb{N},\ p \text{ ist Primzahl}\}$

   Frage: Ist 10.000.719 ein Element von M_1? (Nein. Begründung?)

   Frage: Ist 10.000.721 ein Element von M_1? (Ja. Begründung?)

6. $M_2 = \{(x,y) \in \mathbb{R} \times \mathbb{R};\ x + y = 1,\ x - y = 0\}$, dabei ist $\mathbb{R} \times \mathbb{R} = \{(x,y),\ x,y \in \mathbb{R}\}$. Geometrisch handelt es sich bei den Gleichungen um zwei Geraden, die genau einen Schnittpunkt, nämlich $(x,y) = (\frac{1}{2}, \frac{1}{2})$ haben. Es gilt also $M_2 = \{(\frac{1}{2}, \frac{1}{2})\}$. Man beachte den Unterschied zwischen dem Element $(\frac{1}{2}, \frac{1}{2}) \in M_2$ und der Menge M_2, die hier nur aus einem Element nämlich $\{(\frac{1}{2}, \frac{1}{2})\}$ besteht.

7. $M_3 = \{x \in \mathbb{R},\ x^2 < 0\}$. Da für jede reelle Zahl x gilt $x^2 \geqslant 0$, ist die Eigenschaft $x^2 < 0$ bei $x \in \mathbb{R}$ nie erfüllt, also gilt $M_3 = \emptyset$.

§1.2. Teilmengen

Jede Primzahl ist eine natürliche Zahl, bezeichnet man mit $\mathbb{P}$ die Menge der Primzahlen, so schreibt man für den beschriebenen Tatbestand $\mathbb{P} \subset \mathbb{N}$ ($\mathbb{P}$ ist Teilmenge von $\mathbb{N}$). Man definiert allgemein

Def.: Eine Menge M heißt *Teilmenge* einer Menge N, wenn jedes Element von M auch zu N gehört. Man sagt auch, M ist in N enthalten (oder auch N ist Obermenge von M).
Schreibweise: $M \subset N$. In Elementen ausgedrückt bedeutet dann $M \subset N$ das gleiche wie: $a \in M \Rightarrow a \in N$. Die Gleichung $M \subset N$ nennt man auch *Inklusion*.

Beispiele:

- $\mathbb{P} \subset \mathbb{N}$, jede Primzahl ist auch eine natürliche Zahl. Da z.B. 6 keine Primzahl ist, gilt nicht $\mathbb{N} \subset \mathbb{P}$. Hierfür schreibt man auch $\mathbb{N} \not\subset \mathbb{P}$.
- $\mathbb{N} \subset \mathbb{Z}$, jede natürliche Zahl ist auch eine ganze Zahl
  $\mathbb{Z} \subset \mathbb{Q}$, jede ganze Zahl ist auch eine rational Zahl
  $\mathbb{Q} \subset \mathbb{R}$, jede rationale Zahl ist auch eine reelle Zahl

  Hierfür schreibt man auch kurz $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R}$.
- Für jede Menge M gilt $M \subset M$ und $\emptyset \subset M$. (Die leere Menge ist Teilmenge jeder Menge.) Das letztere gilt, weil eine Implikation „wenn ..., so ... " stets wahr ist, wenn der Vordersatz falsch ist. Für das Objekt a ist die Implikation „$a \in \emptyset \Rightarrow a \in M$" wahr, denn der Vordersatz $a \in \emptyset$ ist falsch. Näheres dazu im Abschnitt 4 über „Beweise".

Um die *Gleichheit zweier Mengen* M und N zu zeigen, zeigt man $M \subset N$ und $N \subset M$.

Die Inklusion hat folgende *Transitivitätseigenschaft:* $M_1 \subset M_2 \subset M_3 \Rightarrow M_1 \subset M_3$.

Aufgabe: Bestimmen Sie alle Teilmengen von $M_3 := \{1,2,3\}$, $M_4 := \{1,2,3,4\}$, ..., $M_n := \{1,2,3,\ldots,n\}$. Vergessen Sie die leere Menge und die Menge selbst nicht!

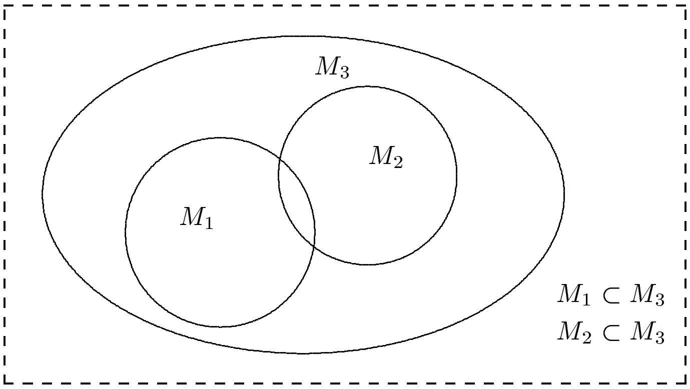
Ist M eine beliebige Menge, so bezeichnet man mit $\mathcal{P}(M)$ die Menge aller Teilmengen (*Potenzmenge*) von M (einschließlich $\emptyset$ und M). Es gilt also $A \in \mathcal{P}(M) \iff A \subset M$. Für das Beispiel M_3 gilt

$$\mathcal{P}(M_3) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1,2\}, \{1,3\}, \{2,3\}, M_3\}.$$

Der Übergang von M zu $\mathcal{P}(M)$ liefert also eine Möglichkeit, aus einer Menge neue Mengen zu konstruieren. Der Konstruktion neuer Mengen aus gegebenen Mengen dient auch der nächste Abschnitt.

§1.3. Operation mit Mengen

Mit Mengen kann man im gewissen Sinne „rechnen". Eine Größer-Kleiner-Beziehung haben wir schon mit dem Beispiel der Teilmenge.
Es ist zweckmäßig und suggestiv, sich mengentheoretische Beziehungen und Operationen bildlich zu veranschaulichen. (Etwa als Teilmenge der Zeichenebene, man spricht dann von *Venn-Diagrammen*). Das folgende Venn-Diagramm veranschaulicht den Begriff *Teilmenge*:

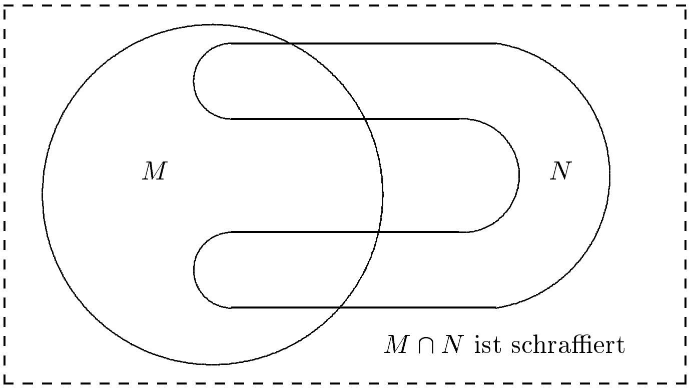


§1.3.1. Durchschnitt

Seien M und N zwei Mengen. Unter dem *Durchschnitt* von M und N – in Zeichen $M \cap N$ – verstehen wir die Menge derjenigen Objekte, die sowohl zu M als auch zu M gehören.

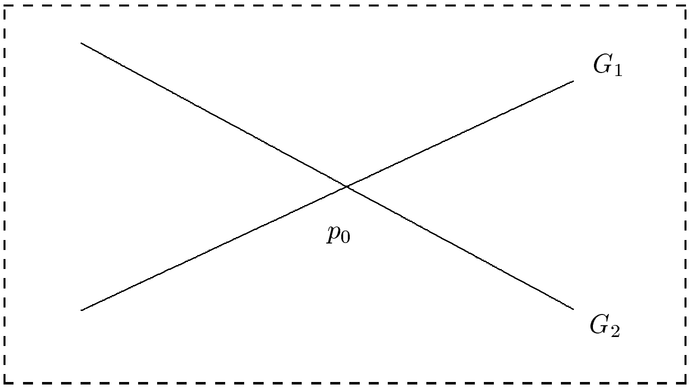
$$M \cap N = \{x;\ x \in M \text{ und } x \in N\}$$

Veranschaulichung in einem Venn-Diagramm:

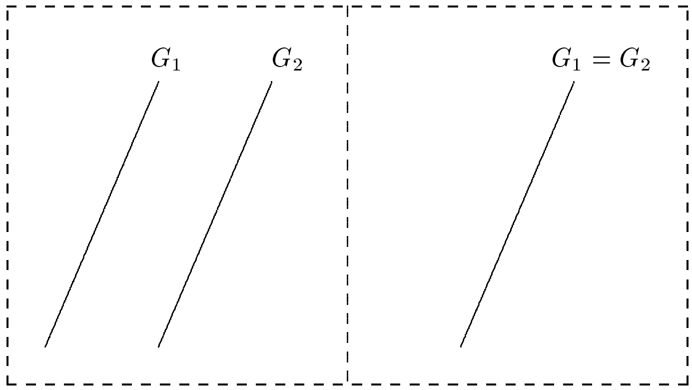


Beispiele:

- Sind G_1 und G_2 Geraden der anschaulichen Ebene (als Punktmenge aufgefaßt), dann gilt $G_1 \cap G_2 = \{p_0\}$, wenn G_1 und G_2 nicht parallel sind und einen Schnittpunkt p_0 haben:



Falls G_1 und G_2 parallel sind gilt: $G_1 \cap G_2 = \emptyset$ oder $G_1 = G_2$.



- Ist

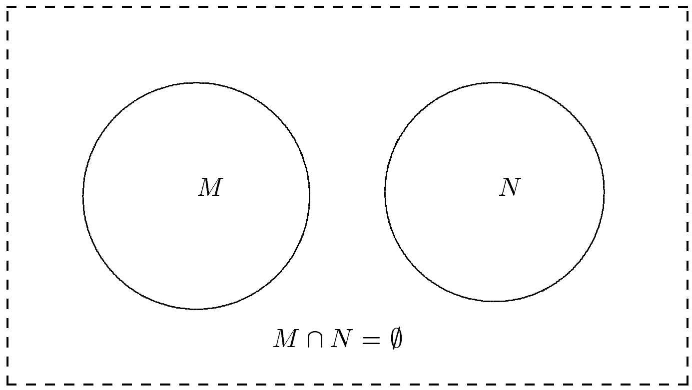
$$\begin{aligned} M_1 &= \{(x,y) \in \mathbb{R} \times \mathbb{R},\ 3x - 5y = -9,\ -4x + 3y = 1\}, \\ M_2 &= \{(x,y) \in \mathbb{R} \times \mathbb{R},\ 3x - 5y = -9\}, \\ M_3 &= \{(x,y) \in \mathbb{R} \times \mathbb{R},\ -4x + 3y = 1\}, \end{aligned}$$

so ist $M_1 = M_2 \cap M_3$.

(M_2 und M_3 beschreiben Geraden, die sich im Punkt $p_0 = (2,3)$ schneiden. Also ist $M_1 = M_2 \cap M_3 = \{p_0\}$.)

- Ist M die Menge der ebenen Vierecke mit gleichlangen Seiten und N die Menge der ebenen Vierecke mit 4 rechten Winkeln, dann ist $M \cap N$ die Menge der Quadrate in der Ebene.

- Gilt $M \cap N = \emptyset$, so sagt man, daß M und N elementfremd oder *disjunkt* sind.



Ist z.B. G die Menge der geraden ganzen Zahlen und U die Menge der ungeraden ganzen Zahlen, dann ist $G \cap U = \emptyset$.

Natürlich kann man den Durchschnitt von mehr als 2 Mengen bilden: Sind $M_1, \ldots, M_n$ Mengen, dann ist $M_1 \cap M_2 \cap \ldots \cap M_n = \{x;\ x \in M_1 \text{ und } x \in M_2 \ldots \text{ und } x \in M_n\}$. Man schreibt auch

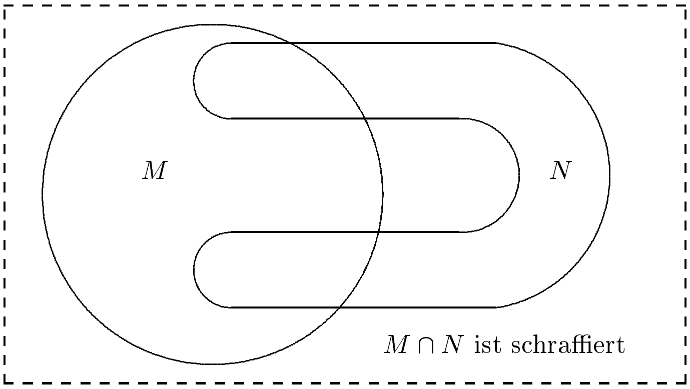
$$M_1 \cap M_2 \cap \ldots \cap M_n = \bigcap_{\nu=1}^{n} M_\nu .$$

§1.3.2. Vereinigung

Seien M und N Mengen. Unter der *Vereinigung* von M und N, in Zeichen $M \cup N$, versteht man die Menge derjenigen Objekte, die zu wenigstens einer der beiden Mengen M, N gehören:

$$M \cup N = \{x;\ x \in M \text{ oder } x \in N\}$$

Man beachte, daß „oder“ in der Mathematik das nicht ausschließende „oder“ bedeutet. „A oder B“ heißt: es gilt A oder B oder beides.
Veranschaulichung durch ein Venn-Diagramm:



Ist $M = M_1 \cup M_2$ und $M_1 \cap M_2 = \emptyset$, so sagt man, daß M die *disjunkte Vereinigung* von M_1 und M_2 ist, und schreibt hierfür $M = M_1 \dot{\cup} M_2$.

Beispiel: $M = \mathbb{Z}$,
$M_1 = G =$ Menge der geraden ganzen Zahlen,
$M_2 = U =$ Menge der ungeraden ganzen Zahlen.

Natürlich läßt sich auch die Vereinigung von mehr als 2 Mengen bilden: Sind $M_1, \ldots, M_n$ Mengen, dann ist $M_1 \cup M_2 \cup \ldots \cup M_n = \{x;\ x \in M_1 \text{ oder } x \in M_2 \ldots \text{ oder } x \in M_n\}$ undman schreibt abkürzend hierfür

$$M_1 \cup M_2 \cup \ldots \cup M_n = \bigcup_{\nu=1}^{n} M_\nu.$$

Bemerkung: Seien A, B, C, M_j $(1 \leqslant j \leqslant n)$ (der Einfachheit halber) Teilmengen einer festen Menge M. Es gilt:

1. $A \cup B = B \cup A, \qquad A \cap B = B \cap A$ (*Kommutativität*)
2. $(A \cup B) \cup C = A \cup (B \cup C)$ und (*Assoziativgesetze*)
   $(A \cap B) \cap C = A \cap (B \cap C)$
3. $A \cap (\bigcup_{j=1}^{n} M_j) = \bigcup_{j=1}^{n} (A \cap N_j)$ und (*Distributivgesetze*)
   $A \cup (\bigcap_{j=1}^{n} M_j) = \bigcap_{j=1}^{n} (A \cup N_j)$
4. Ist $A \subset C$, so gilt:
   $(A \cup B) \cap C = A \cup (B \cap C)$ (*Dedekindsche Identität*)

Es gelten ferner die folgenden Regeln für beliebige Mengen A und B:

(a) $A \cap A = A, \ A \cup A = A$

(b) $A \cap \emptyset = \emptyset, \quad A \cup \emptyset = A$

(c) $A \cap B = A$ genau dann, wenn $A \subset B$
$A \cup B = A$ genau dann, wenn $B \subset A$

(d) $A \cap (A \cup B) = A, \qquad A \cup (A \cap B) = A.$

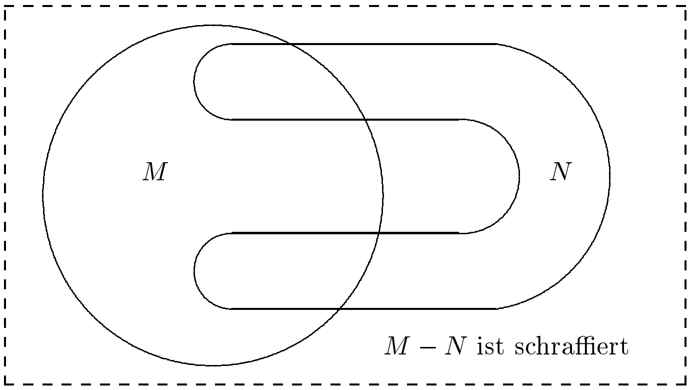
Die Beweise folgen jeweils (mehr oder weniger) unmittelbar aus den Definitionen. Für die Zwecke der linearen Algebra und Analysis lohnt es kaum, sich diese Regeln besonders einzuprägen. In den Beispielen sind sie meist offensichtlicher als in der allgemeinen mengentheoretischen Formulierung. (Versuchen Sie jedoch als Übung, z.B. (c) zu beweisen.)

§1.4. Differenz von Mengen, Komplement

Seien M und N zwei Mengen. Unter der *Differenz* von M und N, in Zeichen M-N, verstehen wir die Menge derjenigen Objekte, die zwar in M, aber *nicht* in N liegen:

$$M - N := \{x;\ x \in M,\ x \notin N\}$$

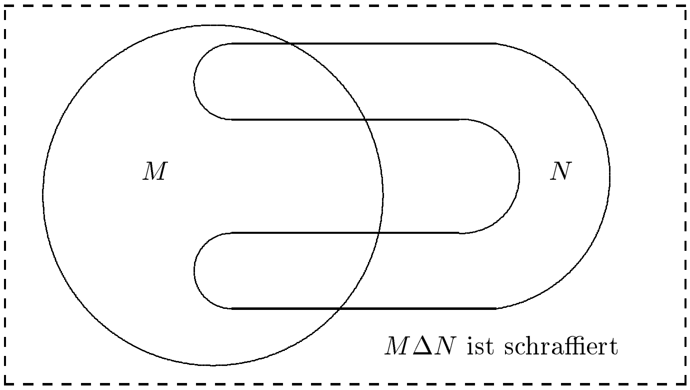
Veranschaulichung im Mengendiagramm:



Beispiel: $M = \{1,2,3,4\}$, $N = \{3,4,5\}$, dann ist $M - N = \{1,2\}$, dagegen ist $N - M = \{5\}$. Die Differenzbildung ist also im Allgemeinen nicht *symmetrisch.* Es gilt stets $(M - N) \cap (N - M) = \emptyset$. Man erhält eine *symmetrische* Bildung durch die Festsetzung

$$A\Delta B = (A - B) \cup (B - A) = (A \cup B) - (A \cap B),$$

dann gilt $B\Delta A = A\Delta B$.

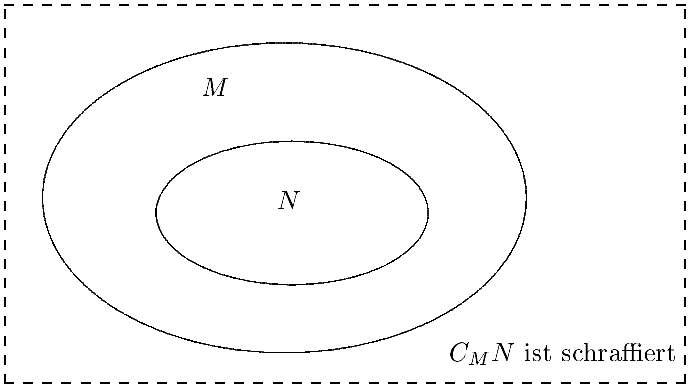


Man nennt $A\Delta B$ die *symmetrische Differenz von* A *und* B.

Im Spezialfall, daß N eine Teilmenge von M ist, nennt man die Differenz $M - N$ auch das *Komplement von N bzgl. M* und verwendet hierfür auch die Bezeichnung $C_M N$.

Beispiel: $M = \mathbb{Z}$, $N = \mathbb{N}$, dann ist $\mathbb{Z} - \mathbb{N} = C_{\mathbb{Z}}\mathbb{N} = \{0, -1, -2, \dots\}$.

Veranschaulichung im Mengendiagramm:



Folgende *Regeln* gelten für Teilmengen A, B einer festen Menge M:

(a) $C_M(A \cup B) = C_M A \cap C_M B$

(b) $C_M(A \cap B) = C_M A \cup C_M B$

(c) $C_M(C_M A) = A$

Diese Regeln lassen sich wesentlich verallgemeinern. (Man nennt sie dann die *de Morganschen Regeln*).

§1.5. Das (cartesische) Produkt

Wir führen eine weitere oft benutzte Konstruktion einer neuen Menge aus zwei gegebenen Mengen M und N ein.
Man kann ein Element $a \in M$ und ein Element $b \in N$ zu einer neuen Menge $\{a, b\}$ zusammenfassen. Zwischen $\{a, b\} = \{b, a\}$ ist keine Reihenfolge ausgezeichnet. Häufig ist jedoch die Reihenfolge wichtig. Man kann z.B. definieren $(a, b) := \{\{a\}, \{a, b\}\}$. Dann gilt $(a, b) = (c, d) \Longleftrightarrow a = c$ und $b = d$, denn sei etwa $(a, b) = (c, d)$, also $\{\{a\}, \{a, b\}\} = \{\{c\}, \{c, d\}\}$. Wir unterscheiden zwei Fälle:
Fall 1: $a = b$. Dann ist $\{a\} = \{a, b\} = \{c\} = \{c, d\}$, also $a = c$ und $b = d$.
Fall 2: $a \neq b$. Dann ist $\{a\} = \{c\}$ und $\{a, b\} = \{c, d\}$, also wieder $a = c$ und $b = d$.

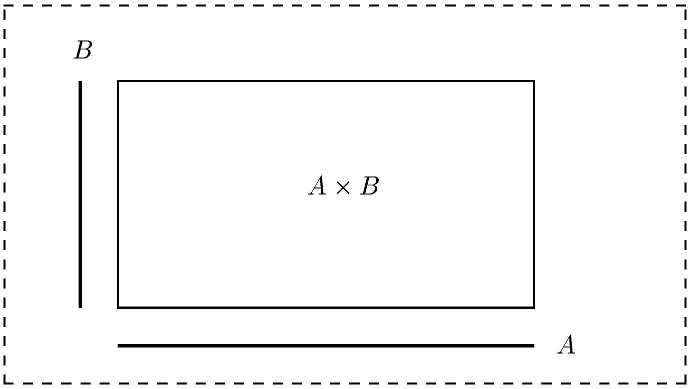
(a, b) heißt *geordnetes Paar*. Wichtig ist die *Gleichheit geordneter PaareGleichheit!von Paaren*: $(a, b) = (c, d)$ genau dann, wenn $a = c$ und $b = d$ gilt. Die Menge, die aus allen geordneten Paaren (a, b), $a \in A$, $b \in B$ besteht, heißt das *(cartesische) Produkt* von $A \times B$:

$$A \times B = \{(a, b);\ a \in A,\ b \in B\}$$

Beispiele:

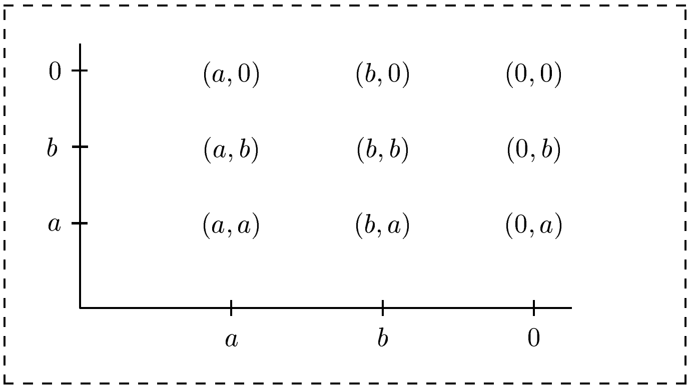
- Sind $A := \{x \in \mathbb{R};\ a \leqslant x \leqslant b\}$ und $B := \{x \in \mathbb{R};\ c \leqslant x \leqslant d\}$ Intervalle $(a < b,\ c < d)$, so ist $A \times B$ ein Rechteck:

$$[a, b] \times [c, d] = \{(x, y) \in \mathbb{R} \times \mathbb{R};\ a \leqslant x \leqslant b, c \leqslant y \leqslant d\}$$



Man veranschaulicht sich das Produkt $A \times B$ zweier Mengen genau als solch ein Rechteck. (Die Veranschaulichung als Venn-Diagramm ist hier nicht geeignet.)

- Sei $S = \{a, b, o\}$ (etwa die Menge der Allele), dann stellt $S \times S$



die möglichen Genkombinationen in einer befruchteten Eizelle dar.

- Sei A die Menge aller Studierenden der Universität Heidelberg (SS98) und B die Menge der an der Universität Heidelberg vorhandenen Studienfächer. Ein Paar $(a, b) \in SA \times B$, $a =$Müller und $b =$Mathematik, bedeutet also, daß Müller Mathematik studiert.

Man kann auch Produkte von mehr als zwei Mengen bilden: Seien $M_1, M_2, \ldots, M_n$ Mengen, so betrachten wir Systeme $(a_1, a_2, \ldots, a_n)$ mit $a_1 \in M_1$, $a_2 \in M_2$, $\ldots$ $a_n \in M_n$. Solche Systeme liefern (geordnete) n-Tupel. (2-Tupel=*Paar*, 3-Tupel=*Tripel*, 4-Tupel=*Quadrupel* etc.)

Wichtig ist die *Gleichheits*definition: Zwei n-Tupel $(a_1, \ldots, a_n)$ und $(b_1, \ldots, b_n)$ heißen *gleich*, wenn $a_1 = b_1$, $a_2 = b_2$, $\ldots$, $a_n = b_n$ gilt. Das (cartesische) Produkt $M_1 \times M_2 \times \ldots \times M_n$ von $M_1, M_2, \ldots, M_n$ wird als die Menge aller n-Tupel definiert:

$$M_1 \times \ldots \times M_n = \{(a_1, a_2, \ldots, a_n) : \ a_1 \in M_1, \ldots, a_n \in M_n\}$$

Ein wichtiger Spezialfall liegt vor, wenn alle *Faktoren* übereinstimmen. $M_1 = M_2 = \ldots = M_n =: M$. Dann schreibt man M^n anstelle von $M_1 \times \ldots M_n$.

Beispiele:

- $\mathbb{R}^2$ ist die Menge aller Paare reeller Zahlen: $\mathbb{R}^2 = \{(x, y); \ x \in \mathbb{R}, y \in \mathbb{R}$
- $\mathbb{R}^3$ ist die Menge aller Tripel reeller Zahlen: $\mathbb{R}^3 = \{(x, y, z); \ x \in \mathbb{R}, y \in \mathbb{R}, z \in \mathbb{R}$

  $\vdots$

- $\mathbb{R}^n$ ist die Menge aller n-Tupel reeller Zahlen: $\mathbb{R}^n = \{(x_1, \ldots, x_n); \ x_1 \in \mathbb{R}, \ldots, x_n \in \mathbb{R}\}$

§1.6. Relationen auf einer Menge

Sei M eine Menge. Eine *Relation auf* M ist eine Teilmenge R von $M \times M$. Für $x, x \in M$ mit $(x, y) \in R$ schreiben wir $x \overset{R}{\sim} y$ oder einfach $x \sim y$ und sagen: x steht in der Relation mit y.
Eine Relation auf M heißt *Äquivalenzrelation*, wenn für beliebige $x, y, z \in M$ gilt.

1. Es ist $x \sim x$. (*Reflexivität*)
2. Gilt $x \sim y$, so auch $y \sim x$). (*Symmetrie*)
3. Gilt $x \sim y$ und $y \sim z$, dann auch $x \sim z$. (*Transitivität*)

Beispiele:

- Sei etwa M die Menge der Einwohner der Bundesrepublik Deutschland. Durch $x \sim y$ genau dann, wenn x und y ihren ersten Wohnsitz in derselben Gemeinde haben, wird eine Äquivalenzrelation definiert.
- In der Menge aller Geraden der Ebene ist die Relation „parallel“ eine Äquivalenzrelation.
- Auf der Menge $\mathbb{Z}$ der ganzen Zahlen ist die Relation $x \sim y$ genau dann, wenn $x - y$ ein ganzzahliges Vielfaches der (festen) natürlichen Zahl m ist, eine Äquivalenzrelation. Man schreibt hierfür auch $x \equiv y \pmod{m}$ oder $x \overset{m}{\equiv} y$.

  Aufgabe: Prüfen Sie die Eigenschaften 1–3 nach.

Aufgabe: Sei M die Menge der HörerInnen der Vorlesung „Analysis 1“ im SS 1998. Durch $x \sim y$ genau dann, wenn

1. x befreundet ist mit y
2. x verwandt ist mit y
3. x per Du ist mit y
4. x verliebt ist in y

sind Relationen definiert. Welche davon sind Äquivalenzrelationen?

Was bringen Äquivalenzrelationen für Vorteile? Statt die mehr als 80 Millionen Bewohner der BRD zu betrachten, braucht man im ersten Beispiel „nur“ etwa 1000 Gemeinden zu betrachten. Äquivalenzrelationen sind eine Art „vergröberte Gleichheit“ .
Ein wichtiger mathematischer Begriff ergibt sich im Zusammenhang mit Äquivalenzrelationen: Der Begriff der *Äquivalenzklasse*.

Satz: Sei M eine Menge, $\sim$ eine Äquivalenzrelation auf M. Für $x \in M$ sei

$$\mathrm{Kl}(x) := \{y;\ y \in M,\ y \sim x\}.$$

Wir nennen $\mathrm{Kl}(x)$ die *Äquivalenzklasse* von x (bzgl. $\sim$). Dann gilt

$$X = \bigcup_{x \in X} \mathrm{Kl}(x).$$

Ferner ist

$$\mathrm{Kl}(x) \cap \mathrm{Kl}(x') = \begin{cases} \emptyset, & \text{falls } x \not\sim x', \\ \mathrm{Kl}(x) = \mathrm{Kl}(x'), & \text{falls } x \sim x'. \end{cases}$$

X ist also die Vereinigung paarweise disjunkter Äquivalenzklassen.

Beweis: Wegen $x \sim x$ gilt $x \in \mathrm{Kl}(x)$, also ist $X = \cup_{x\in X} \mathrm{Kl}(x)$. Sei $x_0 \in \mathrm{Kl}(x) \cap \mathrm{Kl}(x')$, also $x_0 \sim x$ und $x_0 \sim x'$. Sei $x_1 \in \mathrm{Kl}(x)$. Dann gelten $x_1 \sim x$, $x \sim x_0$ und $x_0 \sim x'$. Die Transitivität liefert $x_1 \sim x'$, also $\mathrm{Kl}(x) \subset \mathrm{Kl}(x')$. Aus Symmetriegründen ist auch $\mathrm{Kl}(x') \subset \mathrm{Kl}(x)$, also gilt $\mathrm{Kl}(x) = \mathrm{Kl}(x')$.
Sind also zwei Äquivalenzklassen nicht disjunkt, so sind sie gleich.

Jedes $x' \in \mathrm{Kl}(x)$ heißt ein *Repräsentant* von $\mathrm{Kl}(x)$, insbesondere ist x selbst ein Repräsentant von $\mathrm{Kl}(x)$.
Eigenschaften von Äquivalenzrelationen werden häufig über Eigenschaften einzelner Elemente (=Repräsentanten) der Äquivalenzklassen definiert. Dann muß man sich überzeugen, daß diese Eigenschaft *unabhängig* von der speziellen Auswahl ist. Man spricht dann von *Wohldefiniertheit*.
Ist $\sim$ eine Äquivalenzrelation auf einer Menge X, so kann man die Menge der Äquivalenzklassen als *Elemente* einer neuen Menge auffassen:

$$X/\sim \; := \{\mathrm{Kl}(x);\ x \in X\}$$

$X/\sim$ heißt *Quotient von X nach der Äquivalenzrelation $\sim$*.

Beispiel: Sei $X = \mathbb{Z}$. Wenn $x \sim y$ genau dann gilt, wenn $x - y$ ein ganzzahliges Vielfaches von 2 ist, so wird auf $\mathbb{Z}$ eine Äquivalenzrelation definiert. Da eine ganze Zahl entweder gerade oder ungerade ist, gibt es genau zwei Äquivalenzklassen:

$G =$ Menge der geraden ganzen Zahlen.

$U =$ Menge der ungeraden ganzen Zahlen.

Es ist $\mathbb{Z} = G \cup U$ und $G \cap U = \emptyset$. Nach Definition ist dann $\mathbb{Z}/\sim = \{G, U\}$.
Das Beispiel läßt sich verallgemeinern: Sei M eine natürliche Zahl. Wir definieren eine Relation $\overset{m}{\equiv}$ auf $\mathbb{Z}$ wie folgt (vgl. obiges Beispiel) $x \overset{m}{\equiv} y$ (oder auch $x \equiv y \pmod m$) genau dann. wenn $x - y$ ein ganzzahliges Vielfaches von m ist. Man nennt $\overset{m}{\equiv}$ *Kongruenz modulo* (m). Man prüft leicht nach, daß $\overset{m}{\equiv}$ sogar eine Äquivalenzrelation ist. (Die *Transitivität* ergibt sich so: Ist $x - y = bm$ und $x - z = lm$ mit $b, l \in \mathbb{Z}$, so folgt $x - y = (x - y) + (y - z) = bm + lm = (b + l)m$, also $x \overset{m}{\equiv} y$.
Die Äquivalenzrelation nennt man in diesem Beispiel auch *Restklassen* mod (m). Man überlegt sich leicht, daß $x, y \in \mathbb{Z}$ genau dann kongruent mod (m) sind, wenn x und y bei Division durch m denselben nichtnegativen Rest lassen: Ist $x = mq_1 + r_1$, $0 \leqslant r_1 < m$ und $y = mq_2 + r_2$, $0 \leqslant r_2 < m$, so gilt im Fall $r_1 = r_2$: $x - y = (q_1 - q_2)m = qm$, also $x \equiv y \pmod m$. Gilt umgekehrt diese Kongruenz und ist $x = q_1 m + r_1$ mit $0 \leqslant r_1 < m$ und $y = q_2 m + r_2$ mit $0 \leqslant r_2 < m$, und ist etwa $r_1 = r_2$, dann ist $x - y = (q_1 - q_2)m + r_1 + r_2$. Da $x - y = qm$ gilt ($q \in \mathbb{Z}$), folgt hieraus, daß $r_1 - r_2$ ein ganzzahliges Vielfaches von m ist. Ferner ist $0 \leqslant r_1 - r_2 < m$, und hieraus folgt notwendig $r_1 = r_2$.
Für $x \in \mathbb{Z}$ gilt daher

$$\begin{aligned}
\mathrm{Kl}(x) &= \{n \in \mathbb{Z};\ n \equiv x \pmod m\} \\
&= \{n \in \mathbb{Z};\ n \equiv r \pmod m\} \\
&= \{n \in \mathbb{Z};\ n - r = bm,\ b \in \mathbb{Z}\} \\
&= \{n \in \mathbb{Z};\ n = r + mb,\ b \in \mathbb{Z}\} \\
&=: r + m\mathbb{Z}
\end{aligned}$$

mit $0 \leqslant r < m$. Jede Äquivalenzklasse besitzt also einen Repräsentanten mit $0 \leqslant r < m$.

Die M verschiedenen Äquivalenzklassen $\mathrm{Kl}(0), \mathrm{Kl}(0), \mathrm{Kl}(2), \ldots, \mathrm{Kl}(m-1)$ bilden also eine disjunkte Zerlegung von $\mathbb{Z}$ und der Quotient von $\mathbb{Z}$ nach der Äquivalenzrelation $\overset{m}{\equiv}$ ergibt sich zu

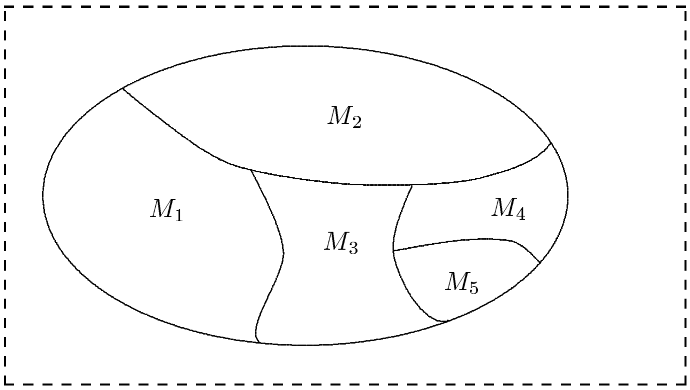
$$\mathbb{Z}/\sim = \mathbb{Z}/m\mathbb{Z} = \{\mathrm{Kl}(0), \mathrm{Kl}(1), \ldots, \mathrm{Kl}(m-1)\}.$$

Die Klasse von 0, wofür man auch $\bar{0}$ schreibt, enthält alle ganze Zahlen, die bei Division durch m den Rest Null ergeben. Die Klasse $\bar{1}$ enthält alle ganzen Zahlen, die bei Division durch m den Rest 1 ergeben etc.
Ist z.B. $m = 5$, so ist

$$\begin{aligned}
\bar{0} &= \mathrm{Kl}(0) = \{\dots, -10, -5, 0, 5, 10, 15, \dots\}\\
\bar{1} &= \mathrm{Kl}(1) = \{\dots, -9\ , -4, 1, 6, 11, 16, \dots\}\\
\bar{2} &= \mathrm{Kl}(2) = \{\dots, -8\ , -3, 2, 7, 12, 17, \dots\}\\
\bar{3} &= \mathrm{Kl}(3) = \{\dots, -7\ , -2, 3, 8, 13, 18, \dots\}\\
\bar{4} &= \mathrm{Kl}(4) = \{\dots, -6\ , -1, 4, 9, 14, 19, \dots\}
\end{aligned}$$

Im Spezialfall $m = 2$ erhält man das frühere Beispiel: Hier ist $\bar{0} = \mathrm{Kl}(0) = G$, $\bar{1} = \mathrm{Kl}(1) = U$, $\mathbb{Z} = G \cup U$ und $\mathbb{Z}/\sim = \mathbb{Z}/2\mathbb{Z} = \{G, U\}$.
Alle geraden Zahlen werden hier in einen Topf geworfen, ebenso alle ungeraden in einen anderen Topf. Die beiden Töpfe haben nichts miteinander zu tun, sie sind disjunkt. Beachten Sie, daß sowohl G als auch U unendlich viele ganze Zahlen enthalten, daß aber $\mathbb{Z}/\sim = \mathbb{Z}/2\mathbb{Z}$ nur aus 2 Elementen – nämlich G und U – besteht.
Ist $\sim$ eine Äquivalenzrelation auf einer Menge X und wählt man in jeder Äquivalenzklasse einen Vertreter aus, dann ist X die disjunkte Vereinigung der entsprechenden Äquivalenzklassen.
Ist umgekehrt von vornherein M zerlegt in eine Vereinigung paarweise disjunkter Mengen $M = \cup_\alpha M_\alpha$, α durchlaufe dabei eine geeignete Indexmenge, und gilt $M_\alpha \cap M_\varrho = \emptyset$ für alle $\alpha \neq \varrho$, dann erhält man eine Äquivalenzrelation auf M, wenn man definiert:

$$x \sim y \quad \Longleftrightarrow \quad \text{es gibt ein } \alpha \text{ mit } x \in M_\alpha \text{ und } y \in M_\alpha.$$



Zwei Elemente aus M_α, die in derselben Teilmenge liegen, werden als „gleich“ (äquivalent) angesehen. Äquivalenz ist eine „vergröbernde Gleichheit“.

Zum Abschluß der Betrachtungen über Mengen und Elemente eine klassische (die sogenannte *Russelsche*) *Antinomie*, die in der Unterhaltungsmathematik meist umschrieben wird mit der Geschichte vom Dorfbarbier, der alle Leute im Dorf rasiert, die sich selbst nicht rasieren. Frage: Rasiert er sich selbst?
Wir nennen eine Menge X *normal*, wenn sie sich nicht selbst als Element enthält, wenn also $X \notin X$ gilt. (Offenbar eine sehr normale Eigenschaft.) Wir betrachten nun die Menge N aller normalen Mengen.
Frage: Ist N normal?
Wäre N normal, also $N \notin N$, so müßte N nach Definition Element von N sein, also $N \in N$, ein Widerspruch. Wäre N hingegen nicht normal, d.h. gilt $N \in N$, so müßte N aufgrund seiner Definition doch normal sein, d.h. $N \notin N$ und man erhält ebenfalls einen Widersprich.

Der Hintergrund dieser und anderer Antinomien ist, daß in naiver Weise zu große Mengen gebildet werden.
Es gibt Grundlegungen der Mengenlehre, die solche Paradoxien vermeiden. Ein solcher Aufbau der Mengenlehre wurde zuerst von E. Zermelo (1908) und mit wesentlichen Ergänzungen von A. E. Fraenkel (1922) durchgeführt. So entstand das *Z*ERMELO-*F*RAENKELSCHE Axiomsystem der Mengenlehre (mit Auswahlaxiom, axiom of *c*hoice) häufig mit *ZFC* abgekürzt. Weiteres kann man etwa in dem eingangs zitierten Büchern von Ebbinghaus oder Friedrichsdorf-Prestel nachlesen.

§2. Abbildungen

§2.1. Erklärung des Abbildungsbegriffes

Der Abbildungsbegriff ist ein zentraler Begriff der Mathematik.
Seien M und N nichtleere Mengen. Eine Abbildung von M nach N (oder: von M in N) ist eine Vorschrift f, die jedem $m \in M$ genau ein Element n aus N zuordnet. Dieses Element n wird mit $f(m)$ oder fm bezeichnet. Es heißt das *Bild* von m unter f (oder Funktionswert an der Stelle m). M heißt der *Definitionsbereich* von f und N der *Zielbereich* (Wertebereich).
Man verwendet für Abbildungen häufig die Kurzschreibweise

$$f : M \longrightarrow N \quad \text{oder} \quad M \xrightarrow{f} N \quad \text{oder} \quad f : M \to N, \; m \longmapsto f(m)$$

Wem diese Erklärung zu schwammig ist, kann folgende Definition verwenden: Eine *Funktion* ist ein Tripel

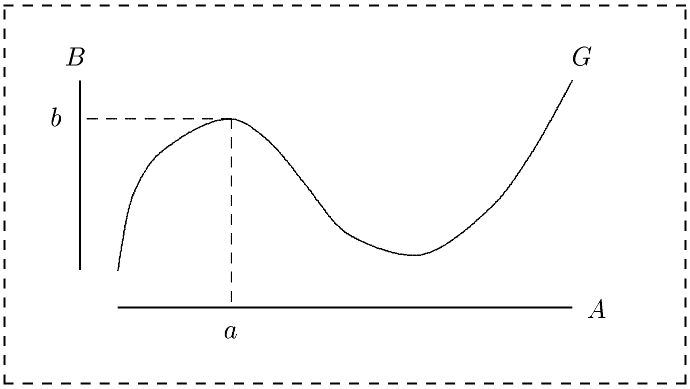
$$f = (A, B, G),$$

dabei sind A und B (nichtleere) Mengen, und G ist eine Teilmenge von $A \times B$ mit folgenden Eigenschaften:

(F_1) Zu jedem $a \in A$ gibt es ein $b \in B$ mit $(a, b) \in G$.

(F_2) Gilt $(a, b) \in G$ und $(a, b') \in G$, so ist $b = b'$.

Das zu a eindeutig bestimmte Element $b \in B$ mit $(a, b) \in G$ wird auch mit fa bezeichnet (oder $f(a)$). Es ist dann $G = \{(a, f(a));\ a \in A\} \subset A \times B$ der sogenannte *Graph* der Abbildung f.



Zwei Abbildungen $f = (A, B, G)$ und $g = (A', B', G')$ heißen *gleich*, wenn $A = A'$, $B = B'$ und $G = G'$ gilt. Letzteres bedeutet $fa = ga$ für alle $a \in A$.

Beispiele: Die vier Funktionen

$$\begin{array}{rrl}
f: & \mathbb{R} \longrightarrow \mathbb{R}, & x \longmapsto \sin x \\
g: & [-\frac{\pi}{2}, \frac{\pi}{2}] \longrightarrow \mathbb{R}, & x \longmapsto \sin x \\
h: & \mathbb{R} \longrightarrow [-1,1], & x \longmapsto \sin x \\
b: & [-\frac{\pi}{2}, \frac{\pi}{2}] \longrightarrow [-1,1], & x \longmapsto \sin x
\end{array}$$

sind als verschieden zu betrachten. Die Zuordnungsvorschrift ist jedesmal dieselbe, dennoch sind die Abbildungen verschieden, sie haben sehr unterschiedliche Eigenschaften.
Die Gleichheit zweier Abbildungen ist nicht immer leicht festzustellen: um etwa einzusehen, daß durch

$$\begin{array}{lll}
f: \ \mathbb{R} \longrightarrow \mathbb{R} & x \longmapsto \sin 2x & \text{und} \\
g: \ \mathbb{R} \longrightarrow \mathbb{R} & x \longmapsto 2 \sin x \cos x &
\end{array}$$

dieselbe Abbildung definiert werden, muß man etwa das *Additionstheorem* des Sinus nutzen. Wesentlich schwieriger ist es zu zeigen, daß durch

$$\begin{array}{rlll}
e: & \mathbb{R} \longrightarrow \mathbb{R} & x \longmapsto \lim\limits_{n \to \infty} \left(1 + \frac{x}{n}\right)^n & \text{und} \\
\exp: & \mathbb{R} \longrightarrow \mathbb{R} & x \longmapsto \sum\limits_{k=0}^{\infty} \frac{x^k}{k!} &
\end{array}$$

dieselben Funktionen definiert werden.

Da Abbildungen (Funktionen) in beiden Grundvorlesungen auf Schritt und Tritt auftreten, begnügen wir uns mit einigen Beispielen, die zeigen, daß man Abbildungen auf viele verschiedene Weisen beschreiben kann.

Weitere Beispiele:

1. Als erstes Beispiel betrachten wir die Abbildung von $\mathbb{Z}$ nach $\mathbb{N}_0$, die jeder ganzen Zahl ihr Quadrat zuordnet. Dann kann man sagen: Sei $f : \mathbb{Z} \to \mathbb{N}_0$ die durch $f(m) = m^2$ für alle $m \in \mathbb{Z}$ gegebene Abbildung. Oder etwas kürzer: Sei

   $$\begin{array}{rcccl}
   f: & \mathbb{Z} & \longrightarrow & \mathbb{N}_0 & \text{die durch} \\
   & m & \longmapsto & m^2 & \text{gegebene Abbildung}
   \end{array}$$

   Oder noch kürzer: Betrachte

   $$\begin{array}{rccc}
   f: & \mathbb{Z} & \longrightarrow & \mathbb{N}_0, \\
   & m & \longmapsto & m^2.
   \end{array}$$

   Oder sogar noch kürzer: Betrachte $f : \mathbb{Z} \to \mathbb{N}_0$, $m \mapsto m^2$.

   Manchmal ist es nicht nötig, der Abbildung einen Namen zu geben. Dann spricht man kurz von der Abbildung $\mathbb{Z} \to \mathbb{N}_0$, $m \mapsto m^2$.

   Die Angabe von Definitions- und Zielbereich (hier $\mathbb{Z}$ und N_0) kann man sich i.a. nicht ersparen. (Auf die Angabe des Zielbereiches kann man manchmal verzichten.)

   Es ist auch nicht zulässig, unsere betrachtete Abbildung einfach m^2 zu nennen. m^2 ist der Wert der Abbildung an der Stelle m, hier also eine Zahl.

   Merke: Zu einer Abbildung (Funktion) gehört ein *Definitionsbereich* (und ein *Zielbereich*).

   Sprechweisen wie „Die Funktion $\sin x$ ist auf ganz $\mathbb{R}$ differenzierbar" sind im Grunde nicht korrekt, denn $\sin x$ ist eine feste Zahl. Aber man kann natürlich vereinbaren, daß man mit der Sprechweise „Die Funktion $f(x)$" grundsätzlich die Funktion $f : M \to N$ und nicht den Funktionswert $f(x)$ meint.

2. Auch die Addition (und die Multiplikation) reeller Zahlen sind Abbildungen, nämlich

$$\begin{array}{ccc} \mathbb{R}\times\mathbb{R} & \longrightarrow & \mathbb{R} \\ (x,y) & \longmapsto & x+y \end{array}$$

bzw.

$$\begin{array}{ccc} \mathbb{R}\times\mathbb{R} & \longrightarrow & \mathbb{R} \\ (x,y) & \longmapsto & xy \end{array}$$

3. Man kann Abbildungen auch mit Worten beschreiben, z.B. sei $f:\mathbb{R}\to\mathbb{R}$ definiert durch

$$f(x) = \begin{cases} 1, & \text{falls } x \textit{ rational} \quad (\text{d.h. } x \in \mathbb{Q}), \\ 0, & \text{falls } x \text{ irrational } (\text{d.h. } x \in \mathbb{R} - \mathbb{Q}). \end{cases}$$

Dies ist ein Beispiel für eine sog. *charakteristische Funktion.*

Ist X eine Menge, $A \subset X$ eine Teilmenge, dann heißt die Funktion

$$\chi_A : X \longrightarrow \mathbb{R}$$

mit

$$f(x) = \begin{cases} 1, & \text{falls } x \in A, \\ 0, & \text{falls } x \in X - A. \end{cases}$$

die *charakteristische Funktion* von A. In dieser Bezeichnung ist also $f = \chi_{\mathbb{Q}}$.

4. Ordnet man jedem Quader des Anschauungsraumes sein Volumen zu, so erhält man eine Abbildung von der Menge der Quader im Anschauungsraum in die Menge $\mathbb{R}$ der reellen Zahlen.

5. Eine Abbildung: $f : M \to N$ mit einem *endlichen* M kann man stets in Form einer Wertetabelle angegeben: Ist etwa $M = \{0,1,2,3\}$ und $N = \mathbb{N}_0$:

m	0	1	2	3
$f(m)$	1	2	5	10

6. Sei M eine beliebige Menge, so heißt die Abbildung

$$\begin{array}{cccc} \mathrm{id}_M : & M & \longrightarrow & M \\ & m & \longmapsto & n \end{array}$$

die *Identität* auf M.

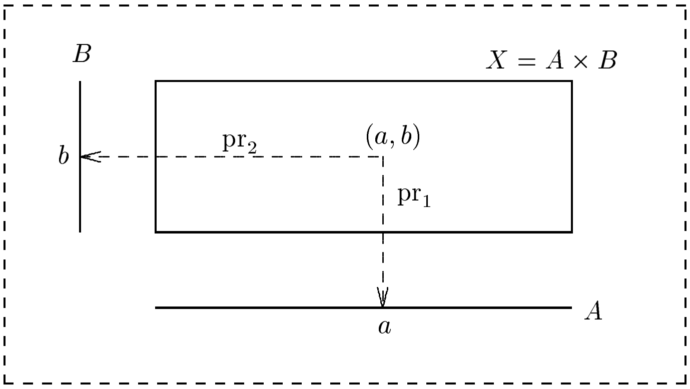
7. Sind A und B Mengen, und ist $X = A \times B$ ihr (cartesisches) Produkt, dann heißen die Abbildungen:

$$\begin{array}{cccc} \mathrm{pr}_1 : & X & \longrightarrow & A \\ & (a,b) & \longmapsto & a \end{array}$$

bzw.

$$\begin{array}{cccc} \mathrm{pr}_1 : & X & \longrightarrow & B \\ & (a,b) & \longmapsto & b \end{array}$$

Projektionen auf den ersten bzw. zweiten Faktor.



8. Sind X und Y Mengen und $y_0 \in Y$. Dann nennt man die Abbildung

$$\begin{array}{ccc} X & \longrightarrow & Y \\ x & \longmapsto & y_0 \end{array}$$

konstante Abbildung (mit dem Wert y_0).

9. Sind M und N Mengen, dann bezeichnet man mit $\mathrm{Abb}(M, N)$ die *Menge aller Abbildungen* von M in N.

Beispiel: Sei $n \in \mathbb{N}$ fest und $M = \{1, 2, \dots, n\}$ und $N = A$ eine beliebige Menge. Eine Abbildung $f : M \to A$ ist dann bestimmt durch die Werte $f(1) =: a_1$, $f(2) =: a_2$, ..., $f(n) =: a_n$ oder durch das n-Tupel $(a_1, a_2, \dots, a_n)$. Geht man umgekehrt von einem n-Tupel $(a_1, \dots, a_n)$ aus, so wird durch $1 \mapsto a_1$, $2 \mapsto a_2$, ..., $n \mapsto a_n$ eine Abbildung von M nach A gegeben. Daher gilt $\mathrm{Abb}(\{1, 2, \dots, n\}, A) = A^n$.

10. Ist $M = M_1 \times \ldots \times M_n$ $(n \in N)$, dann nennt man eine Abbildung $f : M \to N$ eine Funktion von mehreren Veränderlichen (falls $n \geqslant 2$. Statt $f((x_1, \dots, x_n))$ schreibt man einfach $f(x_1, \dots, x_n)$.

$(x_1, \dots, x_n)$ heißt *Argument(liste)* von f und x_j das *j-te Argument*. Bei festem j $(1 \leqslant j \leqslant m)$ und festen $x_1, x_2, \dots, x_{j-1}, x_{j+1}, \dots, x_n$ kann man die Funktion

$$\begin{array}{ccc} M_j & \longrightarrow & N \\ x_j & \longmapsto & f(x_1, \dots, x_{j-1}, x_j, x_{j+1}, \dots, x_n) \end{array}$$

betrachten, man nennt sie die zu f gehörige *j-te partielle Abbildung*.

§2.2. Bilder und Urbilder von Teilmengen

Seien M und N nichtleere Mengen und $f \in \mathrm{Abb}(M, n)$. Für $A \subset M$ setzen wir

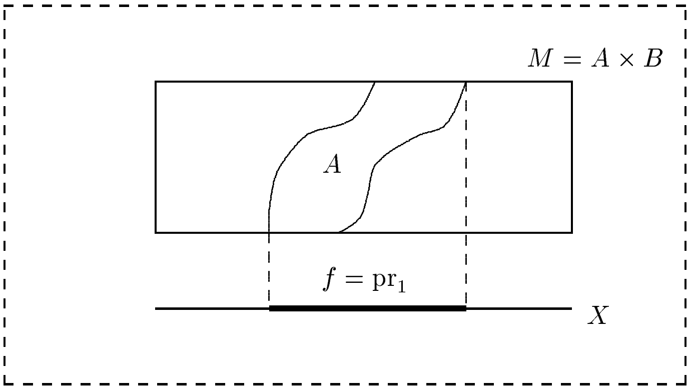
$$\begin{aligned} f(A) &= \{b \in N;\ \text{es gibt ein } a \in A \text{ mit } fa = b\} \\ &= \{fa;\ a \in A\} \end{aligned}$$

und nennen $f(A)$ das *Bild* von A unter f. Insbesondere ist $f(\emptyset) = \emptyset$.
Ist $B \subset N$, so sei

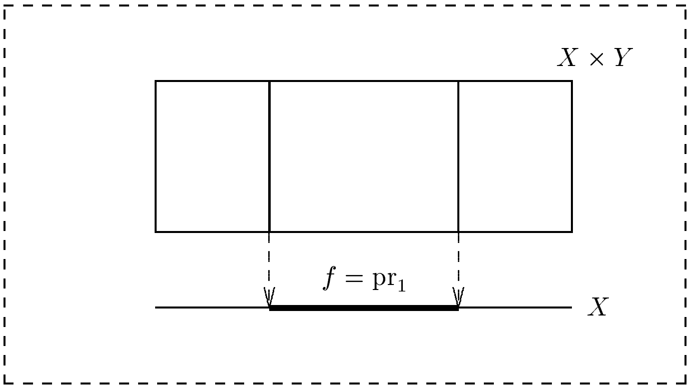
$$f^-(B) = \{m;\ m \in M,\ f(m) \in B\}.$$

Wir nennen $f^-(B)$ das *Urbild* von B unter f. Ist $B = \{n\}$, so schreibt man statt $f^-(\{n\})$ häufig nur $f^-(n)$ und nennt diese Menge auch die *Faser* von n unter f. Beachten Sie, daß hierdurch *keine* Abbildung f^- von N in M definiert ist, denn $f^-(n)$ kann sowohl leer sein, als auch mehr als ein Element enthalten, wie die folgenden *Beispiele* zeigen.

1. Ist etwa $M = X \times Y$ und $f = \mathrm{pr}_1$ die Projektion auf den ersten Faktor von $A \in M$



Man beachte, daß es auch ein $f(x)$ mit $z \notin A$ zum Bild $f(A)$ gehören kann, dann nämlich, wenn es ein $a \in A$ mit $fa = fz$ gibt.



Die Elemente von $f^{-}(B)$ sind gerade die Elemente von M, die bei der Abbildung f in B landen. Es gibt aber Abbildungen, wo kein Element in B landet.

2. Sei f die Abbildung

$$\begin{array}{rccc} f: & \mathbb{R} \times \mathbb{R} & \longrightarrow & \mathbb{R}, \\ & (x,y)) & \longmapsto & x^2 + y^2. \end{array}$$

Ist $c \in \mathbb{R}$ mit $c < 0$, dann ist $f^{-}(c) = \emptyset$, für $c = 0$ ist $f^{-}(0) = \{(0,0)\}$, und für $c > 0$ ist $f^{-}(c)$ eine Kreislinie mit Mittelpunkt $(0,0)$ und dem Radius $\sqrt{c}$.

3. Sei $f : \mathbb{R}^3 \to \mathbb{R}^2$ definiert durch $f(r_1, r_2, r_3) := (r_1 + 2r_2 + 3r_3, 4r_1 + 5r_2 + 6r_3)$. Für $(c_1, c_2) \in \mathbb{R}^2$ ist das Urbild (Faser) $f^{-}\{(c_1, c_2)\}$ nichts anderes als die Lösungsmenge des linearen Gleichungssystems

$$\begin{aligned} x_1 + 2x_2 + 3x_3 &= c_1 \\ 4x_1 + 5x_2 + 6x_3 &= c_2 \end{aligned}$$

4. Für

$$\begin{array}{rccc} f: & \mathbb{R} & \longrightarrow & \mathbb{R}, \\ & x & \longmapsto & \sin x \end{array}$$

ist $f^{-}(\{2\}) = \emptyset$, $f^{-}(\frac{1}{2}) = \{\frac{\pi}{6} + 2\pi b,\ \frac{5\pi}{6} + 2\pi b;\ b \in \mathbb{Z}\}$.

Ist $f : M \to N$ eine Abbildung, dann gelten für Teilmengen X, X_1, X_2 von M bzw. $Y, Y_1, Y_2 \subset N$ die folgenden Regeln:

1.	$X_1 \subset X_2 \Longrightarrow f(X_1) \subset f(X_2)$	1'.	$Y_1 \subset Y_2 \Longrightarrow f^-(Y_1) \subset f^-(Y_2)$
2.	$f(X_1 \cup X_2) = f(X_1) \cup f(X_2)$	2'.	$f^-(Y_1 \cup Y_2) = f^-(Y_1) \cup f^-(Y_2)$
3.	$f(X_1 \cap X_2) = f(X_1) \cap f(X_2)$	3'.	$f^-(Y_1 \cap Y_2) = f^-(Y_1) \cap f^-(Y_2)$
4.	$f^-(f(X)) \supset X$	4'.	$f(f^-(Y)) \supset Y$
5.	$f(M - X) \supset f(M) - f(X)$	5'.	$f^-(N - X) = X - f^-(Y)$

Aufgabe: Konstruieren Sie ein Beispiel, in welchem $f(X_1 \cap X_2) \subset f(X_1) \cap f(X_2)$ gilt, aber nicht $f(X_1 \cap X_2) = f(X_1) \cap f(X_2)$. (Man denke etwa an eine Projektion)

§2.3. Zusammensetzung (Komposition) von Abbildungen

Sind $f : A \to B$ und $g : B \to C$ Abbildungen mit den besonderen Eigenschaften, daß $f(A) = B$ gilt, dann kann man auf das Bild fa jedes Elements $a \in A$ die Abbildung g anwenden und erhält eine Element $g(f(a)) \in C$. Durch diese Hintereinanderausführung wird eine Abbildung von A in C konstruiert:

$$\begin{array}{ccc} A & \longrightarrow & C \\ a & \longmapsto & g(fa) \end{array}$$

Wir bezeichnen diese Abbildung mit $g \circ f$ und nennen sie die *Komposition* (Hintereinanderausführung, Verkettung) von f und g. Auch wenn nur $f(a) \subset B$ gilt, kann man für ein $a \in A$ auf das Bild fa die Abbildung g anwenden, da fa im Definitionsbereich von g liegt. (Man hat dann eigentlich g durch die *Einschränkung* $g \mid f(A)$ zu ersetzen.) Da aber die Einschränkung einer Abbildung $g : B \to C$ auf eine Teilmenge B' definiert ist durch $g'(b') := g(b')$ für alle $b' \in B'$, macht man keinen Unterschied zwischen g' und g. g' ist durch g eindeutig bestimmt.
$g \circ f$ liest man als: „erst f, dann g“ oder „g nach f“. Beachte, wenn $g \circ f$ definiert ist, braucht $f \circ g$ nicht definiert zu sein (selbst wenn die Abbildung $f \circ g$ möglich ist, gilt i.a. $f \circ g \neq g \circ f$). Man verwechsle $g \circ f$ auch nicht mit dem Produkt gf von Funktionen. Ist z.B. $A = B = C = \mathbb{R}$ und $f(x) = x^2$, $g(x) = \sin x$, dann ist $h(x) = g(f(x)) = sin(x^2)$, das Produkt $p(x) = g(x)f(x) = (sinx)(x^2) = x^2 \sin x$ und $(f \circ g)(x) = (\sin x)^2$.
In Situationen, wie sie bei den Zusammensetzungen von Abbildungen auftreten, kann die Verwendung von Diagrammen wie

$$\begin{tikzcd} & B \arrow[dr, "g"] & \\ A \arrow[ur, "f"] \arrow[rr, "g \circ f"'] & & C \end{tikzcd} \qquad \begin{tikzcd} A \arrow[r, "f"] \arrow[rr, bend right=60, "g \circ f"'] & B \arrow[r, "g"] & C \end{tikzcd}$$

oder ähnlichen die Übersicht erhöhen.
Hat man drei Abbildungen

$$f : A \longrightarrow B, \qquad g : B \longrightarrow C, \qquad h : C \longrightarrow D,$$

so kann man die Kompositionen $g \circ f$, $h \circ g$, aber auch $h \circ (g \circ f)$ und $(h \circ c) \circ f$ bilden. Diagramm:

$$\begin{tikzcd}
 & B \arrow[r, "h \circ g"] \arrow[d, "g"] & C \\
A \arrow[ur, "f"] \arrow[r, "g \circ f"] \arrow[urr, bend left=60, "(h \circ g) \circ f"] \arrow[urr, bend right=60, "h \circ (f \circ g)"'] & D \arrow[ur, "h"'] &
\end{tikzcd}$$

Durch Nachrechnen stellt man sofort fest, daß für alle $a \in A$ gilt

$$\begin{aligned}
&(h \circ (g \circ f))(a) = h((g \circ f)a) = h(g(f(a))) \quad \text{und} \\
&((h \circ g) \circ f)(a) = (h \circ g)(fa) = h(g(f(a))),
\end{aligned}$$

man sagt hierfür auch, daß die Zusammensetzung von Abbildungen *assoziativ* ist, läßt die Klammern weg und schreibt einfach $h \circ g \circ f$.

§2.4. Injektive, surjektive, bijektive Abbildungen

Seien M und N nichtleere Mengen und $f \in \operatorname{Abb}(M, N)$.
f heißt

(a) *surjektiv* (oder Abbildung auf), falls $fM = N$, falls also zu jedem $n \in N$ (mindestens) ein $m \in M$ mit $fm = n$ existiert.

(b) *injektiv*, falls aus $fm_1 = fm_2$ $(m_1, m_2 \in M)$ stets $m_1 = m_2$ folgt, mit anderen Worten: jedes $n \in N$ hat höchstens ein Urbild in M.

Äquivalent hierfür ist: Für alle $m_1, m_2 \in M$ mit $m_1 \neq m_2$ gilt $fm_1 \neq fm_2$.

(c) *bijektiv*, wenn f injektiv und surjektiv ist. Anders ausgedrückt: $f : M \to N$ ist genau dann bijektiv, wenn es zu jedem $n \in N$ genau ein $m \in M$ mit $fm = n$ gibt.

Beispiele:

1. Die Abbildung

$$\begin{array}{rccc}
f: & \mathbb{Z} & \longrightarrow & \mathbb{N}_0 \\
 & m & \longmapsto & m^2
\end{array}$$

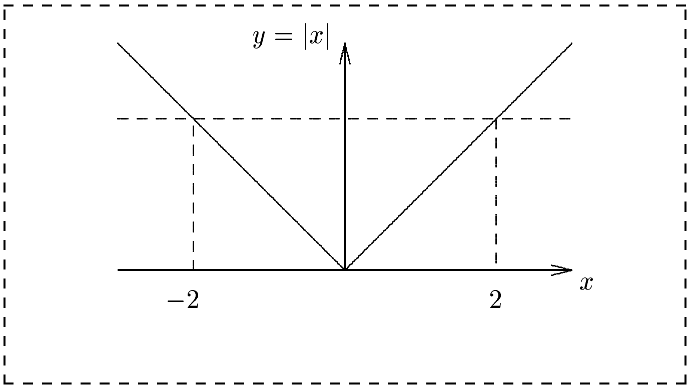
ist weder injektiv noch surjektiv, insbesondere also nicht bijektiv:

m und $-m$ haben dasselbe Bild, also ist f nicht injektiv. 5 hat z.B. kein Urbild, also ist f auch nicht surjektiv.

2. Die Abbildung

$$\begin{array}{rccc}
\operatorname{abs}: & \mathbb{R} & \longrightarrow & \mathbb{R}_+ := \{x \in \mathbb{R};\ x \geqslant 0\} \\
 & x & \longmapsto & \operatorname{abs}(x) = |x|
\end{array}$$

ist surjektiv, aber nicht injektiv, da z.B. 2 und -2 denselben Absolutbetrag haben.



3. Die Abbildung $f : \{1,2,3\} \to \{1,2,3\}$ definiert durch $f(1) = 2$, $f(2) = 3$, $f(3) = 1$ ist sowohl injektiv als auch surjektiv, damit bijektiv.

4. Die Projektion

$$\begin{array}{rccc} \mathrm{pr}_1 : & A \times B & \longrightarrow & A \\ & (a,b) & \longmapsto & a \end{array}$$

auf den ersten Faktor ist surjektiv, aber nicht injektiv, wenn B mehr als ein Element enthält.

5. Wir betrachten die Abbildung

$$\begin{array}{rccc} \mathrm{pr}_1 : & \mathbb{R}^2 & \longrightarrow & \mathbb{R}^2, \\ & (r_1, r_2) & \longmapsto & (3r_1 - 5r_2, -4r_1 + 3r_2). \end{array}$$

Daß f surjektiv ist bedeutet, daß für jedes Paar $(c_1, c_2) \in \mathbb{R} \times \mathbb{R}$ das lineare Gleichungssystem

$$\begin{aligned} 3x_1 - 5x_2 &= c_1 \\ -4x_1 + 3x_2 &= c_2 \end{aligned} \tag{$*$}$$

mindestens eine Lösung hat. Daß f injektiv ist bedeutet, daß für jedes c_1, c_2 für welches $(*)$ überhaupt lösbar ist, die Lösung eindeutig bestimmt ist. Beide Aussagen sind richtig, wie man leicht nachprüft, also ist f *bijektiv.*

Ist $f : M \to N$ eine gegebene Abbildung und $b \in N$. Dann kann es dazu ein $x \in M$ mit

$$f(x) = b \tag{$\star$}$$

geben, nämlich wenn $f^{-}(\{b\}) \neq \emptyset$ gilt, ein solches $x \in A$ braucht es aber nicht zu geben. Wir können folgendes festhalten:
Ist $b \in f(M)$, dann hat die Gleichung $(\star)$ mindestens eine Lösung. Ist $b \notin f(M)$, dann hat die Gleichung $(\star)$ keine Lösung. Ist f jedoch *surjektiv*, d.h. also $f(M) = N$, dann hat die Gleichung $(\star)$ für jedes $b \in N$ mindestens eine Lösung. Ist f injektiv, dann hat die Gleichung $(\star)$ für $b \in f(M)$ eine eindeutig bestimmte Lösung $x \in M$. Ist f bijektiv, dann hat die Gleichung $(\star)$ für jedes $b \in N$ eine eindeutig bestimmte Lösung in M.
Wir haben damit das folgende *Kriterium*: Eine Abbildung $f : M \to N$ ist genau dann bijektiv, wenn für jedes $y \in N$ die Gleichung

$$f(x) = y \tag{$\ddagger$}$$

eine eindeutig bestimmte Lösung $x \in M$ besitzt.

Ist aber $f : M \to N$ bijektiv, so können wir jedem $y \in N$ die eindeutig bestimmte Lösung x der Gleichung (‡) zuordnen: $y \mapsto$ das $x \in M$ mit $f(x) = y$. Wir bezeichnen dieses x auch mit $g(y)$ und erhalten so eine Abbildung

$$\begin{array}{rccc} g: & N & \longrightarrow & M, \\ & y & \longmapsto & x = g(y). \end{array}$$

Die so konstruierte Abbildung ist wieder bijektiv und heißt *Umkehrabbildung* von f. Bezeichnung:

$$g = f^{-1}$$

Ist $f : M \to N$ bijektiv und $g : N \to M$ die Umkehrabbildung, dann können wir die Zusammensetzung

$$\begin{tikzcd} M \arrow[r, "f"] \arrow[rr, bend right, "g \circ f"'] & N \arrow[r, "g"] & M \end{tikzcd}$$

betrachten.
Für $x \in M$ setzen wir $y = fx$, so ist $g(y)$ gerade wieder x. Also ist $g \circ f = \mathrm{id}_M$. Wir können auch die Zusammensetzung

$$\begin{tikzcd} N \arrow[r, "g"] \arrow[rr, bend right, "f \circ g"'] & M \arrow[r, "f"] & N \end{tikzcd}$$

betrachten. Ist $y \in N$ und $x \in X$ das Element mit $fx = y$, so gilt $g(y) = x$ und $f(g(y)) = f(x) = y$, damit $f \circ g = \mathrm{id}_N$. Damit haben wir die Hälfte des folgenden *Bijektivitätskriteriums* bewiesen:

Eine Abbildung $f : M \to N$ ist *genau dann bijektiv*, wenn es eine Abbildung $g : N \to M$ gibt mit $g \circ f = \mathrm{id}_M$ und $f \circ g = \mathrm{id}_N$.
g ist hierdurch eindeutig bestimmt und ist wieder bijektiv. g heißt die *Umkehrabbildung* von f. Bezeichnung: $g = f^{-1}$.
Beweis: Ist f bijektiv, dann hat die Umkehrabbildung die angegebenen Eigenschaften. Sei umgekehrt g eine Abbildung mit den angegebenen Eigenschaften, Dann ist f notwendig injektiv: Ist nämlich $f(a) = f(b)$, so folgt durch Anwendung von g wegen $g \circ f = \mathrm{id}_M$ sofort $a = g(fa) = g(fb) = b$. f ist auch surjektiv: Denn ist $y \in N$ ein beliebig vorgegebenes Element, so ist $f(g(y)) = f \circ g(y) = \mathrm{id}_N(y) = y$, also ist $g(y)$ ein Urbild von y. Daß g durch die beiden Bedingungen $g \circ f = \mathrm{id}_M$ und $f \circ g = \mathrm{id}_N$ eindeutig bestimmt ist, sieht man so: Gilt für eine Abbildung $g' : N \to M$ auch $g' \circ f = \mathrm{id}_M$ und $f \circ g' = \mathrm{id}_N$, dann ist $g'(y) = g(y)$ für alle $y \in N$ zu zeigen. Aus $g \circ f = g' \circ f = \mathrm{id}_M$ folgt $g = g \circ \mathrm{id}_N = g \circ (f \circ g') = (g \circ f) \circ g' = (g' \circ f) \circ g' = g' \circ (f \circ g') = g' \circ \mathrm{id}_N = g'$. Derselbe Beweis zeigt, daß g auch bijektiv ist, da der Beweis völlig symmetrisch ist. Somit ergibt sich auch, daß die Umkehrabbildung von $g = f^{-1}$ wieder f ist:

$$g^{-1} = (f^{-1})^{-1} = f$$

Für eine Teilmenge $B \subset N$ gilt nun gerade

$$g(B) = f^{-1}(B) = f^{-}(B).$$

§2.5. Endliche, abzählbar (unendliche) Mengen, überabzählbare Mengen

Die Sprechweise „Eine Menge M hat 5 Elemente“ ist intuitiv klar, man weiß, was damit gemeint ist. Der intuitiv klare Begriff der *endlichen Menge* und die Anzahl der Elemente einer solchen Menge läßt sich in einfacher Weise präzisieren, wenn man die natürlichen Zahlen zur Verfügung hat, Die *Abschnitte* $\mathbb{A}_n; = \{1, 2, \ldots, n\} = \{x \in \mathbb{N}; 1 \leqslant x \leqslant n\}$ sind Prototypen von *endlichen Mengen* mit (genau) n Elementen.
Eine Menge M, die man *bijektiv* auf einen Abschnitt $\mathbb{A}_n$ abbilden kann, wird man endlich nennen, und n nennt man dann die *Elementanzahl* (Kardinalzahl, Mächtigkeit) von M, Ist $a : \mathbb{A}_n \to M$, $k \mapsto a(k) =: a_k$, $1 \leqslant k \leqslant n$, eine solche Bijektion, so ist also $M = \{a_1, \ldots, a_k\}$ und $a_j \neq a_k$ für $j \neq k$. Die Elemente von M sind mit den natürlichen Zahlen von 1 bis n durchnumeriert. Dieses Vorgehen führt aber nur dann zu einer präzisen Definition, wenn man M nicht gleichzeitig auf zwei verschiedene Abschnitte $\mathbb{A}_m$ und $\mathbb{A}_n$ abbilden kann. Das ist aber nicht möglich, denn es gilt der folgende Satz:

Gibt es eine bijektive Abbildung $f : M \to \mathbb{A}_n$ und eine bijektive Abbildung $g : M \to \mathbb{A}_m$, dann ist $n = m$.

$$\begin{tikzcd}
 & \mathbb{A}_n \arrow[dl, dashed, "f^{-1}"] \arrow[dd, "h"] \\
M \arrow[ur, "f"] \arrow[dr, "g"'] & \\
 & \mathbb{A}_m
\end{tikzcd}$$

Da die Zusammensetzung bijektiver Abbildungen bijektiv ist ($h = g \circ f^{-1}$), genügt es zu zeigen, daß zwei Abschnitte $\mathbb{A}_n$ und $\mathbb{A}_m$ nur dann bijektiv aufeinander abgebildet werden können, wenn $n = m$ gilt. Vor dem Beweis noch zwei Vorbemerkungen:

1. Wenn es eine bijektive Abbildung $h : \mathbb{A}_{n+1} \to \mathbb{A}_m$ gibt, dann gibt es zu jedem festen und mit Element $n_0 \in \mathbb{A}_n$ eine bijektive Abbildung $\tilde{h} : \mathbb{A}_{n+1}$ mit $\tilde{h}(n_0) = m$. (Man muß dabei unter Umständen in $\mathbb{A}_m$ zwei Elemente vertauschen.)

2. Gibt es eine bijektive Abbildung $h : \mathbb{A}_{n+1} \to A_m$, dann gibt es auch eine bijektive Abbildung $h' : \mathbb{A}_n = \mathbb{A}_{n+1} - \{n+1\} \to \mathbb{A}_{m-1} = \mathbb{A}_m - \{m\}$. Man braucht dafür ja nur die Einschränkung von $\tilde{h}$ (siehe 1.) auf $\mathbb{A}_n$ zu nehmen.

Beweis des Satzes:

Wir benutzen vollständige Induktion (siehe S.41) nach n: Sei $S = \{n \in \mathbb{N} :$ für alle m gilt: Gibt es eine bijektive Abbildung $f : \mathbb{A}_n \to \mathbb{A}_m$, dann ist $n = m\}$. Dann ist offensichtlich $1 \in S$, d.h. aus $n = 1$ folgt $m = 1$. Sei im folgenden $n \geqslant 1$, $m > 1$. Sei also $n \in S$.
Induktionsschritt: Sei $h : \mathbb{A}_{n+1} \to \mathbb{A}_m$ bijektiv. Zu zeigen ist, daß $n + 1 = m$ gilt. Nach der Vorbemerkung 1 können wir o.B.d.A. $h(n + 1) = m$. Nach der Vorbemerkung 2 erhält man auch eine bijektive Abbildung

$$\mathbb{A}_n = \mathbb{A}_{n+1} - \{n + 1\} \longrightarrow \mathbb{A}_{m-1} = \mathbb{A}_m - \{m\}.$$

Hier wenden wir nun die Induktionsvoraussetzung an: Es folgt also $n = m-1$ und hieraus $n+1 = m$.

Für $n \neq m$ gibt es also keine bijektive Abbildung $\mathbb{A}_n \to A_m$. Jetzt erst ist folgende Definition gerechtfertigt:

Def.: Eine Menge M heißt *endlich*, wenn $M = \emptyset$ gilt, oder wenn es eine natürliche Zahl n gibt und eine bijektive Abbildung von $\mathbb{A}_n$ auf M existiert. Ist $M = \emptyset$, so sagt man M hat die Elementanzahl (Kardinalzahl, Mächtigkeit) Null. Ist $M \neq \emptyset$, dann nennt man die eindeutig bestimmte natürliche Zahl n die Elementanzahl (Anzahl der Elemente, Kardinalzahl oder Mächtigkeit) von M. *Bezeichnungen:* $\#M = |M| = \operatorname{card} M = n$

Als Übung zeige man:

(a) Ist M eine endliche Menge und N eine Teilmenge von M ($N \subset M$), dann ist auch N endlich, und es gilt: $\#N \leqslant \#M$.

(b) Sind M und N *disjunkte endliche Mengen*, dann ist auch $M \cup N$ endlich, und es gilt: $\#(M \cup N) = \#M + \#N$.

Eine endliche Menge kann also nicht auf eine echte Teilmenge bijektiv abgebildet werden, und eine *injektive* Abbildung zwischen endlichen Mengen M und N gibt es dann und nur dann, wenn $\#M \leqslant \#N$. Anders gewendet: Ist $m := \#M$ echt größer als $n := \#N$, dann gibt es keine injektive Abbildung $M \to N$. Dies bezeichnet man auch als *Dirichletsches Schubfachprinzip*.

Bei *unendlichen Mengen* ist die Situation völlig anders. Dabei heißt eine Menge M *unendlich*, wenn sie nicht endlich ist. $\mathbb{N}_0$ und $\mathbb{N}$ sind z.B. unendliche Mengen, und $\mathbb{N}$ ist eine Teilmenge von $\mathbb{N}_0$. Man stellt sich intuitiv vor, daß $\mathbb{N}_0$ „ein Element mehr" enthält als $\mathbb{N}$. Im Sinne von Cantor haben jedoch $\mathbb{N}$ und $\mathbb{N}_0$ dieselbe Mächtigkeit:

Def.: Zwei Mengen M und N heißen *gleichmächtig* (äquivalent), wenn es eine bijektive Abbildung $f; M \to N$ gibt. In Zeichen $M \sim N$.

Gleichmächtigkeit hat die Eigenschaft einer *Äquivalenzrelation:*

1. $M \sim M$ (mit $f = \mathrm{id}_M$)
2. Aus $M \sim N$ folgt $N \sim M$ (wenn $f : M \to N$ bijektiv, dann ist $g : N \to M$ mit $g = f^{-1}$)
3. Aus $M \sim N$ und $N \sim P$ folgt $M \sim P$, (Die Zusammensetzung bijektiver Abbildungen ist bijektiv)

Die Theorie der Gleichmächtigkeit ist der Ausgangspunkt für eine Klassifikation unendlicher Mengen nach ihrer „Elementanzahl" (Kardinalzahl, Mächtigkeit). Ist z.B. $M = \mathbb{N}_0$ und $N = \mathbb{N}$ und

$$\begin{array}{rccc} f: & \mathbb{N}_0 & \longrightarrow & \mathbb{N}, \\ & n & \longmapsto & n+1, \end{array}$$

dann ist f bijektiv, also

$$\#\mathbb{N}_0 = \#\mathbb{N}.$$

Für alle Mengen M, die zu $\mathbb{N}_0$ (damit auch zu $\mathbb{N}$) gleichmächtig sind, verwendet man für die Elementanzahl (Kardinalzahl) von M das Symbol $\aleph_0$ (*Aleph Null*). Mengen, die zu $\mathbb{N}_0$ gleichmächtig sind, nennt man auch *abzählbar (unendlich)*. Auch die Menge $\mathbb{Z}$ der ganzen Zahlen ist abzählbar (unendlich). Folgende Tabelle liefert eine *Numerierung* der ganzen Zahlen durch die natürlichen Zahlen:

$\mathbb{N}_0$	0	1	2	3	4	$\dots$	$2k-1$	$2k$	$\dots$
$\mathbb{Z}$	0	1	-1	2	-2	$\dots$	k	$-k$	$\dots$

Etwas formaler: Durch

$$f : \mathbb{N}_0 \longrightarrow \mathbb{Z}, \qquad f(n) = \begin{cases} k, & \text{falls } n = 2k-1 \\ -k, & \text{falls } n = 2k \end{cases}$$

wird eine Bijektion von $\mathbb{N}_0$ auf $\mathbb{Z}$ Definiert.

Weiter gilt: *Jede Teilmenge A von $\mathbb{N}_0$ ist endlich oder abzählbar.*

Beweisskizze: Ist A nicht endlich, so definiere man die Abbildung $f : \mathbb{N}_0 \to A$ wie folgt: $f(0) := \min A$ (dieses Minimum existiert nach Eigenschaft der natürlichen Zahlen), dann $f(1) := \min(A - \{f(0)\})$, $f(2) := \min(A - \{f(0), f(1)\})$, usw. Man muß dann allerdings nachweisen, daß das so definierte $f : \mathbb{N}_0 \to A$ bijektiv ist.

Als unmittelbare Folgerung aus dem obigen Satz erhält man nun:

Jede Teilmenge einer abzählbaren Menge ist endlich oder abzählbar.

Zur Vereinfachung der Sprechweise nennt man Mengen, die endlich oder abzählbar sind *höchstens abzählbar.*

Achtung: Die Bezeichnungen in der Literatur sind nicht einheitlich. Was wir „abzählbar“ genannt haben, wird in der Literatur auch häufig mit „abzählbar unendlich“ bezeichnet.

Unser nächstes Ziel ist es, zu zeigen, daß auch die Menge $\mathbb{Q}$ der rationalen Zahlen abzählbar ist. Ein wesentlicher Schritt hierzu ist:

$\boxed{\mathbb{N}_0 \times \mathbb{N}_0 \text{ ist abzählbar.}}$

Wir denken uns die Elemente (m,n) von $\mathbb{N}_0 \times \mathbb{N}_0$ in einem rechteckigen Schema angeordnet

$$\begin{array}{cccccccc}
(0,0) & & (0,1) & & (0,2) & & (0,3) & \dots \\
& \nearrow & & \nearrow & & \nearrow & & \\
(1,0) & & (1,1) & & (1,2) & & (1,3) & \dots \\
& \nearrow & & \nearrow & & \nearrow & & \\
(2,0) & & (2,1) & & (2,2) & & (2,3) & \dots \\
& \nearrow & & \nearrow & & \nearrow & & \\
(3,0) & & (3,1) & & (3,2) & & (3,3) & \dots \\
\vdots & & \vdots & & \vdots & & \vdots &
\end{array}$$

und zählen in der skizzierten Weise ab. Wir beginnen mit $(0,0)$ und dann die erste Diagonale, dann die zweite Diagonale, ... Also

$$\begin{array}{lll}
f(0) = (0,0), & & \\
f(1) = (1,0), & f(2) = (0,1), & \\
f(3) = (2,0), & f(4) = (1,1), & f(5) = (0,2), \\
\quad\vdots & &
\end{array}$$

Die Umkehrabbildung $g : \mathbb{N}_0 \times \mathbb{N}_0 \to \mathbb{N}_0$ ist gegeben durch $g(m,n) = n + \frac{(m+n)(m+n+1)}{2}$. Der mißtrauische Leser prüfe nach, daß $f \circ g = \mathrm{id}_{\mathbb{N}_0}$ und $g \circ f = \mathrm{id}_{\mathbb{N}_0}$ gilt.
Die Abzählbarkeit von $\mathbb{N}_0 \times \mathbb{N}_0$ ergibt sofort die etwas allgemeinere Aussage:

Das Produkt $A \times B$ zweier abzählbarer Mengen ist abzählbar.

Seien nämlich $f_1 : \mathbb{N} \to A$ und $f_2 : \mathbb{N} \to B$ so wird durch

$$\begin{array}{rccc}
f_1 \times f_2 : & \mathbb{N} \times \mathbb{N} & \longrightarrow & A \times B \\
& (m,n) & \longmapsto & (f_1(m), f_2(n))
\end{array}$$

eine bijektive Abbildung definiert. (Beweis?)

Speziell ist $\mathbb{Z} \times \mathbb{Z}$ und ebenso jede unendliche Teilmenge von $\mathbb{Z} \times \mathbb{Z}$.

$\boxed{\mathbb{Q} \text{ ist abzählbar.}}$

Beweis: Ordnet man jedem *gekürzten* Bruch $\frac{p}{q} \in \mathbb{Q}$, $p, q \in \mathbb{Z}$, $q \neq 0$, p und q teilerfremd, das Element $(p, q) \in \mathbb{Z} \times \mathbb{Z}$ zu, so erhält man eine bijektive Abbildung von $\mathbb{Q}$ auf eine unendliche Teilmenge von $\mathbb{Z} \times \mathbb{Z}$. $\mathbb{Q}$ ist also abzählbar.

Eine unendliche Menge, die nicht abzählbar (unendlich) ist, heißt *überabzählbar*.

Frage: Gibt es überabzählbare Mengen?
Sei $M \neq \emptyset$ und $N = \{0, 1\}$ und $F = \mathrm{Abb}(M, N)$, also die Menge aller Abbildungen von M in N (diese nehmen also nur die Wert 0 und 1 an). Ordnet man jedem $m \in M$ die Abbildung $f_m; M \to N$ zu, die durch $f_m(x) = 1$, falls $x = m$ und $f_m(x) = 0$ falls $x \neq m$ definiert ist, so sind M und die Teilmenge $\{fm;\ m \in M\}$ von F äquivalent. M ist jedoch nicht zur ganzen Menge F äquivalent: Andernfalls gäbe es eine bijektive Abbildung $m \to F$, $m \mapsto f^{(m)}$. Definiert man dann die Abbildung $f : M \to N$ durch

$$f(m) = \begin{cases} 1, & \text{falls } f^{(m)} = 0, \\ 0 & , \text{ falls } f^m(m) = 1, \end{cases}$$

dann liegt f in F, stimmt aber mit keinem $f^{(m)}$ überein. Dieser Widerspruch zeigt, daß M und F nicht gleichmächtig sein können, und daß F eine größere Mächtigkeit als M hat.
Nimmt man z.B. für $M = \mathbb{N}_0$, so ist $F = \mathrm{Abb}(\mathbb{N}_0, N)$ die Menge aller Folgen, welche nur die Werte 0 oder 1 annehmen. Diese Menge ist aber überabzählbar. Für die Analysis entscheidend ist

$$\boxed{\mathbb{R} \text{ ist überabzählbar.}}$$

Ist $f = (f_n) \in F = \mathrm{Abb}(\mathbb{N}_0, \{0, 1\})$, dann kann man diesem f einen unendlichen Dezimalbruch (reelle Zahl) zuordnen und umgekehrt:

$$f \longleftrightarrow x_f := \tfrac{f_1}{10} + \tfrac{f_2}{10^2} + \tfrac{f_3}{10^3} + \dots$$

x_f stellt eine reelle Zahl (im Intervall $[0, 1[$) dar. Die Menge der so erhaltenen Dezimalbrüche ist überabzählbar, erst recht alle reellen Zahlen im Intervall $[0, 1[$.

Anmerkungen:

- War wir nebenbei gezeigt haben ist, daß für jede nichtleere Menge M die Potenzmenge $\mathcal{P}(M)$ eine größere Mächtigkeit als M besitzt. Denn definiert man für eine Teilmenge $A \subset M$ die charakteristische Funktion chi_A (siehe S.17), dann ist die Abbildung $A \mapsto \chi_A$ eine Bijektion von der Menge aller Teilmengen von M (also der Potenzmenge) auf die Menge $\mathrm{Abb}(M, \{0, 1\}) = F$. Die Überabzählbarkeit von F haben wir oben bereits mit dem *Cantorschen Diagonalverfahren* gezeigt.

- Für die Mächtigkeit von $\mathbb{R}$ verwendet man das Zeichen $\aleph_1$ (*Aleph 1*).

  Frage: Ist $M \subset \mathbb{R}$, gilt dann notwendig $\#M = \aleph_0 = \#\mathbb{N}_0$ oder $\#M = \aleph_1 = \#\mathbb{R}$?

  Dies ist die bekannte *Kontinuumshypothese*, welche D. Hilbert als erstes Problem mit in seine Liste von zentralen Fragen der Mathematik aufnahm. (Siehe Hilberts Vortrag auf dem Mathematiker-Kongreß 1900 in Paris). Die Antwort wurde erst 1963 von P. Cohen gegeben. Sie ist einigermaßen überraschend:

  Mit den üblichen Axiomen der Mengenlehre (ZFC) läßt sich die Kontinuumshypothese grundsätzlich weder beweisen noch widerlegen.

§3. Verknüpfungen, algebraische Strukturen

§3.1. Definition und Beispiele

Unter den Begriff „Verknüpfung“ fallen die Addition und Multiplikation von Zahlen, die Addition von Vektoren und anderes. Eine abstrakte Behandlung der diesen Operationen gemeinsamen

Eigenschaften (z.B. die Existenz vom neutralen Element) erspart viele Wiederholungen in ähnlichen Situationen. Die Addition reeller Zahlen kann man mit der Abbildungssprache wie folgt beschreiben: Jedem Paar (a, b) reeller Zahlen ist eine weitere reelle Zahl, die Summe von a und b zugeordnet. Es liegt als eine Abbildung:

$$\begin{array}{rccl} \mathrm{ad}: & \mathbb{R}\times\mathbb{R} & \longrightarrow & \mathbb{R} \\ & (a,b) & \longmapsto & \mathrm{ad}(a,b) =: a+b \end{array}$$

vor, die noch gewissen Bedingungen genügen muß.
Auch die Multiplikation reeller Zahlen läßt sich analog auffassen: Jedem Paar (a, b) reeller Zahlen ist eine weitere reelle Zahl, das Produkt von a und b zugeordnet. Es liegt also ebenfalls eine Abb.

$$\begin{array}{rccl} \mathrm{mult}: & \mathbb{R}\times\mathbb{R} & \longrightarrow & \mathbb{R} \\ & (a,b) & \longmapsto & \mathrm{mult}(a,b) =: ab \end{array}$$

vor.

Def.: Eine (innere) *Verknüpfung* auf einer Menge $M \neq \emptyset$ ist eine Abbildung $f : M \times M \to M$.

Beispiele:

1. Die Addition und Multiplikation natürlicher (bzw. ganzer bzw. rationaler bzw. reeller) Zahlen liefert jeweils eine Verknüpfung auf $\mathbb{N}$ (bzw. $\mathbb{Z}$ bzw. $\mathbb{Q}$ bzw. $\mathbb{R}$).

   Dagegen ist die Subtraktion natürlicher Zahlen $(m, n) \mapsto m - n$ keine Verknüpfung auf $\mathbb{N}$, sie liefert lediglich eine Abbildung $\mathbb{N} \times \mathbb{N} \to \mathbb{Z}$.

2. Ist X eine feste nichtleere Menge, so definieren Durchschnitt und Vereinigung Verknüpfungen auf der Potenzmenge $\mathcal{P}(X)$.

   Auch die Abbildung der *symmetrischen Differenz* ist eine Verknüpfung auf $\mathcal{P}(X)$:

   $$\begin{array}{ccc} \mathcal{P}(X)\times\mathcal{P}(X) & \longrightarrow & \mathcal{P}(X) \\ (A,B) & \longmapsto & (A-B)\cup(B-A) \end{array}$$

3. Ist M eine feste nichtleere Menge, so ist die Zusammensetzung (Komposition, Verkettung) von Abbildungen von M in sich eine Verknüpfung mit $\mathrm{Abb}(M, M)$.

4. Verknüpfungen in endlichen Mengen kann man sich durch *Verknüpfungstafeln* (das ist eine Art kleines Einmaleins) beschreiben.

   In $\mathbb{Z}/3\mathbb{Z}$ (vgl. S.35) definieren wir die folgende Addition und Multiplikation:

   $$\begin{array}{c|ccc} + & \overline{0} & \overline{1} & \overline{2} \\ \hline \overline{0} & \overline{0} & \overline{1} & \overline{2} \\ \overline{1} & \overline{1} & \overline{2} & \overline{0} \\ \overline{2} & \overline{2} & \overline{0} & \overline{1} \end{array} \qquad \begin{array}{c|ccc} \cdot & \overline{0} & \overline{1} & \overline{2} \\ \hline \overline{0} & \overline{0} & \overline{0} & \overline{0} \\ \overline{1} & \overline{0} & \overline{1} & \overline{2} \\ \overline{2} & \overline{0} & \overline{2} & \overline{1} \end{array}$$

5. Ist V ein K-Vektorraum, so ist die Addition von Vektoren eine Verknüpfung in V, d.h. eine Abbildung $V \times V \to V$. Bei der Multiplikation mit Skalaren (= Körperelementen) handelt es sich um eine Abbildung $K \times V \to V$. Man nennt dies eine *äußere Verknüpfung* auf V (Genauer: Operation von K auf V).

Für Verknüpfungen auf einer Menge M benutzt man oft die additive Schreibweise:

$$M \times M \longrightarrow M \qquad (x, y) \longmapsto x + y$$

oder die multiplikative Schreibweise

$$M \times M \longrightarrow M \qquad (x, y) \longmapsto x \cdot y,$$

wobei man den Multiplikationspunkt meist wegläßt und statt $x \cdot y$ einfach xy schreibt.
Um gemeinsame Eigenschaften von Verknüpfungen herauszuarbeiten, werden wir für eine Verknüpfung auf einer Menge M ein neutrales Symbol verwenden:

$$M \times M \longrightarrow M \qquad (x, y) \longmapsto x \diamond y,$$

(gelesen: x verknüpft mit y)
Folgende Situation tritt in den Anwendungen häufig auf: Man hat eine Menge M mit einer Verknüpfung $\diamond$ und betrachtet Abbildungen von irgendeiner Menge A in M. Die Verknüpfung in M gibt nun die Möglichkeit, in der Menge $\mathrm{Abb}(A, M)$ eine Verknüpfung zu definieren: Für $f_1, f_2 \in \mathrm{Abb}(A, M)$ definiert man $f_1 \diamond f_2$ als die durch

$$\begin{array}{rccl} f_1 \diamond f_2 : & A & \longrightarrow & M \\ & a & \longmapsto & f_1(a) \diamond f_2(a) \end{array}$$

gegebene Abbildung. Man sagt auch $f_1 \diamond f_2$ ist die durch $\diamond$ auf $\mathrm{Abb}(A, M)$ *induzierte* Verknüpfung.
Ein klassisches Beispiel erhält man, wenn man $A = \mathbb{R}$ und $M = \mathbb{R}$ einmal mit $\diamond = +$ und zum anderen mit $\diamond = \cdot$ als Verknüpfung nimmt. Für $f_1, f_2 \in \mathrm{Abb}(\mathbb{R}, \mathbb{R})$ setzt man als:

$$\begin{array}{rccl} f_1 + f_2 : & A & \longrightarrow & M \\ & a & \longmapsto & (f_1 + f_2)(x) := f_1(a) + f_2(a) \end{array}$$

$$\begin{array}{rccl} f_1 \cdot f_2 : & A & \longrightarrow & M \\ & a & \longmapsto & (f_1 \cdot f_2)(x) := f_1(a) \cdot f_2(a) \end{array}$$

Man spricht von der *punktweisen Addition* und der *punktweisen Multiplikation.*

§3.2. Assoziativität und Kommutativität

Eine Verknüpfung auf einer Menge gestattet es, jeweils mehrere Elemente der Menge in einer bestimmten Weise miteinander zu verknüpfen. Will man mehr als zwei Elemente miteinander verknüpfen, muß man vorsichtig agieren und Klammern setzen, denn das Ergebnis könnte von der Klammerung abhängen. Zum Beispiel brauchen für die Elemente x, y, z die Elemente $x \diamond (y \diamond z)$ und $(x \diamond y) \diamond z$ nicht übereinzustimmen. Häufig tun sie es doch, und deshalb führt man für diesen Sachverhalt einen Namen ein.

Def.: Eine Verknüpfung auf einer Menge M heißt *assoziativ*, wenn für je drei Elemente $x, y, z \in M$ gilt:

$$x \diamond (y \diamond z) = (x \diamond y) \diamond z.$$

Beispiele:

1. Alle Verknüpfungen, die uns bisher begegnet sind, sind *assoziativ* (z.B. auch die symmetrische Differenz als Verknüpfung in $\mathcal{P}(X)$).
2. Es gibt jedoch auch Verknüpfungen, die nicht assoziativ sind:
   Sei z.B. $M = \mathbb{Z}$ und $(m, n) \mapsto m - n$, dann ist für $m, n, k \in \mathbb{Z}$:

   $$(m \diamond n) \diamond k = (m - n) - k$$
   $$m \diamond (n \diamond k) = m - (n - k)$$

3. Ein weiteres Beispiel für eine nicht assoziative Verknüpfung ist durch folgende Verknüpfungstafel auf einer Menge $M = \{a, b\}$ mit zwei Elementen gegeben:

$$\begin{array}{c|cc} \diamond & a & b \\ \hline a & b & a \\ a & b & a \end{array}$$

Hier ist

$$a \diamond (b \diamond b) = a \diamond a = b$$

aber

$$(a \diamond b) \diamond b = a \diamond b = a.$$

Bei einer assoziativen Verknüpfung sind auch Verknüpfungen von mehr als 3 Elementen unabhängig von der Klammerung, etwa

$$\begin{aligned} ((x \diamond y) \diamond u) \diamond v &= (x \diamond y) \diamond (u \diamond v) \\ &= x \diamond (y \diamond (u \diamond v)). \end{aligned}$$

In einer assoziativen Verknüpfung kann man daher auf Klammern ganz verzichten. Für die Verknüpfung endlich vieler Elemente $x_1, \ldots, x_n \in M$ schreibt man auch kurz

$$x_1 \diamond x_2 \diamond \ldots \diamond x_n =: \mathop{\diamond}_{j=1}^{n} x_j.$$

Mit $\diamond = +$ bzw. $\diamond = \cdot$ schreibt man

$$\begin{aligned} x_1 + x_2 + \ldots + x_n &=: \sum_{j=1}^{n} x_j \quad \text{bzw.} \\ x_1 \cdot x_2 \cdots x_n &=: \prod_{j=1}^{n} x_j. \end{aligned}$$

Ist die Verknüpfung $\diamond$ in M assoziativ, so vererbt sich dies auf die induzierte Verknüpfung in $\mathrm{Abb}(A, M)$. Denn für $f_1, f_2 \in \mathrm{Abb}(A, M)$ und beliebiges $a \in A$ gilt

$$\begin{aligned} ((f_1 \diamond f_2) \diamond f_3)(a) &= (f_1 \diamond f_2)(a) \diamond f_3(a) \\ &= (f_1(a) \diamond f_2(a)) \diamond f_3(a) \\ &= f_1(a) \diamond f_2(a) \diamond f_3(a) \\ &= f_1(a) \diamond (f_2(a) \diamond f_3(a)) \\ &= (f_1 \diamond (f_2 \diamond f_3))(a) \end{aligned}$$

Wie wurde die Assoziativität der Verknüpfung in M verwendet?

Werden einfache Beispiele gegeben, etwa die Verknüpfung

$$\begin{array}{ccc} \mathbb{N} \times \mathbb{N} & \longrightarrow & \mathbb{N} \\ (m, n) & \longmapsto & m \diamond n := m^n \end{array}$$

hängt das Resultat der Verknüpfung i.a. von der Reihenfolge ab (i.a. ist $m \diamond n \neq n \diamond m$). Ist das Resultat jedoch unabhängig von der Reihenfolge, gilt also für beliebige $x, y \in M$, $x \diamond y = y \diamond x$, dann kann man x und y bezüglich $\diamond$ vertauschen.

Def.: Eine Verknüpfung $\diamond$ auf einer Menge M heißt *kommutativ*, wenn stets gilt $x \diamond y = y \diamond x$. Zwei beliebige Elemente aus M sind also stets vertauschbar (bzgl. der Verknüpfung $\diamond$).

Beispiele für kommutative Verknüpfungen sind z.B. die Addition und Multiplikation in $\mathbb{R}$, die Addition von Vektoren in einem $\mathbb{K}$-Vektorraum.

Die Multiplikation von Matrizen oder die Komposition von Abbildungen (in $\mathrm{Abb}(M, M)$) sind i.a. nicht kommutativ. Sei z.B. $M = \{1, 2, 3\}$ und $\sigma : M \to M$ bzw. $\tau : M \to M$ die Abbildungen (Permutationen) mit

$$\begin{array}{lll} \sigma(1) = 2, & \sigma(2) = 1, & \sigma(3) = 3, \\ \tau(1) = 1, & \tau(2) = 3, & \tau(3) = 2. \end{array}$$

Dann gilt

$$\begin{array}{rcl} \tau(\sigma(1)) = 3 & \neq & 2 = \sigma(\tau(1)), \\ \tau(\sigma(2)) = 1 & \neq & 3 = \sigma(\tau(2)), \\ \tau(\sigma(3)) = 2 & \neq & 1 = \sigma(\tau(3)), \end{array}$$

also ist $\tau \circ \sigma \neq \sigma \circ \tau$.
Bei einer Verknüpfung, die sowohl assoziativ als auch kommutativ ist, kommt es nicht auf die Reihenfolge der Elemente an: z.B. gilt

$$(x \diamond y) \diamond z = (y \diamond x) \diamond z = z \diamond (y \diamond x) = (z \diamond y) \diamond x,$$

wofür man dann einfach $x \diamond y \diamond z$ schreibt.
Auch die Kommutativität der Verknüpfung in M vererbt sich auf die Verknüpfung in $\mathrm{Abb}(A, M)$.

Bei einer *endlichen* Menge (auf einer endlichen Verknüpfungstafel) läßt sich die Kommutativität leicht nachweisen: Die Verknüpfungstafel muß symmetrisch zur Hauptdiagonalen sein.

§3.3. Neutrale Elemente und Inverse

Bei der Addition der ganzen (natürlichen oder reellen) Zahlen oder der Addition von Vektoren spielt die Zahl 0 bzw. der Nullvektor $\vec{0}$ eine ausgezeichnete Rolle: Für alle ganzen (natürlichen bzw. reellen) Zahlen x gilt:

$$0 + x = x.$$

Für jeden Vektor $\vec{v}$ eines $\mathbb{K}$-Vektorraumes V gilt

$$\vec{0} + \vec{v} = \vec{v}.$$

Eine analoge Rolle spielt das Element 1 bei der Multiplikation in $\mathbb{Z}$ bzw. in $\mathbb{Q}$ bzw. $\mathbb{R}$.

Def.: Sei M eine Menge mit einer Verknüpfung $\diamond$. Ein Element $e \in M$ heißt *neutrales Element* (bzgl. dieser Verknüpfung), wenn stets gilt

$$e \diamond x = x \diamond e = x.$$

Durch diese Forderung ist ein solches Element eindeutig bestimmt: Denn sind e_1 und e_2 neutrale Elemente bzgl. $\diamond$, so gilt $e_1 = e_1 \diamond e_2 = e_2$.

Beispiele: Die Menge der geraden ganzen Zahlen $G = 2\mathbb{Z}$ hat bzgl. der Multiplikation kein neutrales Element. Das neutrale Element in $\mathrm{Abb}(M, M)$ ist id_M.

Zu bemerken ist weiterhin, daß sich auch die Existenz eines neutralen Elements in M auf $\mathrm{Abb}(A, M)$ vererbt. Definiert man nämlich $\epsilon : A \to M$ durch $\epsilon(a) = 1$ für alle $a \in M$, dann ist ϵ ein neutrales Element in $\mathrm{Abb}(A, M)$, wie man unschwer nachrechnet.
Man nennt ein neutrales Element bei additiver Schreibweise auch *Nullelement* (und bezeichnet es mit 0), bei multiplikativer Schreibweise *Einselement* (und bezeichnet es dann mit 1).

Für jede ganze Zahl n gibt es eine ganze Zahl n' mit $n' + n = 0$. Diese ganze Zahl n' ist eindeutig bestimmt, und man bezeichnet sie i.a. mit $-n$ (das Negative von n).

Def.: Sei M eine Menge mit Verknüpfung $\diamond$, die ein neutrales Element besitzt. Ein Element $y \in M$ heißt *Inverses* von $x \in M$, wenn gilt

$$x \diamond y = e = y \diamond x.$$

Anmerkung: Nach Definition gilt: y ist genau dann Inverses von x, wenn x Inverses von y ist. Elemente aus M, die ein Inverses besitzen, heißen auch *invertierbar* (in M).

Beispiele:

1. Betrachtet man die ganzen Zahlen $\mathbb{Z}$ mit der Multiplikation als Verknüpfung, dann sind $+1$ und -1 die einzigen invertierbaren Elemente in $\mathbb{Z}$

2. Betrachte man $\mathbb{Q}$ oder $\mathbb{R}$ mit der Multiplikation als Verknüpfung, so ist jedes Element $r \neq 0$ invertierbar mit Inversem $r^{-1} = \frac{1}{r}$.

3. In $\mathrm{Abb}(M, M)$ mit der Komposition als Verknüpfung sind genau die bijektiven Abbildungen f invertierbar. Das Inverse von f ist die Umkehrabbildung f^{-1}.

Manchmal sind feinere Begriffsbildungen nötig: gilt in einer Menge M mit Verknüpfung $\diamond$ und neutralem Element e für $x, y \in M$ die Gleichung

$$x \diamond y = e,$$

(und nicht notwendig auch $y \diamond x = e$), so sagt man, daß y *Rechtsinverses* von x und x *Linksinverses* von y ist. x nennt man dann auch *rechtsinvertierbar*, y *linksinvertierbar*. Bei einer kommutativen Verknüpfung braucht man solche Unterscheidungen nicht zu machen.
Wir betrachten als Beispiel $\mathrm{Abb}(M, M)$ mit der Komposition als Verknüpfung. Für $f \in \mathrm{Abb}(M, M)$ gilt:

$$\begin{array}{lcl} f \text{ linksinvertierbar} & \iff & f \text{ injektiv,} \\ f \text{ rechtsinvertierbar} & \iff & f \text{ surjektiv.} \end{array}$$

Wenn z.B. f linksinvertierbar ist, dann gibt es also ein $g \in \mathrm{Abb}(M, M)$ mit $g \circ f = \mathrm{id}_M$. Aus $f(x) = f(y)$ folgt durch Anwendung von g, daß $x = (g \circ f)(x) = g(f(x)) = g(f(y)) = (g \circ f)(y) = y$. Also ist f injektiv. Die Umkehrung zu zeigen, sei dem Leser als Übung überlassen.
Bei einer *assoziativen Verknüpfung* Verknüpfung mit neutralem Element e sind Inverse eindeutig bestimmt. Zunächst kann man feststellen: Hat ein Element $x \in M$ sowohl ein Linksinverses y_1 als auch ein Rechtsinverses y_2, so gilt $y_1 = y_2$. Aus der Voraussetzung $y_1 \diamond x = e = x \diamond y_2$ folgt nämlich

$$\begin{aligned} y_1 = y_1 \diamond e &= y_1 \diamond (x \diamond y_2) \\ &= (y_1 \diamond x) \diamond y_2 \\ &= e \diamond y_2 \\ &= y_2. \end{aligned}$$

y_1 ist also auch Rechtsinverses und y_2 auch Linksinverses und beide stimmen überein. Wir haben also:
Satz: Sei M eine Menge mit einer assoziativen Verknüpfung $\diamond$, die ein neutrales Element besitzt. Dann gilt: Ein Element aus M ist genau dann invertierbar, wenn es sowohl links- als auch recht-sinvertierbar ist.
Das Inverse eines invertierbaren Elements ist eindeutig bestimmt und wieder invertierbar (nach zweimaliger Bildung des Inversen kommt man zum Ausgangselement zurück.)
Bei einer assoziativen Verknüpfung mit neutralem Element bezeichnet man das Inverse eines invertierbaren Elements x bei additiver Schreibweise mit $-x$ bei multiplikativer Schreibweise mit x^{-1}. Es gilt daher stets $-(-x) = x$ bzw. $(x^{-1})^{-1} = x$.

Bemerkung: Sind bei einer *assoziativen* Verknüpfung x auf M mit neutralem Element e zwei Elemente x und y invertierbar mit Inversem $\overline{x}$ bzw. $\overline{y}$, so ist auch $x \diamond y$ invertierbar und hat das Inverse $\overline{y} \diamond \overline{x}$. (Achtung: Die Reihenfolge ist vertauscht!) Es gilt also die Regel:

$$\overline{x \diamond y} = \overline{y} \diamond \overline{x}$$

(in multiplikativer Schreibweise also $(xy)^{-1} = y^{-1}x^{-1}$.)
Man braucht bloß anzusetzen:

$$\begin{aligned}(x \diamond y) \diamond (\overline{y} \diamond \overline{x}) &= x \diamond e \diamond \overline{x}\\ &= x \diamond \overline{x}\\ &= e\end{aligned}$$

bzw.

$$\begin{aligned}(\overline{y} \diamond \overline{x}) \diamond (x \diamond y) &= \overline{y} \diamond (\overline{x} \diamond x) \diamond y\\ &= \overline{y} \diamond e \diamond y\\ &= \overline{y} \diamond y\\ &= e\end{aligned}$$

§3.4. Gruppen

Mit den bisher entwickelten Begriffen lassen sich die *fundamentalen algebraischen Strukturen* leicht und einprägsam definieren. Im folgenden stellen wir einige Definitionen zusammen und geben jeweils einige Beispiele. Die Begriffe (*Gruppe*, *Ring*, *Körper*) werden in der Analysis-Vorlesung bzw. Vorlesung Lineare Algebra beim ersten Auftreten diskutiert. Eine weitergehende, tiefere Betrachtung dieser algebraischen Strukturen ist jedoch der Kursusvorlesung „Algebra 1“ vorbehalten.

Def.: Eine *Gruppe* ist eine Menge G mit einer assoziativen Verknüpfung, die ein neutrales Element besitzt und für die jedes Element invertierbar ist.

Bem.: Man kann schwächere Forderungen an den Begriff „Gruppe“ stellen. Hierauf gehen wir an dieser Stelle nicht ein.

Schreibt man (wie indes häufig geschieht) die Verknüpfung in einer Gruppe multiplikativ, dann sind die Forderungen an die Multiplikation die folgenden:

1. Für alle $x, y, z \in G$ gilt:

   $$x(yz) = (xy)z \qquad (\textit{Assoziativität})$$

2. Es gibt ein Element $e \in G$ so, daß für alle $x \in G$ gilt

   $$ex = x = xe \qquad (\textit{Existenz eines (links-) und (rechts-)neutralen Elements})$$

3. Zu jedem $x \in G$ gibt es ein $x^{-1} \in G$ mit

   $$x^{-1}x = e = x^{-1}x \qquad (\textit{Existenz eines (links-) und (rechts-)inversen Elements})$$

Wir haben ausdrücklich *nicht* verlangt, daß für *alle* $x, y \in G$ gilt:

$$\boxed{xy = yx}$$

Eine Gruppe, bei der die Verknüpfung sogar kommutativ ist, heißt *kommutative Gruppe* oder *abelsche Gruppe* (N. H. Abel, 1802–1829)
In einer abelschen Gruppe schreibt man die Verknüpfung meist als Addition.

Bemerkung: Unser Axiomensystem für eine Gruppe ist nicht minimal, es genügt z.B., für das Element nur zu fordern, daß es linksneutral ist, d.h. $ex = x$ für alle $x \in G$ gilt, und es genügt auch, lediglich zu fordern, daß es zu jedem $x \in G$ ein $x^{-1} \in G$ und $x^{-1}x = e$ gibt (Existenz eines Linksinversen). e und x^{-1} sind dann schon eindeutig bestimmt, und es gilt auch $xe = x$ für alle $x \in G$ (e ist also auch rechtsneutral), und aus $x^{-1}x = e$ folgt stets auch $xx^{-1} = e$ (ein Linksinverses ist auch Rechtsinverses). Beweise dafür findet man z.B. in G. Fischer: *Lineare Algebra*, 11. Auflage im Abschnitt 1.2.

Beispiele:

1. Die Menge $\mathbb{Z}$ der ganzen Zahlen ist mit der Addition von ganzen Zahlen eine (abelsche) Gruppe.

2. Bzgl. der Multiplikation ist $\mathbb{Z}$ jedoch keine Gruppe, da nur die Elemente 1 und -1 in $\mathbb{Z}$ invertierbar sind.

3. Die Teilmenge $E_{\mathbb{Z}} := \{1, -1\}$ von $\mathbb{Z}$ mit der Multiplikation als Verknüpfung eine abelsche Gruppe.

4. Für eine beliebige nichtleere Menge M bezeichen wir mit S_M die Menge aller *bijektiven Abbildungen* von M auf sich:

   $$S_M := \{f \in \mathrm{Abb}(M, M),\ f \text{ bijektiv}\}$$

   Mit der Komposition von Abbildungen als Verknüpfung wird S_M zu einer Gruppe, der sogenannten *symmetrischen Gruppe von* M (oder *Permutationsgruppe von* M).

   Im Spezialfall einer endlichen Menge $M = \{1, 2, \ldots, n\}$ schreibt man statt $S_M = S_{\{1,2,\ldots,n\}}$ einfach S_n und spricht von der *symmetrischen Gruppe* (*Permutationsgruppe*) über der Menge mit n Elementen.

   Diese Gruppe hat endlich viele Elemente, nämlich genau $n! := 1 \cdot 2 \cdots n$.

   Besitzt eine Gruppe G nur endlich viele Elemente, so nennt man die Elementanzahl von G auch die *Ordnung von* G.

   $$\boxed{S_n \text{ hat die Ordnung } n!}$$

   Für $n \geqslant 3$ ist S_n nicht abelsch, wie das Beispiel auf S. 31 zeigt.

5. Die „kleinste“ Gruppe, die man sich vorstellen kann hat die Ordnung 1. Da das neutrale Element *immer* zu einer Gruppe gehört, muß in diesem Fall $G = \{e\}$ gelten. Die einzige mögliche Verknüpfung auf G ist die Abbildung

   $$\begin{array}{ccc} G \times G & \longrightarrow & G \\ (e, e) & \longmapsto & e \end{array}$$

6. Ist G eine Gruppe und A irgendeine Menge, so ist $\mathrm{Abb}(A, G)$ mit der induzierten Verknüpfung eine Gruppe.

7. Mit $\mathrm{GL}(n, K)$ oder $\mathrm{GL}_n(K)$ bezeichnet man die Menge aller invertierbaren $n \times n$-Matrizen mit Koeffizienten in K. Mit der Matrizenmultiplikation ist $GL(n, K)$ eine Gruppe (*G*eneral *L*inear Group). Für $n > 1$ ist $\mathrm{GL}(n, K)$ nicht abelsch.

8. In $\mathcal{P}(X)$ definiert die symmetrische Differenz als Verknüpfung eine Gruppenstruktur. Neutrales Element bzgl. dieser Verknüpfung ist die leere Menge.

Weitere Beispiele für Gruppen werden Ihnen in den Vorlesungen begegnen.

§3.5. Ringe

Auf der Menge $\mathbb{Z}$ der ganzen Zahlen sind zwei Verknüpfungen gegebenen: die Addition ganzer Zahlen und die Multiplikation ganzer Zahlen, und beide genügen noch gewissen „Verträglichkeitsbedingungen".

Def.: Ein *Ring* ist eine Menge R, auf der zwei Verknüpfungen „$+$" und „$\cdot$" erklärt sind, die folgende Bedingungen erfüllen:

(a) R ist bzgl. „$+$" (Addition) eine abelsche Gruppe.

(b) Die Multiplikation „$\cdot$" ist assoziativ, und es gibt ein Einselement bzgl. „$\cdot$".

(c) Für $a, b, c \in R$ gilt:

$$a \cdot (b + c) = (a \cdot b) + (a \cdot c)$$
$$(a + b) \cdot c = (a \cdot c) + (b \cdot c)$$

Die Identitäten in (c) regeln die Beziehung zwischen Addition und Multiplikation. Sie heißen *Distributivgesetze*. Meist läßt man die Klammern und Punkte in (c) weg und schreibt statt der Gleichungen in (c) einfach

$$a(b + c) = ab + ac,$$
$$(a + b)c = ac + bc,$$

dabei machen wir Gebrauch von folgender

Vereinbarung: Punktrechnung geht vor Strichrechnung!

Ist die Multiplikation in R kommutativ, d.h. gilt $ab = ba$ für alle $a, b \in R$, so heißt R ein *kommutativer Ring*. Es genügt dann *eines* der beiden Distributivgesetze zu fordern, das andere ist dann eine Folgerung aus der Kommutativität von R.
Von den Rechenregeln in einem Ring beweisen wir exemplarisch:
Für alle $a \in R$ gilt:

$$0a = 0 = a0$$

Beweis: Es ist $0 + 0 = 0$. Hieraus folgt für beliebige $a \in R$ nach dem Distributivgesetz $0a + 0a = (0 + 0)a = 0a = 0a + 0$ und damit $0a = -(0a) + 0a + 0a = -(0a) + ((0a) + 0) = 0$, da $-(0a)$ das additive Inverse von $0a$ ist.

Beispiele für Ringe:

1. Die Menge $\mathbb{Z}$ der ganzen Zahlen ist mit der üblichen Addition und Multiplikation ein Ring (mit Einselement).
2. Die Menge $M(n \times n, \mathbb{R}) = \mathbb{R}^{n \times n}$ der reellen $n \times n$-Matrizen bildet mit der Matrizenaddition und -multiplikation einen Ring, der für $n > 1$ nicht kommutativ ist.
3. Ist $A = [0, 1] = \{x \in \mathbb{R},\ 0 \leqslant x \leqslant 1\}$ und $R = \mathrm{Abb}(A, \mathbb{R})$, dann ist R ein Ring.
4. Betrachtet man in $\mathbb{Z}$ modulo (m) (vgl. S. 13), dann wird die Quotientenmenge (vgl. S. 13)

   $$\mathbb{Z}/\sim = \mathbb{Z}/m\mathbb{Z}$$

   mit den Verknüpfungen

   $$(a + m\mathbb{Z}) \oplus (b + m\mathbb{Z}) = (a + b) + m\mathbb{Z} \quad \text{bzw.}$$
   $$(a + m\mathbb{Z}) \odot (b + m\mathbb{Z}) = (a \cdot b) + m\mathbb{Z}$$

zu einem (kommutativen) Ring mit Einselement.

Der Lese prüfe das nach. Er weise nach, daß die Addition und Multiplikation *wohldefiniert* sind, d.h. nicht von der Auswahl der Repräsentanten in der jeweiligen Restklasse abhängen.

In $\mathbb{Z}/6\mathbb{Z}$ gilt aber z.B. $\overline{2} \odot \overline{3} = (2 + 6\mathbb{Z}) \odot (3 + 6\mathbb{Z}) = 0 + 6\mathbb{Z} = \overline{0}$. Der Ring $\mathbb{Z}/6\mathbb{Z}$ ist ein Ring mit *Nullteilern*.

Def.: Sei R ein Ring mit Einselement. Ein $a \in R$ heißt *Nullteiler*, wenn es ein $b \in R$, $b \neq 0$ gibt mit $ab = 0$ oder $ba = 0$.

In einem kommutativen Ring braucht man nicht zwischen rechten und linken Nullteilern zu unterscheiden. R heißt *nullteilerfrei*, wenn R keine Nullteiler außer dem Nullelement 0 enthält.
Ein nullteilerfreier kommutativer Ring mit Einselement ($1 \neq 0$) heißt auch *Integritätsring* (oder *Integritätsbereich*).

Aufgabe: $\mathbb{Z}/m\mathbb{Z}$ ist genau dann ein Integritätsbereich, wenn m eine Primzahl ist.

Zu einem Ring R mit Einselement bezeichnet man mit

$$E(R) = R^* = \{a \in R, \text{ es gibt ein } b \in R \text{ mit } ab = ba = 1\}$$

die Menge der invertierbaren Elemente in R und nennt diese Elemente auch *Einheiten* von R.

Beispiel: $E_{\mathbb{Z}} = \{-1, 1\}$.

§3.6. Körper

Def.: Ein *Körper* ist ein kommutativer Ring mit Einselement $1 \neq 0$, in dem jedes von Null verschiedene Element invertierbar ist.

Die von Null verschiedenen Elemente bilden dann bzgl. der Multiplikation eine Gruppe. Deshalb kann man die Definition auch so wenden:

Ein *Körper* ist eine Menge K mit zwei Verknüpfungen, einer Addition und einer Multiplikation, die folgende Bedingungen erfüllen:

(a) K ist bzgl. „+“ (Addition) eine abelsche Gruppe.

(b) Bzgl. der Multiplikation ist $K^* = \{x \in K, \ x \neq 0\}$ eine abelsche Gruppe.

(c) Es gelten die Distributivgesetze:

$$a(b + c) = ab + ac$$
$$(a + b)c = ac + bc$$

(Wobei das zweite Distributivgesetz überflüssig ist, da es mit der Kommutativität aus dem ersten folgt.)

Beispiele für Körper:

1. Die Menge $\mathbb{Q}$ der rationalen Zahlen mit der gewöhnliche Addition und Multiplikation ist ein Körper; ebenso die Menge $\mathbb{R}$ der reellen Zahlen.

2. $\mathbb{Q}(\sqrt{2}) := \{a + b\sqrt{2};\ a, b \in \mathbb{Q}\}$ ist mit der von $\mathbb{R}$ geerbten Addition und Multiplikation ein Körper. Man prüfe das nach!

3. Auf einer Menge mit 2 Elementen wird durch die folgenden Verknüpfungstafeln eine Körperstruktur erklärt:

$+$	$\overline{0}$	$\overline{1}$
$\overline{0}$	$\overline{0}$	$\overline{1}$
$\overline{1}$	$\overline{1}$	$\overline{0}$

$\cdot$	$\overline{0}$	$\overline{1}$
$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$

4. $\mathbb{Z}/m\mathbb{Z}$ ist mit der Addition und Multiplikation aus Beispiel 4 auf Seite 35 genau dann ein Körper, wenn m eine Primzahl ist. Zu jeder Primzahl gibt es einen Körper mit genau p Elementen, nämlich $\mathbb{Z}/p\mathbb{Z}$ (Das vorige Beispiel ist der Spezialfall $p = 2$, siehe auch Beispiel 4 auf S.28).

   In der Algebra wird gezeigt, daß für die Elementanzahl eines *endlichen Körpers*, d.h. eines Körpers mit endlichen vielen Elementen gelten muß $q = p^n$ mit p Primzahl und $n \in \mathbb{N}$, und daß es umgekehrt zu jeder Primzahlpotenz p^n tatsächlich einen Körper mit p^n Elementen gibt.

   Es gibt also z.B. Körper mit 65536, 65537 oder $2^{216091} - 1$ Elementen.

5. In $\mathbb{R} \times \mathbb{R}$ definieren wir folgende Operationen:

$$\begin{array}{rcll} (a,b) + (a',b') & := & (a+a', b+b') & \text{und} \\ (a,b) \cdot (a',b') & := & (aa' - bb', ab' + a'b). & \end{array}$$

   Man überzeugt sich leicht davon, daß $\mathbb{R} \times \mathbb{R} = \mathbb{R}^2$ mit diesen Operationen zu einem Körper mit dem Nullelement $0 := (0, =)$ und dem Einselement $(1, 0)$ wird. Das Negative von (a, b) ist $(-a, -b)$, das Inverse von $(a, b) \neq (0, 0)$ ist

$$(a,b)^{-1} = \left(\tfrac{a}{a^2+b^2}, -\tfrac{b}{a^2+b^2}\right).$$

   $\mathbb{R} \times \mathbb{R} = \mathbb{R}^2$ mit diesen Verknüpfungen heißtt *Körper der komplexen Zahlen*, seine Standardbezeichnung ist $\mathbb{C}$ (als Menge ist also $\mathbb{C} = \mathbb{R} \times \mathbb{R}$).

   Die Abbildung

$$\begin{array}{rccl} j: & \mathbb{R} & \longrightarrow & \mathbb{R} \times \mathbb{R} = \mathbb{C} \\ & a & \longmapsto & (a,0) \end{array}$$

   ist injektiv und erfüllt die Eigenschaften

$$\begin{array}{lclclcll} j(a+a') & = & (a+a',0) & = & (a,0)+(a',0) & = & j(a)+j(a') & \text{und} \\ j(aa') & = & (aa',0) & = & (a,0)\cdot(a',0) & = & j(a)\cdot j(a') & \end{array}$$

   wir unterscheiden daher nicht zwischen $\mathbb{R}$ und $j(\mathbb{R}) = \{(a, 0),\ a \in \mathbb{R}\} \subset \mathbb{C}$. Wir wollen daher $a \in \mathbb{R}$ mit seinem Bild $(a, 0) \in \mathbb{C}$ identifizieren und so $\mathbb{R}$ als Teilmenge von $\mathbb{C}$ auffassen.

   Für das spezielle Element $\mathrm{i} := (0, 1) \in \mathbb{C}$ gilt dann

$$\mathrm{i}^2 = (0,1)\cdot(0,1) = (-1,0) = -1.$$

   i heißt *imaginäre Einheit* (Euler, 1737) und für jedes $(a, b) \in \mathbb{C}$ gilt dann

$$z := (a,b) = (a,0) + (0,b) = (a,0) + (0,b)(0,1) = a + b\mathrm{i}.$$

   In dieser Darstellung heißt a der *Realteil* von z und b der *Imaginärteil* von z. Real- und Imaginärteil sind durch z eindeutig bestimmt.

   In $\mathbb{C}$ besitzt also die in $\mathbb{R}$ unlösbare Gleichung

$$\boxed{z^2 + 1 = 0}$$

   eine Lösung (nämlich $z = \pm\mathrm{i}$, weitere Lösungen in $\mathbb{C}$ gibt es nicht).

   Der Körper $\mathbb{C}$ hat folgende fundamentale Eigenschaft:

   In $\mathbb{C}$ hat jede Gleichung

$$a_n z^n + a_{n-1} z^{n-1} + \ldots + a_0 = 0$$

   ($a_n \neq 0$, $n \in \mathbb{N}$) mindestens eine Lösung. Das ist die Aussage des sogenannten *Fundamentalsatzes der Algebra*.

Verzichtet man auf die Forderung, daß die Multiplikation in K kommutativ ist (fordert aber beide Distributivgesetze), so spricht man von einem *Schiefkörper* oder einer *Divisionsalgebra*.

Ein wichtiges *Beispiel* für Schiefkörper sind die sogenannten *Hamiltonschen Quaternionen*. Das ist die Menge aller Viertupel reeller Zahlen ($\mathbb{R}^4$) versehen mit einer Addition und einer Multiplikation. Die Definition der Addition und der Multiplikation merkt man sich am einfachsten, wenn man eine Quaternion schreibt als $a + b \cdot \mathrm{i} + c \cdot \mathrm{j} + d \cdot \mathrm{k}$ mit $a, b, c, d \in \mathbb{R}$ und Symbolen $\mathrm{i}, \mathrm{j}, \mathrm{k}$. Dann wird mit Quaternionen genauso gerechnet wie mit reellen Polynomen, allerdings unter Beachtung von $\mathrm{i} \cdot \mathrm{j} = \mathrm{k} = -\mathrm{j} \cdot \mathrm{i}$, $\mathrm{j} \cdot \mathrm{k} = \mathrm{i} = -\mathrm{k} \cdot \mathrm{j}$, $\mathrm{k} \cdot \mathrm{i} = \mathrm{j} = -\mathrm{i} \cdot \mathrm{k}$ und $\mathrm{i}^2 = \mathrm{j}^2 = \mathrm{k}^2 = -1$.

§4. Beweise

§4.1. Was ist ein Beweis?

Ein mathematischer Satz (,der je nach Bedeutung auch Theorem, Lemma, Hilfssatz heißen kann.) hat im Prinzip immer die Gestalt:

„Aus p folgt q.“

Dabei nennt man p die *Voraussetzung* und q die *Behauptung*. Die Vorstellung dabei ist, daß aus der als richtig erkannten (oder postulierten) Aussage p die neue richtige Aussage q gewonnen wird. Man sagt auch, q wird aus p *bewiesen*, abgeleitet, deduziert oder ähnliches.
Der Aufbau einer mathematischen Theorie beginnt meist mit der Formulierung von *Axiomen* (Grundannahmen, Grundtatsachen), deren Richtigkeit postuliert wird. Durch logisches Schließen werden aus diesen dann weitere Aussagen — mathematische Sätze — abgeleitet.
Jede mathematische Aussage $p, q, \ldots$ ist entweder *wahr* (*richtig*) oder *falsch*, etwas anderes ist ausgeschlossen (sog. „tertium non datur“). Es gibt also nur die Wahrheitswerte w(ahr) und f(alsch).
Mathematische Aussagen $p, q, \ldots$ können zu neuen Aussagen verknüpft werden:

Solche *logische Operationen* sind:

die *Negation*:	p ist nicht richtig	(in Zeichen $\neg p$)
die *Konjunktion*:	p und q	(in Zeichen $p \wedge q$)
die *Disjunktion*:	p oder$q$	(in Zeichen $p \vee q$)
die *Implikation*:	aus p folgt q	(in Zeichen $p \Rightarrow q$)

Wahrheitstafel für *Nicht*::

p	$\neg p$
w	f
f	w

Wahrheitstafel für *Und*:

$\wedge$	w	f
w	w	f
f	f	f

$p \wedge q$ ist also genau dann wahr, wenn sowohl p als auch q wahr sind.

Wahrheitstafel für *Oder*:

$\vee$	w	f
w	w	w
f	w	f

Werden zwei Aussagen p, q durch (das nichtausschließende) *oder* verbunden, so ist die entstehende Aussage genau dann falsch, wenn p und q beide falsch sind.

Wahrheitstafel für die *Implikation*:

$\Rightarrow$	w	f
w	w	f
f	w	w

Man beachte, daß wenn p falsch ist, $p \Rightarrow q$ stets wahr ist. Für die Implikation $p \Rightarrow q$ wird eine ganze Reihe von gleichbedeutenden sprachlichen Wendungen gebraucht:

„Aus p folgt q“.

„p impliziert q“.

„Wenn p gilt, dann gilt auch q“.

„p gilt nur dann, wenn q gilt“.

„p ist hinreichend für q“.

„q ist notwendig für p“.

Als *Umkehrung* der Implikation $p \Rightarrow q$ bezeichnet man die Implikation $q \Rightarrow p$. Ist $p \Rightarrow q$, so braucht $q \Rightarrow p$ nicht richtig zu sein, wie folgendes Beispiel zeigt:
Sei $p \Rightarrow q$ die Aussage: „Wenn a und b positive reelle Zahlen sind, dann ist auch ihr Produkt ab positiv.“ Die Umkehrung ist: „Wenn a und b reelle Zahlen sind und ab positiv ist. dann sind a und b positiv.“ Daß die Umkehrung falsch ist, zeigt das einfache *Gegenbeispiel* $a = b = -1$.

Gilt jedoch $p \Rightarrow q$ und $q \Rightarrow p$, so sagt man:

„p und q sind äquivalente Aussagen“.

„p ist notwendig und hinreichend für q“.

„q ist notwendig und hinreichend für p“.

„p gilt dann und nur dann, wenn q gilt“.

„p gilt genau dann, wenn q gilt“.

Kurzschreibweise: $p \Leftrightarrow q$ (Äquivalenz)

Wahrheitstafel für die *Äquivalenz* ($\Leftrightarrow$):

$\Leftrightarrow$	w	f
w	w	f
f	f	w

Man beachte, daß um $p \Leftrightarrow q$ zu zeigen, immer zwei Überlegungen durchzuführen sind: $p \Rightarrow q$ und $q \Rightarrow p$.

§4.2. Direkte und indirekte Beweise

Der Beweis eine Satzes $p \Rightarrow q$ wird manchmal *indirekt* geführt. Man zeigt

$$\neg q \Rightarrow \neq p.$$

Wenn aus der Negation von q die Negation von p folgt, andererseits aber p richtig ist, entsteht ein Widerspruch, daß zugleich p und q wahr sind. Dieser Widerspruch läßt sich nur dadurch beseitigen, daß die Annahme $\neg q$ falsch ist, also muß q richtig sein.

Will man z.B. die Implikation „Aus $a, b \in \mathbb{R}$, $a < b$ und $ab > 0$ folgt $\frac{1}{b} < \frac{1}{a}$." beweisen, kann man indirekt vorgehen: Wenn die Behauptung $\frac{1}{b} < \frac{1}{a}$ falsch wäre, so würde $\frac{1}{b} \geqslant \frac{1}{a}$ gelten, obwohl $ab > 0$ und $a < b$ vorausgesetzt ist. Multiplikation mit $ab > 0$ ergäbe

$$\tfrac{ab}{b} \geqslant \tfrac{ab}{a}, \quad \text{also} \quad a \geqslant b.$$

Dies widerspricht aber der Voraussetzung $a < b$.

Die Negation gegebener Aussagen ist manchmal kompliziert, wenn die Aussage selber zusammengesetzt ist, oder wenn „für alle" oder „es gibt" in einer Aussage vorkommen.

- Lautet die Aussage:

  „Alle Studierenden mit Hauptfach Mathematik kennen die Beweismethode der vollständigen Induktion.", so lautet das logische Gegenteil: „Es gibt (mindestens) eine(n) Studierende(n) der Mathematik, der die Beweismethode der vollständigen Induktion nicht kennt."

- Die obige Aussage ist vom Typ: „Für jedes $a \in M$ gilt $S(a)$." Die Negation lautet dann: „Es gibt ein $a \in M$, so daß $S(a)$ nicht gilt."

  Die Negation von „Es gibt ein $a \in M$, so daß $S(a)$ gilt" lautet: „Für alle $a \in M$ ist $S(a)$ falsch."

- Die Negation von „Zu jedem $a \in \mathbb{R}$, $a > 0$ gibt es eine natürliche Zahl n mit $na > 1$." kann man in zwei Etappen angehen:

  1. Es gibt ein $a \in \mathbb{R}$, $a > 0$, so daß nicht gilt: Es gibt eine natürliche Zahl n mit $na > 1$.
  2. Es gibt ein $a \in \mathbb{R}$, $a > 0$, so daß für jede natürliche Zahl n gilt: Nicht $na > 1$, d.h. $na \leqslant 1$.

Hilfreich sind auch die folgenden Regeln:

$$\neg(p \wedge q) \iff (\neg p) \vee (\neg q) \quad \text{und}$$
$$\neg(p \vee q) \iff (\neg p) \wedge (\neg q)$$

Aufgabe: Verneinen Sie die Aussage: „Alle Mathematikerinnen und alle Mathematiker sind Nichtraucher."

Wir besprechen zum Schluß noch einige Beispiele für Beweise, wobei es nun nicht in erster Linie auf den Inhalt ankommt, sondern mehr auf das formale Vorgehen.

§4.3. Einige Beispiele

Schon Euklid bekannt war

Satz: Es gibt unendlich viele Primzahlen.

Bemerkung: Der Satz bedeutet, daß die Menge $\mathbb{P}$ der Primzahlen nicht endlich ist.

Wir führen einen indirekten Beweis und nehmen an, daß $\mathbb{P}$ doch endlich ist, etwa $\mathbb{P} = \{p_1, \ldots, p_n\}$. Wir bilden $N = p_1 \cdot \ldots \cdot p_n + 1$. Dann ist N eine natürliche Zahl größer als 1, und N ist größer als alle p_j $(1 \leqslant j \leqslant n)$, insbesondere ist $N \notin \mathbb{P}$. Nach dem Hauptsatz der elementaren Zahlentheorie gibt es eine Primzahl p, die N teilt. Da $p_1, \ldots, p_n$ alle Primzahlen sind, muß p mit einem p_j $(1 \leqslant j \leqslant n)$ übereinstimmen. Damit folgt, daß p auch $N - p_1 \cdot p_2 \cdot \ldots \cdot p_n = 1$ teilt, ein offensichtlicher Widerspruch.

Satz: Die Summe aller ungeraden natürlichen Zahlen (bis zu einer ungeraden Zahl) ist immer eine Quadratzahl.

Anmerkung: Eine ungerade Zahl hat die Gestalt $2n - 1$, wobei n eine beliebige natürliche Zahl ist. Wir betrachten eine Summe der Form $1 + 3 + 5 + \ldots + (2n - 1)$ für ein passendes $n \in \mathbb{N}$. Präziser behaupten wir:

Satz: Für jede natürliche Zahl n gilt:

$$\boxed{1 + 3 + 5 + \ldots + (2n - 1) = n^2}$$

Das entscheidende ist, daß diese Aussage für *alle* natürlichen Zahlen n gilt, für $n = 17$ genauso wie für $n = 65537$ oder $n = 10^{(10^{10})}$.
Wie kann man eine solche Aussage beweisen? Man kann die Behauptung im Prinzip für jedes konkrete n nachprüfen und nachrechnen. Das ist immer noch kein Beweis.

Hier springt das *Beweisprinzip der vollständigen Induktion* in die Bresche.

Man kann die natürlichen Zahlen als Grundobjekte betrachten und etwa durch die sogenannten *Peanoaxiome* charakterisieren. Das Prinzip der vollständigen Induktion gehört dann zu den Axiomen.
Oder man kann die natürlichen Zahlen $\mathbb{N}_0$ als Teilmenge von $\mathbb{R}$ charakterisieren: $\mathbb{N}_0$ ist die kleinste Teilmenge von $\mathbb{R}$, die 0 und mit jeder Zahl x auch die Zahl $x + 1$ enthält. Man sagt $\mathbb{N}_0$ ist die *kleinste induktive Menge*. Hieraus kann man alle Grundeigenschaften der natürlichen Zahlen ableiten. Insbesondere ist die Beweismethode der vollständigen Induktion ein ableitbares Prinzip:

Induktionssatz: Ist $S \subset \mathbb{N}_0$, und gilt

1. $0 \in S$,
2. aus $n \in S$ folgt $n + 1 \in S$,

dann gilt $S = \mathbb{N}_0$.

Nach Voraussetzung ist also S induktiv, und da $\mathbb{N}_0$ die kleinste induktive Menge ist, muß S schon mit $\mathbb{N}_0$ übereinstimmen. Der Induktionsansatz ist die Grundlage für das *Beweisprinzip der vollständigen Induktion.*

Es sei $A(n)$ eine Aussage über die natürliche Zahl n. Gelingt es zu zeigen:

1. $A(0)$ ist richtig (*Induktionsanfang*)
2. Ist $A(n)$ richtig, dann ist auch $A(n + 1)$ richtig (*Induktionsschritt*)

$\Longrightarrow$ $A(n)$ ist für *alle* $n \in \mathbb{N}_0$ richtig.

Zum Beweis betrachtet man die Menge $S = \{n \in \mathbb{N}_0,\ A(n) \text{ ist richtig}\}$, diese erfüllt die Voraussetzungen des Induktionsansatzes, ist also mit $\mathbb{N}_0$ identisch.

Häufig wird folgende Variante des Induktionsansatzes benutzt:

Sei $n_0 \in \mathbb{N}_0$ und $A(n)$ eine für $n \geqslant n_0$ erklärte Aussage. Gilt dann

1. $A(n_0)$ ist richtig,
2. aus der Richtigkeit von $A(n)$ für alle $n \geqslant n_0$ folgt stets die Richtigkeit von $A(n + 1)$,

dann gilt $A(n)$ für alle $n \geqslant n_0$.

Beispiele zur vollständigen Induktion:

1. Für alle $n \in \mathbb{N}$ gilt: $1 + 3 + 5 + \ldots + (2n - 1) = n^2$
   Induktionsanfang: $A(1) : 1 = 1^2$ ist richtig.
   Induktionsschritt: $A(n)$ bedeutet
   $$1 + 3 + \ldots + (2n - 1) = n^2.$$

Addiert man hierzu auf beiden Seiten $2n+1$, so folgt

$$1+3+\ldots+(2n-1)+(2n+1)=n^2+2n+1.$$

Wegen $n^2+2n+1=(n+1)^2$ erhält man

$$1+3+\ldots+(2n-1)+(2(n+1)-1)=(n+1)^2,$$

das ist die Aussage $A(n+1)$.

2. *Geometrische Summenformel:* Für alle $q \in \mathbb{R}$ und alle $n \in \mathbb{N}_0$ gilt

$$\boxed{(1-q)(1+q+q^2+\ldots+q^n)=1-q^{n+1}}$$

Induktionsanfang: $A(0)$: bedeutet $1=1$

Induktionsschritt: Aus der Annahme $A(n)$, also $(1-q)(1+q+q^2+\ldots+q^n)=1-q^{n+1}$ folgt durch Addition von $(1-q)q^{n+1}$

$$(1-q)(1+q+q^2+\ldots+q^n)+(1-q)q^{n+1}=1-q^{n+1}+(1-q)q^{n+1}$$

Durch Ausklammern von $(1-q)$ auf der linken Seite und Ausmultiplizieren auf der rechten Seite erhält man:

$$(1-q)(1+q+q^2+\ldots+q^{n+1})=1-q^{(n+1)+1},$$

das ist die Aussage $A(n+1)$.

3. Die *Bernoullische Ungleichung:* Für alle $x \in \mathbb{R}$, $x>-1$ und alle $n \in \mathbb{N}_0$ gilt

$$\boxed{(1+x)^n \geqslant 1+nx}$$

Induktionsanfang: Für $n_0=0$ gilt $A(0):(1+x)^0 \geqslant 1+0x$

Induktionsschritt: Aus der Aussage $A(n):(1+x)^n \geqslant 1+nx$ folgt durch Multiplikation mit der positiven Zahl $1+x$ die Ungleichung $(1+x)^{n+1} \geqslant (1+nx)(1+x)$. Wegen $x^2 \geqslant 0$ und $n>0$ ist $nx^2 \geqslant 0$ und deshalb

$$(1+x)^{n+1} \geqslant (1+nx)(1+x)=1+(n+1)x+nx^2 \geqslant 1+(n+1)x.$$

4. Eine *fehlerhafte* Anwendung des Induktionssatzes:

Behauptung: Jede Menge M, die aus n reellen Zahlen besteht, besteht aus einander gleichen reellen Zahlen.

Induktionsanfang: $A(1)$ bedeutet: Jede reelle Zahl ist sich selbst gleich. Eine offensichtlich richtige Aussage.

Induktionsschritt: Die Aussage sei richtig für jede Menge mit n Elementen. Dann betrachten wir eine Menge mit Elementen $a_1,\ldots,a_{n+1}$. Die Mengen $\{a_1,\ldots,a_n\}$ und $\{a_2,\ldots,a_{n+1}\}$ haben jeweils n Elemente, erfüllen also die Induktionsvoraussetzung, also gilt $a_1=a_2=\ldots=a_n$ und $a_2=a_3=\ldots=a_{n+1}$, damit gilt dann auch $a_1=a_2=\ldots=a_n=a_{n+1}$.

Wo steckt der Fehler?

Index