

Kapitel 1

Logik und Unterlagen

Im Laufenden Semester werden wir viele mathematische Beweise einführen. Heute werden wir uns mit der Mathematische Logik beschäftigen.

In der Mathematik stoßen wir auf gewisse Grundannahmen, “Axiome”, die wir als gegeben ansehen. Eine dieser Annahmen ist der

Satz vom ausgeschlossenen Dritten

Eine zulässige mathematische Aussage ist entweder wahr oder falsch, jedoch nie beides zugleich.

Beispiel

1. $5 < 7$ Wahr
2. $4 < 2$ Falsch

In der wirklichen Welt ist es anders. Ist z.B. “Mathematik ist schön” wahr oder falsch?

Mit Aussagen kann man “rechnen”. Wir führen nun ein paar geläufige Notationen der Logik ein:

Seien A, B Aussagen

- A und B wird mit $A \wedge B$ bezeichnet
- A oder B wird mit $A \vee B$ bezeichnet

Folgerung (eine wahre Implikation)

- Aus A folgt B wird mit \rightarrow bezeichnet
- Wenn A , dann auch B
- Die Negation der Aussage A wird mit $\neg A$ bezeichnet
- A ist äquivalent zu B wird mit $A \Leftrightarrow B$ bezeichnet
- $(A \rightarrow B) \wedge (B \rightarrow A)$ A wahr genau dann, wenn B wahr ist.

Bemerkung

Die Folgerung ist transitiv. Wenn wir wissen, dass $A \rightarrow B$ und $B \rightarrow C$, dann wissen wir dass $A \rightarrow C$.

Prinzip des Mathematischen Beweises

Wir können aus einer Kette von Folgerungen

$$A \rightarrow B \rightarrow C \cdots \rightarrow S$$

einen mathematischen "Satz" S aus einer Annahme A herleiten. (Ein Beweis ist eine Folge von Implikationen von Aussagen).

Kontraposition (Umkehrschluss)

$A \rightarrow B$ ist gleichbedeutend mit $\neg B \rightarrow \neg A$.

Falls $A \rightarrow B$, so kann A nicht wahr sein wenn B falsch ist (weil wenn A wahr ist, würde B auch wahr sein).

1.1 Prinzip des Indirekten Beweises

Zum Beweis der Aussage $A \rightarrow B$ genügt es die Aussage $\neg B \rightarrow \neg A$ zu zeigen, oder die Annahme $A \wedge \neg B$ zum Widerspruch zu führen.

Indirekter Beweis

Man fügt $\neg B$ als Annahme hinzu und kommt nach einer Kette von erlaubten Schlüssen zu einer falschen Aussage.

Daraus schliesst man, dass die Zusatzannahme $\neg B$ nicht wahr ist.

Beispiel 1.1

- A = "jede natürliche Zahl n hat einen Nachfolger $n + 1$ "
- B = "es gibt keine grösste natürliche Zahl"

Wir beweisen dass B aus A folgt. Nehmen wir an, dass A wahr und B falsch ist.

$\neg B$ = es gibt eine grösste natürliche Zahl N_0 , d.h. $N_0 > l$ für jedes $l \in \mathbb{N}$.

Mittels der Aussage A wissen wir, dass N_0 einen Nachfolger $N_0 + 1$ hat. Für diesen gilt $N_0 + 1 > N_0$. Dies ist aber ein Widerspruch.

Definition 1.1

Eine Menge ist eine Zusammenfassung verschiedener Objekte zu einem Ganzen.

Die Objekte werden Elemente der Menge genannt.

KAPITEL 1. LOGIK UND UNTERLAGEN

Sei A eine Menge, dann wird “ a ist element von A ” mit “ $a \in A$ ” bezeichnet. Seien A, B Mengen, dann wird “jedes Element von A ist ein Element von B ” mit “ $A \subset B$ ” bezeichnet, und man sagt “ A ist in B enthalten” (oder A ist eine Teilmenge von B).

Falls zugleich $A \subset B$ und $B \subset A$ gilt, so sind A und B gleich und man schreibt $A = B$.

Beispiele 1.2

1. Die Menge $\mathbb{N} = \{0, 1, 2, \dots\}$ der natürlichen Zahlen.
2. Die leere Menge mit “ \emptyset ” bezeichnet. Sie ist in jeder Menge enthalten.
3. Die Menge $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$ aller ganze Zahlen.
4. Meistens werden Mengen nicht durch die Liste ihre Elemente gegeben, sondern durch bestimmte Eigenschaften ihrer Elemente definiert

$$\mathbb{P} = \{2, 3, 4, 5, 7, 11, 13, \dots\}$$

die Menge aller Primzahlen $\mathbb{P} : \{p \in \mathbb{N} \mid p \text{ primzahl}\}$

1.2 Zwei Prinzipien

Wir werden die folgenden zwei Beweismethoden häufig benutzen.

1. Prinzip des Indirekten Beweises

Zum Beweis der Aussage $A \rightarrow B$ genügt es, die Aussage $\neg B \rightarrow \neg A$ zu zeigen oder die Annahme $A \wedge \neg B$ zum Widerspruch zu führen.

2. Prinzip der Vollständigen Induktion

Sei für jedes $n \in \mathbb{N}$ eine Behauptung $A(n)$ gegeben. Soll die Behauptung für alle natürlichen Zahlen $n \in \mathbb{N}$ bewiesen werden, so genügen dazu zwei Beweisschritte:

- i) Der Beweis von $A(0)$
- ii) Für jedes $n \in \mathbb{N}$, der Beweis von $A(n+1)$ unter der Voraussetzung, dass $A(n)$ gilt.

Oft gelten aber Behauptungen nicht von $n = 0$.

Soll die Gültigkeit von $A(n)$ für alle $n \geq m$ bewiesen werden so genügen wieder zwei Schritte:

- i) Beweis von $A(m)$
- ii) Für jedes $n \geq m$ impliziert $A(n)$ die Behauptung $A(n+1)$

Das Prinzip der vollständigen Induktion ist genau wie ein Dominoeffekt.

Sie stellen alle Dominosteine auf, einen nach dem anderen. Falls der erste Dominostein fällt ($A(1)$ wahr) und falls wir die Dominosteine genug nah nebeneinander gestellt haben, so dass ein fallender Dominostein den nächsten trifft ($A(k) \rightarrow A(k+1)$), dann wissen wir, dass alle Dominosteine fallen.

Beispiel 1.3 (Induktion)

1. Für alle $n \geq 1$ gilt:

$$A(n): 1 + 3 + 5 + \dots + (2n - 1) = n^2$$

Beweis mittels vollständiger Induktion

- i) $A(i)$ lautet $1 = 1^2$ und gilt.
- ii) Sei $n \geq 1$. Annahme: $A(n)$ gilt. Die linke Seite der Identität $A(n + 1)$ ist

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

womit $A(n + 1)$ bewiesen ist.

2. Als zweites Beispiel der vollständigen Induktion beweisen wir den Fundamentalsatz von Euklid:

Satz 1.4

Jede natürliche Zahl $n \geq 2$ ist ein Produkt von Primzahlen, welches bis auf die Reihenfolge der Faktoren eindeutig ist. Wir werden uns hier aber nicht mit der Eindeutigkeit befassen.

Beweis

Sei $A(n)$ die Aussage: Jede natürliche Zahl m mit $2 \leq m \leq n$ ist ein Produkt von Primzahlen

- i) $A(2)$ gilt, denn 2 ist eine Primzahl.
- ii) Sei $n \geq 2$. Wir nehmen an, dass $A(n)$ gilt. Für $n + 1$ gibt es zwei Möglichkeiten
 - a) $n + 1$ ist eine Primzahl und somit gilt $A(n + 1)$
 - b) $n + 1$ ist keine Primzahl d.h. es gibt ein $2 \leq a \leq n$ welches $n + 1$ teilt. Dann ist $b := \frac{n+1}{a}$ auch ganzzahlig und zudem ist $2 \leq b \leq n$ erfüllt. Aus $A(n)$ folgt, dass sowohl a wie b ein Produkt von Primzahlen sind. Somit ist auch $n + 1 = ab$ ein Produkt von Primzahlen.

Satz 1.5

Die Menge \mathbb{P} der Primzahlen ist unendlich.

Beweis

Nehmen wir das Gegenteil “ \mathbb{P} ist endlich” an, d.h. $\mathbb{P} = \{p_1, p_2, \dots, p_m\}$ in aufsteigender Folge; also $p_1 = 2, p_2 = 3, p_3 = 5, p_4 = 7, \dots$. Wir betrachten die Zahl $k = p_1 p_2 \dots p_i \dots p_m + 1$. Aus Satz 1.4 folgt, dass eine Primzahl p_i (aus der Liste $\{p_1, \dots, p_m\}$) existiert, mit p_i teilt k . Da p_i offensichtlich $p_1 p_2 \dots p_i \dots p_m$ teilt, folgt dass p_i die Restzahl $k - p_1 \dots p_m = 1$ teilt. Das ist ein Widerspruch.

Teilbarkeit

Formale Definition

Eine ganze Zahl a teilt eine ganze Zahl b genau dann, wenn es eine ganze Zahl n gibt, für die $an = b$ ist.

Man sagt dann (Synonyme)	Man schreibt
a teilt b	$a \mid b$
a ist Teiler von b	
b ist teilbar durch a	
b ist Vielfaches von a	

Eigenschaften der Teilbarkeit

- Gilt $a \mid b$ und $b \mid c$, so folgt $a \mid c$
- Für $k \in \mathbb{Z} \setminus \{0\}$ gilt: $a \mid b \iff ka \mid kc$
- $a \mid b$ und $c \mid d \rightarrow ac \mid bd$
- $a \mid b$ und $a \mid c \rightarrow a \mid kb + lc$, für alle $l, k \in \mathbb{Z}$

Formaler Beweis von Satz 1.5

1. $k = (p_1 p_2 \dots p_i \dots p_m) + 1$
Es gibt eine Primzahl p_i die k teilt. $p_i \mid k$ mittels Satz 1.4.
2. Sei $b = p_1 p_2 \dots p_i \dots p_m =$ Produkt aller Primzahlen. Sei $a = p_i$, $n = p_1 p_2 p_{i-1} p_{i+1} \dots p_m$. Dann $b = an$. Das bedeutet, dass a ein Teiler von b ist, d.h. $p_i \mid (p_1 \dots p_m)$
3. $p_i \mid k$ und $p_i \mid (p_1 \dots p_m) \rightarrow p_i \mid k - (p_1 \dots p_m) = 1$.
So erhalten wir einen Widerspruch.

Bemerkung

Letztes mal haben wir gesagt, dass “jedes Element von A ist auch Element von B ” ($\forall x, x \in A \rightarrow x \in B$) mit $A \subset B$ bezeichnet wird. Wir sagen auch “ A ist in B enthalten” oder “ A ist Teilmenge von B ”. Falls $A \subset B$ und eine Element $b \in B$ existiert mit $b \notin A$, so sagen wir “ A ist eine “eigentliche Teilmenge” von B ”. Manchmal schreiben wir $A \subsetneq B$ in diesem Fall.

Es gibt viele Bücher mit der folgenden Notation: “jedes Element von A ist ein Element von B ” wird mit $A \subseteq B$ bezeichnet. Und wenn $A \subseteq B$ und $A \neq B$ dann wird $A \subset B$ statt $A \subsetneq B$ benutzt. $A = B$ falls $x \in A \Leftrightarrow x \in B$.

Satz

$A = B \Leftrightarrow A \subset B$ und $B \subset A$

Beweis

Annahme: $A = B$. Falls $x \in A$, dann gilt, mittels $A = B$, $x \in B$ und damit gilt auch $A \subset B$. Falls $x \in B$, dann gilt $x \in A$ (mittels $A = B$), und damit gilt $B \subset A$.

Wir haben bewiesen, dass $A = B \rightarrow A \subset B$ und $B \subset A$.
Nun nehmen wir $A \subset B$ und $B \subset A$ an. Damit möchten wir $A = B$ zeigen.

Sei $x \in A$. Mittels $A \subset B$ erhalten wir $x \in B$ und somit $x \in A \rightarrow x \in B$. (*)

Sei $x \in B$. Mittels $B \subset A$ erhalten wir $x \in A$ und somit $x \in B \rightarrow x \in A$. (**)

(*) und (**) $\rightarrow A = B$ per Definition.

1.3 Mengenoperationen

Zunächst erinnern wir kurz an die Definitionen der elementaren Operationen auf Mengen.

Seien A und B Mengen. Wir können dann daraus folgende Mengen bilden:

- Die Vereinigung: $A \cup B = \{x \mid x \in A \vee x \in B\}$
- Der Durchschnitt: $A \cap B = \{x \mid x \in A \wedge x \in B\}$
- Die Differenz: $A \setminus B = \{x \mid x \in A \wedge x \notin B\}$
- Symmetrische Differenz: $A \triangle B = (A \setminus B) \cup (B \setminus A) = (A \cup B) \setminus (A \cap B)$

Wir haben dann folgende Eigenschaften

Satz 1.6

Seien A, B, C Mengen.

1. $A \cap B = B \cap A$; $A \cup B = B \cup A$
 $A \cap \emptyset = \emptyset$; $A \cup \emptyset = A$

Bemerkung

- \cup verhält sich wie $+$
 - \cap verhält sich wie die Multiplikation
 - \emptyset verhält sich wie das Nullelement
2. $(A \cup B) \cup C = A \cup (B \cup C)$
 $(A \cap B) \cap C = A \cap (B \cap C)$
 3. $(A \cup B) \cap C = (A \cap C) \cup (B \cap C)$

KAPITEL 1. LOGIK UND UNTERLAGEN

Beweis

Einerseits gilt

$$(A \cup B) \cap C = \{x \in X : x \in A \cup B\} \cap \{x \in X : x \in C\}$$

Andererseits $(A \cap C) \cup (B \cap C) = \{x \in X : x \in A \cap C\} \cup \{x \in X : x \in B \cap C\}$.

Daraus folgt

$$\begin{aligned} (A \cup B) \cap C &\subseteq (A \cap C) \cup (B \cap C) \\ (A \cap C) \cup (B \cap C) &\subseteq (A \cup B) \cap C \end{aligned}$$

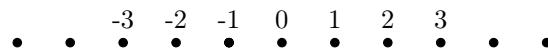
und somit sind die zwei Mengen gleich.

Definition 1.7

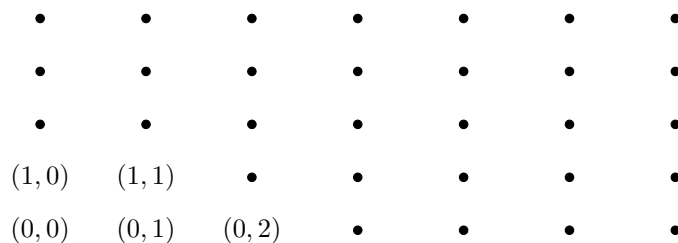
Das Kartesische Produkt $A \times B$ der Mengen A, B ist die Menge der geordneten Paare (a, b) wobei $a \in A, b \in B$

Beispiel

$\mathbb{Z} \times \mathbb{Z} = \{(a, b) : a \in \mathbb{Z}, b \in \mathbb{Z}\}$. Falls \mathbb{Z} als "eindimensionales" Gebilde dargestellt wird



So wird $\mathbb{Z} \times \mathbb{Z}$ als "zweidimensionales" Gebilde dargestellt



Um die Operationen auf mehrere Mengen zu verallgemeinern, sind die folgenden Quantoren nützlich (*)

1. \forall "Für alle" (Allquantor)
2. \exists "Es gibt" (Existenzquantor)
3. $\exists!$ "Es gibt genau ein"

Sei nun I eine beliebige Menge (I =Indexmenge) und sei für alle $i \in I$ eine Menge A_i gegeben. Dann:

- $\bigcup_{i \in I} A_i = \{x \mid \exists i \in I, x \in A_i\}$. Vereinigung besteht aus den Elementen x , für welche es ein $i \in I$ gibt, so dass x zu A_i gehört.
- $\bigcap_{i \in I} A_i = \{x \mid \forall i \in I, x \in A_i\}$. Durchschnitt.

Wir definieren das Kartesische Produkt endlich vieler Mengen $A_1 \dots A_n$:

$$A_1 \times A_n = \prod_{i=1}^n A_i = \{(x_1, \dots, x_n) \mid x_i \in A_i\}$$

Satz 1.8

Seien $A_1 \dots A_k \subset X$, $k \in \mathbb{N}$. Es gilt

1.

$$\left(\bigcap_{i=1}^k A_i \right)^c = \bigcup_{i=1}^k A_i^c$$

2.

$$\left(\bigcup_{i=1}^k A_i \right)^c = \bigcap_{i=1}^k A_i^c$$

Beweis

$$\begin{aligned} \left(\bigcap_{i=1}^k A_i \right)^c &= \left\{ x \mid x \in X \wedge x \notin \bigcap_{i=1}^k A_i \right\} = \{x \mid x \in X, \exists i \in \{1, \dots, k\} : x \notin A_i\} \\ &= \bigcup_{i=1}^k \{x \mid x \in X \wedge x \notin A_i\} = \bigcup_{i=1}^k A_i^c \end{aligned}$$

und

$$\begin{aligned} \left(\bigcup_{i=1}^k A_i \right)^c &= \left\{ x \mid x \in X \wedge x \notin \bigcup_{i=1}^k A_i \right\} = \{x \mid x \in X, \forall i \in \{1, \dots, k\} : x \notin A_i\} \\ &= \bigcap_{i=1}^k \{x \mid x \in X \wedge x \notin A_i\} = \bigcap_{i=1}^k A_i^c \end{aligned}$$

(Siehe Analysis Serie 1, 1. Semester, Aufgabe 2.e)

(*) Wir haben gesehen, dass wir manchmal eine Aussage verneinen müssen. Deshalb müssen wir lernen wie man Aussagen mit Quantoren verneinen kann.

$$\neg (\forall n : A(n)) \Leftrightarrow (\exists n : \neg A(n))$$

$$\neg (\exists n : A(n)) \Leftrightarrow (\forall n : \neg A(n))$$

$$\neg (\forall x \in \mathbb{R} : x^2 \geq 0) \Leftrightarrow \exists x \in \mathbb{R} : x^2 < 0$$

1.4 Abbildungen

Seien X, Y Mengen.

Definition 1.9

Eine Funktion oder Abbildung $f : X \rightarrow Y$ der Menge X in die Menge Y ist eine Vorschrift (ein Gesetz) die (das) jedem Element $x \in A$ genau ein Element $y = f(x) \in Y$ zuordnet.

Es gibt verschiedene wichtige Objekte die in Zusammenhang mit einer Abbildung auftreten

$X =$ Definitionsbereich oder Definitionsmenge (domain)

$Y =$ Wertebereich oder Zielmenge (range)

$f(X) = \{f(x) \mid x \in X\}$ ist das sog. Bild oder die Bildmenge

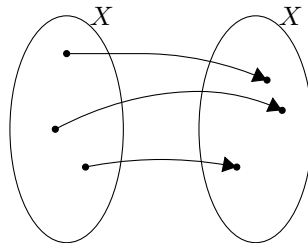
$f^{-1}(y) = x$ heisst Urbild von y .

Der Graph einer Funktion f ist die Menge aller Paare $(x, f(x))$ wobei x alle Elemente der Menge X durchläuft. Er ist eine Teilmenge von $X \times Y$.

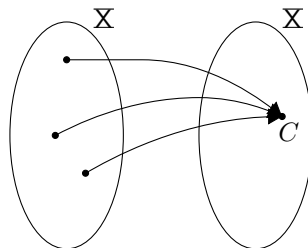
$$Gr(f) := \{(x, f(x)) \mid x \in X\}$$

Beispiel 1.10

1. (Identität) Für jede Menge X , ist $id_X : X \rightarrow X$ definiert durch $id_X(x) = x, \forall x \in X$



2. (Konstante) Sei X Menge und $c \in X$. Die konstante Abbildung mit Wert c ist $f(x) = c, \forall x \in X$



3. Seien X, Y Mengen. Dann sind
 $pr_x : X \times Y \rightarrow X \quad pr_y : X \times Y \rightarrow Y$
 $(x, y) \mapsto x \quad (x, y) \mapsto y$
 die Projektionen auf den ersten bzw. zweiten Faktor.

4. Sinus

$$\begin{aligned} f : \mathbb{R} &\rightarrow [-1, 1] \\ x &\mapsto \sin x \end{aligned}$$

5.

$$\begin{aligned} f : \mathbb{R} &\rightarrow \mathbb{R} \\ x &\mapsto x^2 + x \end{aligned}$$

Definition 1.11

Sei $f : X \rightarrow Y$ eine Abbildung

1. f heisst injektiv falls aus $f(x_1) = f(x_2)$ stets $x_1 = x_2$ folgt, also falls jedes $y \in Y$ höchstens ein Urbild hat.
2. f heisst surjektiv falls es für jedes $y \in Y$ ein $x \in X$ gibt mit $f(x) = y$

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

Also wenn jedes Element $y \in Y$ mindestens ein Urbild hat.

3. f heisst bijektiv falls f injektiv und surjektiv ist, d.h. falls jedes $y \in Y$ genau ein Urbild hat.

Beispiel 1.12

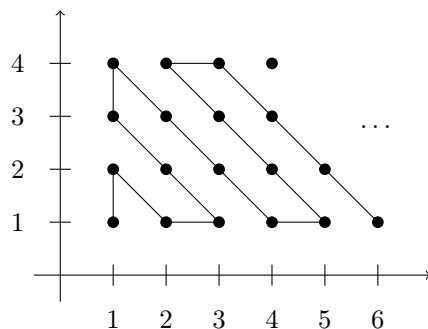
- | | |
|---|---|
| <ol style="list-style-type: none"> 1. $id_X : X \rightarrow X$ bijektiv. 2. Eine konstante Abbildung
 $f : X \rightarrow X, x \mapsto c$ ist <ul style="list-style-type: none"> • injektiv $\Leftrightarrow X = \{c\}$ • surjektiv $\Leftrightarrow X = \{c\}$ 3. Die Projektionen <ul style="list-style-type: none"> • $pr_x : X \times Y \rightarrow X$ • $pr_y : X \times Y \rightarrow Y$ sind stets surjektiv. 4. $f : \mathbb{R} \rightarrow [-1, 1]$
 $x \mapsto \sin x$
 Surjektiv, nicht injektiv | <ol style="list-style-type: none"> 5. $f : \mathbb{R} \rightarrow \mathbb{R}$
 $x \mapsto x^2$
 Nicht surjektiv
 Nicht injektiv 6. $f : \mathbb{N} \rightarrow \mathbb{N}$
 $n \mapsto 2n$
 ist injektiv. $f(\mathbb{N})$ ist die Menge aller geraden Zahlen 7. Eine Menge A hat n Elemente falls es eine bijektive $f : \{1, \dots, n\} \rightarrow A$ gibt. Die Zahl n wird dann die Kardinalität von A genannt und mit A, gelegentlich auch mit $\#A$ bezeichnet. |
|---|---|

Definition Kardinalität

Wir sagen zwei Mengen X und Y sind gleichmächtig falls eine bijektive Abbildung $f : X \rightarrow Y$ existiert.

KAPITEL 1. LOGIK UND UNTERLAGEN

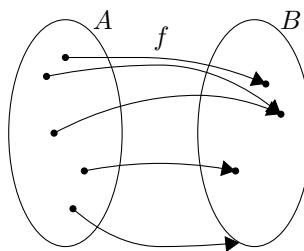
Mit dem ersten Cantorschen Diagonalverfahren kann man die rationalen Zahlen abzählen, d.h. \mathbb{Q} und \mathbb{N} sind gleichmächtig



1.5 Dedekind Schubladen Prinzip

Sei $f : A \rightarrow B$ eine beliebige Abbildung zwischen endlichen Mengen. Falls $|B| < |A|$ dann ist f nicht injektiv, d.h. es gibt $b \in B$ und $a_1, a_2 \in A$ mit

- i) $a_1 \neq a_2$
- ii) $f(a_1) = f(a_2) = b$



$$3 = |B| < 5 = |A|$$

Mit Abbildungen kann man "operieren". Die wichtigste Operation ist die Verkettung (oder Komposition) zweier Abbildungen.

Definition

Abbildungen $f : X \rightarrow Y$, $g : Y \rightarrow Z$ kann man miteinander ausführen. Dies ergibt eine neue Abbildung

$$X \xrightarrow{f} Y \xrightarrow{g} Z$$

$$F := g \circ f : X \rightarrow Z, x \mapsto g(f(x))$$

Man sagt $\begin{cases} g \text{ nach } f \\ g \text{ komponiert mit } f \\ g \circ f \end{cases}$

Zwei Funktionen f und g können verkettet werden wenn der Wertebereich der ersten Funktion mit dem Definitionsbereich der zweiten Funktion übereinstimmt.

Zu Beachten: In dieser Notation steht die zuerst angewandte Abbildung rechts. Das bedeutet bei $g \circ f$ wird zuerst die Funktion f angewandt und dann die Funktion g .

- Die Identische Abbildung verhält sich bei der Komposition neutral, für eine Funktion

$f : X \rightarrow Y$ gilt also

$$f \circ id_X = f = id_Y \circ f$$

wobei

$$id_X : X \rightarrow X$$

$$x \mapsto x$$

$$id_Y : Y \rightarrow Y$$

$$y \mapsto y$$

- Die Komposition von Funktionen ist assoziativ, d.h. für Funktionen f, g, h gilt

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

- Aber die Komposition von Funktionen ist im Allgemeinen nicht kommutativ!

$$f \circ g \neq g \circ f$$

Zum Beispiel:

$$f : \mathbb{R} \rightarrow \mathbb{R}$$

$$x \mapsto x^2$$

$$g : \mathbb{R} \rightarrow \mathbb{R}$$

$$x \mapsto x + 1$$

$$f \circ g = f(g(x)) = f(x + 1) = (x + 1)^2 = x^2 + 2x + 1$$

$$g \circ f = g(f(x)) = g(x^2) = x^2 + 1$$

1.6 Die inverse Abbildung (Umkehrfunktion)

Sei $f : X \rightarrow Y$ eine bijektive Funktion.

Die inverse Funktion $g : Y \rightarrow X$ einer bijektiven Funktion $f : X \rightarrow Y$ ist die Funktion, die jedem Element y der Zielmenge dessen eindeutig bestimmtes Urbildelement zuweist. (bei bijektiven Funktionen hat die Urbildmenge jedes Elements y genau ein Element).

$g(y) := x$, eindeutig definiertes $x \in X$, mit $f(x) = y$. Dann ist definitionsgemäss $(g \circ f)(x) = x$, d.h. $g \circ f : id_X$. Die eindeutig definierte Abbildung g wird

KAPITEL 1. LOGIK UND UNTERLAGEN

(auch) mit f^{-1} bezeichnet und Umkehrfunktion von f genannt.

Für $f \circ f^{-1}$: Sei $y \in Y$ und x erfülle $f(x) = y$. Dann ist $(f \circ f^{-1})(y) = f(f^{-1}(y)) = f(x) = y$

$$f \circ f^{-1} = id_Y$$

Beispiel

1.

$$\begin{aligned} f : \mathbb{R} &\rightarrow \mathbb{R} \\ x &\mapsto 2x + 3 \end{aligned}$$

Die Funktion ist bijektiv.

Die Umkehrfunktion ist gegeben durch

$$\begin{aligned} f^{-1} : \mathbb{R} &\rightarrow \mathbb{R} \\ x &\mapsto \frac{x - 3}{2} \end{aligned}$$

2. Sei $\mathbb{R}^+ = [0, \infty]$ die Menge der nichtnegativen reellen Zahlen und

$$\begin{aligned} f : \mathbb{R}^+ &\rightarrow \mathbb{R}^+ \\ x &\mapsto x^2 \end{aligned}$$

Dann ist f bijektiv und die Umkehrfunktion ist gegeben durch

$$\begin{aligned} f^{-1} : \mathbb{R}^+ &\rightarrow \mathbb{R}^+ \\ x &\mapsto \sqrt{x} \end{aligned}$$

Verallgemeinerungen Falls $f : X \rightarrow Y$ *injektiv* ist, kann man die Umkehrabbildung $f^{-1} : f(\mathbf{X}) \rightarrow \mathbf{X}$ definieren. Das heisst, die Funktion f^{-1} erfüllt: wenn $f(x) = y$, dann $f^{-1}(y) = x$.

Vorsicht: $f^{-1} \circ f = id_{\mathbf{X}}$ aber $f \circ f^{-1} = id_{f(\mathbf{X})}$ und $f \circ f^{-1} = id_Y$ nur genau dann wenn $f(X) = Y$, d.h. f bijektiv ist.