Skript zu der Vorlesung

Mathematik für Informatiker 1

Prof. Dr. Mark Groves

WS 2017/2018

2. Februar 2018

Inhaltsverzeichnis

1 Mengen, Funktionen und Relationen

1.1 Mengenlehre

Definition (Cantor, 1895)

“Unter einer **Menge** verstehen wir jede Zusammenfassung von bestimmten wohl unterschiedenen Objekten unserer Anschauung oder unseres Denkens zu einem Ganzen.”

Die Objekte, die zu einer Menge zusammengefasst sind, heißen **Elemente** dieser Menge. Eine Menge **enthält** ihre Elemente.

Wir können eine Menge festlegen, indem wir ihre Elemente explizit zwischen geschweiften Klammern angeben.

Beispiele

1. Die Menge aller Vokale im englischen Alphabet ist $\{a,e,i,o,u\}$.

2. Die Menge aller ungeraden positiven ganzen Zahlen, die kleiner als 10 sind, ist $\{1,3,5,7,9\}$.

Wir können eine Menge auch festlegen, indem wir die charakteristische Eigenschaft ihrer Elemente angeben.

Beispiel

Die Menge

$$\{x : x \text{ ist eine gerade, positive ganze Zahl, die kleiner als 10 ist}\}$$

ist

$$\{2,4,6,8\}.$$

Wir benutzen besondere Symbole für gewisse Mengen:

$\mathbb{N} = \{1,2,3,\ldots\}$ (die Menge der **natürlichen Zahlen**)

$\mathbb{N}_0 = \{0,1,2,3,\ldots\}$ (die Menge der nichtnegativen ganzen Zahlen)

$\mathbb{Z} = \{\ldots,-2,-1,0,1,2,\ldots\}$ (die Menge der ganzen Zahlen)

$\mathbb{Q} = \left\{\frac{m}{n} : m \in \mathbb{Z}, n \in \mathbb{N}\right\}$ (die Menge der **rationalen Zahlen**)

$\mathbb{R}$ ist die Menge aller reellen Zahlen.

$\mathbb{C}$ ist die Menge aller komplexen Zahlen.

$\emptyset = \{\}$ ist die **leere Menge**.

Bemerkung

Eine Menge ist eine **nicht geordnete** Sammlung von Objekten, so dass

$$\{2,4,6,8\} = \{4,8,6,2\}.$$

Wir schreiben

$$x \in A$$

für die Tatsache, dass x Element von A ist, und

$$x \notin A$$

für die Tatsache, dass x kein Element von A ist.

Definition

Eine Menge A heißt **Teilmenge** einer Menge B, wenn jedes Element von A auch Element von B ist. In diesem Fall schreiben wir "$A \subseteq B$".

Beispiele

1. $\{1,3,5\} \subseteq \{1,3,5,7\}$
2. $\emptyset \subseteq \mathbb{N} \subseteq \mathbb{N}_0 \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$
3. $\{1,3,5\} \nsubseteq \{1,2,3,4\}$

Definitionen

1. Zwei Mengen A und B sind **gleich**, wenn $A \subseteq B$ und $B \subseteq A$. In diesem Fall schreiben wir "$A = B$".

2. Eine Menge A heißt **echte Teilmenge** von B, falls $A \subseteq B$ und $A \neq \emptyset$, $A \neq B$. In diesem Fall schreiben wir $A \subset B$ und sagen: A ist echt enthalten in B.

Wir können Mengen kombinieren, um weitere Mengen zu bilden.

Definitionen

A und B seien Mengen.

1. Die **Vereinigungsmenge** oder **Vereinigung** von A und B ist die Menge

   $A \cup B = \{x : x \in A \text{ oder } x \in B\}$.

   "A vereinigt mit B"

2. Die **Schnittmenge** oder der **Durchschnitt** von A und B ist die Menge

   $A \cap B = \{x : x \in A \text{ und } x \in B\}$.

   "A durchschnitten B"

3. Die **Differenz** von A und B ist die Menge

   $A \setminus B = \{x : x \in A \text{ und } x \notin B\}$.

   "A ohne B"

Bemerkungen

1. In der Mathematik benutzen wir das Wort "oder" immer **im nicht ausschließenden Sinne**. "$x \in A$ oder $x \in B$" bedeutet also "$x \in A$" oder "$x \in B$" oder beides.

2. Falls $A \cap B = \emptyset$ (d. h. A und B haben keine gemeinsamen Elemente), sagen wir: A und B sind **disjunkt**.

Beispiel

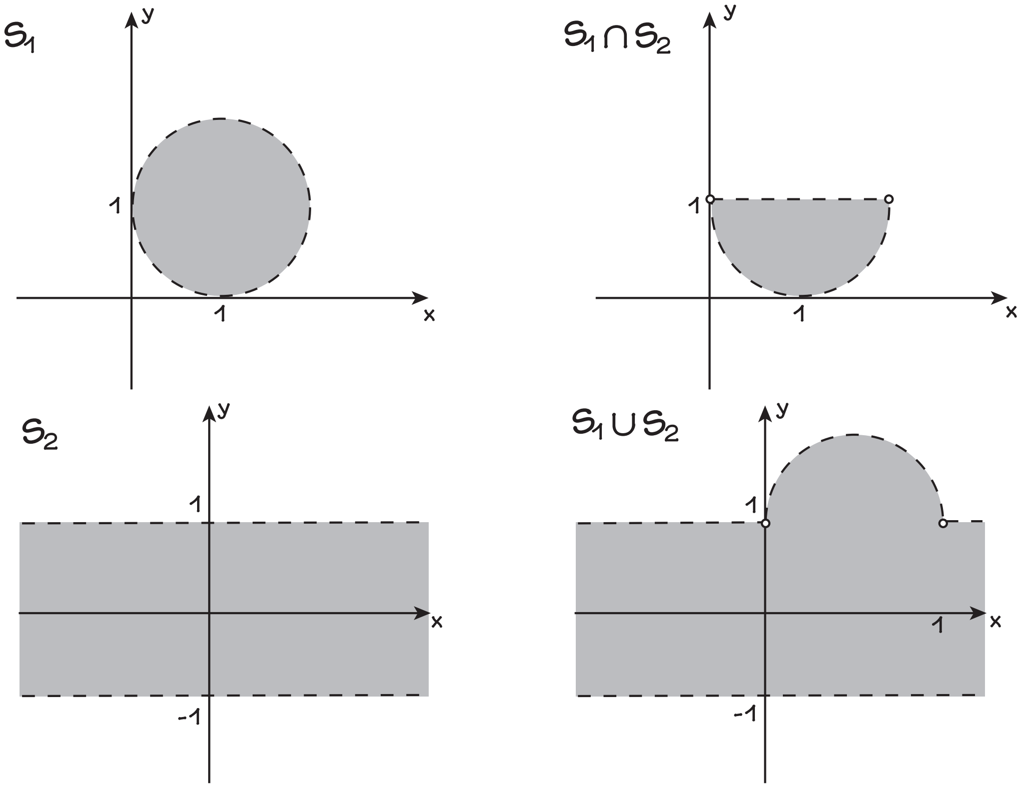
$$S_1 = \{(x,y) : (x-1)^2 + (y-1)^2 < 1\}, \;\; S_2 = \{(x,y) : |y| < 1\}$$

seien Teilmengen der Ebene

$$P = \{(x,y) : x,y \in \mathbb{R}\}.$$

Zeichnen Sie die Mengen S_1,S_2,$S_1 \cap S_2$ und $S_1 \cup S_2$.

Lösung



Zeichenerklärung

— “Rand” gehört zur Menge

- - “Rand” gehört nicht zur Menge

● “Eckpunkt” gehört zur Menge

○ “Eckpunkt” gehört nicht zur Menge

$\square$

Im letzten Beispiel betrachteten wir S_1 und S_2 als Teilmengen einer **Universalmenge** P.

Definition

A sei Teilmenge einer Universalmenge U. Die Menge

$$\overline{A} \underset{\substack{\uparrow \\ \text{definitionsgemäß gleich}}}{:=} U \setminus A$$

heißt **Komplement** von A in U.

Gesetze der Mengenoperationen

X, Y und Z seien Teilmengen der Universalmenge U.

$$\left.\begin{aligned} X \cup \emptyset &= X \\ X \cap U &= X \end{aligned}\right\} \textbf{ Identitätsgesetze}$$

$$\left.\begin{aligned} X \cup \overline{X} &= U \\ X \cap \overline{X} &= \emptyset \end{aligned}\right\} \textbf{ Dominationsgesetze}$$

$$\left.\begin{aligned} (X \cup Y) \cup Z &= X \cup (Y \cup Z) \\ (X \cap Y) \cap Z &= X \cap (Y \cap Z) \end{aligned}\right\} \textbf{ Assoziativgesetze}$$

$$\left.\begin{aligned} X \cup Y &= Y \cup X \\ X \cap Y &= Y \cap X \end{aligned}\right\} \textbf{ Kommutativgesetze}$$

$$\left.\begin{aligned} X \cap (Y \cup Z) &= (X \cap Y) \cup (X \cap Z) \\ X \cup (Y \cap Z) &= (X \cup Y) \cap (X \cup Z) \end{aligned}\right\} \textbf{ Distributivgesetze}$$

Wir betrachten diese Grundgesetze der Mengenoperationen als **Axiome** (gegebene, nicht beweisbare Gesetze) und leiten weitere Ergebnisse von ihnen her.

Lemma

A und B seien Teilmengen der Universalmenge U. Es gelten:

$$\left.\begin{aligned} A \cup A = A \\ A \cap A = A \end{aligned}\right\} \textbf{Idempotenzgesetz}$$

$$\overline{\overline{A}} = A \quad \textbf{(Involutionsgesetz)}$$

$$\left.\begin{aligned} \overline{A \cup B} = \overline{A} \cap \overline{B} \\ \overline{A \cap B} = \overline{A} \cup \overline{B} \end{aligned}\right\} \textbf{de Morgansche Gesetze}$$

Beweis

Es gilt:

$$\begin{aligned} A \cup A &= (A \cup A) \cap U && \text{(Identitätsgesetz)} \\ &= (A \cup A) \cap (A \cup \overline{A}) && \text{(Dominationsgesetz)} \\ &= A \cup (A \cap \overline{A}) && \text{(Distributivgesetz)} \\ &= A \cup \emptyset && \text{(Dominationsgesetz)} \\ &= A && \text{(Identitätsgesetz)} \end{aligned}$$

Die anderen Aussagen werden in ähnlicher Weise bewiesen. □

Bemerkung

Unsere Definition von einer Menge als "Sammlung von Objekten" ist etwas naiv und kann zu Problemen führen.

(i) Als Elemente können Mengen andere Mengen haben.

Beispiel

A sei eine Menge. Die Menge aller Teilmengen von A heißt die **Potenzmenge** von A und wird mit $P(A)$ bezeichnet.

Für $A = \{1,2\}$ ist z. B.

$$P(A) = \{\emptyset, \{1\}, \{2\}, \{1,2\}\}.$$

(ii) Eine Menge kann sich selbst als Element haben. L sei die Liste aller Dinge in Prof. Groves' Uni-Tasche. Diese Liste L stellt eine Menge durch Aufzählung dar:

$$L = \{\text{Lehrbuch, Stift, Vorlesungsskript, Hammer}\}.$$

(Der Hammer ist zum Kaputtschlagen von Handys, die während der Vorlesung klingeln.) Oft legt Prof. Groves auch die Liste in seine Tasche. Wir müssen also L in

$$L = \{\text{Lehrbuch, Stift, Vorlesungsskript, Hammer}, L\}$$

abändern. Damit enthält die Menge L sich selbst.

(iii) **Die Russellsche Antimonie**

M sei die Menge aller Mengen, die sich selbst nicht enthalten. Frage: Enthält M sich selbst, d. h. ist $M \in M$?

– Falls $M \in M$, gilt definitionsgemäß $M \notin M$.

– Falls $M \notin M$, gilt definitionsgemäß $M \in M$.

Damit führt die Existenz von M zu einem logischen Widerspruch.

Um solche Probleme zu vermeiden, brauchen wir eine viel subtilere Definition des Begriffs "Menge". Es handelt sich hier um die **axiomatische Mengenlehre**, die in dieser Vorlesung nicht behandelt wird.

Geordnete n-Tupel

Eine Menge ist eine **nicht geordnete** Zusammenfassung von Objekten. Manchmal ist die Ordnung allerdings wichtig.

Definition

A und B seien beliebige Mengen.

- Ein Paar (a,b) mit $a \in A$ und $b \in B$ heißt **geordnetes Paar** mit a als erster Komponente und b als zweiter Komponente.

- Die Menge aller solchen geordneten Paare

$$\underset{\text{“A kreuz B”}}{\underset{\uparrow}{A \times B}} := \{(a,b) : a \in A, b \in B\}$$

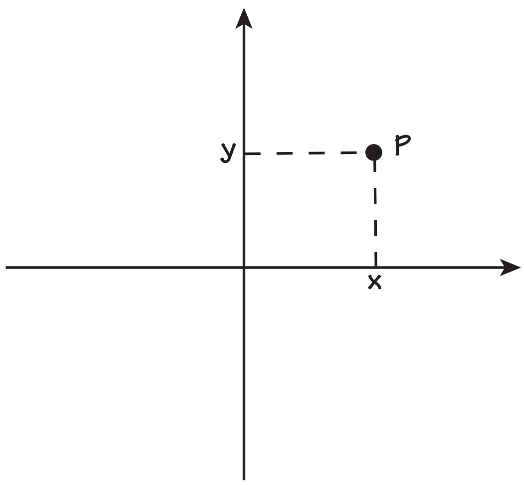
  heißt **Produktmenge** oder **kartesisches Produkt** von A und B.

Beispiel

Die Lage eines Punktes P der Ebene läßt sich durch ein geordnetes Paar reeller Zahlen beschreiben:

$P(x,y)$

horizontale Koordinate ↗ ↖ vertikale Koordinate



Damit ist die Ebene die Menge aller geordneten Paare reeller Zahlen, d. h. die Menge $\mathbb{R} \times \mathbb{R}$. Statt $\mathbb{R} \times \mathbb{R}$ schreibt man meist $\mathbb{R}^2$.

Diese Idee läßt sich verallgemeinern.

Definition

$A_1, \ldots, A_n$ seien n beliebige Mengen. Die Menge

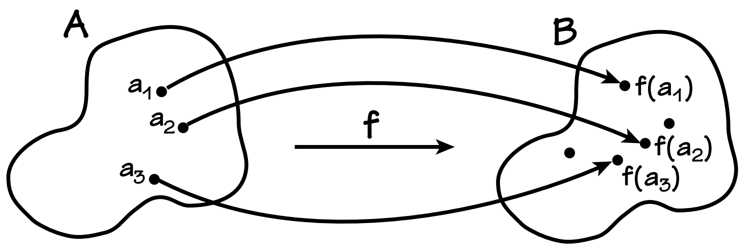
$$A_1 \times A_2 \times \ldots \times A_n = \{(a_1, \ldots, a_n) : a, \in A_1, \ldots, a_n \in A_n\}$$

aller **geordneten n-Tupel** $(a_1, \ldots, a_n)$ mit $a_i \in A_i, i = 1, \ldots, n$ heißt **Produktmenge** oder **kartesisches Produkt** von $A_1, \ldots, A_n$.

1.2 Funktionen

Definition

A und B seien Mengen. Eine **Funktion** oder **Abbildung** $f : A \to B$ ("f von A nach B") ist eine Vorschrift, die jedem Element $a \in A$ **genau ein** Element $f(a) \in B$ **zuordnet**.



Die Menge A ist die **Urmenge** von f

Die Menge B ist die **Zielmenge** von f

Beispiele

1. Wir sind daran gewöhnt, Funktionen durch explizite Formeln zu definieren, z. B.
$$f : \mathbb{R} \to \mathbb{R}, \qquad f(x) = \sin x.$$

2. Wir brauchen jedoch nur die maßgebende Zuordnung anzugeben, z. B.
$$f : \{1,3,5\} \to \mathbb{N}, \qquad \begin{aligned} f(1) &= 3, \\ f(3) &= 4, \\ f(5) &= 7. \end{aligned}$$

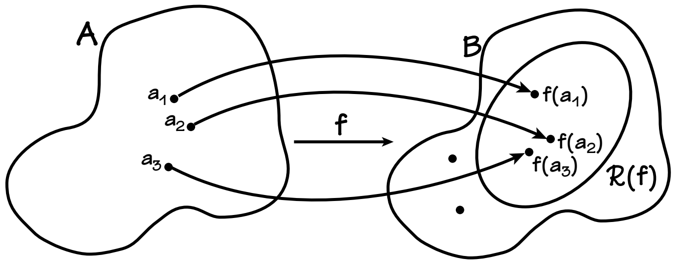
Definitionen

$f : A \to B$ sei eine Funktion.

Das Element $f(a) \in B$ heißt **Bild** oder **(Funktions)wert** von $a \in A$ unter f.

Die Menge aller Funktionswerte von f, d. h.
$$\mathcal{R}(f) := \{f(a) : a \in A\},$$

heißt **Bildmenge** oder **Wertebereich** von f; sie ist Teilmenge von B.



Beispiele

1. $f : \mathbb{R} \to \mathbb{R}, \quad f(x) = \sin x.$

   Es gilt:
$$\begin{aligned} \mathcal{R}(f) &= \{\sin x : x \in \mathbb{R}\} \\ &= [-1,1]. \end{aligned}$$

2. $f : \{1,3,5\} \to \mathbb{N}, \qquad \begin{aligned} f(1) &= 3, \\ f(3) &= 4, \\ f(5) &= 7. \end{aligned}$

   Es gilt:
$$\begin{aligned} \mathcal{R}(f) &= \{f(1), f(3), f(5)\} \\ &= \{3,4,7\}. \end{aligned}$$

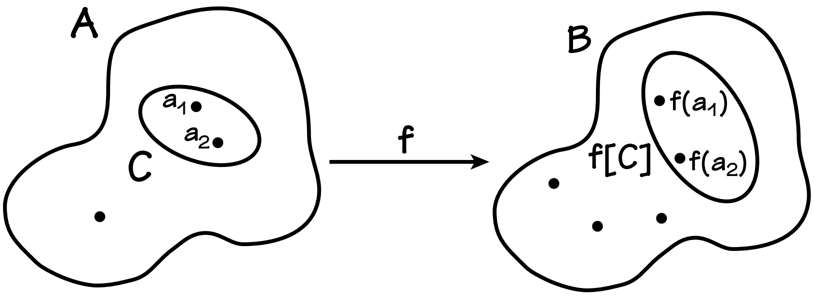
s

Definition

$f : A \to B$ sei eine Funktion und C sei Teilmenge von A. Die Menge aller Funktionswerte von f, die aus Elementen von C stammen, d. h.

$$f[C] := \{f(a) : a \in C\}$$

heißt das **Bild** von C unter der Funktion f.



Beispiele

1. $f : \mathbb{R} \to \mathbb{R}, \;\; f(x) = \sin x.$

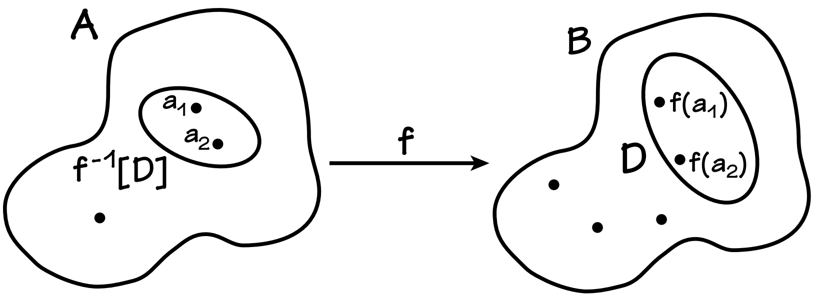
   Es gilt:
$$\begin{aligned} f([0,\pi]) &= \{\sin x : x \in [0,\pi]\} \\ &= [0,1]. \end{aligned}$$

2. $f : \{1,3,5\} \to \mathbb{N}, \qquad \begin{aligned} f(1) &= 3, \\ f(3) &= 4, \\ f(5) &= 7. \end{aligned}$

   Es gilt:
$$\begin{aligned} f(\{1,3\}) &= \{f(1), f(3)\} \\ &= \{3,4\}. \end{aligned}$$

Definition

$f : A \to B$ sei eine Funktion und D sei Teilmenge von B. Die Menge aller Elemente von A, deren Bilder unter f in D liegen, d. h.
$$f^{-1}[D] := \{a \in A : f(a) \in D\}$$
heißt das **Urbild** von D unter der Funktion f.



Beispiele

1. $f : \mathbb{R} \to \mathbb{R}, \quad f(x) = \sin x.$

   Es gilt:
$$\begin{aligned} f^{-1}([0,1]) &= \{x : \sin x \in [0,1]\} \\ &= \bigcup_{n \in \mathbb{Z}} [2n\pi, (2n+1)\pi] \end{aligned}$$

2. $f : \{1,3,5\} \to \mathbb{N}, \qquad \begin{aligned} f(1) &= 3, \\ f(3) &= 4, \\ f(5) &= 7. \end{aligned}$

   Es gilt:
$$f^{-1}(\{77\}) = \emptyset$$

Definitionen

Eine Funktion $f : A \to B$ heißt

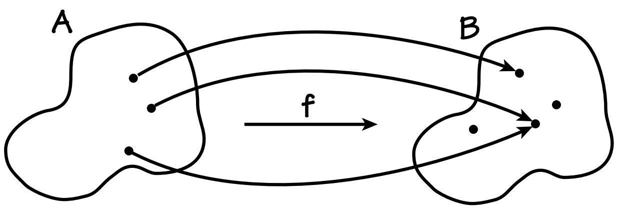
(i) **injektiv**, falls
$$a_1 \neq a_2 \Rightarrow f(a_1) \neq f(a_2);$$
$$\text{“}a_1 \neq a_2 \text{ impliziert } f(a_1) \neq f(a_2)\text{”}$$

(ii) **surjektiv**, falls
$$\mathcal{R}(f) = B;$$

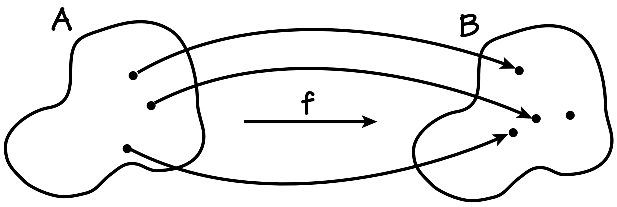
(iii) **bijektiv**, falls sie injektiv und surjektiv ist.

Beispiele

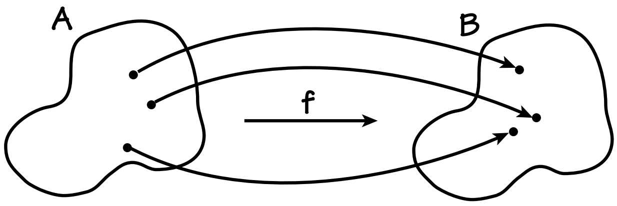
1.



Diese Funktion ist weder injektiv noch surjektiv.

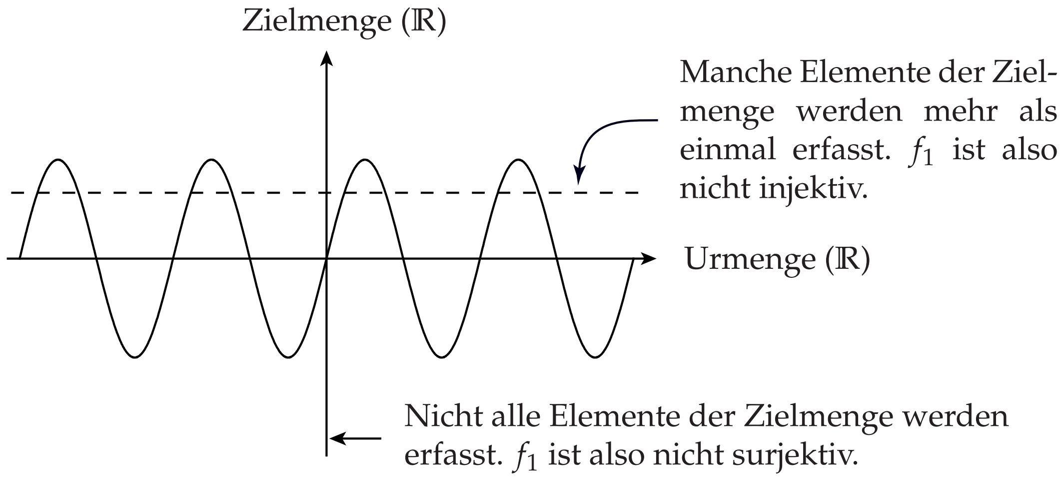
2. 

Diese Funktion ist injektiv, aber nicht surjektiv.

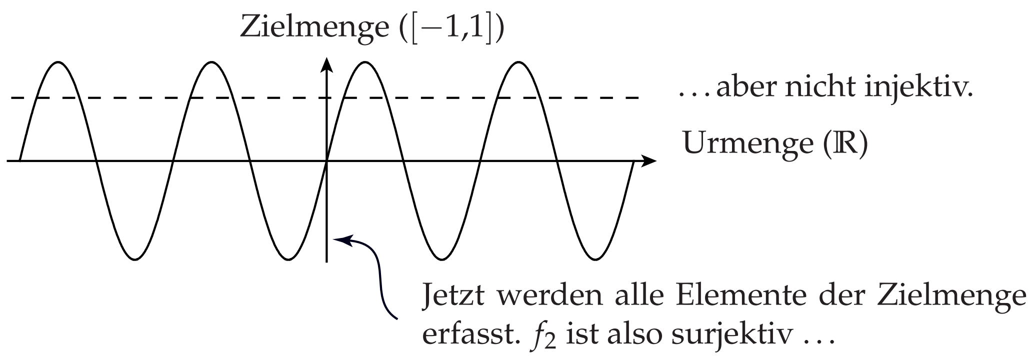
3. 

Diese Funktion ist injektiv und surjektiv, also bijektiv.

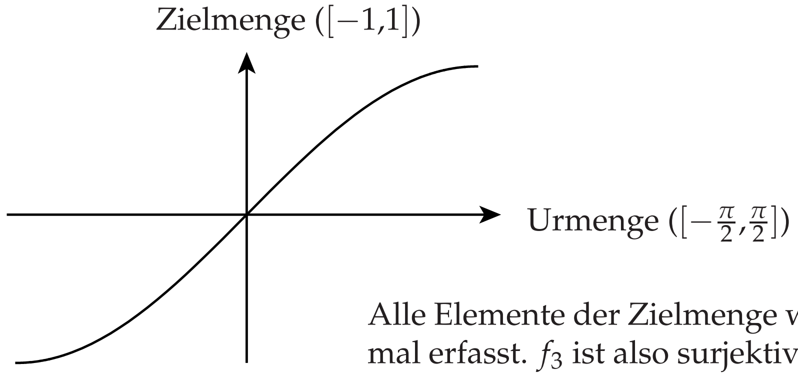
4. $f_1 : \mathbb{R} \to \mathbb{R}, f_1(x) = \sin x$



5. $f_2 : \mathbb{R} \to [-1,1], f_2(x) = \sin x$



6. $f_3 : [-\frac{\pi}{2}, \frac{\pi}{2}] \to [-1,1], f_3(x) = \sin x$



Alle Elemente der Zielmenge werden genau einmal erfasst. f_3 ist also surjektiv und injektiv, also bijektiv.

Beispiele 4–6 verdeutlichen, dass die Wahl der Mengen A und B **ein wesentlicher Teil** der Definition einer Funktion $f : A \to B$ ist.

Bemerkung

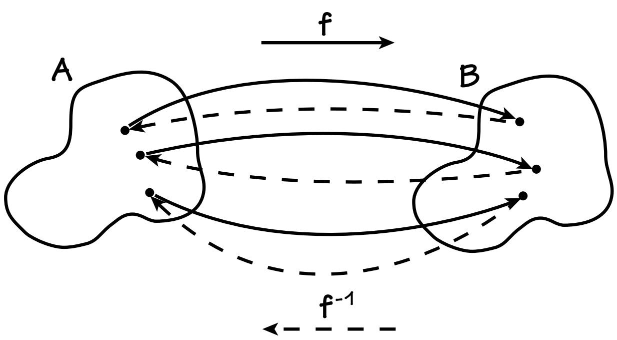
Betrachten Sie eine bijektive Funktion $f : A \to B$. Weil f injektiv ist, existiert zu jedem Element b in der Bildmenge von f **genau ein Element** a in der Urmenge von f, das auf b abgebildet wird. Weil f surjektiv ist, ist die Bildmenge von f gleich B. Somit haben wir eine neue Funktion definiert:

Definition

$f : A \to B$ sei eine bijektive Funktion. Die Funktion $f^{-1} : B \to A$,

$$f^{-1}(b) := a, \qquad \text{wobei } a \text{ das eindeutige Element aus } A \text{ mit der Eigenschaft } b = f(a) \text{ ist,}$$

heißt **Umkehrfunktion** von f.



Bemerkung

$f^{-1} : B \to A$ ist ebenfalls bijektiv, und es gilt

$$f^{-1}(f(a)) = a, \qquad a \in A,$$
$$f(f^{-1}(b)) = b, \qquad b \in B.$$

Beispiel

Die Umkehrfunktion der bijektiven Funktion

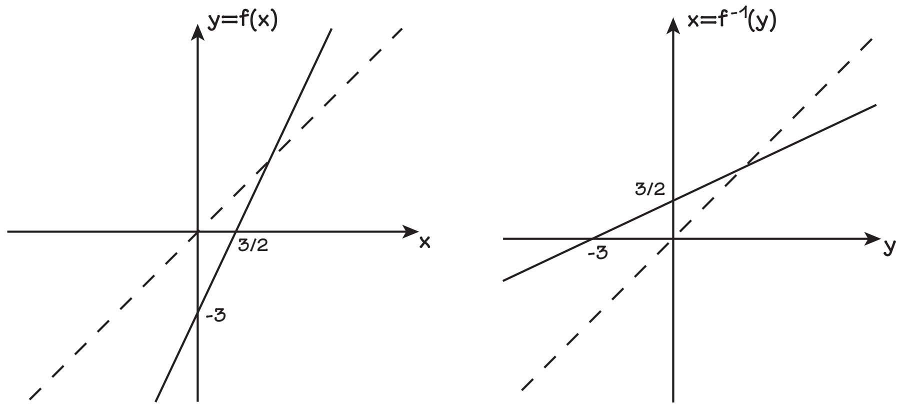
$$f : \mathbb{R} \to \mathbb{R}, \qquad f(x) = 2x - 3$$

ist

$$f^{-1} : \mathbb{R} \to \mathbb{R}, \qquad f^{-1}(y) = \frac{y}{2} + \frac{3}{2},$$

weil

$$y = 2x - 3 \quad \Leftrightarrow \quad x = \frac{y}{2} + \frac{3}{2}.$$



Geometrisch gesehen tauschen wir die Rollen der horizontalen und vertikalen Achsen. Die Graphen von f und f^{-1} sind also durch eine Spiegelung an der Geraden $y = x$ miteinander verwandt.

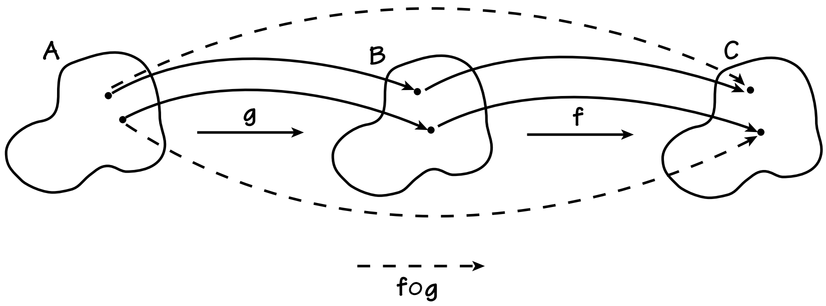
Definition

$g : A \to B$ und $f : B \to C$ seien Funktionen.

Die Funktion

$$\underset{\substack{\uparrow \\ \text{“}f\text{ nach }g\text{”}}}{f \circ g} : A \to C, \qquad (f \circ g)(a) = f(g(a))$$

heißt **Komposition** von f und g.



Proposition

Es seien $g : A \to B$ und $f : B \to C$ Funktionen.

1. Ist $f \circ g : A \to C$ injektiv, so ist $g : A \to B$ injektiv.
2. Ist $f \circ g : A \to C$ surjektiv, so ist $f : B \to C$ surjektiv.

Beweis

1. Wir wissen:

   - Aus $(f \circ g)(a_1) = (f \circ g)(a_2)$ folgt $a_1 = a_2$.

   Wir müssen zeigen:

   - Aus $g(a_1) = g(a_2)$ folgt $a_1 = a_2$.

   Es sei also $g(a_1) = g(a_2)$. Dann ist $f(g(a_1)) = f(g(a_2))$, d.h. $(f \circ g)(a_1) = (f \circ g)(a_2)$. Folglich gilt $a_1 = a_2$.

2. Wir wissen:

   - Zu jedem $c \in C$ existiert $a \in A$ mit $(f \circ g)(a) = c$.

   Wir müssen zeigen:

   - Zu jedem $c \in C$ existiert $b \in B$ mit $f(b) = c$.

   Es sei also $c \in C$. Dann gibt es $a \in A$ mit $(f \circ g)(a) = c$, d.h. $f(g(a)) = c$. Folglich hat $b = g(a)$ die Eigenschaft $f(b) = c$. $\square$

1.3 Relationen

Definition

Es sei $f : A \to B$ eine Abbildung. Der **Graph** von f ist die Teilmenge

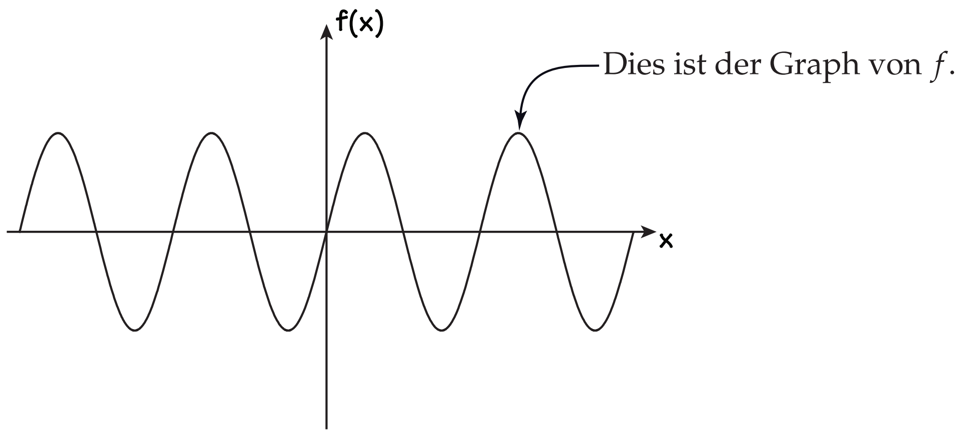
$$\mathcal{G}_f := \{(a, f(a)) : a \in A\}$$

von $A \times B$.

Beispiele

1. $f : \mathbb{R} \to \mathbb{R}, \quad f(x) = \sin x$.

   $\mathcal{G}_f = \{(x, \sin x) : x \in \mathbb{R}\}$ können wir als Teilmenge von $\mathbb{R}^2$ gut visualisieren:



2. $f : \{1,3,5\} \to \mathbb{N}, \qquad \begin{array}{l} f(1) = 3 \\ f(3) = 4, \\ f(5) = 7. \end{array}$

   Der Graph von f ist die Teilmenge $\{(1,3),(3,4),(5,7)\}$ von

   $\{1,3,5\} \times \mathbb{N} = \{(1,1),(1,2),(1,3),\ldots,(3,1),(3,2),(3,3),\ldots,(5,1),(5,2),(5,3),\ldots\}$.

Bemerkung

Wir definierten eine Funktion $f : A \to B$ als Vorschrift, die jedem Element $a \in A$ genau ein Element $f(a) \in B$ zuordnet. Der Graph von f ist lediglich die Menge dieser Zuordnungen:

$(a,b) \in \mathcal{G}_f$	bedeutet	b ist das Element von B, das a zugordnet wird, d.h. $b = f(a)$

f wird also vollständig von $\mathcal{G}_f$ wiedergegeben, und somit können wir f durch seinen Graphen **definieren**.

Definitionen

A und B seien Mengen.

1. Eine **Relation** R zwischen A und B ist eine Teilmenge der Produktmenge $A \times B$.

   Oft schreiben wir aRb statt $(a,b) \in R$ und sagen: 'a steht in Relation zu b'.

2. Die Menge A wird als **Quellmenge** oder **Vorbereich** der Relation bezeichnet. Die Menge B ist die **Zielmenge** oder der **Nachbereich** der Relation.

Beispiel

Es seien M und F die Mengen aller Männer bzw. aller Frauen. Die Teilmenge

$$\{(m,f) \in R : m \text{ ist der Ehemann von } f\}$$

von $M \times F$ ist eine Relation zwischen M und F.

Es gilt z.B.

- (Prince Charles, Camilla Parker-Bowles) $\in R$,
- (Donald Trump, Hillary Clinton) $\notin R$.

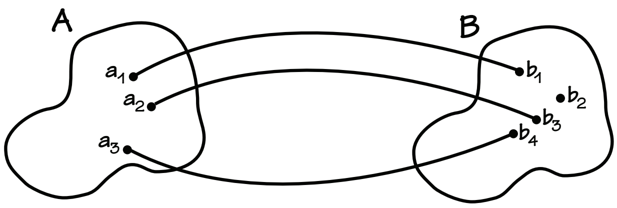
Definitionen

Eine Relation R zwischen zweier Mengen A und B heißt

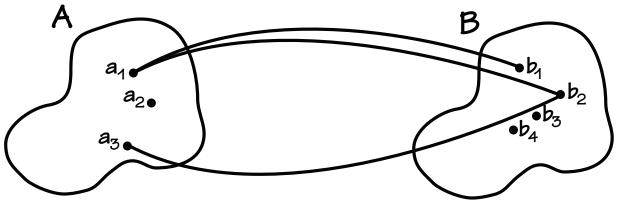
1. **linkstotal**, falls es zu jedem $a \in A$ ein $b \in B$ mit aRb gibt,
2. **rechtstotal**, falls es zu jedem $b \in B$ ein $a \in A$ mit aRb gibt,
3. **linkseindeutig**, falls aus a_1Rb und a_2Rb die Gleichheit $a_1 = a_2$ folgt,
4. **rechtseindeutig**, falls aus aRb_1 und aRb_2 die Gleichheit $b_1 = b_2$ folgt,

Beispiele

Es seien $A = \{a_1,a_2,a_3\}$, $B = \{b_1,b_2,b_3,b_4\}$.

1. 

   Die Relation $R = \{(a_1,b_1),(a_2,b_3),(a_3,b_4)\}$ ist linkstotal und links- und rechtseindeutig, aber nicht rechtstotal.

2. 

   Die Relation $R = \{(a_1,b_1),(a_1,b_2),(a_3,b_2)\}$ ist weder linkstotal, rechtstotal, linkseindeutig noch rechtseindeutig.

Bemerkungen

Es seien A und B Mengen.

Eine Funktion $f : A \to B$ ist eine linkstotale, rechtseindeutige Relation zwischen A und B. f ist genau dann injektiv, wenn die Relation linkseindeutig ist, und genau dann surjektiv, wenn die Relation rechtstotal ist.

Definitionen

Eine Relation zwischen einer Menge A und sich selbst heißt **homogen**. Wir sprechen in diesem Fall von ‘einer Relation auf einer Menge A’. Homogene Relationen werden häufig mit dem Symbol $\sim$ bezeichnet und heißen

1. **reflexiv**, falls $a \sim a$ für alle $a \in A$,
2. **konnex**, falls $a \sim b$ oder $b \sim a$ für alle $a,b \in A$ mit $a \neq b$,
3. **symmetrisch**, falls $a \sim b \Rightarrow b \sim a$,
4. **asymmetrisch**, falls $a \sim b \Rightarrow b \not\sim a$,
5. **antisymmetrisch**, falls $a \sim b$ und $b \sim a \Rightarrow a = b$,
6. **transitiv**, falls $a \sim b$ und $b \sim c \Rightarrow a \sim c$.

Beispiele

Die Tabelle zeigt einige homogene Relationen auf $\mathbb{N}$.

$x \sim y$, falls	reflexiv?	symmetrisch?	transitiv?
$x \leq y$	ja ($x \leq x$)	nein ($3 \leq 4$, $4 \not\leq 3$)	ja ($x \leq y$, $y \leq z \Rightarrow x \leq z$)
$x \mid y$	ja ($x \mid x$)	nein ($3 \mid 6$, $6 \nmid 3$)	ja ($x \mid y$, $y \mid z \Rightarrow x \mid z$)
$x + y = 7$	nein ($2x \neq 7$ für alle $x \in \mathbb{N}$)	ja	nein ($3 + 4 = 7$ und $4 + 3 = 7$, $3 + 3 = 6$)

$x \sim y$, falls	konnex?	asymmetrisch?	antisymmetrisch?
$x \leq y$	ja	nein (reflexiv)	ja ($x \leq y, y \leq x \Rightarrow x = y$)
$x \vert y$	nein ($3 \nmid 5$, $5 \nmid 3$)	nein (reflexiv)	ja ($x \vert y, y \vert x \Rightarrow x = y$)
$x + y = 7$	nein ($3 + 2 \neq 7$, $2 + 3 \neq 7$)	nein (symmetrisch)	nein ($3 + 4 = 7, 4 + 3 = 7$)

Definition

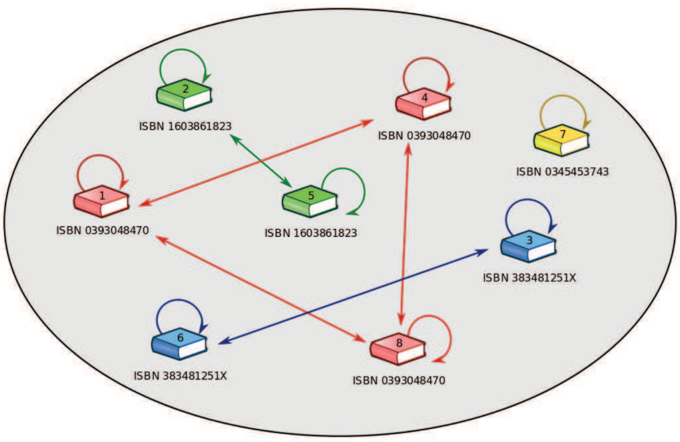
Eine Relation $\sim$ auf einer Menge M heißt **Äquivalenzrelation**, falls sie reflexiv, symmetrisch und transitiv ist.

Beispiel

Es sei M die Menge aller Bücher in der Bibliothek. Die Relation

$$a \sim b \qquad \Leftrightarrow \qquad a \text{ und } b \text{ haben dieselbe ISBN}$$

ist eine Äquivalenzrelation auf M:



Definition

Es sei $n \in \mathbb{N}$. Zwei Zahlen $a, b \in \mathbb{Z}$ heißen **kongruent modulo** n, falls $n \vert (a - b)$. In diesem Fall schreiben wir

$$a \equiv b \ (\text{mod } n).$$

Proposition

Es sei $n \in \mathbb{N}$. Die Formel

$$a \sim b \qquad \Leftrightarrow \qquad a \equiv b \pmod{n}$$

definiert eine Äquivalenzrelation auf $\mathbb{Z}$.

Beweis

- $\sim$ ist reflexiv: $a \sim a$ für alle $a \in \mathbb{Z}$, denn $a - a = 0$ und $n|0$.
- $\sim$ ist symmetrisch: Es gelte $a \sim b$, so dass $n|(a-b)$. Folglich gilt auch $n|(b-a)$, d.h. $b \sim a$.
- $\sim$ ist transitiv: Es gelten $a \sim b$ und $b \sim c$, so dass $n|(a-b)$ und $n|(b-c)$. Folglich gilt es ganze Zahlen q_1 und q_2 derart, dass $a - b = q_1 n$ und $b - c = q_2 n$. Es ist also $a - c = (a-b) + (b-c) = (q_1 + q_2)n$ und $n|(a-c)$, d.h. $a \sim c$.

□

Definition

Es seien $\sim$ eine Äquivalenzrelation auf einer Menge M und $m \in M$.

Die Teilmenge

$$[m] := \{x \in M : x \sim m\}$$

heißt die **Äquivalenzklasse** von m in M.

Lemma

Es sei $\sim$ eine Äquivalenzrelation auf eine Menge M. Dann bilden die Äquivalenzklassen von $\sim$ eine **Partition** von M, d.h.

1. für alle $x, y \in M$ gilt entweder $[x] \cap [y] = \emptyset$ oder $[x] = [y]$,
2. $\bigcup\limits_{x \in M} [x] = M$.

Beweis

1. Es sei $[x] \cap [y] \neq \emptyset$. Wähle $z \in [x] \cap [y]$.

   Es gilt nun

   $$\begin{aligned} a \in [x] &\Rightarrow a \sim x \\ &\Rightarrow a \sim z \qquad \text{(denn } a \sim x \text{ und } x \sim z\text{)} \\ &\Rightarrow a \sim y \qquad \text{(denn } a \sim z \text{ und } z \sim y\text{)} \\ &\Rightarrow a \in [y], \end{aligned}$$

   so dass $[x] \subseteq [y]$. Dasgleiche Argument ergibt $[y] \subseteq [x]$, so dass $[x] = [y]$ ist.

2. Wähle $m \in M$. Aus $m \sim m$ folgt $m \in [m]$ und daher

   $$m \in [m] \subseteq \bigcup_{x \in M} [x],$$

   so dass $M \subseteq \bigcup_{x \in M} [x]$. Definitionsgemäß gilt $\bigcup_{x \in M} [x] \subseteq M$. □

Bemerkung

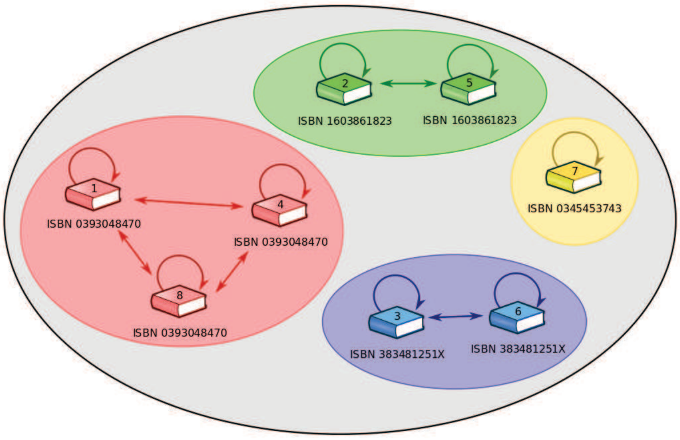
Insbesondere folgt $[x] = [y]$ aus $x \sim y$.

Beispiele

1. Es sei M die Menge aller Bücher in der Bibliothek. Die Äquivalenzklassen der Äquivalenzrelation

   $$a \sim b \qquad \Leftrightarrow \qquad a \text{ und } b \text{ haben dieselbe ISBN}$$

   bilden eine Partition von M:



2. Es seien $n \in \mathbb{N}$ und $\sim$ die Äquivalenzrelation

$$a \sim b \qquad \Leftrightarrow \qquad a \equiv b \pmod{n}$$

auf $\mathbb{Z}$.

Um die Äquivalenzklassen zu bestimmen, brauchen wir das folgende Ergebnis, das später bewiesen wird:

- Zu jedem $a \in \mathbb{Z}$ gibt es eindeutige Zahlen $q_a \in \mathbb{Z}$ (den **Quotienten**) und $r_a \in \{0, \ldots, n-1\}$ (den **Rest**) derart, dass

$$a = q_a n + r_a.$$

Aus

$$a - x = (q_a - q_x)n + r_a - r_x$$

folgt nun

$$a \sim x \qquad \Leftrightarrow \qquad r_a = r_x,$$

so dass

$$[x] = \{a \in \mathbb{Z} : r_a = r_x\}.$$

Es gibt also n verschiedene Äquivalenzklassen, nämlich

$$\begin{aligned}
&[0] = \{0, n, 2n, \ldots\} \cup \{-n, -2n, \ldots\},\\
&[1] = \{1, n+1, 2n+1, \ldots\} \cup \{-n+1, -2n+1, \ldots\},\\
&[2] = \{2, n+2, 2n+2, \ldots\} \cup \{-n+2, -2n+2, \ldots\},\\
&\vdots\\
&[n-1] = \{n-1, 2n-1, 3n-1, \ldots\} \cup \{-1, -1-n, \ldots\},
\end{aligned}$$

und diese bilden eine Partition von $\mathbb{Z}$:

$$\mathbb{Z} = \bigcup_{i=0}^{n-1} [i], \qquad [i] \cap [j] = \emptyset \text{ für } i \neq j.$$

Lemma

Es sei $\{X_i\}_{i\in I}$ eine Partition einer Menge X, d.h.

$$\bigcup_{i\in I} X_i = X, \qquad X_i \cap X_j = \emptyset \text{ für } i \neq j.$$

Dann definiert die Formel

$$a \sim b \qquad \Leftrightarrow \qquad a,b \in X_{i^\star} \text{ für irgendein } i^\star \in I$$

eine Äquivalenzrelation auf X, deren Äquivalenzklassen die Mengen X_i, $i \in I$ sind.

Ist ferner $\approx$ eine weitere Äquivalenzrelation auf X, deren Äquivalenzklassen genau die Mengen X_i, $i \in I$ sind, so stimmt $\approx$ mit $\sim$ überein.

Definition

Eine Relation $\preceq$ auf einer Menge M heißt **partielle Ordnung**, falls sie reflexiv, antisymmetrisch und transitiv ist. Sie ist eine **Totalordnung**, falls sie auch konnex ist.

Bemerkung

Für eine Ordnung $\preceq$ schreiben wir oft $a \prec b$, falls $a \preceq b$ aber $a \neq b$.

Beispiele

1. Die Relation
$$a \preceq b \qquad \Leftrightarrow \qquad a|b$$
ist eine partielle Ordnung aber keine Totalordnung auf $\mathbb{N}$.

2. Die Relation
$$a \preceq b \qquad \Leftrightarrow \qquad a \leq b$$
ist eine Totalordnung auf $\mathbb{R}$.

3. Die Relation $\preceq$, wobei

$$\begin{aligned}(a_1,\dots,a_n) \prec (b_1,\dots,b_n), \text{ falls entweder } & a_1 < b_1 \\ \text{oder } & a_1 = b_1 \text{ und } a_2 < b_2 \\ & \vdots \\ \text{oder } & a_1 = b_1, \dots, a_{n-1} = b_{n-1} \text{ und } a_n < b_n,\end{aligned}$$

definiert eine Totalordnung auf $\mathbb{N}^n$.

Im Falle $n = 4$ gilt z.B.

- $(1,2,3,5) \prec (1,2,4,3)$, denn $3 < 4$,
- $(1,7,9,11) \prec (1,7,9,14)$, denn $11 < 14$.

4. Auf der Menge aller Ketten von natürlichen Zahlen wird eine Totalordnung durch die Regel

$$\begin{aligned}a_1 a_2 \dots a_m \prec b_1 b_2 \dots b_n, \text{ falls entweder } & (a_1,\dots,a_t) \prec (b_1,\dots,b_t) \\ \text{order } & (a_1,\dots,a_t) = (b_1,\dots,b_t) \text{ und } m < n\end{aligned}$$

definiert, wobei $t = \min(m,n)$.

Schreiben wir a, …, z statt $1,\dots,26$, so erhalten wir die **lexikographische Ordnung**: Es gilt z.B.

- zumuten $\prec$ Zumutung
- faulen $\prec$ faulenzen

2 Körper und Zahlen

2.1 Körper

Definition

Es sei X eine nichtleere Menge. Eine **(binäre) Verknüpfung** $\odot$ auf X ist eine Abbildung $X \times X \to X$.

In der Regel verwenden wir die Notation $x_1 \odot x_2$ an Stelle von $\odot(x_1,x_2)$.

Definition

Ein **Körper** ist eine mit zwei Verknüpfungen + ('Addition') und . ('Multiplikation') versehene nichtleere Menge X, die die folgenden Eigenschaften haben.

(A1)	$x+(y+z)=(x+y)+z \quad \forall x,y,z \in X$	**(Assoziativgesetz der Addition)**
(A2)	$x+y=y+x \quad \forall x,y \in X$	**(Kommutativgesetz der Addition)**
(A3)	Es existiert ein Element $0 \in X$ mit der Eigenschaft $x+0=0+x=x \quad \forall x \in X$	**(Existenz eines neutralen Elements der Addition)**
(A4)	Zu jedem $x \in X$ existiert ein Element $-x \in X$ derart, dass $x+(-x)=-x+x=0$	**(Existenz additiver inverser Elemente)**
(A5)	$x.(y.z)=(x.y).z \quad \forall x,y,z \in X$	**(Assoziativgesetz der Multiplikation)**
(A6)	$x.y=y.x \quad \forall x,y \in X$	**(Kommutativgesetz der Multiplikation)**
(A7)	Es existiert ein Element $1 \in X \setminus \{0\}$ mit der Eigenschaft $1.x=x.1=x \quad \forall x \in X$	**(Existenz eines neutralen Elements der Multiplikation)**
(A8)	Zu jedem $x \in X \setminus \{0\}$ existiert ein Element $x^{-1} \in X$ derart, dass $x.x^{-1}=x^{-1}.x=1$	**(Existenz multiplikativer inverser Elemente)**
(A9)	$x.(y+z)=x.y+x.z \quad \forall x,y,z \in X$	**(Distributivgesetz)**

In der Regel verwenden wir die Schreibweise $(X, +, .)$ für einen Körper.

Bemerkung

Insgesamt besagen diese Eigenschaften, die wir auch die **Axiome der Arithmetik** nennen, dass die 'üblichen' Regeln der Arithmetik innerhalb eines Körpers gelten.

Lemma (Rechenregeln)

Es seien x,y,z,w Elemente eines Körpers $(K, +, .)$. Dann gilt:

1. $x + y = x + z \Rightarrow y = z$
2. $-(-x) = x$ und $-x = (-1).x$
3. $x.(-y) = -(x.y)$
4. $x.y = x.z,\ x \neq 0 \Rightarrow y = z$
5. $x.y = 0 \Rightarrow x = 0$ oder $y = 0$
6. Die Gleichung $x + y = z$ für x hat die eindeutige Lösung $x = z + (-y)$.
7. Die Gleichung $y.x = z,\ y \neq 0$ für x hat die eindeutige Lösung $x = y^{-1}.z$.
8. $x.y^{-1} + z.w^{-1} = (x.w + z.y)(y.w)^{-1}, \qquad y,w \neq 0$

Beweis

4. $$\begin{aligned} & x.y = x.z \\ & \Rightarrow x^{-1}.(x.y) = x^{-1}.(x.z) && \text{(Multiplikation mit } x^{-1}\text{)} \\ & \Rightarrow (x^{-1}.x).y = (x^{-1}.x).z && \text{(A5)} \\ & \Rightarrow 1.y = 1.z && \text{(A8)} \\ & \Rightarrow y = z && \text{(A7)} \end{aligned}$$

Die anderen Aussagen werden in ähnlicher Weise bewiesen. □

Beispiele

1. Die Menge der reellen Zahlen bildet einen Körper bezüglich Addition und Multiplikation. In der Regel schreiben wir $a.b$, $a.b^{-1}$ und $a + (-b)$ als ab, a/b bzw. $a - b$.

2. Es sei p eine Primzahl und $\sim$ die Äquivalenzrelation

$$a \sim b \qquad \Leftrightarrow \qquad a \equiv b \text{ (mod } p\text{), d.h. } p|(b-a)$$

auf $\mathbb{Z}$. Die Menge

$$\mathbb{Z}_p := \{[0], \ldots, [p-1]\}$$

der Äquivalenzklassen bildet einen Körper $(\mathbb{Z}_p, \oplus, \odot)$ mit

$$[a] \oplus [b] := [a+b], \qquad [a] \odot [b] := [ab].$$

- Zunächst müssen wir zeigen, dass $\oplus$ und $\odot$ wohldefiniert sind, d.h.

$$[a] = [c], [b] = [d] \quad \Rightarrow \quad [a+b] = [c+d], [ab] = [cd].$$

$[a] = [c]$ und $[b] = [d]$ bedeutet

$$a - c = q_1 p, \qquad b - d = q_2 p$$

für irgendwelche ganzen Zahlen q_1 und q_2. Somit ist

$$(a+b) - (c+d) = (q_1 + q_2)p, \qquad ab - cd = (bq_1 + cq_2)p,$$

d.h. $[a+b] = [c+d]$ und $[ab] = [cd]$.

- Die Axiome (A1)–(A7) und (A9) lassen sich leicht verifizieren (die neutralen Elemente der Addition und Multiplikation sind $[0]$ bzw. $[1]$ und das additive inverse Element zu $[a]$ ist $-[a] := [-a]$).

- Nun zeigen wir, dass jedes $[a]$ mit $a \in 1, \ldots, p-1$ ein multiplikatives inverses Element hat.

Falls $[a]$ kein multiplikatives inverses Element hat, so gilt **keine** der Gleichungen

$$\underbrace{[0][a]}_{=[0a]} = [1], \ \underbrace{[1][a]}_{=[1a]} = [1], \ \underbrace{[2][a]}_{=[2a]} = [1], \ \ldots, \ \underbrace{[p-1][a]}_{=[(p-1)a]} = [1].$$

Zwei der Klassen $[0a]$, $[1a]$, $\ldots$, $[(p-1)a]$ sind also gleich. Nennen wir sie $[ia]$ und $[ja]$, wobei $i > j$ ist. Somit gilt $p|(i-j)a$. Aus $1 \leq i - j < p$ folgt $p|a$, aber dies ist nur für $a = 0$ möglich.

Definition

Ein Körper $(K, +, \cdot)$ heißt **geordnet**, falls es eine Relation $\prec$ auf K mit den folgenden Eigenschaften gibt:

(O1) Für alle $x,y \in K$ gilt genau eine der Beziehungen
$x = y, \qquad x \prec y, \qquad y \prec x$
(**Trichotomiegesetz**)

(O2) Für alle $x,y,z \in K$ gilt
$x \prec y, y \prec z \;\Rightarrow\; x \prec z$
(**Transitivität**)

(O3) Für alle $x,y,z \in K$ gilt
$x \prec y \;\Rightarrow\; x + z \prec y + z$

(O4) Für alle $x,y,z \in K$ gilt
$x \prec y, 0 \prec z \;\Rightarrow\; x.z \prec y.z$

(O3), (O4): **Monotoniegesetze**

Bemerkung

(O1) und (O2) sind äquivalent zur Aussage, dass $\preceq$ eine Totalordnung ist, d.h. sie ist reflexiv, antisymmetrisch, transitiv und konnex. (O3) und (O4) besagen, dass sie mit den Axiomen der Arithmetik (A1)–(A9) verträglich ist.

Beispiele

1. Bezüglich der Relation
$$a \prec b \qquad \Leftrightarrow \qquad a < b$$
ist $\mathbb{R}$ ein geordneter Körper.

2. Es sei p eine Primzahl. Es gibt keine Relation $\prec$ auf $\mathbb{Z}_p$, bezüglich derer $\mathbb{Z}_p$ ein geordneter Körper ist.

   Nehmen wir an, es gibt eine solche Relation. Unten zeigen wir, dass $[0] \prec [1]$ ist. Dann folgt durch Monotonie
$$\underbrace{[0]+[1]}_{=[1]} \prec \underbrace{[1]+[1]}_{=[2]}, \quad \underbrace{[1]+[1]}_{=[2]} \prec \underbrace{[2]+[1]}_{=[3]}, \ \ldots, \quad \underbrace{[p-2]+[1]}_{=[p-1]} \prec \underbrace{[p-1]+[1]}_{=[p]}$$
   und folglich durch Transitivität
$$[1] \prec [p] = [0].$$
   Dies widerspricht aber Trichotomie.

Notationen

1. Falls $0 \prec c$ ist, sagen wir: "c ist positiv".
   Falls $c \prec 0$ ist, sagen wir: "c ist negativ".

2. Manchmal schreiben wir $b \succ a$ statt $a \prec b$.

Lemma

Es seien x,y,z,w Elemente eines Körpers $(K, +, .)$. Dann gilt:

1. $x + z \prec y + z \quad \Rightarrow \quad x \prec y$
2. $x \prec y, z \preceq w \quad \Rightarrow \quad x + z \prec y + w$
3. $x \succ 0, y \succeq 0 \quad \Rightarrow \quad x + y \succ 0$
4. $x \prec y \quad \Rightarrow \quad -y \prec -x$
5. $x \prec y, z \preceq w \quad \Rightarrow \quad x + (-w) \prec y + (-z)$
6. $x \prec y, z \prec 0 \quad \Rightarrow \quad y.z \prec x.z$
7. $0 \prec x \prec y \quad \Rightarrow \quad 0 \prec y^{-1} \prec x^{-1}$

Die Aussagen 1-6 bleiben richtig, wenn wir überall "$\prec$" durch "$\preceq$" ersetzen.

Beweis

In diesem Beweis benutzen wir ohne Weiteres die üblichen (aus den Axiomen der Arithmetik folgenden) Rechenregeln.

1. Es gilt:

$$
\begin{aligned}
& x + z \prec y + z \\
\Rightarrow\ & x + \Big(z + (-z)\Big) \prec y + \Big(z + (-z)\Big) && \text{(O3)} \\
\Rightarrow\ & x \prec y
\end{aligned}
$$

4. Es gilt:

$$\begin{aligned} & x \prec y \\ \Rightarrow\ & x + \Big(-(x+y)\Big) \prec y + \Big(-(x+y)\Big) && \text{(O3)} \\ \Rightarrow\ & -y \prec -x \end{aligned}$$

6. Aus Aussage 4 folgt

$$z \prec 0 \quad \Rightarrow \quad 0 \prec -z$$

Es gilt also:

$$\begin{aligned} & x \prec y \\ \Rightarrow\ & x.(-z) \prec y.(-z) && \text{(O4)} \\ \Rightarrow\ & -x.z \prec -y.z \\ \Rightarrow\ & y.z \prec x.z && \text{(Aussage 4)} \end{aligned}$$

Die anderen Aussagen werden in ähnlicher Weise bewiesen. □

Wir können auch interessantere Aussagen beweisen.

Lemma

1. $x^2 \succ 0$ für alle $x \neq 0$
2. $1 \succ 0$
3. $x.y \succ 0$ für alle $x,y \prec 0$
4. $0 \prec x \prec 1 \quad \Rightarrow \quad x^2 \prec x$
5. $x \succ 1 \quad \Rightarrow \quad x^2 \succ x$

Beweis

1. Weil $x \neq 0$ ist, folgt aus (O1):

$$\begin{array}{lrll} \text{Entweder} & x \succ 0 & \Rightarrow x.x \succ 0.x & \text{(O4} \\ & & \Rightarrow x^2 \succ 0 & \\ \text{oder} & x \prec 0 & \Rightarrow x.x. \succ 0.x & \text{(Aussage 6 des letzten Lemmas)} \\ & & \Rightarrow x^2 \succ 0 & \end{array}$$

2. Da $1^2 = 1$ ist, folgt diese Behauptung aus Aussage 1.

3. Da $x,y \prec 0$ sind, impliziert Aussage 4 des letzten Lemmas $-x, -y \succ 0$. Daher gilt

$$\begin{aligned} & -x \succ 0 \\ \Rightarrow\ & -x.(-y) \succ 0.(-y) && \text{(O4)} \\ \Rightarrow\ & x.y \succ 0 \end{aligned}$$

4. Es gilt:

$$\begin{aligned} x \prec 1 \Rightarrow\ & x.x \prec 1.x && \text{(O4, weil } 0 \prec x) \\ \Rightarrow\ & x^2 \prec x \end{aligned}$$

5. Aus $x \succ 1, 1 \succ 0$ folgt $x \succ 0$ (O2) und daher gilt:

$$\begin{aligned} 1 \prec x \Rightarrow\ & 1.x \prec x.x && \text{(O4)} \\ \Rightarrow\ & x \prec x^2. \end{aligned}$$

□

2.2 Ungleichungen

In diesem Abschnitt diskutieren wir, wie die Lösungsmenge geweisser elementarer Ungleichungen für reelle Zahlen zu bestimmen ist. Wir benutzen hier die Ergebnisse

$$\begin{aligned} x^2 < a^2 \quad & \Leftrightarrow \quad -a < x < a \\ x^2 > a^2 \quad & \Leftrightarrow \quad x < -a \text{ oder } x > a \end{aligned}$$

für $a > 0$, die aus den Ordnungsaxiomen folgen.

Beispiele

1. Für welche reellen Zahlen x gilt die Ungleichung

$$x^2 - 4x + 1 < 3?$$

2. Für welche reellen Zahlen x gilt die Ungleichung

$$\frac{2-x}{3+x} < 4?$$

Lösungen

1. Offensichtlich gilt

$$\begin{aligned}
& x^2 - 4x + 1 < 3 \\
\Leftrightarrow\ & \underbrace{x^2 - 4x - 2}_{} < 0 \\
& \left.\begin{aligned} &= x^2 - 4x + 4 - 4 - 2 \\ &= (x-2)^2 - 6 \end{aligned}\right\} \textbf{quadratische Ergänzung} \\
\Leftrightarrow\ & (x-2)^2 - 6 < 0 \\
\Leftrightarrow\ & (x-2)^2 < 6 \\
\Leftrightarrow\ & -\sqrt{6} < x - 2 < \sqrt{6} \\
\Leftrightarrow\ & 2 - \sqrt{6} < x < 2 + \sqrt{6}
\end{aligned}$$

Daher ist
$$\{x : x^2 - 4x + 1 < 3\} = (2 - \sqrt{6}, 2 + \sqrt{6}).$$

2. Betrachte die Ungleichung
$$\frac{2-x}{3+x} < 4$$

Falls $3 + x > 0$ gilt:
$$\begin{aligned}
& \frac{2-x}{3+x} < 4 \\
\Leftrightarrow\quad & 2 - x < 4(3+x) \\
\Leftrightarrow\quad & 2 - x < 12 + 4x \\
\Leftrightarrow\quad & -10 < 5x \\
\Leftrightarrow\quad & -2 < x
\end{aligned}$$

Falls $3 + x < 0$, gilt:
$$\begin{aligned}
& \frac{2-x}{3+x} < 4 \\
\Leftrightarrow\quad & 2 - x > 4(3+x) \\
\Leftrightarrow\quad & 2 - x > 12 + 4x \\
\Leftrightarrow\quad & -10 > 5x \\
\Leftrightarrow\quad & -2 > x \\
& \quad\ \uparrow \\
& \text{Dies gilt } \textbf{immer} \text{ für } 3 + x < 0
\end{aligned}$$

Daher ist
$$\left\{x : \frac{2-x}{3+x} < 4\right\} = (-\infty, -3) \cup (-2, \infty).$$

Definition

Eine reellwertige Funktion f heißt **monoton steigend**, falls

$$x < y \Rightarrow f(x) \leq f(y)$$

und **streng monoton steigend**, falls

$$x < y \Rightarrow f(x) < f(y).$$

Beispiele

Die Funktionen

$$\begin{array}{ll} f_1(x) = \sqrt{x}, & x \in [0,\infty), \\ f_2(x) = e^x, & x \in \mathbb{R}, \\ f_3(x) = \log x, & x \in (0,\infty) \end{array}$$

sind streng monoton steigend (dies werden wir später beweisen).

Monoton steigende Funktionen können bei der Lösung von Ungleichungen sehr hilfreich sein.

Beispiel

Für welche reellen Zahlen x gilt die Ungleichung

$$\log\left(\frac{1}{2}x^2 + x + 1\right) > 0?$$

Lösung

Zunächst bemerken wir:

$$\begin{array}{ll} \log\left(\tfrac{1}{2}x^2 + x + 1\right) > 0 & \tfrac{1}{2}x^2 + x + 1 > 1 \\ \Rightarrow \underbrace{e^{\log\left(\frac{1}{2}x^2+x+1\right)}}_{=\frac{1}{2}x^2+x+1} > \underbrace{e^0}_{=1} & \Rightarrow \log\left(\tfrac{1}{2}x^2 + x + 1\right) > \underbrace{\log 1}_{=0} \\ (x \mapsto e^x \text{ ist streng} & (x \mapsto \log x \text{ ist} \\ \text{monoton steigend}) & \text{streng monoton steigend}) \end{array}$$

Also gilt:

$$
\begin{aligned}
& \log\left(\tfrac{1}{2}x^2 + x + 1\right) > 0 \\
\Leftrightarrow\ & \tfrac{1}{2}x^2 + x + 1 > 1 \\
\Leftrightarrow\ & \underbrace{x^2 + 2x}_{\substack{= x^2 + 2x + 1 - 1 \\ = (x+1)^2 - 1}} > 0 \quad \text{quadratische Ergänzung} \\
\Leftrightarrow\ & (x+1)^2 - 1 > 0 \\
\Leftrightarrow\ & (x+1)^2 > 1 \\
\Leftrightarrow\ & x + 1 < -1 \quad \text{oder} \quad x + 1 > 1 \\
\Leftrightarrow\ & x < -2 \qquad \text{oder} \quad x > 0
\end{aligned}
$$

Daher ist

$$\left\{x : \log\left(\frac{1}{2}x^2 + x + 1\right) > 0\right\} = (-\infty, -2) \cup (0,\infty).$$

Es gibt eine Reihe nützlicher Ungleichungen, in denen

$$|x| := \begin{cases} x, & x \geq 0 \\ -x, & x < 0 \end{cases}$$

vorkommt. Folgendes Lemma folgt aus der Definition von $|x|$.

Lemma

Für alle $x,y,z,a,b \in \mathbb{R}$ mit $z \neq 0$, $b > 0$ gilt:

(1) $|xy| = |x||y|$

(2) $\left|\dfrac{x}{z}\right| = \dfrac{|x|}{|z|}$

(3) $|x| = \sqrt{x^2}$

(4) $-|x| \leq x \leq |x|$

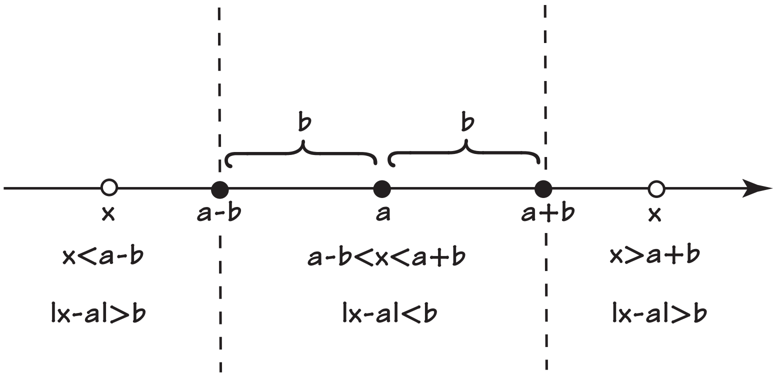
(5) $|x-a| < b \quad \Leftrightarrow \quad a-b < x < a+b$

(6) $|x-a| > b \quad \Leftrightarrow \quad x < a-b$ oder $x > a+b$

Aussagen (5) und (6) bleiben richtig, wenn "$<$" und "$>$" durch "$\leq$" und "$\geq$" ersetzt werden.

Bemerkung

Geometrisch gesehen ist $|x-a|$ die Distanz zwischen den Punkten x und a auf der Zahlengeraden:



● fester Punkt
○ beweglicher Punkt

Lemma (Dreiecksungleichung)

Für alle $x,y \in \mathbb{R}$ gilt
$$|x+y| \leq |x| + |y|.$$

Beweis

Es gilt
$$\begin{aligned} & -|x| \leq x \leq |x| \\ & -|y| \leq y \leq |y| \\ \Rightarrow & -(|x|+|y|) \leq x+y \leq |x|+|y| \\ \Rightarrow & |x+y| \leq |x|+|y| \qquad \text{(Aussage (5) des letzten Lemmas).} \end{aligned}$$

□

Korollar (umgekehrte Dreiecksungleichung)

Für alle $x,y \in \mathbb{R}$ gilt

$$|x+y| \geq \Big||x| - |y|\Big|.$$

Beweis

$$|x| \;=\; |x+y-y| \;\leq\; |x+y| + |-y| \;=\; |x+y| + |y|,$$

so dass

$$|x+y| \geq |x| - |y|. \tag{1}$$

Ebenfalls gilt

$$|y+x| \geq |y| - |x|$$

und daher

$$|x+y| \geq |y| - |x|. \tag{2}$$

Das Ergebnis folgt nun aus (1) und (2). □

Schließlich notieren wir zwei weitere allgemeinnützliche Ungleichungen.

Lemma

Für alle $a,b \in \mathbb{R}$ gilt

$$ab \leq \frac{1}{2}(a^2 + b^2).$$

Beweis

Offensichtlich gilt

$$\begin{aligned} &(a-b)^2 \geq 0 \\ \Rightarrow\; &a^2 - 2ab + b^2 \geq 0 \\ \Rightarrow\; &a^2 + b^2 \geq 2ab \\ \Rightarrow\; &\tfrac{1}{2}(a^2 + b^2) \geq ab. \end{aligned}$$

□

Korollar

Für alle nichtnegativen Zahlen $x,y \in \mathbb{R}$ gilt

$$\underbrace{\sqrt{xy}}_{\substack{\textbf{geometrisches}\\ \textbf{Mittel}\text{ von } x,\, y}} \quad \leq \quad \underbrace{\tfrac{1}{2}(x+y)}_{\substack{\textbf{arithmetrisches}\\ \textbf{Mittel}\text{ von } x,\, y}} \quad .$$

Beweis

Wir benutzen das letzte Lemma mit $a = \sqrt{x}$, $b = \sqrt{y}$. □

2.3 Die natürlichen Zahlen

In diesem Abschnitt definieren wir $\mathbb{N}$ als Teilmenge von $\mathbb{R}$ und leiten ihre Eigenschaften aus den Axiomen der reellen Zahlen her.

Definition

Eine Teilmenge M von $\mathbb{R}$ heißt **induktiv**, falls

- $1 \in M$;
- $x \in M \quad \Rightarrow \quad x+1 \in M$.

Definition (Die Menge der natürlichen Zahlen)

Die Menge $\mathbb{N}$ der natürlichen Zahlen ist die Schnittmenge aller induktiven Teilmengen von $\mathbb{R}$.

Proposition

1. $\mathbb{N}$ ist eine induktive Teilmenge von $\mathbb{R}$.
2. Ist M eine induktive Teilmenge von $\mathbb{R}$ mit $M \subseteq \mathbb{N}$, so ist $M = \mathbb{N}$.

Beweis

1. Da 1 Element in allen induktiven Teilmengen von $\mathbb{R}$ ist und $\mathbb{N}$ die Schnittmenge aller solchen Mengen ist, ist 1 auch Element in $\mathbb{N}$.

   Es sei $n \in \mathbb{N}$. Dann ist n Element in allen induktiven Teilmengen von $\mathbb{R}$. Folglich ist $n+1$ Element in allen induktiven Teilmengen von $\mathbb{R}$, so dass $n+1$ auch Element in $\mathbb{N}$ ist.

2. Es sei M eine induktive Teilmenge von $\mathbb{R}$. Nach der Definition von $\mathbb{N}$ als Schnittmenge aller solchen Mengen ist $\mathbb{N} \subseteq M$. Falls $M \subseteq \mathbb{N}$ ist, gilt also $M = \mathbb{N}$.

$\square$

Als ersten Vorteil dieser Vorgehensweise stellen wir fest, dass das Prinzip der vollständigen Induktion unmittelbar aus der Definition von $\mathbb{N}$ folgt.

Satz (Prinzip der vollständigen Induktion)

$\mathcal{P}(n), n \in \mathbb{N}$ sei eine Aussageform mit folgenden Eigenschaften:

(i) $\mathcal{P}(1)$ ist wahr;

(ii) $\mathcal{P}(k) \Rightarrow \mathcal{P}(k+1)$ für alle $k \in \mathbb{N}$.

Dann ist $\mathcal{P}(n)$ wahr für alle $n \in \mathbb{N}$.

Beweis

Es sei
$$M = \{n \in \mathbb{N} : \mathcal{P}(n) \text{ ist wahr}\}.$$
Aus (i) folgt, dass $1 \in M$ ist, und (2) zeigt, dass aus $n \in M$ auch $n+1 \in M$ folgt. Damit ist M induktiv, und definitionsgemäß ist M Teilmenge von $\mathbb{N}$. Der obigen Proposition zufolge ist also $M = \mathbb{N}$. Dies ist aber genau die Aussage, dass $\mathcal{P}(n)$ für alle $n \in \mathbb{N}$ wahr ist. $\square$

Beispiele

Beweisen Sie folgende Aussagen durch vollständige Induktion:

1. $\sum_{i=1}^{n} i^2 = \frac{1}{6}n(n+1)(2n+1)$ für alle $n \in \mathbb{N}$;
2. $\prod_{i=2}^{n} \left(1 - \frac{1}{i^2}\right) = \frac{n+1}{2n}$ für alle $n \in \mathbb{N}$ mit $n \geq 2$;
3. $2|(n^2+3n)$ für alle $n \in \mathbb{N}$.

Lösungen

1. $\mathcal{P}(n)$ sei die Aussageform

$$\sum_{i=1}^{n} i^2 = \frac{1}{6}n(n+1)(2n+1).$$

<u>Induktionsanfang</u> (Beweis von $\mathcal{P}(1)$)

Es ist

$$\sum_{i=1}^{1} i^2 = 1^2 = 1, \qquad \frac{1}{6}.1.(1+1)(2.1+1) = 1,$$

so dass $\mathcal{P}(1)$ richtig ist.

<u>Induktionsschluss</u>

Wir beweisen, dass die **Induktionsvoraussetzung**

$$\mathcal{P}(k): \quad \sum_{i=1}^{k} i^2 = \frac{1}{6}k(k+1)(2k+1) \tag{1}$$

die **Induktionsbehauptung**

$$\mathcal{P}(k+1): \quad \sum_{i=1}^{k+1} i^2 = \frac{1}{6}(k+1)(k+2)(2(k+1)+1)$$

impliziert.

Aus (1) ergibt sich durch Addition der Zahl $(k+1)^2$:

$$\underbrace{\sum_{i=1}^{k} i^2 + (k+1)^2}_{=\sum_{i=1}^{k+1} k^2} = \underbrace{\tfrac{1}{6}k(k+1)(2k+1) + (k+1)^2}$$

$$\begin{aligned}
&= \tfrac{1}{6}(k+1)[k(2k+1) + 6(k+1)] \\
&= \tfrac{1}{6}(k+1)(2k^2 + 7k + 6) \\
&= \tfrac{1}{6}(k+1)(k+2)(2k+3) \\
&= \tfrac{1}{6}(k+1)(k+2)(2(k+1)+1).
\end{aligned}$$

Damit haben wir $\mathcal{P}(k) \Rightarrow \mathcal{P}(k+1)$ bewiesen.

2. $\mathcal{P}(n)$ sei die Aussageform

$$\prod_{i=2}^{n}\left(1 - \frac{1}{i^2}\right) = \frac{n+1}{2n}.$$

Induktionsanfang (Beweis von $\mathcal{P}(2)$)

Es ist

$$\prod_{i=2}^{2}\left(1 - \frac{1}{i^2}\right) = 1 - \frac{1}{4} = \frac{3}{4}, \qquad \frac{2+1}{2.2} = \frac{3}{4},$$

so dass $\mathcal{P}(2)$ richtig ist.

Induktionsschluss

Wir beweisen, dass die **Induktionsvoraussetzung**

$$\mathcal{P}(k): \quad \prod_{i=2}^{k}\left(1 - \frac{1}{i^2}\right) = \frac{k+1}{2k} \tag{2}$$

die **Induktionsbehauptung**

$$\mathcal{P}(k+1): \quad \prod_{i=2}^{k+1}\left(1 - \frac{1}{i^2}\right) = \frac{(k+1)+1}{2(k+1)}$$

impliziert.

Aus (2) ergibt sich durch Multiplikation mit der Zahl $\left(1-\frac{1}{(k+1)^2}\right)$:

$$\underbrace{\left(1-\frac{1}{(k+1)^2}\right)\prod_{i=2}^{k}\left(1-\frac{1}{i^2}\right)}_{=\prod_{i=2}^{k+1}\left(1-\frac{1}{i^2}\right)} = \underbrace{\left(1-\frac{1}{(k+1)^2}\right)\frac{k+1}{2k}}_{\begin{aligned}&=\frac{k+1}{2k}-\frac{1}{2k(k+1)}\\&=\frac{(k+1)^2-1}{2k(k+1)}\\&=\frac{k(k+2)}{2k(k+1)}\\&=\frac{(k+1)+1}{2(k+1)}.\end{aligned}}$$

Damit haben wir $\mathcal{P}(k) \Rightarrow \mathcal{P}(k+1)$ bewiesen.

3. $\mathcal{P}(n)$ sei die Aussageform

$$2|(n^2+3n)$$

<u>Induktionsanfang</u> (Beweis von $\mathcal{P}(1)$)

Es ist

$$1^2+3.1=4, \qquad 2|4,$$

so dass $\mathcal{P}(1)$ richtig ist.

<u>Induktionsschluss</u>

Wir beweisen, dass die **Induktionsvoraussetzung**

$$\mathcal{P}(k): \quad 2|(k^2+3k)$$

die **Induktionsbehauptung**

$$\mathcal{P}(k+1): \quad 2|\Big((k+1)^2+3(k+1)\Big)$$

impliziert.

Es ist

$$\begin{aligned}(k+1)^2+3(k+1) &= k^2+2k+1+3k+3\\ &= \underbrace{k^2+3k}_{\text{teilbar durch 2}} + \underbrace{2(k+2)}_{\text{teilbar durch 2}}\end{aligned}$$

so dass

$$2\Big|\Big((k+1)^2+3(k+1)\Big).$$

Damit haben wir $\mathcal{P}(k) \Rightarrow \mathcal{P}(k+1)$ bewiesen. □

Die Arithmetik und Ordnung der natürlichen Zahlen

Die Arithmetik der natürlichen Zahlen wird von der Arithmetik der reellen Zahlen geerbt. Insbesondere besagt das folgende Lemma, dass die Addition und Multiplikation der reellen Zahlen Verknüpfungen auf $\mathbb{N}$ definieren.

Lemma

$\mathbb{N}$ ist abgeschlossen bezüglich der Addition und Multiplikation der reellen Zahlen: Sind m, n Elemente in $\mathbb{N}$, so sind $m+n$ und $m.n$ ebenfalls Elemente in $\mathbb{N}$.

Beweis

Dies beweisen wir durch vollständige Induktion. Sei $m \in \mathbb{N}$ und zu $n \in \mathbb{N}$ sei $\mathcal{P}(n)$ die Aussageform

$$m+n \in \mathbb{N}.$$

Induktionsanfang (Beweis von $\mathcal{P}(1)$)

Da $m \in \mathbb{N}$ ist und $\mathbb{N}$ induktiv ist, ist auch $m+1 \in \mathbb{N}$. Damit ist $\mathcal{P}(1)$ richtig.

Induktionsschluss

Wir beweisen, dass die **Induktionsvoraussetzung**

$$\mathcal{P}(k): \quad m+k \in \mathbb{N}$$

die **Induktionsbehauptung**

$$\mathcal{P}(k+1): \quad m+(k+1) \in \mathbb{N}$$

impliziert.

Falls $m+k \in \mathbb{N}$ ist, folgt aus der Induktivität von $\mathbb{N}$, dass $(m+k)+1 \in \mathbb{N}$ ist. Es ist aber $(m+k)+1 = m+(k+1)$ (Assoziativgesetz der Addition (A1)), so dass $m+(k+1) \in \mathbb{N}$ ist.

Damit haben wir $\mathcal{P}(k) \Rightarrow \mathcal{P}(k+1)$ bewiesen.

Die Abgeschlossenheit von $\mathbb{N}$ bezüglich der Multiplikation wird in ähnlicher Weise bewiesen. $\square$

Bemerkung

Axiome (A1), (A2), (A5), (A6), (A7) und (A9) gelten also für $\mathbb{N}$ und definieren die Arithmetik der natürlichen Zahlen.

Die Ordnung der natürlichen Zahlen wird von der Ordnung der reellen Zahlen geerbt.

Lemma

Für jede natürliche Zahl gilt $n \geq 1$.

Beweis

Dies beweisen wir durch vollständige Induktion. Es sei $P(n)$ die Aussage $n > 1$.

<u>Induktionsanfang</u> (Beweis von $\mathcal{P}(1)$)

Die Aussage $1 \geq 1$ ist trivialerwise richtig.

<u>Induktionsschluss</u>

Wir beweisen, dass die **Induktionsvoraussetzung**

$$\mathcal{P}(k): \quad k \geq 1$$

die **Induktionsbehauptung**

$$\mathcal{P}(k+1): \quad k+1 \geq 1$$

impliziert.

Da $1 > 0$ ist, gilt $k+1 > k$ (O3) und aus dieser Aussage, $\mathcal{P}(k)$ und (O2) folgt $k+1 \geq 1$.

Damit haben wir $\mathcal{P}(k) \Rightarrow \mathcal{P}(k+1)$ bewiesen. $\square$

Satz (das Wohlordnungsaxiom der natürlichen Zahlen)

Jede nichtleere Teilmenge M von $\mathbb{N}$ besitzt ein kleinstes Element.

Beweis

Definiere

$$K = \{k \in \mathbb{N} : k \leq m \text{ für alle } m \in M\}.$$

Es gilt nun

- $K \neq \emptyset$ $(1 \in K)$;
- $K \neq \mathbb{N}$ (für alle $m \in M$ ist $m + 1 \notin K$).

Es gibt also $\ell \in K$ mit $\ell + 1 \notin K$. Ansonsten hätten wir nämlich $1 \in K$ und $k \in K \;\Rightarrow\; k + 1 \in K$ und daher wäre $K = \mathbb{N}$ ($\mathbb{N}$ hat keine echte Teilmenge, die induktiv ist).

Da $\ell \in K$ ist, ist $\ell \leq m$ für alle $m \in M$. Falls $\ell \in M$ ist, ist ℓ also ein kleinstes Element von M. Nehmen wir an, $\ell \notin M$. Dann gilt

$$\begin{aligned} & \ell < m && \text{für alle } m \in M \\ \Rightarrow\; & \ell + 1 \leq m && \text{für alle } m \in M \\ \Rightarrow\; & \ell + 1 \in K, \end{aligned}$$

ein Widerspruch. $\square$

Nun benutzen wir das Wohlordnungsaxiom, um das Divisionslemma zu beweisen.

Lemma (Division mit Rest)

Zu jedem $a \in \mathbb{Z}$ und $n \in \mathbb{N}$ gibt es eindeutige Zahlen $q^\star \in \mathbb{Z}$ (den **Quotienten**) und $r^\star \in \{0, \ldots, n-1\}$ (den **Rest**) derart, dass

$$a = q^\star n + r^\star.$$

Beweis

Es sei

$$R = \{r \in \mathbb{N}_0 : a = qn + r \text{ für irgendein } q \in \mathbb{Z}\}.$$

Die Menge R ist nicht leer:

- Ist $a \geq 0$, so gilt $a = 0.n + a$, so dass $a \in R$.
- Ist $a < 0$, so gilt $a = a.n + a(1-n)$, so dass $a(1-n) \in R$.

Die Menge

$$S = \{r + 1 : r \in R\}$$

ist also ein nichtleere Teilmenge von $\mathbb{N}$. Dem Wohlordnungsaxiom der natürichen Zahlen zufolge hat sie ein kleinstes Element $s^\star$, so dass $r^\star := s^\star - 1$ ein kleinstes Element von R ist. Definitionsgemäss gibt es $q^\star \in \mathbb{Z}$ mit

$$a = q^\star n + r^\star.$$

- Nun zeigen wir, dass $r^\star \leq n - 1$. Aus $r^\star \geq n$, also $0 \leq r^\star - n < r^\star$, und

  $$a = n(q^\star + 1) + (r^\star - n)$$

  folgt nämich $r^\star - n \in R$, und dies widerspricht der Tatsache, dass $r^\star$ ein kleinstes Element von R ist.

- Schließlich zeigen wir, dass $q^\star$, $r^\star$ eindeutig sind. Es seien q_1, $q_2 \in \mathbb{Z}$ und r_1, $r_2 \in \{0,\ldots,n-1\}$ mit

  $$a = nq_1 + r_1, \qquad a = nq_2 + r_2. \tag{$\star$}$$

  Ist $q_1 > q_2$, so gilt

  $$r_2 = a - nq_2 = \underbrace{a - nq_1}_{= r_1} + n\underbrace{(q_1 - q_2)}_{\geq 1} \geq r_1 + n \geq n,$$

  und dies widerspricht $r_2 < n$. Analog führt die Annahme $q_2 > q_1$ zum Widerspruch $r_1 \geq n$. Folglich ist $q_1 = q_2$ und aus $(\star)$ folgt dann $r_1 = r_2$. □

Das Divisionslemma hat wiederum eine wichtige Andwendung in der Berechnung vom größten gemeinsamen Teiler zweier Zahlen.

Definition

Es seien a und b natürlich Zahlen. Die natürliche Zahl d ist ein **größter gemeinsamer Teiler** von a und b, falls sie die folgenden Eigenschaften hat:

(i) $d|a$ und $d|b$.

(ii) Hat eine weitere natürliche Zahl c die Eigenschaft $c|a$ und $c|b$, so gilt $c|d$.

Bemerkung

Der größte gemeinsame Teiler von a und b ist eindeutig. Sind d_1 und d_2 größte gemeinsame Teiler von a und b so gilt nach (ii) $d_1|d_2$ und $d_2|d_1$, so dass $d_1 = d_2$ ist.

Wir bezeichnen den größten gemeinsamen Teiler von a und b mit (a,b).

Proposition

Es seien a und b natürliche Zahlen mit $a \geq b$ und $q \in \mathbb{N}_0$ und $r \in \{1,\dots,b-1\}$ mit

$$a = bq + r.$$

Dann gilt

$$(a,b) = (b,r).$$

(Ist $r = 0$, so ist offensichtlich $(a,b) = b$.)

Beweis

Wir zeigen, dass $d := (b,r)$ die beiden Eigenschaften von (a,b) besitzt.

- Offensichtlich gilt $d|b$ und und $d|r$, so dass $d|\underbrace{(qb+r)}_{=a}$ und $d|b$.
- Es sei $c \in \mathbb{N}$ mit $c|a$ und $c|b$. Dann gilt $c|b$ und $c|\underbrace{(a-bq)}_{=r}$, so dass $c|d$ (denn $d = (b,r)$). □

Beispiel

Berechnen Sie $(2406,654)$.

Lösung

Wir wenden die obige Proposition iterativ. Es gilt:

$$\begin{aligned}
2406 &= 654.3 + 444 & (2406,654) &= (654,444)\\
654 &= 444.1 + 210 & &= (444,210)\\
444 &= 210.2 + 24 & &= (210,24)\\
210 &= 24.8 + 18 & &= (24,18)\\
24 &= 18.1 + 6 & &= (18,6)\\
18 &= 6.3 & &= 6
\end{aligned}$$

Bemerkung

Dies ist der **Euklidscher Algorithmus** für die Berechnung von (a,b), die wir tabellarisch zusammenfassen können:

$$\begin{array}{rll}
a = bq_1 + r_1, & (0 \leq r_1 < b) & (a,b) = (b,r_1)\\
b = r_1q_2 + r_2, & (0 \leq r_2 < r_1) & (b,r_1) = (r_1,r_2)\\
r_1 = r_2q_3 + r_3, & (0 \leq r_3 < r_2) & (r_1,r_2) = (r_2,r_3)\\
\vdots & \vdots & \vdots\\
r_{k-3} = r_{k-2}q_{k-1} + r_{k-1}, & (0 \leq r_{k-1} < r_{k-2}) & (r_{k-3},r_{k-2}) = (r_{k-2},r_{k-1})\\
r_{k-2} = r_{k-1}q_k + \underbrace{r_k}_{=0} & & (r_{k-2},r_{k-1}) = r_{k-1}
\end{array}$$

Der Algorithmus terminiert nach höchstens b Schritten, denn die Reste strikt kleiner werden und alle kleiner gleich b sind.

Proposition

Es seien a und b natürliche Zahlen und $d = (a,b)$. Dann gibt es ganze Zahlen u, v mit

$$d = ua + vb.$$

Beweis

Wir können u und v mit Hilfe des **erweiterten Euklidschen Algorithmus** berechnen:

- Es seien $u_0 = 1$, $u_1 = 0$ und $v_0 = 0$, $v_1 = 1$.
- Für $i = 1,\dots,k$ seien
$$u_{i+1} = u_{i-1} - q_i u_1, \qquad v_{i+1} = v_{i-1} - q_i v_i.$$

Durch vollständige Induktion können wir leicht
$$r_{i-1} = u_i a + v_i b, \qquad i = 2,\dots,k,$$
zeigen, und insbesondere gilt
$$d = u_k a + v_k b.$$
□

Bemerkung

Die Zahlen u und v heißen **Bézoutkoeffizienten**.

Beispiel

Es seien $u_0 = 1$, $u_1 = 0$ und $v_0 = 0$, $v_1 = 1$ und
$$\begin{aligned}
2406 &= 654.3 + 444, & u_2 &= u_0 - 3u_1 = 1, & v_2 &= v_0 - 3v_1 = -3,\\
654 &= 444.1 + 210, & u_3 &= u_1 - u_2 = -1, & v_3 &= v_1 - v_2 = 4,\\
444 &= 210.2 + 24, & u_4 &= u_2 - 2u_3 = 3, & v_4 &= v_2 - 2v_3 = -11,\\
210 &= 24.8 + 18, & u_5 &= u_3 - 8u_4 = -25, & v_5 &= v_3 - 8v_4 = 92,\\
24 &= 18.1 + 6, & u_6 &= u_4 - u_5 = 28, & v_6 &= v_4 - v_5 = -103,\\
18 &= 6.3
\end{aligned}$$

Folglich ist
$$6 = 28.2406 - 103.654$$

Bemerkung

Es sei p eine Primzahl und $b \in \{1,\dots,p-1\}$. Da $(p,b) = 1$ ist, gibt es Bézoutkoeffizienten u, v derart, dass
$$up + vb = 1.$$
Foglich gilt
$$[v][b] = [1]$$
in $\mathbb{Z}_p$, d.h. $[v]$ ist das multiplikative inverse Element zu $[b]$.

Beispiel

Finden Sie $[6533]^{-1}$ in $\mathbb{Z}_{7039}$.

Lösung

Es gilt

$$581.7039 - 626.6533 = 1$$

und folglich ist

$$[6533]^{-1} = [-626] = [6413]$$

in $\mathbb{Z}_{7039}$.

Proposition (chinesischer Restsatz)

Es seien m, n natürliche Zahlen mit $m,n \geq 2$ und $(m,n) = 1$ und a, $b \in \mathbb{Z}$. Dann haben die Gleichungen

$$\begin{aligned} &x \equiv a \ (\mathrm{mod}\ n), \\ &x \equiv b \ (\mathrm{mod}\ m) \end{aligned}$$

eine Lösung, und diese Lösung ist eindeutig bis auf ganzzahlige Vielfache von nm.

Beweis

- Da $(m,n) = 1$ ist, gibt es Bézoutkoeffizienten u, v derart, dass

  $$un + vm = 1.$$

  Somit ist

  $$x = avm + bun$$

  eine Lösung der angegebenen Gleichungen, denn

  $$\begin{aligned} x = a + (-a+b)un \quad &\Rightarrow \quad x \equiv a \ (\mathrm{mod}\ n), \\ x = b + (a-b)vm \quad &\Rightarrow \quad x \equiv b \ (\mathrm{mod}\ m). \end{aligned}$$

- Ist x eine Lösung, so ist offensichtlich $x + pnm$ ebenfalls eine Lösung für alle $p \in \mathbb{Z}$.

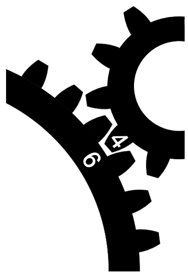
- Sind x_1 und x_2 Lösungen, so gilt

$$x_1 \equiv x_2 \pmod{n}, \quad x_1 \equiv x_2 \pmod{m},$$

d.h. $n|(x_1 - x_2)$ und $m|(x_1 - x_2)$. Daraus folgt $nm|(x_1 - x_2)$, denn n und m teilerfremd sind. $\square$

Beispiel

Zwei Zahnräder mit 13 bzw. 17 Zähnen greifen ineinander. Zähne und Lücken sind von 1 bis 13 bzw. von 1 bis 17 jeweils im Drehsinn nummeriert. Zu Beginn treffen Zahn und Lücke mit der Nummer 1 aufeinander. Nach wie vielen Schritten befindet sich der Zahn der Nummer 4 vom kleinen Rad in der Lücke mit der Nummer 6 vom größeren Rad?



Lösung

Es sei x die Anzahl der Schritte, so dass

$$x \equiv 4 \pmod{13},$$
$$x \equiv 6 \pmod{17}$$

Es ist $(13,17) = 1$, denn 13 und 17 sind Primzahlen, und

$$4.13 - 3.17 = 1,$$

so dass

$$x = -4.3.17 + 6.4.13 = 108$$

die obigen Gleichungen löst. Diese Gleichungen sind äquivalent zu

$$x \equiv 108 \pmod{221},$$

so dass sich die Zahnräder nach 108-1, 329-1, 550-1, ... Schritten in den abgebildeten Poisitionen befinden.

Die ganzen und rationalen Zahlen

Definition

Die Menge $\mathbb{Z}$ der ganzen Zahlen ist die durch die Formel

$$\mathbb{Z} = \{n : n \in \mathbb{N}\} \cup \{0\} \cup \{-n : n \in \mathbb{N}\}$$

definierte Teilmenge von $\mathbb{R}$.

Bemerkung

Man zeigt leicht, dass

- $\mathbb{Z}$ abgeschlossen bezüglich der Addition und Multiplikation der reellen Zahlen ist;
- alle Körperaxiome mit Ausnahme der Existenz multiplikativer Inverser (A8) gelten.

Definition

M sei eine mit zwei Verknüpfungen $+,.$ versehene Menge, wobei $+,.$ die Axiome (A1)-(A7) und (A9) erfüllen. In diesem Fall heißt M **kommutativer Ring (mit Identität)**.

Da die Ordnung der reellen Zahlen geerbt wird, handelt es sich bei $\mathbb{Z}$ um einen **geordneten Ring.**

Definition

Die Menge $\mathbb{Q}$ der rationalen Zahlen ist die durch die Formel

$$\mathbb{Q} = \left\{ \frac{m}{n} : m \in \mathbb{Z}, n \in \mathbb{Z} \setminus \{0\} \right\}$$

definierte Teilmenge von $\mathbb{R}$.

Proposition

M sei mit $+, .$ ein Körper und N sei Teilmenge von M. Es gelte

1. N ist abgeschlossen bezüglich $+$ und $.$;
2. Es sind $0 \in N$ und $1 \in N$;
3. N ist abgeschlossen bezüglich der Inversen:

$$a \in N \;\Rightarrow\; -a \in N, \qquad a \in N \setminus \{0\} \;\Rightarrow\; a^{-1} \in N.$$

Dann ist N mit $+, .$ ein Körper.

Satz

$\mathbb{Q}$ bildet mit der Addition und Multiplikation der reellen Zahlen einen Körper.

Beweis

Wir beachten $\mathbb{Q}$ als Teilmenge von $\mathbb{R}$ und prüfen, ob die in der obigen Proposition genannten Kriterien erfüllt sind.

1. $\mathbb{Q}$ ist abgeschlossen bezüglich der Addition und Multiplikation der reellen Zahlen, denn mit $a, c \in \mathbb{Z}$ und $b, d \in \mathbb{Z} \setminus \{0\}$ ist

$$\frac{a}{b} + \frac{c}{d} = \frac{a.d + b.c}{b.d} \in \mathbb{Q},$$
$$\frac{a}{b} . \frac{c}{d} = \frac{a.c}{b.d} \in \mathbb{Q}.$$

2. Für jedes $n \in \mathbb{Z} \setminus \{0\}$ ist

$$0 = \frac{0}{n}, \qquad 1 = \frac{n}{n},$$

so dass $0, 1$ Elemente in $\mathbb{Q}$ sind.

3. Für $m \in \mathbb{Z}$, $n \in \mathbb{Z} \setminus \{0\}$ ist

$$-\left(\frac{m}{n}\right) = \frac{(-m)}{n} \in \mathbb{Q}$$

und für $m, n \in \mathbb{Z} \setminus \{0\}$ ist

$$\left(\frac{m}{n}\right)^{-1} = \frac{n}{m} \in \mathbb{Q}.$$

$\mathbb{Q}$ ist also abgeschlossen bezüglich der Inversen.

$\square$

Da die Ordnung der reellen Zahlen geerbt wird, ist $\mathbb{Q}$ also ein geordneter Körper.

2.4 Abzählbarkeit

Definition

Eine nichtleere Menge M heißt **endlich**, falls es eine natürliche Zahl n und eine bijektive Funktion $f : \mathbb{N}_n \to M$ gibt, wobei

$$\mathbb{N}_n = \{m \in \mathbb{N} : m \leq n\}$$

ist. In diesem Fall hat M n Elemente.

Bemerkung

Eine endliche Menge M kann nicht gleichzeitig n_1 und n_2 Elemente mit $n_1 \neq n_2$ haben. In diesem Fall gäbe es Bijektionen $f_1 : \mathbb{N}_{n_1} \to M$ und $f_2 : \mathbb{N}_{n_2} \to M$, so dass $g := f_1^{-1} \circ f_2 : \mathbb{N}_{n_2} \to \mathbb{N}_{n_1}$ und $g^{-1} : \mathbb{N}_{n_1} \to \mathbb{N}_{n_2}$ Bijektionen wären. Die Existenz solcher Funktionen schließt aber das folgende Lemma aus.

Lemma (Schubfachprinzip)

Es seien m und n natürliche Zahlen mit $m < n$. Dann gibt es keine Injektion $\mathbb{N}_n \to \mathbb{N}_m$.

Beweis

Es sei

$$S = \{n \in \mathbb{N}\text{: Es existieren eine natürliche Zahl } m < n \text{ und eine Injektion } f : \mathbb{N}_n \to \mathbb{N}_m\}.$$

Falls $S \neq \emptyset$ ist, hat S dem Wohlordnungsaxiom zufolge ein kleinstes Element k. Es existieren also eine natürliche Zahl $\ell < k$ und eine Injektion $g : \mathbb{N}_k \to \mathbb{N}_\ell$.

Es ist $\ell \neq 1$, denn keine Funktion $\mathbb{N}_k \to \mathbb{N}_1 = \{1\}$ ist eine Injektion für $k > 1$. Damit ist $\ell > 1$, so dass $\ell = q + 1$ und daher $k = p + 1$ für igendwelche natürlichen Zahlen p, q sind.

Bemerke:

$$\mathbb{N}_k = \mathbb{N}_p \cup \{p+1\}, \qquad \mathbb{N}_\ell = \mathbb{N}_q \cup \{q+1\}.$$

- Falls $q + 1$ nicht in $g[\mathbb{N}_p]$ ist, ist die durch die Formel
$$h(x) = g(x), \qquad x \in \mathbb{N}_p$$
definierte Funktion $h : \mathbb{N}_p \to \mathbb{N}_q$ injektiv.

- Falls $q + 1$ in $g[\mathbb{N}_p]$ ist, existiert $x_1 \in \mathbb{N}_p$ mit $g(x_1) = q + 1$. Folglich ist $g(p+1) \neq q + 1$. Damit ist die durch die Formel
$$h(x) = \begin{cases} g(x), & x \neq x_1, \\ g(p+1), & x = x_1 \end{cases}$$
definierte Funktion $h : \mathbb{N}_p \to \mathbb{N}_q$ injektiv.

In beiden Fällen haben wir eine Injektion $h : \mathbb{N}_p \to \mathbb{N}_q$ mit $q < p$ und $p < k$ konstruiert. Dies widerspricht aber der Definition von k. □

Bemerkung

Das Schubfachprinzip wird oft folgendermaßen formuliert:

> Falls man n Objekte in $m < n$ Schubfächer einteilen möchte, gibt es mindestens ein Schubfach, in dem mehr als ein Objekt landet.

Mit anderen Worten existiert keine Injektion $f : M \to S$, wobei M die Menge der Objekte und S die Menge der Schubfächer ist. Definitionsgemäß existieren Bijektionen $f_1 : \mathbb{N}_n \to M$ und $f_2 : \mathbb{N}_m \to S$. Die Existenz einer Injektion $f : M \to S$ impliziert, dass $f_2^{-1} \circ f \circ f_1 : \mathbb{N}_n \to \mathbb{N}_m$ injektiv ist. Dies widerspricht dem obigen Lemma.

Definitionen

1. Die leere Menge betrachten wir als endlich mit 0 Elemente.

2. Eine nichtleere Menge M ist **unendlich**, falls sie nicht endlich ist.

Lemma

$\mathbb{N}$ ist unendlich.

Beweis

Nehmen wir an $\mathbb{N}$ ist endlich. Dann gibt es eine natürliche Zahl n und eine Bijektion $f : \mathbb{N}_n \to \mathbb{N}$. Damit ist

$$\mathbb{N} = \{a_1, \dots, a_n\},$$

wobei $a_i = f(i)$, $i = 1, \dots, n$ ist.

Betrachte nun die Zahl

$$a = a_1 + \dots + a_n + 1.$$

Sie ist eine natürliche Zahl, denn $\mathbb{N}$ ist unter Addition und Addition von 1 abgeschlossen. Außerdem gilt $a > a_i$ und daher $a \neq a_i$, $i = 1, \dots, n$. Folglich ist a nicht Element der Menge $\{a_1, \dots, a_n\}$. Dies ist ein Widerspruch. $\square$

Bemerkung

Mit demselben Beweis zeigt man, dass die Mengen $\mathbb{Z}$, $\mathbb{Q}$ und $\mathbb{R}$ ebenfalls unendlich sind.

Lemma

Eine nichtleere Menge M ist unendlich, falls es eine Injektion $f : \mathbb{N} \to M$ gibt.

Beweis

Nehmen wir an, M ist endlich. Dann gibt es eine natürliche Zahl n und eine Bijektion $f_n : \mathbb{N}_n \to M$. Es sei $i : \mathbb{N}_{n+1} \to \mathbb{N}$ die **Inklusion**

$$i(x) = x, \qquad x = 1, \dots, n+1.$$

Damit ist $h := f_n^{-1} \circ f \circ i : \mathbb{N}_{n+1} \to \mathbb{N}_n$ eine Injektion. Dies widerspricht aber dem Schubfachprinzip. $\square$

Definitionen

1. Eine nichtleere Menge M heißt **abzählbar unendlich**, falls es eine bijektive Funktion $f : \mathbb{N} \to M$ gibt.

2. Eine endliche oder abzählbar unendliche Menge heißt **abzählbar**.

3. Eine nicht abzählbare Menge heißt **überabzählbar**.

Beispiele

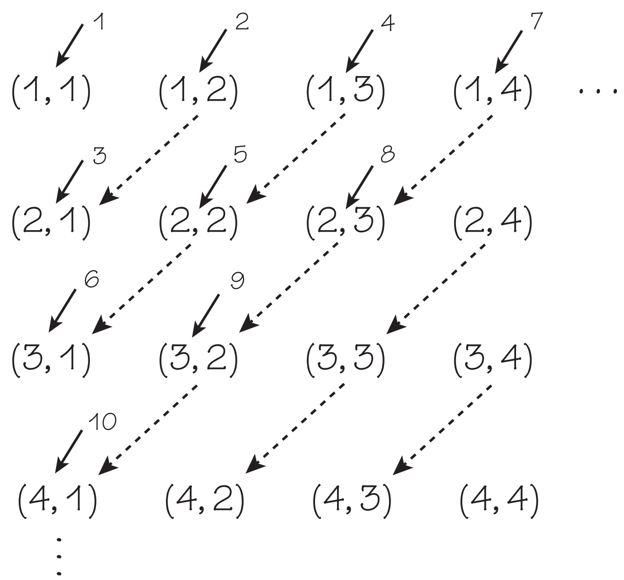
1. Die Menge $\mathbb{Z}$ ist abzählbar unendlich. So zählt man ihre Elemente ab:

$$\begin{array}{lcccccccc} \text{Zielmenge } (\mathbb{Z}) & 0 & 1 & -1 & 2 & -2 & 3 & -3 & \cdots \\ & \uparrow & \uparrow & \uparrow & \uparrow & \uparrow & \uparrow & \uparrow & \\ \text{Urmenge } (\mathbb{N}) & 1 & 2 & 3 & 4 & 5 & 6 & 7 & \cdots \end{array}$$

2. Die Produktmenge

$$\mathbb{N} \times \mathbb{N} = \{(n_1,n_2) : n_1,n_2 \in \mathbb{N}\}$$

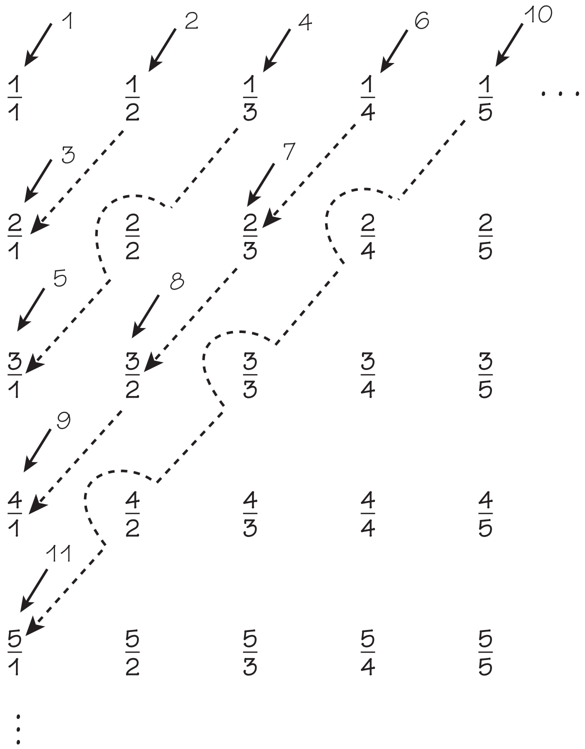
ist abzählbar unendlich. So zählt man ihre Elemente ab:



Zeichenerklärung

durchgezogene Pfeile: $\mathbb{N} \to \mathbb{N} \times \mathbb{N}$
gestrichelte Pfeile: Abzählungsrichtung

3. Die Menge aller positiven rationalen Zahlen ist abzählbar unendlich. So zählt man ihre Elemente ab:



Zeichenerklärung

durchgezogene Pfeile: $\mathbb{N} \to \mathbb{Q}$
gestrichelte Pfeile: Abzählungsrichtung

4. Die Menge $\mathbb{R}$ ist nicht abzählbar. Sie ist unendlich, da die Inklusion $\mathbb{N} \to \mathbb{R}$ offensichtlich injektiv ist. Dass sie nicht abzählbar unendlich ist, beweisen wir durch Widerspruch.

Nehmen wir an, $\mathbb{R}$ ist abzählbar unendlich. Es existiert also eine bijektive Funktion $f : \mathbb{N} \to \mathbb{R}$. Wir bezeichnen $f(n)$ mit $N_n{,}d_n^1 d_n^2 d_n^3 \ldots$, wobei N_n eine ganze Zahl ist und $d_n^1, d_n^2, d_n^3, \ldots \in \{0,1,\ldots,9\}$ sind:

$$
\begin{array}{ccc}
\text{Urmenge } (\mathbb{N}) & & \text{Zielmenge } (\mathbb{R}) \\
1 & \to & N_1{,}d_1^1 d_1^2 d_1^3 \ldots \\
2 & \to & N_2{,}d_2^1 d_2^2 d_2^3 \ldots \\
3 & \to & N_3{,}d_3^1 d_3^2 d_3^3 \ldots \\
\vdots & & \vdots
\end{array}
$$

(Hier benutzen wir die Dezimalschreibweise für reelle Zahlen, die Nichteindeutigkeiten wie $0{,}999\ldots = 1{,}000\ldots$ enthält.)

D_j sei eine ganze Zahl zwischen 1 und 8 mit $D_j \neq d_j^j$. Betrachte nun die reelle Zahl

$$0{,}D_1 D_2 D_3 \ldots$$

- Diese Zahl ist nicht gleich $f(1)$, da $D_1 \neq d_1^1$ ist.
- Sie ist ebenfalls nicht gleich $f(2)$, da $D_2 \neq d_2^2$ ist.
- Sie ist tatsächlich nicht gleich $f(j)$ für alle $j \in \mathbb{N}$, da $D_j \neq d_j^j$ ist.

Sie ist also nicht Element der Bildmenge von f: Dies widerspricht der Annahme, dass f surjektiv ist.

5. Die Potenzmenge

$$P(\mathbb{N}) = \{\emptyset, \{1\}, \{1,2\}, \{2\}, \{1,2,3\}, \ldots\}$$

von $\mathbb{N}$ (die Menge aller Teilmengen von $\mathbb{N}$) ist nicht abzählbar. Sie ist unendlich, da die durch die Formel

$$f(n) = \{n\}$$

definierte Funktion $f : \mathbb{N} \to P(\mathbb{N})$ injektiv ist. Dass sie nicht abzählbar unendlich ist, folgt aus dem folgenden Lemma.

Lemma

M sei eine nichtleere Menge. Es existiert keine surjektive Funktion $f : M \to P(M)$.

Beweis

$f : M \to P(M)$ sei eine surjektive Funktion. Wir betrachten die Teilmenge

$$A = \{m \in M : m \notin f(m)\}$$

von M und zeigen durch Widerspruch, dass A nicht in der Bildmenge von f liegt.

Nehmen wir an, es existiert $n \in M$ mit $f(n) = A$. Dann gilt:

- $n \in A \Rightarrow n \notin f(n) \Rightarrow n \notin A$
- $n \notin A \Rightarrow n \in f(n) \Rightarrow n \in A$.

Damit haben wir einen Widerspruch. □

2.5 Primzahlen und das RSA-Verfahren

Wir beginnen mit einem hilfreichen Korollar des erweiterten Euklidischen Algorithmus.

Proposition

Es seien a und b natürliche Zahlen und p eine Primzahl mit der Eigenschaft $p|ab$. Dann gilt $p|a$ oder $p|b$.

Beweis

Wir nehmen an, $p \nmid a$, so dass $(p,a) = 1$. Dann gibt es Bézoutkoeffizienten u und v mit

$$1 = pu + av$$

und folglich gilt

$$b = \underbrace{bpu + abv}_{\text{teilbar durch } p}.$$

□

Bemerkung

Dieses Ergebnis gilt nicht, wenn p keine Primzahl ist. Es gilt bspw. $4|2.6$ aber $4 \nmid 2$ und $4 \nmid 6$.

Korollar

Ist eine Primzahl Teiler eines Produkts $a_1 \cdots a_m$ natürlicher Zahlen, so teilt sie einen der Faktoren.

Korollar

Ist $(a,n) = 1$ und $(b,n) = 1$, so ist $(ab,n) = 1$.

Beweis

Haben ab und n einen gemeinsamen Teiler, so haben sie einen gemeinsamen Primteiler p. Aus $p|ab$ folgt aber $p|a$ oder $p|b$. $\square$

Definition

Eine **zusammengesetzte Zahl** ist eine natürliche Zahl, die größer als 1 ist und keine Primzahl ist.

Bemerkung

Der Ausdruck “zusammengesetzte Zahl” beschreibt die Tatsache, dass jede natürliche Zahl $n > 1$, die keine Primzahl ist, zerlegt werden kann, bis alle ihrer Faktoren Primzahlen sind. z. B.:

$$\begin{aligned} 360 &= 3.120 \\ &= 3.30.4 \\ &= 3.3.10.2.2. \\ &= \underbrace{2.2.2.3.3.5}_{\substack{\textbf{Primfaktorenzerlegung} \\ \text{von } 360}} \end{aligned}$$

Satz (Fundamentalsatz der elementaren Zahlentheorie)

Jede natürliche Zahl $n > 1$ besitzt eine eindeutige Primfaktorenzerlegung.

Beweis

- Nehmen wir an, es existiert eine natürliche Zahl $n > 1$ ohne Primfaktorenzerlegung. Dem Wohlordnungsaxiom von $\mathbb{N}$ zufolge gibt es eine kleinste solche natürliche Zahl N.

  Insbesondere ist N keine Primzahl. Es existieren also natürliche Zahlen $a,b > 1$ mit der Eigenschaft, dass
  $$N = ab.$$
  Da $a,b < N$, haben a und b Primfaktorenzerlegungen, so dass $N = ab$ ebenfalls eine Primfaktorenzerlegung hat. Damit haben wir einen Widerspruch.

- Nehmen wir an, es existiert eine natürliche Zahl $n > 1$ mit zwei Primfaktorenzerlegungen. Dem Wohlordnungsaxiom von $\mathbb{N}$ zufolge gibt es eine kleinste solche natürliche Zahl N.

  Insbesondere haben die beiden Primfaktorenzerlegungen von N keinen gemeinsamen Primfaktor p (sonst wäre N/p eine kleinere natürliche Zahl mit zwei Primfaktorenzerlegungen). Es gibt also Primzahlen p und q und natürliche Zahlen a und b derart, dass
  $$N = pa = qb$$
  aber $q \nmid a$ und $p \nmid b$. Dann gilt aber $q|pa$ aber $q \nmid p$ und $q \nmid a$ sowie $p|qb$ aber $p \nmid q$ und $q \nmid b$. Dies ist ein Widerspruch. □

Definition

Für eine natürliche Zahl $n \geq 2$ sei $\phi(n)$ die Anzahl der Elemente a aus $\{1,\ldots,n\}$, die teilerfremd zu n sind, d.h. $(a,n) = 1$ erfüllen. Man nennt $\phi : \{2,3,\ldots\} \to \mathbb{N}$ die **Euler-Funktion**.

Beispiel

$\phi(6) = 2$, da 1, 5 keinen gemeinsamen Teiler mit 6 haben.

Proposition (Eigenschaften der Eulerschen-Funktion)

1. Ist p eine Primzahl und $k \geq 1$, so gilt $\phi(p^k) = p^k(1 - \frac{1}{p})$.

2. Sind p, q Primzahlen, so gilt $\phi(pq) = (p-1)(q-1)$.

Beweis

1. Unter den Zahlen $1, 2, \ldots, p^k$ sind lediglich die Zahlen $p, 2p, 3p, \ldots, p^{k-1}p$ nicht teilerfremd zu p^k. Somit ist
$$\phi(p^k) = p^k - p^{k-1} = p^k(1 - \tfrac{1}{p}).$$

2. Unter den Zahlen $1, 2, \ldots, pq$ sind lediglich die Zahlen $p, 2p, 3p, \ldots, qp$ sowie $q, 2q, 3q, \ldots, pq$ nicht teilerfremd zu pq (wobei wir die Zahl pq zweimal gezählt haben). Somit ist
$$\phi(pq) = pq - p - q + 1 = (p-1)(q-1). \qquad \square$$

Lemma (Satz von Euler)

Es sei $n \geq 2$ und $a \in \mathbb{N}$ mit $(a,n) = 1$. Dann ist
$$a^{\phi(n)} \equiv 1 \pmod{n}.$$

Beweis

Betrachte die Menge $S_1 = \{m_1, m_2, \ldots, m_{\phi(n)}\}$ der Zahlen aus $\{1, \ldots, n\}$, die teilerfremd zu n sind. Die Elemente der Menge $S_2 = \{am_1, am_2, \ldots, am_{\phi(n)}\}$ sind auch teilerfremd zu n. Rechnen wir modulo n, so sind S_1 und S_2 also gleich. Somit ist
$$m_1 m_2 \cdots m_{\phi(n)} \equiv a^{\phi(n)} m_1 m_2 \cdots m_{\phi(n)} \pmod{n}.$$
Da m_j und n teilerfremd sind, gibt es M_j mit
$$M_j m_j \equiv 1 \pmod{n},$$
so dass wir $m_1, \ldots, m_{\phi(n)}$ in der lezten Gleichung mit Hilfe von $M_1, \ldots, M_{\phi(n)}$ kürzen können. Dies liefert
$$1 \equiv a^{\phi(n)} \pmod{n}. \qquad \square$$

Korollar (kleiner Satz von Fermat)

Es sei p eine Primzahl und $a \in \mathbb{N}$ mit $(a,p) = 1$. Dann ist

$$a^{p-1} \equiv 1 \pmod{p}.$$

Beweis

Dies folgt aus dem Satz von Euler, denn $\phi(p) = p - 1$. □

Das RSA-Verfahren

Wie kann Alice geheime Informationen an Bob verschicken, ohne das Eve belauschen kann?

Bob bereitet seine **public key** und **private key** vor:

- Er wählt sehr große zwei Primzahlen p und q (mit mindestens 100 Dezimalstellen) und berechnet

$$n = pq, \qquad \phi(n) = (p-1)(q-1).$$

- Er wählt eine Zahl d mit $(d,\phi(n)) = 1$ und berechnet eine Zahl e mit

$$de \equiv 1 \pmod{\phi(n)}$$

  (mit Hilfe des erweiterten Euklidischen Algorithmus).

- Die Zahlen n und d werden veröffentlicht. Sie sind sein **public key**.

- Die Zahlen p, q und e bleiben geheim. Sie sind sein **private key**.

Nun kann Alice jede Zahl $x < n$ verschlüsselt an Bob verschicken.

- Sie berechnet
$$c \equiv x^d (\text{mod n})$$
und schickt diese Zahl an Bob.

Und Bob kann Alices Nachricht enschlüsseln:

- Er berechnet
$$y \equiv c^e (\text{mod n}).$$
(Unten zeigen wir, dass $x \equiv y \pmod{n}$ ist.

Eve braucht e, um Alices Nachricht zu entschlüssen. Dafür braucht sie $\phi(n)$ und folglich auch p und q. Dies kann sie theoretisch aus n berechnen. Es ist aber rechnerisch extrem schwierig, eine große Zahl in Primfaktoren zu zerlegen. Modulares Rechnen ist dagegen rechnerisch recht einfach, so dass Bob und Alice ihre Rechnungen fast mühelos durchführen können.

Lemma

Es gilt
$$x \equiv y \pmod{n}.$$

Beweis

Zunächst bemerken wir, dass
$$y \equiv c^e \equiv x^{de} \pmod{n}$$
ist. Ferner gilt $\phi(n)|(de-1)$, so dass
$$de - 1 = \ell\phi(n)$$
für irgendein $\ell \in \mathbb{Z}$ und folglich ist
$$y \equiv x^{\ell\phi(n)+1} \equiv (x^{\phi(n)})^\ell x \pmod{n}.$$
Diese Gleichung gilt auch mod p und mod q, denn p und q sind Teiler von n.

Nun unterscheiden wir zwei Fälle.

- Sind x und n teilerfremd, so gilt dem Satz von Euler zufolge
$$x^{\phi(n)} \equiv 1 \pmod{n}$$
und folglich
$$y \equiv x \pmod{n}.$$

- Es gilt $p|x$ oder $q|x$. Es sei $p|x$, so dass q und x teilerfremd sind (der andere Fall wird in ähnlicher Weise behandelt). Es gilt
$$x^{\phi(n)} \equiv x^{(p-1)(q-1)} \equiv (x^{q-1})^{p-1} \equiv 1 \pmod{q}$$
(wegen des kleinen Satzes von Fermat) und folglich
$$y \equiv x \pmod{q},$$
d.h.
$$q|(y-x). \tag{1}$$
Auf der anderen Seite gilt $p|x$, so dass
$$p|(y-x) \tag{2}$$
(denn $y = x^{de}$).

Da p und q teilerfremd sind, folgt aus (1), (2)
$$\underbrace{pq}_{=n}|(y-x),$$
d.h.
$$y \equiv x \pmod{n}.$$ □

2.6 Schranken, Maxima, Minima, Suprema und Infima

Definition

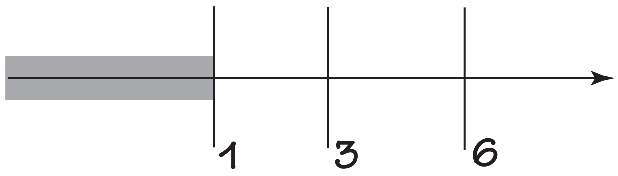
S sei eine nichtleere Teilmenge von $\mathbb{R}$.

S heißt **nach oben beschränkt**, falls es eine reelle Zahl M gibt, so dass
$$x \leq M \text{ für jedes } x \in S.$$
M ist **eine obere Schranke** für S.

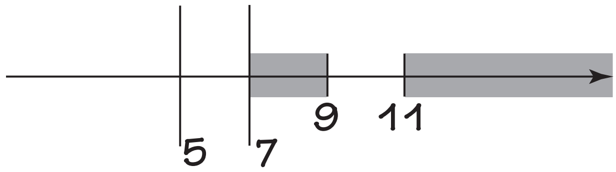
S heißt **nach unten beschränkt**, falls es eine reelle Zahl m gibt, so dass
$$x \geq m \text{ für jedes } x \in S.$$
m ist **eine untere Schranke** für S.

Beispiele

1. $(-\infty,1]$ ist nach oben beschränkt. Das Diagramm zeigt einige obere Schranken:



2. $[7,9] \cup [11,\infty)$ ist nach unten beschränkt. Das Diagramm zeigt einige untere Schranken:



Bemerkung

Wir können auch nichtleere Teilmengen anderer Zahlbereiche wie $\mathbb{N}$, $\mathbb{Z}$ oder $\mathbb{Q}$ betrachten. Die obere (untere) Schranke soll dann Element des relevanten Zahlbereichs sein.

Nun erinnern wir uns an das Wahlordnungsaxiom der natürlichen Zahlen:

- Jede nichtleere Teilmenge von $\mathbb{N}$ besitzt ein kleinstes Element.

Dieses Axiom gilt in modifizierter Form auch für die ganzen Zahlen.

Lemma

Jede nach unten beschränkte, nichtleere Teilmenge von $\mathbb{Z}$ besitzt ein kleinstes Element.

Beweis

Es sei M eine nach unten beschränkte, nichtleere Teilmenge von $\mathbb{Z}$. Die Zahl $\ell \in \mathbb{Z}$ sei eine untere Schranke für M, so dass $m \geq \ell$ für alle $m \in M$ ist. Daher ist

$$N = \{m - \ell + 1 : m \in M\}$$

eine nichtleere Menge natürlicher Zahlen. Dem Wohlordnungsaxiom der natürlichen Zahlen zufolge hat sie also ein kleinstes Element k. Damit gilt $m - \ell + 1 \geq k$, d.h. $m \geq m^\star := k + \ell - 1$ für alle $m \in M$. Da die Zahl $m^\star$ Element in M ist, ist sie ein kleinstes Element für M. $\square$

Das Wohlordnungsaxiom gilt aber absolut nicht für die reellen Zahlen.

Lemma

Die nichtleere, nach unten beschränkte Teilmenge $(0,1)$ von $\mathbb{R}$ besitzt kein kleinstes Element.

Beweis (durch Widerspruch)

Nehmen wir an, $(0,1)$ besitzt ein kleinstes Element x, so dass

$$\begin{aligned} &x \in (0,1), \\ &x \leq y \qquad \text{für alle} \quad y \in (0,1). \end{aligned} \qquad (\star)$$

Aus

$$0 < x < 1$$

folgt

$$0 < \frac{x}{2} < x < 1,$$

so dass $y = x/2$ $(\star)$ widerspricht. $\square$

Bemerkungen

1. Falls x rational ist, ist $x/2$ ebenfalls rational. Derselbe Beweis zeigt also, dass $\{x \in \mathbb{Q} : 0 < x < 1\}$ ebenfalls kein kleinstes Element besitzt. Das Wohlordnungsaxiom gilt also auch nicht für $\mathbb{Q}$.

2. Dieselben Ergebnisse gelten für größte Elemente. Jede nach oben beschränkte, nichtleere Teilmenge von $\mathbb{N}$ oder $\mathbb{Z}$ besitzt ein größtes Element. Dies gilt nicht für $\mathbb{R}$ oder $\mathbb{Q}$.

3. **Manche** nichtleere, nach oben (unten) beschränkte Mengen reeller Zahlen haben ein größtes (kleinstes) Element. Das Intervall $[0,1]$ hat z. B. sowohl ein größtes Element (1) als auch ein kleinstes Element (0).

Lemma

1. Die Menge X reeller Zahlen habe ein größtes Element. Dann ist dieses größte Element von X eindeutig.

2. Die Menge X reeller Zahlen habe ein kleinstes Element. Dann ist dieses kleinste Element von X eindeutig.

Beweis

1. Nehmen wir an, X hat zwei größte Elemente M_1,M_2. Dann gilt

$$
\begin{array}{ll}
M_1 \in X, & M_2 \in X \\
x \leq M_1 \quad \underbrace{\text{für alle } x \in X}_{\text{insbesondere für } x = M_2} & x \leq M_2 \quad \underbrace{\text{für alle } x \in X,}_{\text{insbesondere für } x = M_1} \\
\Rightarrow M_2 \leq M_1 & \Rightarrow M_1 \leq M_2
\end{array}
$$

Damit ist $M_1 = M_2$.

Die zweite Aussage wird in ähnlicher Weise bewiesen. □

Das Vollständigkeitsaxiom der reellen Zahlen

(V) M sei eine nichtleere, nach oben beschränkte Menge reeller Zahlen. Die Menge aller oberen Schranken für M hat ein kleinstes Element.

Definition

Die kleinste obere Schranke einer nichtleeren, nach oben beschränkten Menge $M \subset \mathbb{R}$ heißt **Supremum** oder **obere Grenze** von M und wird geschrieben als

$$\sup M.$$

Satz

M sei eine nichtleere, nach unten beschränkte Menge reeller Zahlen. Die Menge aller unteren Schranken für M hat ein größtes Element.

Beweis

Wir betrachten

$$N = \{-m : m \in M\}$$

Weil M nach unten beschränkt ist, ist N nach oben beschränkt. Dem Vollständigkeitsaxiom von $\mathbb{R}$ zufolge besitzt N eine kleinste obere Schranke $(\sup N)$, und $-\sup N$ ist eine größte untere Schranke für M.

Definition

Die größte untere Schranke einer nichtleeren nach unten beschränkten Menge $M \subset \mathbb{R}$ heißt **Infimum** oder **untere Grenze** von M und wird geschrieben als

$$\inf M.$$

Beispiel

Zeigen Sie, dass $\inf(0,1) = 0$.

Lösung

0 ist offensichtlich eine untere Schranke für (0,1). Wir zeigen durch Widerspruch, dass 0 die größte untere Schranke für (0,1) ist.

Nehmen wir an, $m > 0$ ist eine untere Schranke für (0,1). Offensichtlich ist $m < 1$. Aus

$$0 < m < 1$$

folgt

$$0 < \frac{m}{2} < m < 1,$$

und daher ist $m/2$ Element in (0,1), das kleiner als die untere Schranke m ist. □

Definition

Falls das Supremum einer nichtleeren, nach oben beschränkten Menge $M \subset \mathbb{R}$ Element von M ist, heißt es auch **Maximum** von M und wird geschrieben als

$$\max M.$$

Falls das Infimum einer nichtleeren, nach unten beschränkten Menge $M \subset \mathbb{R}$ Element von M ist, heißt es auch **Minimum** von M und wird geschrieben als

$$\min M.$$

Beispiele

- $\inf(0,1) = 0, \qquad (0,1)$ hat kein Minimum
- $\inf[0,1] = 0, \qquad \min[0,1] = 0$
- $\sup(0,1) = 1, \qquad (0,1)$ hat kein Maximum
- $\sup[0,1] = 1, \qquad \max[0,1] = 1.$

Lemma

X sei eine nichtleere, nach oben (unten) beschränkte Menge reeller Zahlen und M (m) sei eine obere (untere) Schranke für X. Dann gilt:

$$M = \sup X \quad \Leftrightarrow \quad \begin{array}{l}\text{Zu jedem } \varepsilon > 0 \text{ existiert} \\ x \in X \text{ mit } x > M - \varepsilon\end{array}$$

$$m = \inf X \quad \Leftrightarrow \quad \begin{array}{l}\text{Zu jedem } \varepsilon > 0 \text{ existiert} \\ x \in X \text{ mit } x < m + \varepsilon\end{array}$$

Beweis

$\Rightarrow$ Die Aussage

Es existiert $\varepsilon > 0$, so dass $x \leq M - \varepsilon$ für alle $x \in X$ $\Rightarrow M \neq \sup X$

ist offensichtlich richtig. Damit haben wir die Kontraposition der zu beweisenden Aussage bewiesen.

$\Leftarrow$ Dies zeigen wir durch Widerspruch.

Nehmen wir an, $M_1 < M$ ist eine obere Schranke für X. Wir setzen nun $\varepsilon = M - M_1$, und es existiert $x \in X$ mit $x > M - (M - M_1)$, d. h. $x > M_1$. Also ist M_1 keine obere Schranke für X.

Die zweite Aussage wird in ähnlicher Weise bewiesen. □

Lemma

A und B seien nichtleere, nach oben beschränkte Mengen reeller Zahlen. Dann gilt

$$\sup(A + B) = \sup A + \sup B,$$

wobei

$$A + B := \{a + b : a \in A, b \in B\}.$$

Beweis

$M := \sup A + \sup B$ ist eine obere Schranke für $A + B$, weil

$$\begin{aligned} a &\leq \sup A && \text{für alle } a \in A \\ b &\leq \sup B && \text{für alle } b \in B \end{aligned}$$

$$\Rightarrow \qquad a + b \leq \sup A + \sup B \qquad \text{für alle } a \in A, b \in B.$$

Wir wissen:

Zu jedem $\varepsilon_1 > 0$ existiert $a \in A$ mit $a > \sup A - \varepsilon_1$

Zu jedem $\varepsilon_2 > 0$ existiert $b \in B$ mit $b > \sup B - \varepsilon_2$

Wir wollen beweisen:

Zu jedem $\varepsilon > 0$ existiert $x \in A + B$ mit $x > M - \varepsilon$.

Wir wählen $\varepsilon > 0$ und setzen $\varepsilon_1 = \varepsilon/2, \varepsilon_2 = \varepsilon/2$, so dass $x = a + b$ die Ungleichung

$$x > \underbrace{\sup A + \sup B}_{= M} - \varepsilon$$

erfüllt. □

2.7 Rationale und irrationale Zahlen

Lemma (die Archimedische Eigenschaft der reellen Zahlen)

1. Die Teilmenge $\mathbb{N}$ of $\mathbb{R}$ ist nicht nach oben beschränkt.

2. Zu jedem $\varepsilon > 0$ gibt es ein $n \in \mathbb{N}$, so dass

   $$\frac{1}{n} < \varepsilon$$

   ist.

Beweis

1. Dies beweisen wir durch Widerspruch. Wir nehmen an, dass $\mathbb{N}$ nach oben beschränkt ist. Dem Vollständigkeitsaxiom der reellen Zahlen zufolge hat $\mathbb{N}$ also eine kleinste obere Schränke x_0. Daher existiert $n \in \mathbb{N}$ mit $n > x_0 - 1$ (verwende das letzte Lemma mit $\varepsilon = 1$). Da $\mathbb{N}$ induktiv ist, liegt auch $n + 1$ in $\mathbb{N}$. Die Aussage $n + 1 > x_0$ steht aber im Widerspruch dazu, dass x_0 eine obere Schranke für $\mathbb{N}$ ist.

2. Weil $\mathbb{N}$ nicht nach oben beschränkt ist, gibt es ein $n \in \mathbb{N}$, so dass $n > \frac{1}{\varepsilon}$ ist (sonst wäre $\frac{1}{\varepsilon}$ eine obere Schranke für $\mathbb{N}$). □

Proposition

Es sei M eine nichtleere, nach unten beschränkte Teilmenge von $\mathbb{R}$, die nur ganze Zahlen enthält. Dann hat M ein kleinstes Element.

Beweis

Es sei s eine untere Schranke für M. Wegen der Archimedischen Eigenschaft der reellen Zahlen existiert eine natürliche Zahl t, so dass $t \geq -s$ ist. Damit ist $\ell := -t$ eine ganzzahlige untere Schranke für M und M eine nichtleere, nach unten beschränkte Teilmenge von $\mathbb{Z}$. Es wurde schon gezeigt, dass eine solche Menge ein kleinstes Element besitzt. □

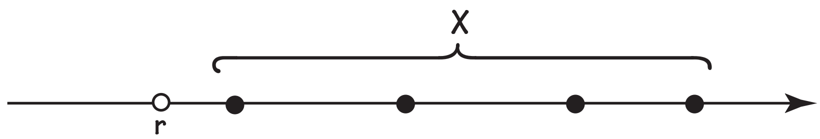
Wir können die Archimedische Eigenschaft der reellen Zahlen benutzen, um interessante Eigenschaften von $\mathbb{Z}$ und $\mathbb{Q}$ herzuleiten.

Proposition

Es sei r eine reelle Zahl. Dann existiert ein eindeutige ganze Zahl m mit

$$m - 1 \leq r < m.$$

Beweis



Die Menge $X = \{x \in \mathbb{Z} : x > r\}$ ist nach unten beschränkt und hat daher ein kleinstes Element m. Damit gilt $m > r$ und $m - 1 \leq r$.

Erfüllen m_1 und m_2 die angegebene Gleichung, so sind sie beide kleinste Elemente von X, so dass $m_1 = m_2$ ist. □

Lemma

Jedes Intervall $(\alpha, \beta), \alpha < \beta$ enthält eine rationale Zahl.

Beweis

Wegen der Archimedischen Eigenschaft der reellen Zahlen existiert $n \in \mathbb{N}$, so dass

$$\frac{1}{n} < \beta - \alpha. \tag{1}$$

Außerdem existiert ein eindeutiges Element $m \in \mathbb{Z}$ mit der Eigenschaft

$$m - 1 \leq n\alpha < m. \tag{2}$$

Aus (2) folgt

$$\frac{m}{n} > \alpha$$

und aus (1), (2) folgt

$$\begin{aligned} \frac{m}{n} &\leq \alpha + \frac{1}{n} \\ &< \alpha + \beta - \alpha \\ &= \beta. \end{aligned}$$

Die rationale Zahl $\frac{m}{n}$ liegt also im Intervall (α, β). □

Definition

Eine reelle Zahl, die nicht rational ist, heißt **irrational**.

Im folgenden Satz wird gezeigt, dass es irrationale Zahlen gibt.

Satz

Die Menge

$$S = \{q \in \mathbb{Q} : q > 0, q^2 < 2\}$$

reeller Zahlen ist nicht leer und nach oben beschränkt. Ihr Supremum r löst die Gleichung $r^2 = 2$ und ist nicht rational.

Beweis

Die Menge S ist offenbar nicht leer $(1 \in S)$. Sie ist außerdem nach oben beschränkt, denn jedes $q \in S$ erfüllt $q \leq 2$, weil

$$q > 2 \Rightarrow q^2 > 4 \Rightarrow q \notin S.$$

Dem Vollständigkeitsaxiom zufolge hat S also ein Supremum $r \in \mathbb{R}$. Offensichtlich ist $r > 0$ (es gilt sogar $r \geq 1$, da $1 \in S$ ist).

Nun beweisen wir $r^2 = 2$, indem wir die Möglichkeiten $r^2 < 2$ und $r^2 > 2$ ausschließen.

Falls $r^2 < 2$: Wir wählen $\varepsilon > 0$ klein genug, so dass $r^2 < (r+\varepsilon)^2 < 2$:

$$\begin{aligned} r^2 &< (r+\varepsilon)^2 \\ &= r^2 + 2r\varepsilon + \varepsilon^2 \\ &< r^2 + 2r\varepsilon + \varepsilon \quad && \text{für } \varepsilon < 1 \\ &< 2 && \text{für } \varepsilon < \frac{2-r^2}{2r+1} \end{aligned}$$

Wählen wir ε so, dass $r+\varepsilon$ rational ist, ist also $r+\varepsilon \in S$. Aber $r+\varepsilon > \sup S$, ein Widerspruch.

Falls $r^2 > 2$: Wir wählen $\varepsilon > 0$ klein genug, so dass $2 < (r-\varepsilon)^2 < r^2$:

$$\begin{aligned} r^2 &> (r-\varepsilon)^2 \\ &= r^2 - 2\varepsilon r + \varepsilon^2 \\ &> r^2 - 2\varepsilon r - \varepsilon \\ &> 2 && \text{für} \quad \varepsilon < \frac{r^2-2}{2r+1} \end{aligned}$$

Dann ist $r-\varepsilon$ eine obere Schranke für S (die übrigens auch rational gewählt werden kann), weil

$$\begin{aligned} q > r-\varepsilon \Rightarrow q^2 &> (r-\varepsilon)^2 \\ &> 2 \\ &\Rightarrow q \notin S. \end{aligned}$$

Dies widerspricht der Tatsache, dass r die kleinste obere Schranke für S ist.

Nun beweisen wir durch Widerspruch, dass r nicht rational ist.

Nehmen wir an, r ist eine rationale Zahl, so dass

$$r = \frac{p}{q}, \qquad p,q \in \mathbb{Z}, \quad q \neq 0,$$

wobei wir den Bruch $\frac{p}{q}$ als gekürzt voraussetzen (p,q enthalten keine gemeinsamen Faktoren). Dann gilt:

$$
\left.\begin{aligned}
2 &= \frac{p^2}{q^2} \\
&\Rightarrow p^2 = 2q^2 \\
&\Rightarrow p^2 \text{ ist gerade} \\
&\Rightarrow p \text{ ist gerade} \\
&\Rightarrow p = 2m, \quad m \in \mathbb{Z} \\
&\Rightarrow 4m^2 = 2q^2 \\
&\Rightarrow q^2 = 2m^2 \\
&\Rightarrow q^2 \text{ ist gerade} \\
&\Rightarrow q \text{ ist gerade} \\
&\Rightarrow q = 2n, \quad n \in \mathbb{Z}
\end{aligned}\right\} \text{Also enthalten } p,q \text{ den gemeinsamen Faktor 2.}
$$

Damit haben wir einen Widerspruch. □

Bemerkungen

1. Eine positive Zahl r mit der Eigenschaft $r^2 = n, n \in \mathbb{N}$ heißt **Wurzel** von n und wird als $\sqrt{n}$ geschrieben. Der letzte Beweis zeigt, dass $\sqrt{2}$ existiert und irrational ist. Das folgende Argument zeigt, dass sie auch eindeutig ist.

   Nehmen wir an, es gibt zwei positive reelle Zahlen r_1,r_2 mit
   $$r_1^2 = 2, \qquad r_2^2 = 2.$$
   Dann gilt:
   $$
   \begin{aligned}
   & r_1^2 - r_2^2 = 0 \\
   \Rightarrow\ & (r_1 - r_2)\underbrace{(r_1 + r_2)}_{>0} = 0 \\
   \Rightarrow\ & r_1 - r_2 = 0 \\
   \Rightarrow\ & r_1 = r_2.
   \end{aligned}
   $$

2. Der obige Beweis zeigt, dass das Vollständigkeitsaxiom für die rationalen Zahlen nicht gilt. Die Teilmenge
   $$S = \{q \in \mathbb{Q} : q > 0, q^2 < 2\}$$
   von $\mathbb{Q}$ ist nicht leer $(1 \in S)$ und nach oben beschränkt (die rationale Zahl 2 ist eine obere Schranke). Falls S ein Supremum r in $\mathbb{Q}$ hat, muss $r^2 = 2$ sein. Es gibt aber keine rationale Zahl mit dieser Eigenschaft.

Lemma

Jedes Intervall $(\alpha, \beta), \alpha < \beta$ enthält eine irrationale Zahl.

Beweis

Wegen der Archimedischen Eigenschaft der reellen Zahlen existiert $n \in \mathbb{N}$, so dass

$$\frac{1}{n} < \sqrt{2}(\beta - \alpha).$$

Folglich gilt

$$\frac{1}{\sqrt{2}n} < \beta - \alpha. \tag{1}$$

Außerdem existiert ein eindeutiges Element $m \in \mathbb{Z}$ mit der Eigenschaft

$$m - 1 \leq \sqrt{2}n\alpha < m, \tag{2}$$

Aus (1), (2) folgt

$$\alpha < \frac{m}{\sqrt{2}n} < \beta.$$

Die Zahl $\frac{m}{\sqrt{2}n}$ ist irrational. Falls sie rational wäre, hätten wir

$$\begin{aligned} \frac{m}{\sqrt{2}n} &= \frac{p}{q}, \qquad p,q \in \mathbb{Z}, q \neq 0 \\ \Rightarrow \sqrt{2} &= \underbrace{\frac{mq}{np}}_{\text{rational}}, \end{aligned}$$

ein Widerspruch.

Die irrationale Zahl $\frac{m}{\sqrt{2}n}$ liegt also im Intervall (α,β). □

Bemerkung

Zu jedem $r \in \mathbb{R}$ und $\varepsilon > 0$ existieren $q \in \mathbb{Q}$ und $i \in \mathbb{R} \setminus \mathbb{Q}$, so dass

$$|r - q| < \varepsilon, \qquad |r - i| < \varepsilon.$$

Dieses Ergebnis besagt, dass eine reelle Zahl sich beliebig nah durch rationale bzw. irrationale Zahlen approximieren lässt. Wir sagen: $\mathbb{Q}$ und $\mathbb{R} \setminus \mathbb{Q}$ sind **dichte** Teilmengen von $\mathbb{R}$.

Lemma

1. $\mathbb{Q}$ ist abzählbar unendlich.

2. $\mathbb{R} \setminus \mathbb{Q}$ ist überabzählbar.

Beweis

1. Wir haben schon bewiesen, dass $\mathbb{Q} \cap (0,\infty)$ abzählbar unendlich ist. Derselbe Beweis zeigt, dass $\mathbb{Q} \cap (-\infty,0)$ ebenfalls abzählbar unendlich ist. Aus
$$\mathbb{Q} = \underbrace{[\mathbb{Q} \cap (-\infty,0)]}_{\text{abzählbar}} \cup \underbrace{\{0\}}_{\text{abzählbar}} \cup \underbrace{[\mathbb{Q} \cap (0,\infty)]}_{\text{abzählbar}}$$
folgt, dass $\mathbb{Q}$ abzählbar ist.

2. Dies beweisen wir durch Widerspruch. Wir nehmen an, $\mathbb{R} \setminus \mathbb{Q}$ ist abzählbar. Dann gilt:
$$\mathbb{R} = \underbrace{\mathbb{Q}}_{\text{abzählbar}} \cup \underbrace{\mathbb{R} \setminus \mathbb{Q}}_{\text{abzählbar}}$$
so dass $\mathbb{R}$ abzählbar ist. Wir haben aber schon bewiesen, dass $\mathbb{R}$ nicht abzählbar ist.

□

2.8 Komplexe Zahlen

Definitionen

Eine **komplexe Zahl** ist ein geordnetes Paar (a,b), wobei a und b reelle Zahlen sind.

Die Menge aller komplexen Zahlen bezeichnen wir mit $\mathbb{C}$.

Lemma

Mit den durch die Formeln

$$(a,b) + (c,d) := (a + c,b + d), \qquad (\textbf{Addition})$$
$$(a,b).(c,d) := (ac - bd,ad + bc) \qquad (\textbf{Multiplikation})$$

definierten Verknüpfungen bildet die Menge $\mathbb{C}$ einen Körper. Dabei sind die neutralen Elemente der Addition und Multiplikation $(0,0)$ bzw. $(1,0)$ und

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

Lemma

1. Die Teilmenge $X = \{(a{,}0) : a \in \mathbb{R}\}$ von $\mathbb{C}$ bildet einen Teilörper von $(\mathbb{C}, +, .)$
2. Die Abbildung $\psi : (a{,}0) \mapsto a$ ist eine Bijektion $X \to \mathbb{R}$ mit

$$\psi(x_1 + x_2) = \psi(x_1) + \psi(x_2), \qquad \psi(x_1.x_2) = \psi(x_1)\psi(x_2)$$

für alle x_1, $x_2 \in X$.

Beweis

1. Wir müssen zeigen:

   (i) Die neutralen Elemente der Addition und Multiplikation gehören zu X. Dies ist trivial: $(0{,}0)$, $(1{,}0) \in X$.

   (ii) X ist abgeschlossen bezüglich $+$ und .. Dies folgt aus

$$(a{,}0) + (b{,}0) = (a + b{,}0), \tag{1}$$
$$(a{,}0).(b{,}0) = (ab{,}0) \tag{2}$$

   (iii) X ist abgeschlossen bezüglich der Inversen. Dies folgt aus

$$-(a{,}0) = (-a{,}0),$$
$$(a{,}0)^{-1} = (a^{-1}{,}0), \qquad a \neq 0.$$

2. Dies folgt aus (1) und (2). □

Bemerkung

Die obige Notation für komplexe Zahlen ist etwas umständlich und wird üblicherweise vereinfacht wie folgt.

- Wir identifizieren die Teilmenge X von $\mathbb{C}$ mit $\mathbb{R}$ und schreiben $(a{,}0)$ als a.

- Wir definieren $\mathrm{i} = (0,1)$ und bemerken, dass

$$\begin{aligned} \mathrm{i}.\mathrm{i} &= (0,1).(0,1) \\ &= (-1,0) \\ &= -1. \end{aligned}$$

- Damit gilt

$$\begin{aligned} (a,b) &= (a,0) + (0,b) \\ &= (a,0) + (0,1).(b,0) \\ &= a + \mathrm{i}b. \end{aligned}$$

Wir schreiben also (a,b) als $a + \mathrm{i}b$ und arbeiten mit den üblichen Rechenregeln und dem Zusatz $\mathrm{i}^2 = -1$.

Beispiel

Es seien $z_1 = (x_1,y_1)$, $z_2 = (x_2,y_2)$. Dann gilt

$$\begin{aligned} z_1 z_2 &= (x_1,y_1).(x_2,y_2) \\ &= (x_1x_2 - y_1y_2, x_1y_2 + x_2y_1). \end{aligned}$$

Schreibe nun $z_1 = x_1 + \mathrm{i}y_1$, $z_2 = x_2 + \mathrm{i}y_2$. Dann gilt

$$\begin{aligned} z_1 z_2 &= (x_1 + \mathrm{i}y_1)(x_2 + \mathrm{i}y_2) \\ &= x_1x_2 + x_1y_2\mathrm{i} + x_2y_1\mathrm{i} + y_1y_2\mathrm{i}^2 \\ &= x_1x_2 - y_1y_2 + (x_1y_2 + x_2y_1)\mathrm{i}. \end{aligned}$$

Definitionen

Betrachte die komplexe Zahl $z = x + \mathrm{i}y$.

1. x ist der **Realteil** von z. Wir schreiben $x = \operatorname{Re} z$.

2. y ist der **Imaginärteil** von z. Wir schreiben $y = \operatorname{Im} z$.

3. $x - \mathrm{i}y$ ist die zu z **konjugiert komplexe Zahl**. Wir schreiben $x - \mathrm{i}y = \bar{z}$.

4. $\sqrt{x^2 + y^2}$ ist der **Betrag** von z. Wir schreiben $\sqrt{x^2 + y^2} = |z|$.

z heißt **reell**, falls $\operatorname{Im} z = 0$ ist, und **imaginär**, falls $\operatorname{Re} z = 0$ ist.

Proposition

Für jede komplexe Zahl z gilt

1. $z + \bar{z} = 2\operatorname{Re} z$,

2. $z - \bar{z} = 2\mathrm{i}\operatorname{Im} z$,

3. $z\bar{z} = |z|^2$.

Proposition

Für alle komplexen Zahlen z_1, z_2 gelten die Regeln

1. $\overline{z_1 + z_2} = \bar{z}_1 + \bar{z}_2$,

2. $\overline{z_1 z_2} = \bar{z}_1 \bar{z}_2$,

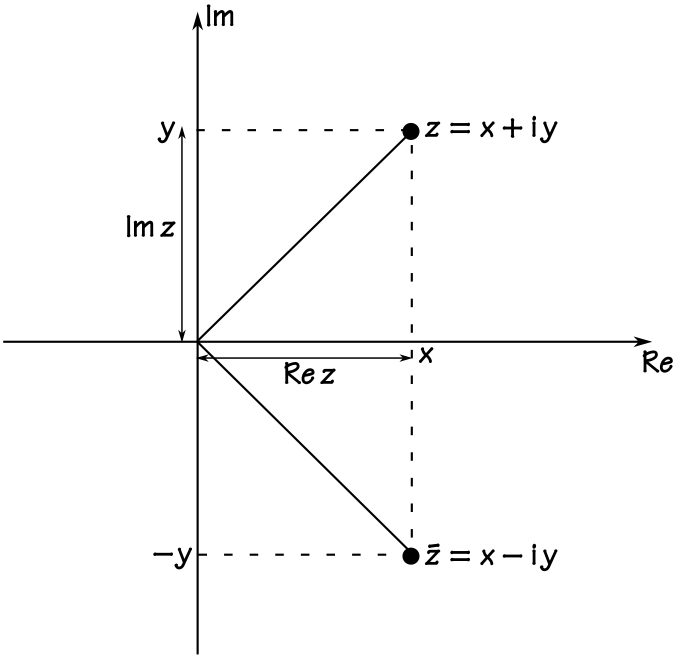
3. $\overline{\dfrac{1}{z_1}} = \dfrac{1}{\bar{z}_1}$, falls $z_1 \neq 0$,

4. $\bar{\bar{z}}_1 = z_1$,

5. $|\bar{z}_1| = |z_1|$.

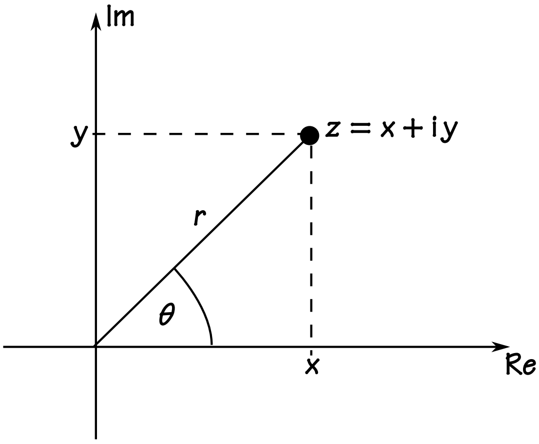
Geometrische Darstellungen komplexer Zahlen

Da eine komplexe Zahl ein geordnetes Paar (x,y) reeller Zahlen ist, können wir sie als Punkt in der Koordinatenebene (**komplexer Ebene** oder **Gaußscher Zahlenebene**) darstellen:



$\bar{z}$ wird von z durch eine Spiegelung an der reellen Achse hergeleitet.

Es ist auch hilfreich, Polarkoordinaten einzuführen:



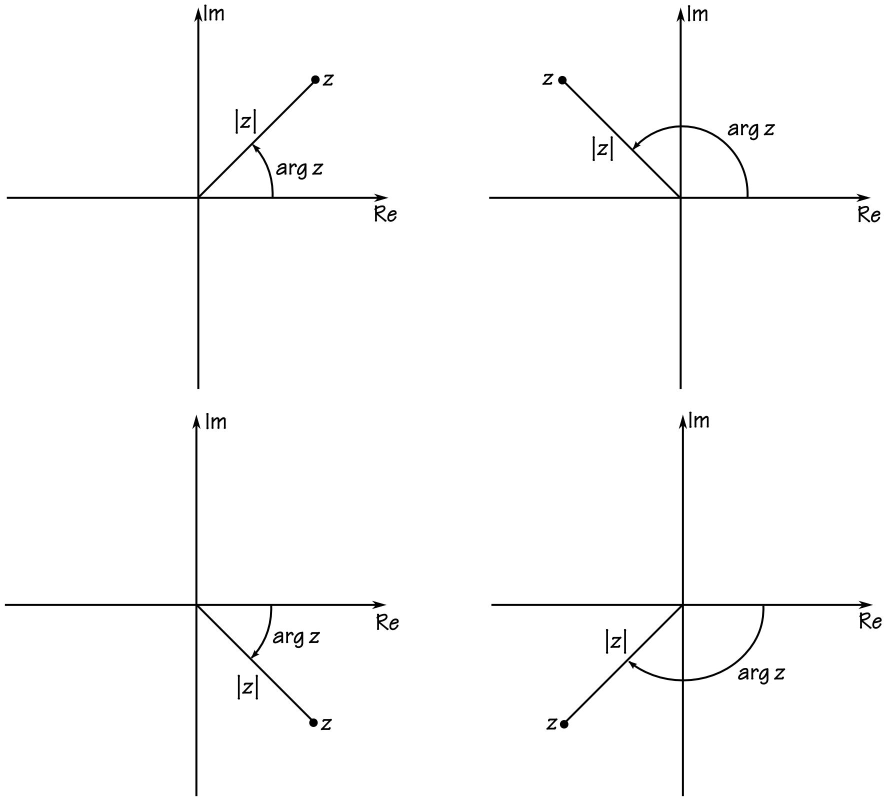
Hier gilt

$$\begin{aligned} x &= r\cos\theta, \\ y &= r\sin\theta, \\ r &= \sqrt{x^2+y^2}, \\ \tan\theta &= \frac{y}{x}. \end{aligned}$$

Bemerke insbesondere, dass

$$r = |z|.$$

Der Winkel θ heißt **Argument** der komplexen Zahl $z = x + \mathrm{i}y$. Er ist nicht eindeutig: Er ist nur bis auf ganzzahlige Vielfache von 2π bestimmt. Diese Mehrdeutigkeit wird behoben, indem man sich auf Werte von θ im Intervall $(-\pi,\pi]$ einschränkt. In diesem Fall ist θ das **Haupt-** oder **Prinzipalargument** von z und wird mit $\arg z$ bezeichnet:



In der Regel definieren wir $\arg 0 = 0$.

Beispiel

Beschreiben Sie die folgenden Mengen geometrisch.

(i) $\{z \in \mathbb{C} : |z - (1 + \mathrm{i})| = 3\}$

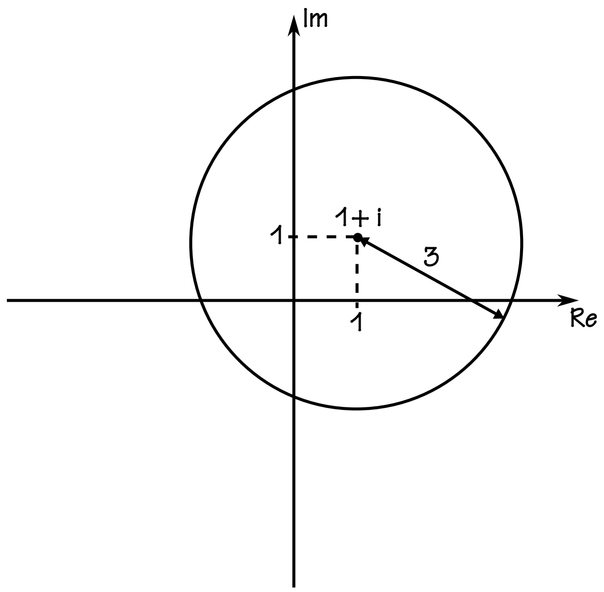
(ii) $\{z \in \mathbb{C} : 1 < |z| \leq 3\}$

(iii) $\{z \in \mathbb{C} : |z - \mathrm{i}| < |z + \mathrm{i}|\}$

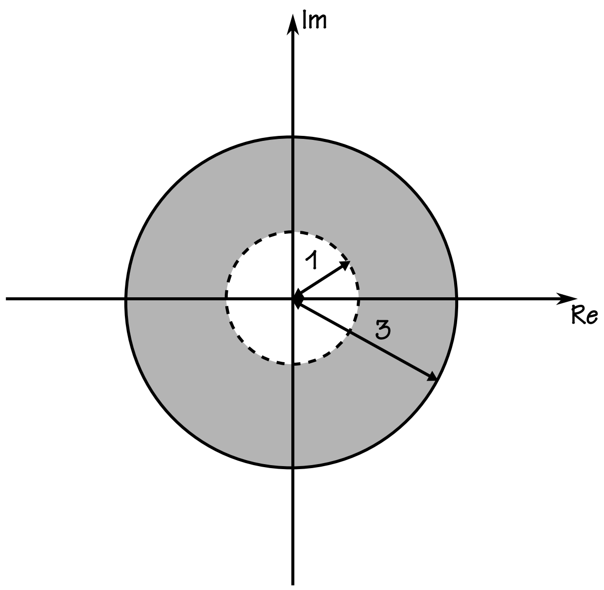
(iv) $\{z \in \mathbb{C} : -\pi/4 < \arg z \leq \pi/4\}$

Lösung

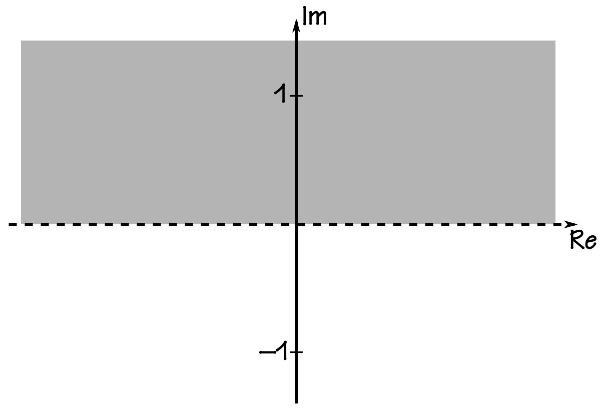
(i) $\{z \in \mathbb{C} : |z - (1 + \mathrm{i})| = 3\}$ ist die Menge der komplexen Zahlen, deren Distanz zur komplexen Zahl $1 + \mathrm{i}$ gleich 3 ist. Sie ist daher ein Kreis mit Mittelpunkt $1 + \mathrm{i}$ und Radius 3:



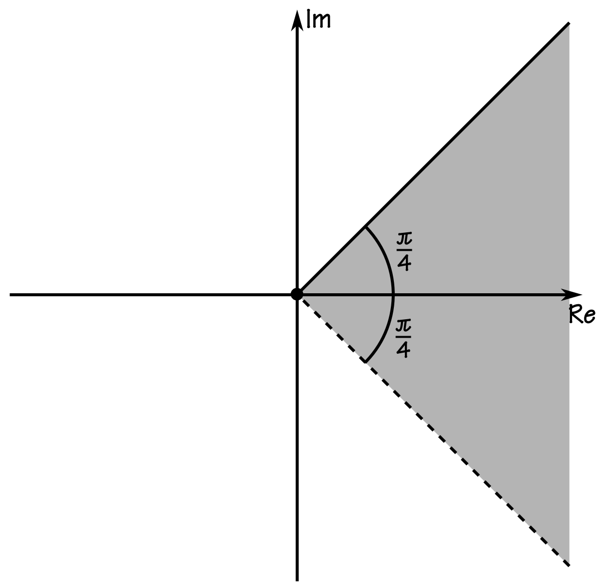
(ii) $\{z \in \mathbb{C} : 1 < |z| \leq 3\}$ ist die Menge der komplexen Zahlen, deren Distanz zum Nullpunkt größer als 1 und kleiner als oder gleich 3 ist. Es handelt sich daher um einen Annulus mit Mittelpunkt 0 und Radien 1 und 3:



(iii) $\{z \in \mathbb{C} : |z - \mathrm{i}| < |z + \mathrm{i}|\}$ ist die Menge der komplexen Zahlen, die näher an i als an $-i$ liegen. Sie ist also die obere Halbebene:



(iv) $\{z \in \mathbb{C} : -\pi/4 < \arg z \leq \pi/4\}$ ist die Menge der komplexen Zahlen, deren Winkel zur reellen Achse zwischen $-\pi/4$ und $\pi/4$ liegt. Es handelt sich daher um einen Sektor:



Lemma

Betrachte die komplexen Zahlen

$$
\begin{aligned}
z_1 &= x_1 + \mathrm{i}y_1 = r_1 \cos\theta_1 + \mathrm{i}r_1 \sin\theta_1, \\
z_2 &= x_2 + \mathrm{i}y_2 = r_2 \cos\theta_2 + \mathrm{i}r_2 \sin\theta_2.
\end{aligned}
$$

Es gelten die Regeln

$$z_1 z_2 = r_1 r_2 \cos(\theta_1 + \theta_2) + \mathrm{i} r_1 r_2 \sin(\theta_1 + \theta_2) \tag{i}$$

und

$$z_1^n = r_1^n \cos n\theta_1 + \mathrm{i} r_1^n \sin n\theta_1, \qquad n = 1,2,3,\ldots. \qquad \textbf{(Satz von de Moivre)} \tag{ii}$$

Beweis

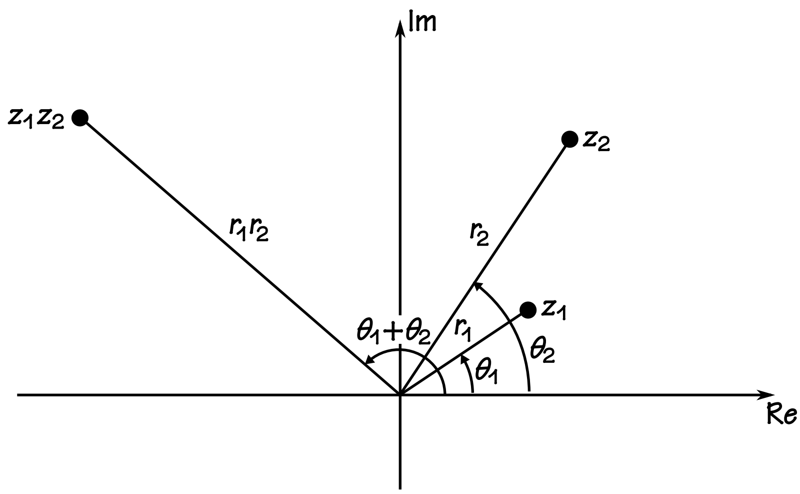
(i) Es gilt

$$\begin{aligned} z_1 z_2 &= (r_1 \cos\theta_1 + \mathrm{i} r_1 \sin\theta_1)(r_2 \cos\theta_2 + \mathrm{i} r_2 \sin\theta_2) \\ &= r_1 r_2 \cos\theta_1 \cos\theta_2 + \mathrm{i}^2 r_1 r_2 \sin\theta_1 \sin\theta_2 + \mathrm{i} r_1 r_2 \cos\theta_1 \sin\theta_2 + \mathrm{i} r_1 r_2 \sin\theta_1 \cos\theta_2 \\ &= r_1 r_2 (\cos\theta_1 \cos\theta_2 - \sin\theta_1 \sin\theta_2) + \mathrm{i} r_1 r_2 (\cos\theta_1 \sin\theta_2 + \sin\theta_1 \cos\theta_2) \\ &= r_1 r_2 \cos(\theta_1 + \theta_2) + \mathrm{i} r_1 r_2 \sin(\theta_1 + \theta_2). \end{aligned}$$

(ii) Dieses Ergebnis folgt induktiv aus (i). □

Bemerkung

Wir können (i) geometrisch interpretieren: Die Distanz des Punktes $z_1 z_2$ zum Nullpunkt in der komplexen Ebene ist das Produkt der Distanzen der beiden Punkten z_1 und z_2 zum Nullpunkt und der Winkel des Punktes $z_1 z_2$ zur reellen Achse ist die Summe der Winkel der beiden Punkten z_1 und z_2 zur reellen Achse:



Funktionen einer komplexen Veränderlichen

Wir beginnen mit den Definitionen der Exponential-, trigonometrischen und hyperbolischen Funktionen.

Definitionen

Für $z \in \mathbb{C}$ definieren wir

$$\begin{aligned} \mathrm{e}^z &:= \mathrm{e}^x(\cos y + \mathrm{i}\sin y), \qquad \text{wobei } x = \operatorname{Re} z,\, y = \operatorname{Im} z, \\ \sin z &:= \frac{1}{2\mathrm{i}}(\mathrm{e}^{\mathrm{i}z} - \mathrm{e}^{-\mathrm{i}z}), \\ \cos z &:= \frac{1}{2}(\mathrm{e}^{\mathrm{i}z} + \mathrm{e}^{-\mathrm{i}z}), \\ \sinh z &:= \frac{1}{2}(\mathrm{e}^{z} - \mathrm{e}^{-z}), \\ \cosh z &:= \frac{1}{2}(\mathrm{e}^{z} + \mathrm{e}^{-z}). \end{aligned}$$

Weitere spezielle Funktionen wie $\tan(\cdot)$, $\cot(\cdot)$, usw. werden durch diese Grundfunktionen auf der üblichen Art und Weise definiert.

Proposition

Es gelten

$$\begin{aligned} &\cosh z = \cos(\mathrm{i}z), && z \in \mathbb{C}, \\ &\sinh z = -\mathrm{i}\sin(\mathrm{i}z), && z \in \mathbb{C}, \\ &\mathrm{e}^{\mathrm{i}\theta} = \cos\theta + \mathrm{i}\sin\theta, && \theta \in \mathbb{R}, \qquad \textbf{(Eulers Formel)} \end{aligned}$$

und die Grundidentitäten für die Beziehungen zwischen den Exponential-, trigonometrischen und hyperbolischen Funktionen sind weiterhin gültig.

Bemerkung

Wir können die komplexe Zahl z in Polarkoordinaten als $z = r\cos\theta + \mathrm{i}r\sin\theta$ schreiben und durch Eulers Formel als $z = r\mathrm{e}^{\mathrm{i}\theta}$ umschreiben.

Bemerkungen (Nullstellen)

1. Die Berechnung

$$\begin{aligned} |\mathrm{e}^z| &= |\mathrm{e}^x(\cos y + \mathrm{i}\sin y)| \\ &= |\mathrm{e}^x||\cos y + \mathrm{i}\sin y| \\ &= \mathrm{e}^x \end{aligned}$$

für $z = x + \mathrm{i}y$ mit $x,y \in \mathbb{R}$ zeigt, dass

$$|\mathrm{e}^z| = \mathrm{e}^{\operatorname{Re} z}.$$

Insbesondere hat die Exponentialfunktion keine Nullstellen in der komplexen Ebene.

2. Es gilt

$$\begin{aligned} \sin z = 0 \quad &\Leftrightarrow \quad z = 0, \pm\pi, \pm 2\pi, \ldots, \\ \cos z = 0 \quad &\Leftrightarrow \quad z = \pm\frac{\pi}{2}, \pm\frac{3\pi}{2}, \pm\frac{5\pi}{2}, \ldots \end{aligned}$$

(siehe unten).

3. Aus den Formeln in der letzten Proposition folgt

$$\begin{aligned} \sinh z = 0 \quad &\Leftrightarrow \quad z = 0, \pm\pi\mathrm{i}, \pm 2\pi\mathrm{i}, \ldots, \\ \cosh z = 0 \quad &\Leftrightarrow \quad z = \pm\frac{\pi\mathrm{i}}{2}, \pm\frac{3\pi\mathrm{i}}{2}, \pm\frac{5\pi\mathrm{i}}{2}, \ldots. \end{aligned}$$

Beispiel

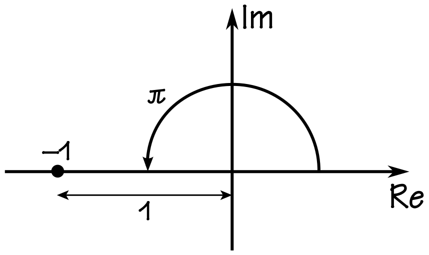
Finden Sie die Nullstellen der Funktion $\cos(\cdot) : \mathbb{C} \to \mathbb{C}$.

Lösung

Es gilt

$$\begin{aligned}
&\cos z = 0 \\
\Leftrightarrow\ &\frac{1}{2}(\mathrm{e}^{\mathrm{i}z} + \mathrm{e}^{-\mathrm{i}z}) = 0 \\
\Leftrightarrow\ &\mathrm{e}^{\mathrm{i}z} = -\mathrm{e}^{-\mathrm{i}z} \\
\Leftrightarrow\ &\mathrm{e}^{2\mathrm{i}z} = -1.
\end{aligned}$$

Schreibe nun $z = x + \mathrm{i}y$ und bemerke, dass $-1 = 1\mathrm{e}^{\mathrm{i}\pi}$:



- $|-1| = 1$
- $\arg(-1) = \pi$

Daher gilt

$$\begin{aligned}
&\mathrm{e}^{2\mathrm{i}z} = -1 \\
\Leftrightarrow\ &\mathrm{e}^{2i(x+\mathrm{i}y)} = -1 \\
\Leftrightarrow\ &\mathrm{e}^{-2y}\mathrm{e}^{2\mathrm{i}x} = 1\mathrm{e}^{\mathrm{i}\pi} \\
\Leftrightarrow\ &\mathrm{e}^{-2y} = 1, \qquad 2x = \pi + 2n\pi, \quad n = 0, \pm 1, \pm 2, \ldots \\
\Leftrightarrow\ &y = 0, \qquad x = \frac{\pi}{2} + n\pi, \quad n = 0, \pm 1, \pm 2, \ldots.
\end{aligned}$$

Es ist also

$$\cos z = 0 \quad \Leftrightarrow \quad z = \pm\frac{\pi}{2}, \pm\frac{3\pi}{2}, \pm\frac{5\pi}{2}, \ldots. \qquad \square$$

Definition

Es sei $n \in \mathbb{N}_0$. Ein **komplexes Polynom n-ten Grades** ist ein Ausdruck der Form

$$a_n z^n + a_{n-1} z^{n-1} + \ldots + a_1 z + a_0,$$

wobei $a_0, \ldots, a_n$ konstante komplexe Zahlen sind und $a_n \neq 0$ ist.

Satz (Fundamentalsatz der Algebra)

Es sei $n \in \mathbb{N}$. Jedes komplexe Polynom n-ten Grades hat eine komplexe Nullstelle.

Korollar

Es sei $n \in \mathbb{N}$. Jedes Polynom

$$z^n + a_{n-1}z^{n-1} + \ldots + a_1 z + a_0$$

n-ten Grades hat n komplexe Nullstellen $z_1, \ldots, z_n$ (die nicht notwendigerweise verschieden sind), und lässt sich daher als

$$z^n + a_{n-1}z^{n-1} + \ldots + a_1 z + a_0 = (z - z_1)(z - z_2)\ldots(z - z_n)$$

zerlegen, wobei wir ohne Beschränkung der Allgemeinheit $a_n = 1$ gesetzt haben.

Bemerkung

Falls die Koeffizienten $a_0, \ldots, a_n$ reell sind, kommen alle Nullstellen in konjugiert komplexen Paaren vor (im Sonderfall können sie reell sein). Es sei nämlich $z^\star$ eine Nullstelle. Dann gilt

$$\begin{aligned}
& a_n(z^\star)^n + a_{n-1}(z^\star)^{n-1} + \ldots + a_1(z^\star) + a_0 = 0 \\
\Rightarrow\ & \overline{a_n(z^\star)^n + a_{n-1}(z^\star)^{n-1} + \ldots + a_1(z^\star) + a_0} = 0 \\
\Rightarrow\ & \bar{a}_n(\bar{z}^\star)^n + \bar{a}_{n-1}(\bar{z}^\star)^{n-1} + \ldots + \bar{a}_1\bar{z}^\star + \bar{a}_0 = 0 \\
\Rightarrow\ & a_n(\bar{z}^\star)^n + a_{n-1}(\bar{z}^\star)^{n-1} + \ldots + a_1\bar{z}^\star + a_0 = 0, \qquad \text{(da } a_0, \ldots, a_n \text{ reell sind)}
\end{aligned}$$

so dass $\bar{z}^\star$ ebenfalls eine Nullstelle ist.

Definition

Eine **n-te Wurzel** einer komplexen Zahl a ist eine Lösung der Gleichung

$$z^n = a.$$

Beispiel

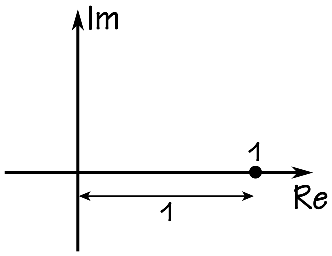
Finden Sie alle fünften Einheitswurzeln und interpretieren Sie das Ergebnis geometrisch.

Lösung

Wir müssen alle Lösungen der Gleichung

$$z^5 = 1$$

finden. Schreibe nun $z = re^{i\theta}$ und bemerke, dass $1 = 1e^{i0}$:



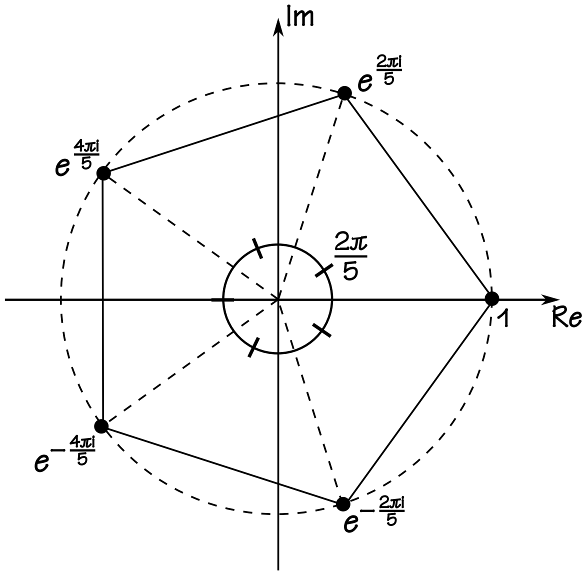
- $|1| = 1$
- $\arg(1) = 0$

Daher gilt

$$\begin{aligned}
& z^5 = 1 \\
\Leftrightarrow\ & r^5 e^{5i\theta} = 1e^{i0} \\
\Leftrightarrow\ & r^5 = 1, \qquad 5\theta = 0 + 2n\pi, \quad n = 0, \pm 1, \pm 2, \ldots \\
\Leftrightarrow\ & r = 1, \qquad \underbrace{\theta = \frac{2n\pi}{5},}_{\substack{\text{Die fünf Werte dieses Ausdrucks in} \\ (-\pi,\pi] \text{ sind } 0,\ \frac{2\pi}{5},\ \frac{4\pi}{5},\ -\frac{2\pi}{5},\ -\frac{4\pi}{5}}} \quad n = 0, \pm 1, \pm 2, \ldots.
\end{aligned}$$

Die fünften Einheitswurzel sind also

$$\underbrace{e^{i0},}_{=1} \quad e^{\frac{2\pi i}{5}}, \quad e^{\frac{4\pi i}{5}}, \quad e^{-\frac{2\pi i}{5}}, \quad e^{-\frac{4\pi i}{5}}.$$



Die Wurzeln sind fünf gleichmäßig verteilte Punkte auf einem Kreis mit Mittelpunkt 0 und Radius 1.

Sie bilden die Eckpunkte eines regelmäßigen Fünfecks.

Das folgende Lemma wird durch die Methode im obigen Beispiel bewiesen.

Lemma

Es sei n eine natürliche Zahl und a eine von Null verschiedene komplexe Zahl. Dann hat a genau n verschiedene n-te Wurzeln.

Falls $n \geq 3$ ist, so sind sie n gleichmäßig verteilte Punkte auf einem Kreis mit Mittelpunkt 0 und Radius $|a|^{1/n}$. Sie bilden somit ein regelmäßiges n-Eck.

Proposition

Es seien a, b, c konstante komplexe Zahlen mit $a \neq 0$. Das quadratische Polynom

$$az^2 + bz + c$$

besitzt

- genau die eine Nullstelle $-b/(2a)$, falls $b^2 - 4ac = 0$,
- genau die zwei Nullstellen $-b/(2a) + z_1$, $-b/(2a) + z_2$ wobei z_1, z_2 die beiden Wurzeln aus $(b^2 - 4ac)/(4a^2)$ sind, falls $b^2 - 4ac \neq 0$.

Beweis

Quadratische Ergänzung ergibt

$$az^2 + bz + c = a\left(z + \frac{b}{2a}\right)^2 - \left(\frac{b^2}{4a} - c\right). \qquad \square$$

Bemerkung

Da $z_2 = -z_1$ ist, missbrauchen wir oft die Notation und fassen die obige Proposition als

$$z = -\frac{b}{2a} \pm \sqrt{\frac{b^2 - 4ac}{4a^2}}$$

zusammen, wobei $\sqrt{(b^2 - 4ac)/4a^2}$ entweder für z_1 oder für z_2 steht.

Beispiel

Finden Sie alle komplexen Nullstellen des Polynoms

$$z^3 - 3z^2 + 4z - 2.$$

Lösung

1 ist offenbar eine Nullstelle, so dass $(z-1)$ Faktor des Polynoms ist. Aus der Rechnung

$$\begin{array}{r|l}
 & z^2 - 2z + 2 \\
\hline
z - 1 & z^3 - 3z^2 + 4z - 2 \\
 & z^3 - z^2 \\
\hline
 & -2z^2 + 4z - 2 \\
 & -2z^2 + 2z \\
\hline
 & 2z - 2 \\
 & 2z - 2 \\
\hline
 & 0
\end{array}$$

folgt
$$z^3 - 3z^2 + 4z - 2 = (z-1)(z^2 - 2z + 2).$$
Die Nullstellen des Polynoms
$$z^2 - 2z + 2$$
finden wir mit Hilfe der Formel aus der letzten Proposition. Sie sind
$$\frac{2}{2} \pm \sqrt{\frac{4 - 4.1.2}{4}} \;=\; 1 \pm \sqrt{-1} \;=\; 1 \pm \mathrm{i}.$$

Damit ist
$$z^3 - 3z^2 + 4z - 2 = (z-1)(z-1-\mathrm{i})(z-1+\mathrm{i}). \qquad \square$$

3 Folgen und Reihen

3.1 Folgen

Informell formuliert ist eine Folge eine unendliche (geordnete) Liste von Zahlen:

$$\begin{array}{ll} 1, \tfrac{1}{2}, \tfrac{1}{3}, \tfrac{1}{4}, \tfrac{1}{5}, \ldots & \text{Folge} \\ \uparrow\ \uparrow\ \uparrow\ \uparrow\ \uparrow & \\ 1\ \ 2\ \ 3\ \ 4\ \ 5 & \text{Position in der Folge} \end{array}$$

Definition

Eine **(reelle) Folge** ist eine Funktion $\mathbb{N} \to \mathbb{R}$.

Die obige Folge ist die Funktion $a : \mathbb{N} \to \mathbb{R}$ mit

$$a(n) = \frac{1}{n}.$$

Notation

$a : \mathbb{N} \to \mathbb{R}$ sei eine Folge.

In der Regel kürzen wir “$a(n)$” auf “a_n” ab, und statt “$a : \mathbb{N} \to \mathbb{R}$” schreiben wir “$\{a_n\}$” (in Anlehnung an die informelle Definition einer Folge als geordnete Liste).

Die obige Folge wird also geschrieben als

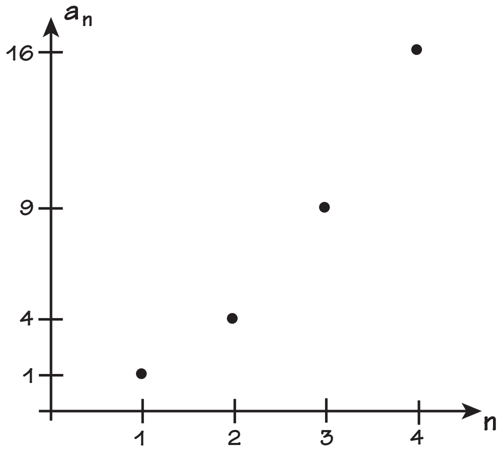
$$\{a_n\}, \qquad a_n = \frac{1}{n}$$

oder einfach

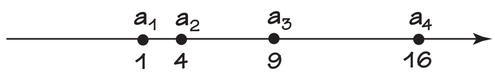
$$\left\{\frac{1}{n}\right\}.$$

Beispiele

1. Die Folge $\{a_n\}$, $a_n = n^2$ “wächst” mit zunehmenden Werten von n:

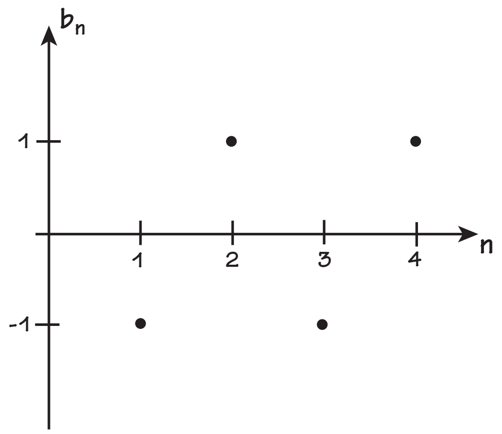


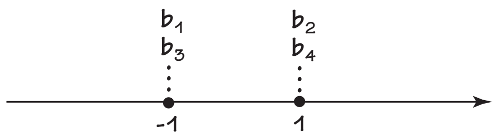
Da eine Folge nur eine Funktion ist, können wir ihren Graphen zeichnen.



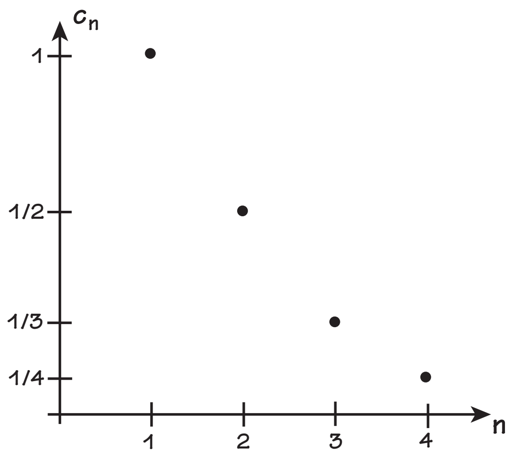
Die Funktionswerte a_n können wir ebenfalls auf einer Zahlengeraden eintragen.

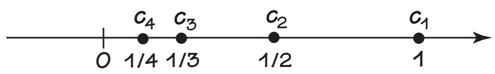
2. Die Folge $\{b_n\}$, $b_n = (-1)^n$ “oszilliert” zwischen -1 und 1:





3. Die Folge $\{c_n\}$, $c_n = \frac{1}{n}$ “konvergiert” gegen 0:





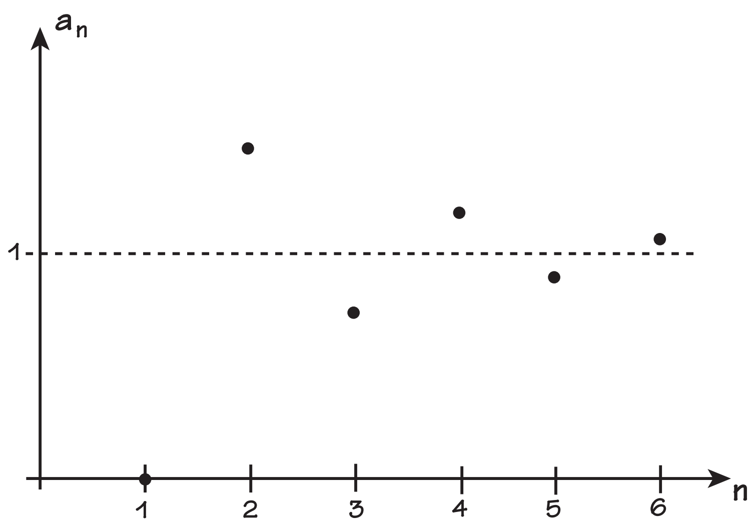
Konvergenz

Was bedeutet die Aussage “$\{a_n\}$ konvergiert gegen ℓ”?

Informelle Antwort: Je größer der Wert von n, desto näher kommt a_n an ℓ, vielleicht ohne ℓ jemals zu erreichen.

Beispiel

Betrachte die Folge $\{a_n\}$, $a_n = 1 + (-1)^n/n$:



Aus dem Diagramm folgt, dass der Abstand zwischen a_n und 1, also $|a_n - 1|$, beliebig klein wird:

- $|a_n - 1| < \frac{1}{2}$ für $n > 2$
- $|a_n - 1| < \frac{1}{10}$ für $n > 10$
- $|a_n - 1| < \frac{1}{50}$ für $n > 50$

Und tatsächlich: Wenn wir einen größten Wert ε für den Abstand $|a_n - 1|$ vorschreiben, können wir immer einen kleinsten Wert N für n finden, so dass

- $|a_n - 1| < \varepsilon$ für $n > N$

(N kann jede natürliche Zahl sein, die größer als $1/\varepsilon$ ist)

Definition

Eine reelle Folge $\{a_n\}$ **konvergiert** gegen den **Grenzwert** oder **Limes** ℓ, wenn es zu jedem $\varepsilon > 0$ eine natürliche Zahl N gibt mit

$$|a_n - \ell| < \varepsilon \quad \text{für alle } n > N.$$

In diesem Fall schreiben wir

$$a_n \to \ell \quad \text{für} \quad n \to \infty$$

und

$$\ell = \lim_{n \to \infty} a_n.$$

Hat die Folge $\{a_n\}$ einen Grenzwert, so heißt die Folge **konvergent**. Ansonsten ist sie **divergent**.

Beispiele

1. Eine konstante Folge $\{a_n\}$, $a_n = a$ konvergiert gegen a.

   Bemerke, dass $|a_n - a| = 0$ ist. Für jedes $\varepsilon > 0$ gilt also

   $$|a_n - a| < \varepsilon \quad \text{für alle} \quad n > 1.$$

2. Die Folge $\left\{\frac{1}{n}\right\}$ konvergiert gegen 0.

   Die Archimedische Eigenschaft der reellen Zahlen besagt: Zu jedem $\varepsilon > 0$ existiert eine natürliche Zahl N mit

   $$\frac{1}{N} < \varepsilon.$$

   Daher gilt:

   $$\left|\frac{1}{n} - 0\right| = \frac{1}{n} < \frac{1}{N} < \varepsilon \qquad \text{für alle} \quad n > N.$$

3. Es sei $k > 0$. Die Folge $\left\{\frac{1}{n^k}\right\}$ konvergiert gegen 0.

   Der Archimedischen Eigenschaft der reellen Zahlen zufolge gibt es zu jedem $\varepsilon > 0$ eine natürliche Zahl N mit

   $$\frac{1}{N} < \varepsilon^{\frac{1}{k}}.$$

   Daher gilt:

   $$\left|\frac{1}{n^k} - 0\right| = \frac{1}{n^k} < \frac{1}{N^k} < \varepsilon \qquad \text{für alle} \quad n > N.$$

4. Die Folgen $\left\{\frac{1}{n!}\right\}$ and $\left\{\frac{1}{a^n}\right\}$, wobei $|a| > 1$, konvergieren gegen 0.

   Hier nutzen wir die folgenden Fakten aus:

   - $n! \geq n$ für alle $n \in \mathbb{N}$ (Beweis durch vollständige Induktion).
   - Es existiert eine natürliche Zahl N_1, so dass $|a|^n \geq n$ für alle $n > N_1$ ist. (Dies wird unten unter ‘Größenordnungen’ bewiesen.)

   Aus Beispiel 2 wissen wir: Zu jedem $\varepsilon > 0$ existiert eine natürliche Zahl N_2 mit

   $$\frac{1}{n} < \varepsilon \qquad \text{für alle} \quad n > N_2.$$

Definiere $N_1 = 1$ in dem ersten Fall. Es gilt

$$\left\{\begin{matrix} \left|\dfrac{1}{n!} - 0\right| \\ \\ \left|\dfrac{1}{a^n} - 0\right| \end{matrix}\right\} = \left\{\begin{matrix} \dfrac{1}{n!} \\ \\ \dfrac{1}{|a|^n} \end{matrix}\right\} \underset{\substack{\text{falls} \\ n > N_1}}{\underset{\uparrow}{\leq}} \frac{1}{n} \underset{\substack{\text{falls} \\ n > N_2}}{\underset{\uparrow}{<}} \varepsilon$$

für alle $n > N := \max(N_1, N_2)$.

Lemma

Der Grenzwert einer konvergenten Folge ist eindeutig.

Beweis

$\{a_n\}$ sei eine konvergente Folge mit $a_n \to \ell_1$ und $a_n \to \ell_2$ für $n \to \infty$. Dann gilt:

Zu jedem $\varepsilon_1 > 0$ existiert $N_1 \in \mathbb{N}$ mit $\lvert a_n - \ell_1\rvert < \varepsilon_1$ für $n > N_1$	Zu jedem $\varepsilon_2 > 0$ existiert $N_2 \in \mathbb{N}$ mit $\lvert a_n - \ell_2\rvert < \varepsilon_2$ für $n > N_2$

Bemerke, dass

$$\begin{aligned} |\ell_1 - \ell_2| &= |\ell_1 - a_n + a_n - \ell_2| \\ &\leq |a_n - \ell_1| + |a_n - \ell_2| && \text{(Dreiecksungleichung)} \\ &< \varepsilon_1 + \varepsilon_2 && \text{für } n > \max(N_1, N_2) \end{aligned}$$

Nun wählen wir $\varepsilon > 0$ und setzen $\varepsilon_1 = \frac{\varepsilon}{2}$, $\varepsilon_2 = \frac{\varepsilon}{2}$, so dass

$$0 \leq |\ell_1 - \ell_2| < \varepsilon.$$

Da diese Ungeichung für jedes $\varepsilon > 0$ gilt, ist

$$|\ell_1 - \ell_2| = 0$$

gelten. Es ist also $\ell_1 = \ell_2$. $\square$

Definitionen

1. Eine Folge $\{a_n\}$ ist **nach oben (unten) beschränkt**, falls es eine reelle Zahl $M_1(M_2)$ mit der Eigenschaft

$$a_n \leq M_1 \quad (a_n \geq M_2) \qquad \text{für alle } n \in \mathbb{N}$$

gibt.

2. Eine Folge $\{a_n\}$ ist **beschränkt**, falls sie nach oben und nach unten beschränkt ist.

Bemerkung

$$\begin{array}{l} \text{Es existieren } M_1, M_2 \in \mathbb{R} \text{ mit} \\ M_1 \leq a_n \leq M_2 \text{ für alle } n \in \mathbb{N} \end{array} \quad \Leftrightarrow \quad \begin{array}{l} \text{Es existiert } M > 0 \text{ mit} \\ -M \leq a_n \leq M \text{ für alle } n \in \mathbb{N} \end{array}$$

Eine Folge ist also genau dann beschränkt, wenn es $M > 0$ mit $|a_n| \leq M$ für jedes $n \in \mathbb{N}$ gibt.

Lemma

Jede konvergente Folge ist beschränkt.

Beweis

$\{a_n\}$ konvergiere gegen ℓ. Dann existiert eine natürliche Zahl N mit der Eigenschaft

$$\begin{aligned} |a_n - \ell| &< 1 \qquad \text{für alle } n > N \\ \Rightarrow \ell - 1 < a_n &< \ell + 1 \qquad \text{für alle } n > N \end{aligned}$$

Nun definieren wir

$$\begin{aligned} M_1 &= \min\{a_1, \ldots, a_N, \ell - 1\}, \\ M_2 &= \max\{a_1, \ldots, a_N, \ell + 1\}, \end{aligned}$$

so dass

$$M_1 \leq a_n \leq M_2 \qquad \text{für alle } n \in \mathbb{N}.$$

□

Satz (Rechenregeln für konvergente Folgen)

$\{a_n\}, \{b_n\}, \{c_n\}$ seien konvergente Folgen mit $c_n \neq 0$, $n \in \mathbb{N}$ und $\lim\limits_{n\to\infty} c_n \neq 0$. α sei eine reelle Zahl.

Dann sind $\{\alpha a_n\}, \{a_n + b_n\}, \{a_n b_n\}, \left\{\frac{1}{c_n}\right\}$ ebenfalls konvergent, und es gilt

$$\lim_{n\to\infty} \alpha\, a_n = \alpha \lim_{n\to\infty} a_n, \tag{1}$$

$$\lim_{n\to\infty} (a_n + b_n) = \lim_{n\to\infty} a_n + \lim_{n\to\infty} b_n, \tag{2}$$

$$\lim_{n\to\infty} a_n b_n = \lim_{n\to\infty} a_n \lim_{n\to\infty} b_n, \tag{3}$$

$$\lim_{n\to\infty} \frac{1}{c_n} = \frac{1}{\lim\limits_{n\to\infty} c_n}. \tag{4}$$

Beweis

Wir beweisen die dritte Aussage. Definiere

$$a := \lim_{n\to\infty} a_n,$$
$$b := \lim_{n\to\infty} b_n.$$

Wir wissen:

Zu jedem $\varepsilon_1 > 0$ existiert $N_1 \in \mathbb{N}$ mit $|a_n - a| < \varepsilon_1$ for $n > N_1$

Zu jedem $\varepsilon_2 > 0$ existiert $N_2 \in \mathbb{N}$ mit $|b_n - b| < \varepsilon_2$ for $n > N_2$

Wir wollen beweisen:

Zu jedem $\varepsilon > 0$ existiert $N \in \mathbb{N}$ mit

$$|a_n b_n - ab| < \varepsilon \qquad \text{für } n > N.$$

Wir können

$$a_n b_n - ab = (a_n - a)b_n + a(b_n - b)$$

schreiben, so dass

$$\begin{aligned} |a_n b_n - ab| &= |(a_n - a)b_n + a(b_n - b)| \\ &\leq |(a_n - a)b_n| + |a(b_n - b)| \qquad \text{(Dreiecksungleichung)} \\ &= |a_n - a||b_n| + |a||b_n - b|. \end{aligned}$$

Weil $\{b_n\}$ konvergent ist, ist sie beschränkt. Es existiert also $M > 0$ mit

$$|b_n| \leq M \qquad \text{für jedes } n \in \mathbb{N}$$

und daher

$$|a_n b_n - ab| < M\varepsilon_1 + |a|\varepsilon_2 \qquad \text{für jedes } n > N,$$

wobei $N := \max(N_1, N_2)$ ist.

Nun wählen wir $\varepsilon > 0$ und setzen

$$\begin{aligned} \varepsilon_1 &= \frac{\varepsilon}{2M}, \qquad & \varepsilon_2 &= \frac{\varepsilon}{2|a|}, \qquad & &\text{falls } |a| \neq 0, \\ \varepsilon_1 &= \frac{\varepsilon}{M}, \qquad & \varepsilon_2 &= 1, \qquad & &\text{falls } |a| = 0. \end{aligned}$$

Dann gilt:

$$|a_n b_n - ab| < \varepsilon \qquad \text{für jedes } n > N.$$

Die anderen Aussagen werden in ähnlicher Weise beweisen. □

Beispiel

Zeigen Sie:

$$\lim_{n\to\infty} \frac{3n^3 + 7n^2 + 1}{4n^3 - 8n + 63} = \frac{3}{4}.$$

Lösung

Es gilt:

$$\begin{aligned} \frac{3n^3 + 7n^2 + 1}{4n^3 - 8n + 63} &= \frac{3 + \frac{7}{n} + \frac{1}{n^3}}{4 - \frac{8}{n^2} + \frac{63}{n^3}} \\ &\to \frac{3}{4} \qquad \text{für } n \to \infty, \end{aligned}$$

weil

$$\frac{1}{n}, \frac{1}{n^2}, \frac{1}{n^3} \to 0 \qquad \text{für } n \to \infty.$$

□

Folgendes Ergebnis ist oft sehr hilfreich.

Lemma

$\{a_n\}, \{b_n\}, \{c_n\}$ seien Folgen mit

$$a_n \to \ell, \ c_n \to \ell \qquad \text{für } n \to \infty$$

und

$$a_n \le b_n \le c_n, \qquad n \in \mathbb{N}.$$

Dann ist $\{b_n\}$ ebenfalls konvergent und

$$b_n \to \ell \qquad \text{für } n \to \infty.$$

Beweis

Wir wissen:

Zu jedem $\varepsilon_1 > 0$ existiert $N_1 \in \mathbb{N}$, so dass

$$|a_n - \ell| < \varepsilon_1 \qquad \text{für } n > N_1$$

d.h.

$$\ell - \varepsilon_1 < a_n < \ell + \varepsilon_1 \qquad \text{für } n > N_1$$

Zu jedem $\varepsilon_2 > 0$ existiert $N_2 \in \mathbb{N}$, so dass

$$|c_n - \ell| < \varepsilon_2 \qquad \text{für } n > N_2$$

d.h.

$$\ell - \varepsilon_2 < c_n < \ell + \varepsilon_2 \qquad \text{für } n > N_2$$

Wir wollen beweisen:

Zu jedem $\varepsilon > 0$ existiert $N \in \mathbb{N}$ mit

$$|b_n - \ell| < \varepsilon \qquad \text{für } n > N$$

d.h.

$$\ell - \varepsilon < b_n < \ell + \varepsilon \qquad \text{für } n > N$$

Es gilt

$$\ell - \varepsilon_1 \underset{\substack{\uparrow \\ \text{für } n > N_1}}{<} a_n \le b_n \le c_n \underset{\substack{\uparrow \\ \text{für } n > N_2.}}{<} \ell + \varepsilon_2 \qquad \text{für } n > N := \max(N_1, N_2),$$

Nun wählen wir $\varepsilon > 0$ und setzen $\varepsilon_1 = \varepsilon$, $\varepsilon_2 = \varepsilon$, so dass

$$\ell - \varepsilon < b_n < \ell + \varepsilon \qquad \text{für } n > N.$$

$\square$

Beispiel

Zeigen Sie:

$$\lim_{n\to\infty} (\sqrt{n+1} - \sqrt{n}) = 0.$$

Lösung

Bemerke:

$$\begin{aligned}
\sqrt{n+1} - \sqrt{n} &= (\sqrt{n+1} - \sqrt{n}) \left(\frac{\sqrt{n+1} + \sqrt{n}}{\sqrt{n+1} + \sqrt{n}} \right) \\
&= \frac{1}{\sqrt{n+1} + \sqrt{n}} \\
&< \frac{1}{\sqrt{n}} \qquad\qquad \text{weil } \sqrt{n+1} + \sqrt{n} > \sqrt{n} \text{ ist}
\end{aligned}$$

Aus

$$\underbrace{0}_{\substack{\to 0 \\ \text{für } n\to\infty}} < \frac{1}{\sqrt{n+1} + \sqrt{n}} < \underbrace{\frac{1}{\sqrt{n}}}_{\substack{\to 0 \\ \text{für } n\to\infty}}$$

folgt

$$\frac{1}{\sqrt{n+1} + \sqrt{n}} \to 0 \qquad \text{für } n \to \infty,$$

so dass

$$\sqrt{n+1} - \sqrt{n} \to 0 \qquad \text{für } n \to \infty.$$

□

Monotone Folgen

Definitionen

1. Eine Folge $\{a_n\}$ heißt **monoton steigend (fallend)**, falls

$$a_n \leq a_{n+1} \qquad (a_n \geq a_{n+1})$$

für jedes $n \in \mathbb{N}$.

2. Eine Folge $\{a_n\}$ heißt **streng monoton steigend (fallend)**, falls

$$a_n < a_{n+1} \qquad (a_n > a_{n+1})$$

für jedes $n \in \mathbb{N}$.

Satz

1. $\{a_n\}$ sei eine monoton steigende, nach oben beschränkte Folge. Dann ist $\{a_n\}$ konvergent.
2. $\{a_n\}$ sei eine monoton fallende, nach unten beschränkte Folge. Dann ist $\{a_n\}$ konvergent.

Beweis

1. Die Menge $M = \{a_n : n \in \mathbb{N}\}$ ist eine nicht leere, nach oben beschränkte Teilmenge von $\mathbb{R}$. Dem Vollständigkeitsaxiom von $\mathbb{R}$ zufolge hat M ein Supremum ℓ. Wir zeigen, dass $\{a_n\}$ gegen ℓ konvergiert.

   Wir benutzen folgende Eigenschaft vom Supremum s einer nichtleeren, nach oben beschränkten Menge X: Zu jedem $\varepsilon > 0$ existiert $x \in X$ mit $x > s - \varepsilon$.

   Wir wenden diese Eigenschaft von ℓ auf M an: Zu jedem $\varepsilon > 0$ existiert $N \in \mathbb{N}$ mit
   $$a_N > \ell - \varepsilon.$$
   Daher gilt:
   $$\ell + \varepsilon > \ell \underset{\substack{\uparrow \\ \ell = \sup M}}{\geq} a_n \underset{\substack{\uparrow \\ \{a_n\} \text{ ist} \\ \text{monoton steigend}}}{\geq} a_N > \ell - \varepsilon \qquad \text{für } n > N$$

   Wir haben bewiesen:

   Zu jedem $\varepsilon > 0$ existiert $N \in \mathbb{N}$, so dass
   $$|a_n - \ell| < \varepsilon \qquad \text{für } n > N.$$

Die zweite Aussage wird in ähnlicher Weise bewiesen. □

Bemerkung

Eine monoton steigende (fallende) Folge ist genau dann konvergent, wenn sie nach oben (unten) beschränkt ist.

Das folgende Ergebnis wird durch vollständige Induktion beweisen.

Satz (Rekursionssatz)

Gegeben seien eine reelle Zahl a und Funktionen $f_{n+1} : \mathbb{R}^{n+1} \to \mathbb{R}$, $n = 0,1,2,\ldots$.

Dann existiert genau eine Folge $\{x_n\}_{n\in\mathbb{N}_0}$ mit den Eigenschaften

1. $x_0 = a$;
2. $x_{n+1} = f_{n+1}(x_0,\ldots,x_n)$, $n = 0,1,2,\ldots$.

Beispiel

Es seien a und x_0 positive reelle Zahlen. Zeigen Sie, dass die durch das Rekursionsschema

$$x_{n+1} = \frac{1}{2}\left(x_n + \frac{a}{x_n}\right), \qquad n = 0,1,2,\ldots$$

definierte Folge $\{x_n\}_{n\in\mathbb{N}}$ konvergent ist, und bestimmen Sie ihren Grenzwert.

Lösung

Offenbar ist $x_n > 0$ für alle $n \in \mathbb{N}_0$ (Beweis durch vollständige Induktion). Insbesondere ist $\{x_n\}$ nach unten beschränkt.

Die Berechnung

$$x_{n+1} = \frac{1}{2}\left(x_n + \frac{a}{x_n}\right) \geq \sqrt{x_n \frac{a}{x_n}} = \sqrt{a}, \qquad n = 0,1,2,\ldots,$$

zeigt, dass $x_n^2 \geq a$ für $n = 1,2,\ldots$. Aus

$$\frac{a}{x_n} \leq x_n$$

folgt

$$x_{n+1} \;=\; \frac{1}{2}\left(x_n + \frac{a}{x_n}\right) \;\leq\; \frac{1}{2}(x_n + x_n) \;=\; x_n, \qquad n = 1,2,\ldots.$$

Die Folge $\{x_n\}_{n\in\mathbb{N}}$ is also monoton fallend.

Da $\{x_n\}_{n\in\mathbb{N}}$ monoton fallend und nach unten beschränkt ist, ist sie konvergent. Ihr Grenzwert x ist das Infimum der Menge $\{x_n : n \in \mathbb{N}\}$ und erfüllt $x \geq \sqrt{a}$. Aus der Gleichung

$$x_{n+1} = \frac{1}{2}\left(x_n + \frac{a}{x_n}\right)$$

und den Grenzwerten

$$\lim_{n\to\infty} x_n = x, \qquad \lim_{n\to\infty} x_{n+1} = x$$

folgt

$$x = \frac{1}{2}\left(x + \frac{a}{x}\right) \quad \Leftrightarrow \quad x = \pm\sqrt{a}$$

und daher $x = \sqrt{a}$. □

Divergenz

Es ist ebenfalls notwendig, die Aussagen "$\{a_n\}$ konvergiert nicht gegen l" bzw. "$\{a_n\}$ ist nicht konvergent" richtig zu formulieren.

"$\{a_n\}$ konvergiert gegen ℓ"

bedeutet

"Zu jedem $\varepsilon > 0$ existiert $N \in \mathbb{N}$, so dass
$|a_n - \ell| < \varepsilon$ für alle $n > N$" (1)

d. h.

$$\underbrace{\forall \varepsilon > 0\ \exists N \in \mathbb{N}\ \forall n > N\ |a_n - \ell| < \varepsilon}$$

Die Verneinung dieser Aussage ist

$$\exists\, \varepsilon > 0\ \forall N \in \mathbb{N}\ \exists n > N |a_n - \ell| \geq \varepsilon$$

d. h.

"Es gibt $\varepsilon > 0$, so dass für alle $N \in \mathbb{N}$
eine natürliche Zahl $n > N$ mit $|a_n - \ell| \geq \varepsilon$
existiert." (2)

Die Aussage "$\{a_n\}$ ist konvergent" bedeutet, dass es eine Zahl l mit der Eigenschaft (1) gibt. Die Aussage "$\{a_n\}$ ist divergent" ist also die Verneinung

$$\begin{aligned} & \neg\exists\ell\ (1) \\ \Leftrightarrow\quad & \forall\ell\ \neg(1) \\ \Leftrightarrow\quad & \forall\ell\ (2) \end{aligned}$$

Sie bedeutet also, dass (2) für alle Zahlen ℓ gilt.

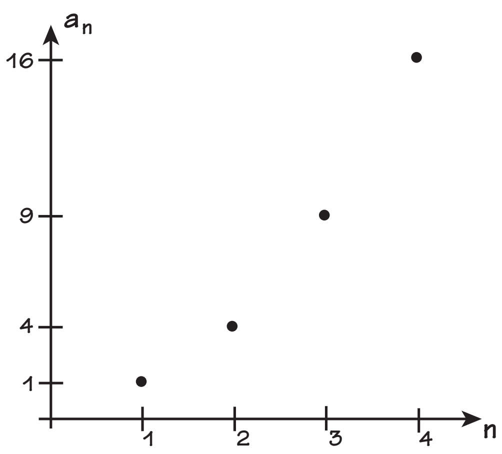
Wir setzen uns nun mit unbeschränkten Folgen auseinander. Da alle konvergenten Folgen beschränkt sind, sind unbeschränkte Folgen divergent.

Definitionen

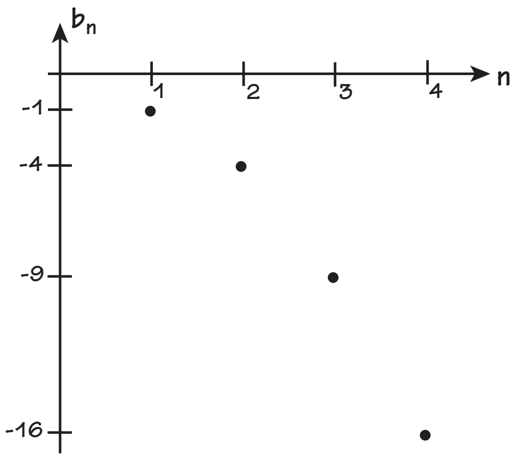
1. Wir schreiben
$$\text{“}a_n \to \infty \qquad \text{für } n \to \infty\text{”},$$
wenn es zu jedem $M > 0$ eine natürliche Zahl N gibt, so dass
$$a_n > M \qquad \text{für alle } n > N.$$

2. Wir schreiben
$$\text{“}a_n \to -\infty \qquad \text{für } n \to \infty\text{”},$$
wenn es zu jedem $M < 0$ eine natürliche Zahl N gibt, so dass
$$a_n < M \qquad \text{für alle } n > N.$$

Beispiele



Die Folge $\{a_n\}$ mit $a_n = n^2$ erfüllt $a_n \to \infty$ für $n \to \infty$.

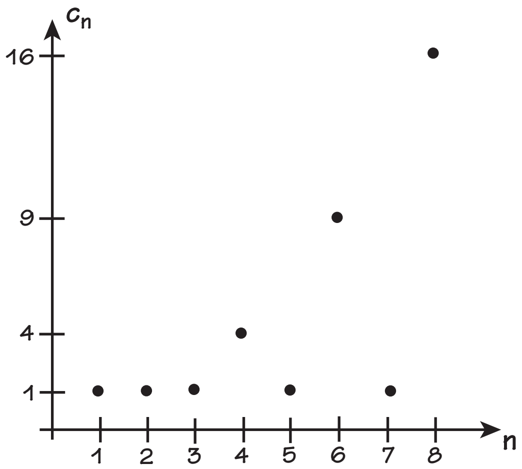


Die Folge $\{b_n\}$ mit $b_n = -n^2$ erfüllt $b_n \to -\infty$ für $n \to \infty$.

Bemerkung

Dass eine Folge $\{a_n\}$ nicht nach oben (unten) beschränkt ist, impliziert nicht $a_n \to \infty$ ($a_n \to -\infty$) für $n \to \infty$.

Die Folge $\{c_n\}$ mit $c_{2m+1} = 1$, $m = 0,1,2,\ldots$ und $c_{2m} = m^2$, $m = 1,2,\ldots$ ist nicht nach oben beschränkt, erfüllt jedoch nicht $c_n \to \infty$ für $n \to \infty$.



Lemma

1. Die Folge $\{a_n\}$ erfülle $|a_n| \to \infty$ für $n \to \infty$. Dann gilt $1/a_n \to 0$ für $n \to \infty$.

2. Die Folge $\{b_n\}$ erfülle $b_n \neq 0$, $n \in \mathbb{N}$ und $b_n \to 0$ für $n \to \infty$. Dann gilt $1/|b_n| \to \infty$ für $n \to \infty$.

Beweis

1. Wir wissen:

   Zu jedem $M > 0$ existiert $N_1 \in \mathbb{N}$, so dass
$$|a_n| > M \qquad \text{für } n > N_1.$$

Wir wollen beweisen:

Zu jedem $\varepsilon > 0$ existiert $N \in \mathbb{N}$, do dass

$$\left|\frac{1}{a_n}\right| < \varepsilon \qquad \text{für } n > N.$$

Wähle $\varepsilon > 0$ und setze $M = 1/\varepsilon$. Laut Voraussetzung existiert $N_1 \in \mathbb{N}$, so dass

$$|a_n| > \frac{1}{\varepsilon} \qquad \text{für } n > N_1.$$

Daraus folgt:

$$\left|\frac{1}{a_n}\right| = \frac{1}{|a_n|} < \varepsilon \qquad \text{für } n > N := N_1.$$

2. Diese Aussage wird in ähnlicher Weise bewiesen. □

Beispiele

1. Aus dem zweiten Teil des letzten Lemmas folgt

$$\begin{aligned}
&n^k \to \infty && \text{für } n \to \infty, \quad k > 0, \\
&|a|^n \to \infty && \text{für } n \to \infty, \quad |a| > 1, \\
&n! \to \infty && \text{für } n \to \infty.
\end{aligned}$$

2. Aus

$$n^n \geq n, \qquad n \in \mathbb{N}$$

(Beweis durch vollständige Induktion) folgt $n^n \to \infty$ für $n \to \infty$.

3. Später untersuchen wir den Logarithmus und zeigen insbesondere, dass $\log n \to \infty$ für $n \to \infty$.

Lemma (Größenordnungen)

Es seien a und k reelle Zahlen mit $|a| > 1$ und $k > 0$. Es gelten folgende Regeln:

$$\frac{\log n}{n^k} \to 0 \text{ für } n \to \infty \qquad \text{“Potenzen schlagen Logarithmen”}$$

$$\frac{n^k}{|a|^n} \to 0 \text{ für } n \to \infty \qquad \text{“Exponentiale schlagen Potenzen”}$$

$$\frac{|a|^n}{n!} \to 0 \text{ für } n \to \infty \qquad \text{“Fakultäten schlagen Exponentiale”}$$

$$\frac{n!}{n^n} \to 0 \text{ für } n \to \infty \qquad \text{“Superexponentiale schlagen Fakultäten”}$$

Beweis

- Die ersten zwei Behauptungen werden später bewiesen.
- Wähle $m \in \mathbb{N}$, so dass $m < |a| \leq m+1$ ist. Es sei $n \geq m+1$. Dann gilt

$$\frac{|a|^n}{n!} = \frac{|a|}{1} \cdot \frac{|a|}{2} \cdot \ldots \cdot \frac{|a|}{m} \cdot \underbrace{\frac{|a|}{m+1}}_{\leq 1} \cdots \underbrace{\frac{|a|}{n-1}}_{\leq 1} \cdot \frac{|a|}{n} \leq \frac{|a|^m}{m!} \cdot \frac{|a|}{n},$$

  und aus

$$\underbrace{0}_{\to 0} < \frac{|a|^n}{n!} \leq \underbrace{\frac{|a|^m}{m!} \cdot \frac{|a|}{n}}_{\to 0}$$

  folgt

$$\frac{|a|^n}{n!} \to 0$$

  für $n \to \infty$.
- Dies ist eine Übungsaufgabe (Blatt 8, Aufgabe 1(e)). $\square$

Teilfolgen

Definition

Eine **Teilfolge** der Folge

$$a_1, a_2, a_3, a_4, \ldots \qquad \text{(Schreibweise: } \{a_n\}\text{)}$$

ist eine Folge der Form

$$a_{n_1}, a_{n_2}, a_{n_3}, \ldots, \qquad \text{(Schreibweise: } \{a_{n_k}\}\text{)}$$

wobei

$$n_1, n_2, n_3, \ldots$$

eine streng monoton steigende Folge natürlicher Zahlen ist.

Beispiel

Die Folge

$$1, 3, 5, 7, \ldots$$

ist Teilfolge der Folge

$$1, 2, 3, 4, 5, 6, 7, \ldots$$

Bemerkung

Eine Teilfolge erbt gewisse Eigenschaften der ursprünglichen Folge, z. B.

$$\begin{array}{lcl} \{a_n\} \text{ konvergiert gegen } l & \Rightarrow & \{a_{n_k}\} \text{ konvergiert gegen } l \\ \{a_n\} \text{ ist beschränkt} & \Rightarrow & \{a_{n_k}\} \text{ ist beschränkt} \end{array}$$

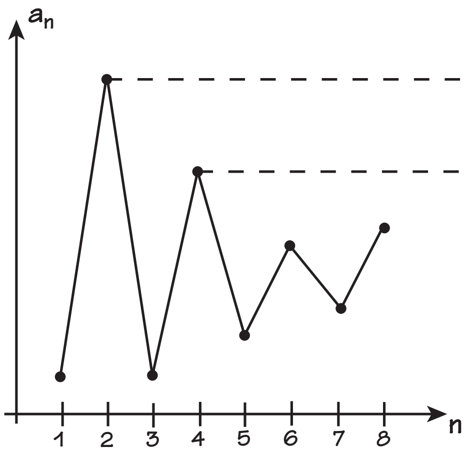
Eine Teilfolge kann aber "besser" als die ursprüngliche Folge sein.

Lemma

Jede Folge $\{a_n\}$ enthält eine Teilfolge, die entweder monoton steigend oder monoton fallend ist.

Beweis

Wir nennen die natürliche Zahl n einen “Aussichtspunkt” der Folge $\{a_n\}$, falls $a_m < a_n$ für alle $m > n$:



2 und 4 sind Aussichtspunkte dieser Folge.

Wir unterscheiden zwei Fälle:

- $\{a_n\}$ hat unendlich viele Aussichtspunkte

  $$n_1 < n_2 < n_3 < \dots$$

  In diesem Fall ist die Folge $\{a_{n_k}\}$ eine streng monoton fallende Teilfolge von $\{a_n\}$.

- $\{a_n\}$ hat nur endlich viele Aussichtspunkte.

  In diesem Fall konstruieren wir eine monoton steigende Teilfolge $\{a_{n_k}\}$ von $\{a_n\}$ durch die folgende Methode.

  Wähle n_1 größer als alle Aussichtspunkte.

  Für $k \geq 1$ wähle n_{k+1}, so dass $a_{n_{k+1}} \geq a_{n_k}$ ist. (Dies ist möglich, weil n_k kein Aussichtspunkt ist.) $\square$

Korollar (Satz von Bolzano-Weierstraß)

Jede beschränkte Folge hat eine konvergente Teilfolge.

Beweis

Jede beschränkte Folge hat entweder eine monoton steigende Teilfolge oder eine monoton fallende Teilfolge. Diese Teilfolge erbt die Beschränktheit der ursprunglichen Folge und ist daher konvergent. □

Cauchy-Folgen

Falls eine Folge $\{a_n\}$ konvergiert, liegt a_n für großes n nahe am Grenzwert. Die Differenz $a_n - a_m$ soll also für große m,n fast Null sein. In diesem Abschnitt zeigen wir, dass diese Eigenschaft eine konvergente Folge in der Tat charakterisiert.

Definition

Eine Folge $\{a_n\}$ heißt **Cauchy-Folge**, falls es zu jedem $\varepsilon > 0$ eine natürliche Zahl N mit der Eigenschaft

$$|a_m - a_n| < \varepsilon \qquad \text{für alle } m,n > N$$

gibt.

Lemma

Jede konvergente Folge ist eine Cauchy-Folge.

Beweis

$\{a_n\}$ sei eine konvergente Folge mit Grenzwert l.

Wir wissen:

Zu jedem $\varepsilon_1 > 0$ existiert also $N_1 \in \mathbb{N}$, so dass

$$|a_n - l| < \varepsilon_1 \qquad \text{für } n > N_1.$$

Wir wollen beweisen:

Zu jedem $\varepsilon > 0$ existiert also $N \in \mathbb{N}$, so dass

$$|a_n - a_m| < \varepsilon \qquad \text{für } n,m > N.$$

Es gilt

$$\begin{aligned} |a_n - a_m| &= |a_n - l - (a_m - l)| \\ &\leq |a_n - l| + |a_m - l| \\ &< 2\varepsilon_1 \qquad \text{für } m,n > N_1. \end{aligned}$$

Wähle $\varepsilon > 0$ und setze $\varepsilon_1 = \frac{\varepsilon}{2}$, so dass

$$|a_n - a_m| < \varepsilon \qquad \text{für } n,m > N := N_1.$$

□

Um die Umkehrung zu beweisen, brauchen wir zwei Hilfslemmata.

Lemma

$\{a_{n_k}\}$ sei eine Teilfolge der Cauchy-Folge $\{a_n\}$ mit $a_{n_k} \to l$ für $n_k \to \infty$. Dann konvergiert $\{a_n\}$ ebenfalls gegen l.

Beweis

Wir wissen:

Zu jedem $\varepsilon_1 > 0$ existiert $N_1 \in \mathbb{N}$ mit $\lvert a_n - a_m \rvert < \varepsilon_1$ für $m,n > N_1$	Zu jedem $\varepsilon_2 > 0$ existiert $N_2 \in \mathbb{N}$ mit $\lvert a_{n_k} - l \rvert < \varepsilon_2$ für $n_k > N_2$

Wir wollen beweisen:

Zu jedem $\varepsilon > 0$ existiert $N \in \mathbb{N}$, so dass

$$|a_n - l| < \varepsilon \quad \text{für } n > N.$$

Es gilt:

$$\begin{aligned} |a_n - l| &= |a_n - a_{n_k} + a_{n_k} - l| \\ &\leq |a_n - a_{n_k}| + |a_{n_k} - l| \\ &< \varepsilon_1 + \varepsilon_2 \qquad \text{für } n, n_k > N_1,\ n_k > N_2. \end{aligned}$$

Wähle $\varepsilon > 0$ und setze $\varepsilon_1 = \frac{\varepsilon}{2}, \varepsilon_2 = \frac{\varepsilon}{2}$, so dass

$$|a_n - l| < \varepsilon \qquad \text{für } n > N := \max(N_1, N_2).$$

□

Lemma

Jede Cauchy-Folge ist beschränkt.

Beweis

$\{a_n\}$ sei eine Cauchy-Folge. Es existiert also $N \in \mathbb{N}$, so dass

$$|a_n - a_m| < 1 \qquad \text{für } n, m > N.$$

Insbesondere gilt

$$|a_n - a_{N+1}| < 1 \qquad \text{für } n > N$$

und daher

$$a_{N+1} - 1 < a_n < a_{N+1} + 1 \qquad \text{für } n > N.$$

Nun definieren wir

$$\begin{aligned} M_1 &= \min\{a_1, \dots, a_N, a_{N+1} - 1\}, \\ M_2 &= \max\{a_1, \dots, a_N, a_{N+1} + 1\}, \end{aligned}$$

so dass

$$M_1 \leq a_n \leq M_2 \qquad \text{für } n \in \mathbb{N}.$$

□

Korollar

Jede Cauchy-Folge ist konvergent.

Beweis

Jede Cauchy-Folge ist beschränkt und enthält daher wegen des Satzes von Bolzano-Weierstraß eine konvergente Teilfolge. Aber eine Cauchy-Folge mit einer konvergenter Teilfolge ist selber konvergent. □

3.2 Reihen

In diesem Abschnitt behandeln wir "unendliche Summen" der Form

$$a_1 + a_2 + a_3 + \dots$$

Wir brauchen zunächst eine vernünftige Definition solcher Summen.

Definitionen

$\{a_n\}$ sei eine reelle Folge. Die Folge $\{s_n\}$ mit

$$\begin{aligned} s_1 &= a_1, \\ s_2 &= a_1 + a_2, \\ s_3 &= a_1 + a_2 + a_3, \\ &\vdots \end{aligned}$$

ist **die zu $\{a_n\}$ gehörende Reihe**. Das n-te Glied s_n heißt **n-te Partialsumme** der Reihe $\{s_n\}$.

Falls $\{s_n\}$ konvergiert, heißt ihr Grenzwert die **Summe** der Reihe, und in diesem Fall schreiben wir

$$\lim_{n\to\infty} s_n$$

als

$$\sum_{n=1}^{\infty} a_n.$$

Beispiele

1. **Die geometrische Reihe**

   Gegeben seien reelle Zahlen a, r mit $|r| < 1$. Daraus bilden wir die Folge $\{ar^{n-1}\}$ und die dazugehörende Reihe $\{s_n\}$ mit

$$
\begin{aligned}
s_n &= a + ar + ar^2 + \ldots + ar^{n-1} \\
&= a\frac{1-r^n}{1-r} \qquad \text{(Beweis durch vollständige Induktion)}
\end{aligned}
$$

Es gilt

$$
\begin{aligned}
\lim_{n\to\infty} s_n = \lim_{n\to\infty} \frac{a(1-r^n)}{1-r} \\
= \frac{a}{1-r}, \qquad \text{weil} \qquad r^n \to 0 \text{ für } n \to \infty,
\end{aligned}
$$

so dass

$$
\sum_{n=1}^{\infty} ar^{n-1} = \frac{a}{1-r}.
$$

Betrachte insbesondere den Fall $a = \frac{9}{10}, r = \frac{1}{10}$:

$$
\sum_{n=1}^{\infty} 9.10^{-n} = 1,
$$

d. h.

$$
\underbrace{\frac{9}{10} + \frac{9}{100} + \frac{9}{1000} + \ldots}_{\textbf{Definition} \text{ der Dezimalzahl } 0{,}9999\ldots} \qquad = 1
$$

2. **Die harmonische Reihe**

Betrachte die Folge $\left\{\frac{1}{n}\right\}$ und die dazugehörende Reihe $\{s_n\}$ mit

$$
s_n = 1 + \frac{1}{2} + \frac{1}{3} + \ldots + \frac{1}{n}.
$$

Es gilt:

$$
\begin{aligned}
s_{2n} - s_n &= \frac{1}{n+1} + \frac{1}{n+2} + \ldots + \frac{1}{2n} \\
&\geq \frac{1}{2n} + \frac{1}{2n} + \ldots + \frac{1}{2n} \\
&= \frac{n}{2n} \\
&= \frac{1}{2}
\end{aligned}
$$

$\{s_n\}$ ist also keine Cauchy-Folge ($|s_m - s_n|$ wird nicht beliebig klein für große Werte von m,n) und ist daher nicht konvergent.

Notation

Es ist üblich, von der obigen rigorosen Notation abzuweichen und die zur Folge $\{a_n\}$ gehörende Reihe einfach als

$$\sum_{n=1}^{\infty} a_n$$

zu schreiben. Man schreibt z. B.

- Die Reihe $\sum\limits_{n=1}^{\infty} ar^{n-1}$ mit $|r| < 1$ ist konvergent.
- Die Reihe $\sum\limits_{n=1}^{\infty} \frac{1}{n}$ ist divergent.

Demnach bedeutet die Notation

$$\sum_{n=1}^{\infty} a_n$$

zweierlei: erstens die Reihe selbst (d. h. die Partialsummenfolge), zweitens die Summe der Reihe (d. h. den Grenzwert der Partialsummenfolge).

Bemerkung

$\{a_n\}$ sei eine Folge und $\{s_n\}$ sei die dazugehörende Partialsummenfolge. Es ist hilfreich, die Aussagen (i) $s_n \to s$ für $n \to \infty$; (ii) $\{s_n\}$ ist eine Cauchy-Folge in der neuen Notation zu formulieren:

(i) $\sum\limits_{k=1}^{\infty} a_k$ ist konvergent mit Summe s, falls es zu jedem $\varepsilon > 0$ eine natürliche Zahl N gibt, so dass

$$\underbrace{\left|\sum_{k=1}^{n} a_k - s\right|}_{= s_n - s} < \varepsilon \qquad \text{für } n > N.$$

(ii) $\sum\limits_{k=1}^{\infty} a_k$ erfüllt das Cauchy-Kriterium, falls es zu jedem $\varepsilon > 0$ eine natürliche Zahl N gibt, so dass

$$\underbrace{\left|\sum_{k=n+1}^{m} a_k\right|}_{= s_m - s_n} < \varepsilon \qquad \text{für } m > n > N.$$

Folgendes Ergebnis kann nützlich sein, um die Konvergenz einer Reihe auszuschließen.

Lemma

$\sum\limits_{n=1}^{\infty} a_n$ sei eine konvergente Reihe. Dann gilt

$$a_n \to 0 \qquad \text{für } n \to \infty.$$

Beweis

Dieses Lemma folgt unmittelbar aus dem Cauchy-Kriterium mit $m = n + 1$. $\square$

Bemerkung

Das obige Lemma liefert eine notwendige, aber keineswegs hinreichende Bedingung für die Konvergenz einer Reihe. Die harmonische Reihe

$$\sum_{n=1}^{\infty} \frac{1}{n}$$

ist z. B. divergent, obwohl

$$\lim_{n\to\infty} \frac{1}{n} = 0.$$

Das nächste Resultat folgt unmittelbar aus den entsprechenden Ergebnissen für Folgen.

Lemma

$\sum\limits_{n=1}^{\infty} a_n$, $\sum\limits_{n=1}^{\infty} b_n$ seien konvergente Reihen und c sei eine reelle Zahl. Dann sind die Reihen $\sum\limits_{n=1}^{\infty} (a_n + b_n)$ und $\sum\limits_{n=1}^{\infty} ca_n$ ebenfalls konvergent mit

$$\sum_{n=1}^{\infty} (a_n + b_n) = \sum_{n=1}^{\infty} a_n + \sum_{n=1}^{\infty} b_n,$$
$$\sum_{n=1}^{\infty} ca_n = c \sum_{n=1}^{\infty} a_n.$$

Reihen mit nichtnegativen Gliedern

In diesem Abschnitt studieren wir Reihen $\sum\limits_{n=1}^{\infty} a_n$ mit $a_n \geq 0$. In diesem Fall schreiben wir oft

$$\text{“}\sum_{n=1}^{\infty} a_n < \infty\text{”} \quad \text{für} \quad \text{“}\sum_{n=1}^{\infty} a_n \text{ ist konvergent”}.$$

Lemma

Die Reihe $\sum\limits_{n=1}^{\infty} a_n$ mit $a_n \geq 0$ ist genau dann konvergent, wenn die zu $\{a_n\}$ gehörende Partialsummenfolge $\{s_n\}$ nach oben beschränkt ist.

Beweis

Aus

$$s_{k+1} = s_k + a_{k+1}, \quad a_{k+1} \geq 0 \qquad \text{für } k = 1,2,3\ldots$$

folgt

$$s_{k+1} \geq s_k \qquad \text{für } k = 1,2,3\ldots,$$

so dass $\{s_n\}$ monoton steigend ist. $\{s_n\}$ ist also genau dann konvergent, wenn sie nach oben beschränkt ist. $\square$

Satz (Vergleichskriterien)

$\{a_n\}$ und $\{b_n\}$ seien Folgen mit

$$0 \leq a_n \leq b_n, \qquad n = 1,2,3,\dots\ .$$

Dann gilt:

1. Falls $\sum\limits_{n=1}^{\infty} b_n$ konvergiert, so konvergiert auch $\sum\limits_{n=1}^{\infty} a_n$.
2. Falls $\sum\limits_{n=1}^{\infty} a_n$ divergiert, so divergiert auch $\sum\limits_{n=1}^{\infty} b_n$.

Beweis

1. $\{s_n\}$ und $\{t_n\}$ seien die zu $\{a_n\}$ bzw. $\{b_n\}$ gehörenden Partialsummenfolgen. Bemerke:
$$s_n \leq t_n, \qquad n = 1,2,3,\dots$$
Es gilt:
$$\begin{aligned} & \sum_{n=1}^{\infty} b_n && \text{konvergiert} \\ \Rightarrow\ & \{t_n\} && \text{ist nach oben beschränkt} \\ \Rightarrow\ & \{s_n\} && \text{ist nach oben beschränkt} \\ \Rightarrow\ & \sum_{n=1}^{\infty} a_n && \text{konvergiert} \end{aligned}$$
2. Diese Aussage ist die Kontraposition der ersten Aussage.

$\square$

Beispiele

Konvergieren die Reihen

$$\sum_{n=1}^{\infty} \frac{1}{\left(\frac{11}{10}\right)^n - \sqrt{n} + \sin^2 n^3}, \qquad \sum_{n=1}^{\infty} \frac{n+1}{n^2+77}\ ?$$

Lösung

Um zu entscheiden, ob eine Reihe konvergiert, müssen wir ihre Glieder a_n nur für große Werte von n untersuchen.

- Die Reihe
$$\sum_{n=1}^{\infty} \frac{1}{\left(\frac{11}{10}\right)^n - \sqrt{n} + \sin^2 n^3}$$
konvergiert. Es gilt:
$$\begin{aligned}\left(\tfrac{11}{10}\right)^n - \sqrt{n} + \sin^2 n^3 &\geq \left(\tfrac{11}{10}\right)^n - \sqrt{n} \\ &\geq \tfrac{1}{2}\left(\tfrac{11}{10}\right)^n \qquad \text{für hinreichend große Werte von } n\end{aligned}$$
(Aus
$$\frac{\sqrt{n}}{\left(\frac{11}{10}\right)^n} \to 0 \qquad \text{für } n \to \infty$$
"Exponentiale schlagen Potenzen"

folgt
$$\frac{\sqrt{n}}{\left(\frac{11}{10}\right)^n} < \frac{1}{2} \qquad \text{für hinreichend großes } n. \;)$$
Es existiert also $N \in \mathbb{N}$, so dass
$$\frac{1}{\left(\frac{11}{10}\right)^n - \sqrt{n} + \sin^2 n^3} \leq 2\left(\frac{10}{11}\right)^n \qquad \text{für } n > N,$$
und weil
$$\sum_{n=N+1}^{\infty} 2\left(\frac{10}{11}\right)^n$$
konvergiert, so konvergiert auch
$$\sum_{n=N+1}^{\infty} \frac{1}{\left(\frac{11}{10}\right)^n - \sqrt{n} + \sin^2 n^3}.$$

- Die Reihe
$$\sum_{n=1}^{\infty} \frac{n+1}{n^2+77}$$

ist divergent. Es gilt:

$$\begin{aligned} &n+1 > n && \text{für alle } n, \\ &n^2 + 77 < 2n^2 && \text{für hinreichend großes } n. \end{aligned}$$

Es existiert also $N \in \mathbb{N}$, so dass

$$\frac{n+1}{n^2+77} > \frac{1}{2n} \qquad \text{für} \quad n > N$$

und weil

$$\sum_{n=N+1}^{\infty} \frac{1}{2n}$$

divergiert, so divergiert auch

$$\sum_{n=N+1}^{\infty} \frac{n+1}{n^2+77}.$$

□

Mit Hilfe der Vergleichskriterien können wir weitere Kriterien für Konvergenz/ Divergenz einer Reihe herleiten.

Satz

$\sum\limits_{n=1}^{\infty} a_n$ sei eine Reihe mit $a_n > 0$ für alle n.

1. **Quotientenkriterium**

   Es sei
   $$q = \lim_{n\to\infty} \frac{a_{n+1}}{a_n}$$
   (falls dieser Grenzwert existiert). Dann gilt:

   (a) Ist $q < 1$, so konvergiert $\sum\limits_{n=1}^{\infty} a_n$;

   (b) Ist $q > 1$, so divergiert $\sum\limits_{n=1}^{\infty} a_n$;

   (c) Ist $q = 1$, gibt es keine Aussage.

2. **Wurzelkriterium**

   Es sei
   $$r = \lim_{n\to\infty} \sqrt[n]{a_n}$$
   (falls dieser Grenzwert existiert). Dann gilt:

   (a) Ist $r < 1$, so konvergiert $\sum\limits_{n=1}^{\infty} a_n$;

   (b) Ist $r > 1$, so divergiert $\sum\limits_{n=1}^{\infty} a_n$;

   (c) Ist $r = 1$, gibt es keine Aussage.

3. **Integralkriterium**

   $f : [1,\infty) \to \mathbb{R}$ sei positiv und monoton fallend mit
   $$f(n) = a_n, \qquad n = 1,2,3,\ldots.$$
   Dann konvergiert $\sum\limits_{n=1}^{\infty} a_n$ genau dann, wenn $\lim\limits_{n\to\infty} \int_1^{n+1} f(x)\,\mathrm{d}x$ existiert.

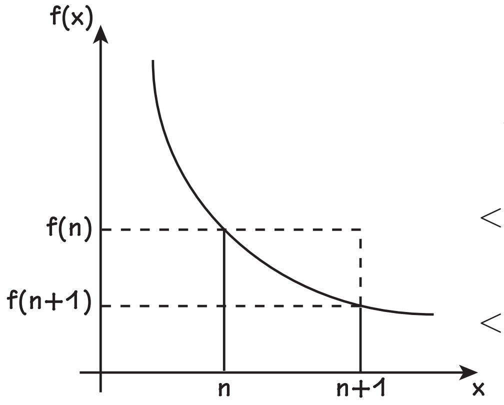
Beweis

1. (a) Wähle $\widetilde{q}$ mit $q < \widetilde{q} < 1$. Aus
   $$\lim_{n\to\infty} \frac{a_{n+1}}{a_n} = q$$
   folgt die Existenz einer natürlichen Zahl N mit
   $$\frac{a_{n+1}}{a_n} < \widetilde{q} \qquad \text{für } n > N.$$
   Daher gilt
   $$a_{N+1+k} < \widetilde{q}^k a_{N+1}, \qquad k = 1,2,3,\ldots$$
   (Beweis durch vollständige Induktion), so dass
   $$\sum_{n=N+2}^{\infty} a_n = \sum_{k=1}^{\infty} a_{N+1+k} < a_{N+1} \sum_{k=1}^{\infty} \widetilde{q}^k < \infty.$$

   (b) Aus
   $$\lim_{n\to\infty} \frac{a_{n+1}}{a_n} > 1$$
   folgt $a_{n+1} > a_n$ für hinreichend großes n. Daher konvergiert a_n nicht gegen 0 für $n \to \infty$.

2. Diese Aussage wird in ähnlicher Weise beweisen.

3. Bemerke:

- 

$f(n+1)$	Flächeninhalt des "unteren Rechtecks"
$< \int_n^{n+1} f(x)\,\mathrm{d}x$	Flächeninhalt unterhalb der Kurve
$< f(n)$	Flächeninhalt des "oberen Rechtecks"

- $\lim\limits_{n\to\infty} \int_1^{n+1} f(x)\,\mathrm{d}x$ existiert genau dann, wenn $\sum\limits_{n=1}^{\infty} \int_n^{n+1} f(x)$ konvergiert.

Falls $\sum\limits_{n=1}^{\infty} \int_n^{n+1} f(x)\,\mathrm{d}x$ konvergiert, gilt

$$\begin{aligned}\sum_{n=2}^{\infty} a_n &= \sum_{n=1}^{\infty} a_{n+1}\\ &= \sum_{n=1}^{\infty} f(n+1)\\ &< \sum_{n=1}^{\infty} \int_n^{n+1} f(x)dx\\ &< \infty\end{aligned}$$

Falls $\sum\limits_{n=1}^{\infty} \int_n^{n+1} f(x)\,\mathrm{d}x$ nicht konvergiert, gilt

$$a_n = f(n) > \int_n^{n+1} f(x)\,\mathrm{d}x,$$

und daher ist $\sum\limits_{n=1}^{\infty} a_n$ ebenfalls divergent. □

Beispiele

1. r,k seien reelle Zahlen mit $k > 0, r > 1$. Die Reihe

$$\sum_{n=1}^{\infty} \frac{n^k}{r^n}$$

konvergiert, weil

$$\begin{aligned}
\lim_{n\to\infty} \frac{\frac{(n+1)^k}{r^{n+1}}}{\frac{n^k}{r^n}} &= \lim_{n\to\infty} \frac{1}{r}\left(\frac{n+1}{n}\right)^k \\
&= \frac{1}{r}\lim_{n\to\infty}\left(\frac{n+1}{n}\right)^k \\
&= \frac{1}{r} \\
&< 1.
\end{aligned}$$

Daraus lässt sich folgern, dass

$$\frac{n^k}{r^n} \to 0 \qquad \text{für} \qquad n \to \infty$$

"Exponentiale schlagen Potenzen".

2. Betrachte die Reihe
$$\sum_{n=1}^{\infty} \frac{1}{n^k}, \quad k > 0.$$

Wir berechnen

$$\int_1^{n+1} \frac{1}{x^k}\,\mathrm{d}x = \begin{cases} \dfrac{1}{k-1} - \dfrac{1}{k-1} \cdot \dfrac{1}{(n+1)^{k-1}}, & k \neq 1, \\ \log(n+1), & k = 1, \end{cases}$$

so dass
$$\lim_{n\to\infty} \int_1^{n+1} \frac{1}{x^k}\,\mathrm{d}x$$
existiert genau dann, wenn $k > 1$ ist. Die obige Reihe konvergiert also genau dann, wenn $k > 1$ ist.

Absolute und bedingte Konvergenz

In diesem Abschnitt geben wir die Einschränkung $a_n \geq 0$ bei der Reihe $\sum\limits_{n=1}^{\infty} a_n$ auf.

Definition

Die Reihe $\sum\limits_{n=1}^{\infty} a_n$ heißt **absolut konvergent**, falls $\sum\limits_{n=1}^{\infty} |a_n|$ konvergent ist.

Lemma

Die Reihe

$$\sum_{n=1}^{\infty} a_n$$

sei absolut konvergent. Dann ist sie konvergent.

Beweis

$\sum\limits_{n=1}^{\infty} |a_n|$ ist konvergent und erfüllt daher das Cauchy-Kriterium:

Zu jedem $\varepsilon > 0$ existiert $N \in \mathbb{N}$, so dass

$$\left| \sum_{k=n+1}^{m} |a_k| \right| < \varepsilon \qquad \text{für } m > n > N.$$

Aus der Dreiecksungleichung folgt

$$\left| \sum_{k=n+1}^{m} a_k \right| \leq \sum_{k=n+1}^{m} |a_k| = \left| \sum_{k=n+1}^{m} |a_k| \right| < \varepsilon \qquad \text{für } m > n > N.$$

Die Reihe $\sum\limits_{n=1}^{\infty} a_n$ erfüllt also das Cauchy-Kriterium und ist daher konvergent. □

Beispiele

1. Die Reihe

$$1 - \frac{1}{4} + \frac{1}{9} - \frac{1}{16} + \ldots \qquad \left(\sum_{n=1}^{\infty} \frac{(-1)^{n+1}}{n^2} \right)$$

ist absolut konvergent und daher konvergent, weil

$$1 + \frac{1}{4} + \frac{1}{9} + \frac{1}{16} + \ldots \qquad \left(\sum_{n=1}^{\infty} \frac{1}{n^2} \right)$$

konvergent ist.

2. Die Reihe
$$1 - \frac{1}{2} + \frac{1}{3} - \frac{1}{4} + \dots \qquad \left(\sum_{n=1}^{\infty} \frac{(-1)^{n+1}}{n}\right)$$
ist allerdings nicht absolut konvergent, weil
$$1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \dots \qquad \left(\sum_{n=1}^{\infty} \frac{1}{n}\right)$$
nicht konvergent ist.

Definition

Eine Reihe der Form
$$\sum_{n=1}^{\infty} (-1)^{n+1} a_n = a_1 - a_2 + a_3 - a_4 + \dots, \qquad a_n > 0$$
heißt **alternierende Reihe**.

Satz (Leibniz-Kriterium)

$\{a_n\}$ sei eine monoton fallende Folge positiver Zahlen mit $\lim\limits_{n\to\infty} a_n = 0$.

Dann konvergiert die alternierende Reihe $\sum\limits_{n=1}^{\infty} (-1)^{n+1} a_n$ und
$$a_1 - a_2 \leq \sum_{n=1}^{\infty} (-1)^{n+1} a_n \leq a_1. \tag{$\star$}$$

Beweis

Wir betrachten die Partialsummen
$$s_1, s_3, s_5, \dots \qquad (s_{2n+1},\, n = 0,1,2,\dots)$$
und
$$s_2, s_4, s_6 \qquad (s_{2n},\, n = 1,2,\dots)$$
getrennt. Es gilt:

(i) $s_1 \geq s_3 \geq s_5 \geq \dots \qquad (s_{2n+3} = s_{2n+1} \underbrace{-a_{2n+2} + a_{2n+3}}_{\leq\ 0})$

(ii) $s_2 \leq s_4 \leq s_6 \leq \dots \qquad (s_{2n+2} = s_{2n} + \underbrace{a_{2n+1} - a_{2n+2}}_{\geq\ 0})$

Die Folgen $\{s_{2n}\}, \{s_{2n+1}\}$ sind beide beschränkt:

$$s_2 \leq s_{2n} = s_{2n+1} - a_{2n+1} \leq s_{2n+1} \leq s_1 \quad \text{für} \quad n = 1,2,3,\dots,$$

d. h.

$$s_2 \leq s_{2n}, s_{2n+1} \leq s_1, \qquad \text{für} \quad n = 1,2,3,\dots .$$

$\{s_{2n}\}$ und $\{s_{2n+1}\}$ sind also konvergent. Wir bezeichnen die Grenzwerte mit s bzw. t, so dass

$$s_2 \leq s, t \leq s_1.$$

Es gilt:

$$
\begin{aligned}
& s_{2n+1} - s_{2n} = a_{2n+1}, \qquad n = 1,2,3,\dots \\
\Rightarrow \quad & \underbrace{\lim_{n\to\infty} (s_{2n+1} - s_{2n})}_{\substack{= \lim\limits_{n\to\infty} s_{2n+1} - \lim\limits_{n\to\infty} s_{2n} \\ = s - t}} = \underbrace{\lim_{n\to\infty} a_{2n+1}}_{=0} \\
\Rightarrow\ & s = t
\end{aligned}
$$

Aus $s_{2k} \to s, s_{2k+1} \to s$ für $k \to \infty$ folgt $s_n \to s$ für $n \to \infty$.

Die Abschätzung $(\star)$ ist eine Umschreibung von $s_2 \leq s \leq s_1$. $\square$

Beispiel

Dem Leibniz-Kriterium zufolge konvergiert die Reihe

$$1 - \frac{1}{2} + \frac{1}{3} - \frac{1}{4} + \frac{1}{5} - \frac{1}{6} + \dots$$

Definition

Eine Reihe $\sum\limits_{n=1}^{\infty} a_n$, die konvergent, aber nicht absolut konvergent ist, heißt **bedingt konvergent**.

Umordnungen

Die Konvergenz der Reihe

$$1 - \frac{1}{2} + \frac{1}{3} - \frac{1}{4} + \frac{1}{5} - \dots$$

folgt aus dem Leibniz-Kriterium. Ihre Summe s erfüllt

$$\frac{1}{2} \le s \le 1.$$

Auf der anderen Seite haben wir die Berechnung

$$\begin{aligned}
s &= 1 - \tfrac{1}{2} + \tfrac{1}{3} - \tfrac{1}{4} + \tfrac{1}{5} - \dots \\
&= \underbrace{1 - \tfrac{1}{2}} - \tfrac{1}{4} + \underbrace{\tfrac{1}{3} - \tfrac{1}{6}} - \tfrac{1}{8} + \underbrace{\tfrac{1}{5} - \tfrac{1}{10}} - \tfrac{1}{12} + \dots \\
&= \quad \tfrac{1}{2} \quad - \tfrac{1}{4} \quad + \tfrac{1}{6} \quad - \tfrac{1}{8} \quad + \tfrac{1}{10} \quad - \tfrac{1}{12} + \dots \\
&= \tfrac{1}{2}\left(1 - \tfrac{1}{2} + \tfrac{1}{3} - \dots\right) \\
&= \tfrac{1}{2}s \\
\Rightarrow \quad s &= 0.
\end{aligned}$$

Ein Blick auf die rigorose Definition einer Reihe erklärt den Grund für diesen Paradoxon:

- Die Reihe
$$1 - \frac{1}{2} + \frac{1}{3} - \frac{1}{4} + \frac{1}{5} - \dots$$
ist die Folge
$$\left.\begin{aligned}
&1, \\
&1 - \tfrac{1}{2}, \\
&1 - \tfrac{1}{2} + \tfrac{1}{3}, \\
&1 - \tfrac{1}{2} + \tfrac{1}{3} - \tfrac{1}{4}, \\
&\dots
\end{aligned}\right. \qquad \{s_n\}$$

- Die Reihe
$$1 - \frac{1}{2} - \frac{1}{4} + \frac{1}{3} - \frac{1}{6} - \frac{1}{8} + \dots$$

ist die Folge

$$
\begin{array}{ll}
1, & \\
1-\frac{1}{2}, & \\
1-\frac{1}{2}-\frac{1}{4}, & \qquad\qquad \{t_n\} \\
1-\frac{1}{2}-\frac{1}{4}+\frac{1}{3}, & \\
\dots &
\end{array}
$$

Warum soll $\lim\limits_{n\to\infty} s_n = \lim\limits_{n\to\infty} t_n$?

Definition

$\sum\limits_{n=1}^{\infty} a_n$ sei eine Reihe und $f : \mathbb{N} \to \mathbb{N}$ sei eine Bijektion. Die Reihe $\sum\limits_{n=1}^{\infty} b_n$ mit $b_n = a_{f(n)}$ ist eine **Umordnung** der Reihe $\sum\limits_{n=1}^{\infty} a_n$.

Satz

$\sum\limits_{n=1}^{\infty} a_n$ sei eine absolut konvergente Reihe und $\sum\limits_{n=1}^{\infty} b_n$ sei eine Umordnung von $\sum\limits_{n=1}^{\infty} a_n$. Dann ist $\sum\limits_{n=1}^{\infty} b_n$ ebenfalls absolut konvergent und

$$\sum_{n=1}^{\infty} a_n = \sum_{n=1}^{\infty} b_n, \qquad \sum_{n=1}^{\infty} |a_n| = \sum_{n=1}^{\infty} |b_n|.$$

Beweis

Wir wissen:

Zu jedem $\varepsilon_1 > 0$ existiert $N_1 \in \mathbb{N}$ mit

$$\left| \sum_{k=1}^{n} a_k - \sum_{k=1}^{\infty} a_k \right| = \left| \sum_{k=n+1}^{\infty} a_k \right| < \varepsilon_1$$

für $n > N_1$.

Zu jedem $\varepsilon_2 > 0$ existiert $N_2 \in \mathbb{N}$ mit

$$\left| \sum_{k=1}^{n} |a_k| - \sum_{k=1}^{\infty} |a_k| \right| = \left| \sum_{k=n+1}^{\infty} |a_k| \right| < \varepsilon_2$$

für $n > N_2$.

Wir wollen beweisen:

Zu jedem $\varepsilon > 0$ existiert $M \in \mathbb{N}$ mit

$$\left| \sum_{k=1}^{m} b_k - \sum_{k=1}^{\infty} a_k \right| < \varepsilon$$

für $m > M$.

Zu jedem $\varepsilon > 0$ existiert $M \in \mathbb{N}$ mit

$$\left| \sum_{k=1}^{m} |b_k| - \sum_{k=1}^{\infty} |a_k| \right| < \varepsilon$$

für $m > M$.

Wähle $n > \max(N_1,N_2)$ und M groß genug, so dass $a_1, \ldots, a_n$ in der Liste $b_1, \ldots, b_M$ erscheinen.

Für $m > M$ ist

$$\sum_{k=1}^{m} b_k - \sum_{k=1}^{n} a_k = \text{Summe gewisser } a_k\text{, wobei } a_1, \ldots, a_n \text{ nicht dabei sind,}$$

so dass

$$\begin{aligned}\left| \sum_{k=1}^{m} b_k - \sum_{k=1}^{n} a_k \right| &\leq \text{Summe gewisser } |a_k|\text{, wobei } |a_1|, \ldots, |a_n| \text{ nicht dabei sind} \\ &\leq \sum_{k=n+1}^{\infty} |a_k|\end{aligned}$$

und daher

$$\begin{aligned}\left| \sum_{k=1}^{\infty} a_k - \sum_{k=1}^{m} b_k \right| &= \left| \sum_{k=1}^{\infty} a_k - \sum_{k=1}^{n} a_k - \sum_{k=1}^{m} b_k + \sum_{k=1}^{n} a_k \right| \\ &\leq \left| \sum_{k=1}^{\infty} a_k - \sum_{k=1}^{n} a_k \right| + \left| \sum_{k=1}^{m} b_k - \sum_{k=1}^{n} a_k \right| \\ &\leq \left| \sum_{k=n+1}^{\infty} a_k \right| + \sum_{k=n+1}^{\infty} |a_k| \\ &< \varepsilon_1 + \varepsilon_2.\end{aligned}$$

Wähle $\varepsilon > 0$ und setze $\varepsilon_1 = \varepsilon/2$, $\varepsilon_2 = \varepsilon/2$, so dass

$$\left| \sum_{k=1}^{\infty} a_k - \sum_{k=1}^{m} b_k \right| < \varepsilon \qquad \text{für } m > M,$$

d.h.

$$\sum_{k=1}^{\infty} b_k = \sum_{k=1}^{\infty} a_k.$$

Wir ersetzen nun a_k, b_k durch $|a_k|$, $|b_k|$ und wiederholen das obige Argument. Das Ergebnis ist

$$\sum_{k=1}^{\infty} |b_k| = \sum_{k=1}^{\infty} |a_k|,$$

so dass $\sum_{k=1}^{\infty} b_k$ absolut konvergent ist. □

Satz

$\sum\limits_{n=1}^{\infty} a_n$ sei eine bedingt konvergente Reihe und α sei eine beliebige reelle Zahl. Es existiert eine Umordnung $\sum\limits_{n=1}^{\infty} b_n$ von $\sum\limits_{n=1}^{\infty} a_n$ mit

$$\sum_{n=1}^{\infty} b_n = \alpha.$$

Beweis

Es seien $\{p_k\}$ und $\{n_k\}$ die Folgen, die aus den positiven bzw. negativen Gliedern von $\{a_k\}$ bestehen. Da $\sum_{k=1}^{\infty} a_k$ konvergent ist, gilt $p_k \to 0$ und $q_k \to 0$ für $k \to \infty$.

Die Reihen $\sum_{k=1}^{\infty} p_k$ und $\sum_{k=1}^{\infty} n_k$ sind beide divergent: Wenn beide konvergent wären, wäre $\sum_{k=1}^{\infty} |a_k| = \sum_{k=1}^{\infty} p_k - \sum_{k=1}^{\infty} n_k$ konvergent; wenn nur eine konvergent wäre, wäre $\sum_{k=1}^{\infty} a_k$ als Summe einer konvergenten und einer divergenten Reihe divergent. Insbesondere ist die Partialsummenfolge $\{\sum_{k=1}^{n} p_k\}$ monoton steigend und nicht nach oben beschränkt, während die Partialsummenfolge $\{\sum_{k=1}^{n} n_k\}$ monoton fallend und nicht nach unten beschränkt ist.

Es sei $\alpha > 0$.

- Es sei N_1 die kleinste natürliche Zahl mit der Eigenschaft

$$S_1 := \sum_{k=1}^{N_1} p_k > \alpha.$$

- Es sei M_1 die kleinste natürliche Zahl mit der Eigenschaft

$$S_1 + \underbrace{\sum_{k=1}^{M_1} n_k}_{:= T_1} < \alpha.$$

- Für $j = 2,3,\ldots$ sei N_j die kleinste natürliche Zahl mit der Eigenschaft

$$S_1 + T_1 + \ldots + S_{j-1} + T_{j-1} + \underbrace{\sum_{k=N_{j-1}+1}^{N_j} p_k}_{:= S_j} > \alpha.$$

- Für $j = 2,3,\ldots$ sei M_j die kleinste natürliche Zahl mit der Eigenschaft

$$S_1 + T_1 + \ldots + S_{j-1} + T_{j-1} + S_j + \underbrace{\sum_{k=M_{j-1}+1}^{M_j} q_k}_{:= T_j} < \alpha.$$

Die Reihe

$$S_1 + T_1 + S_2 + T_2 + S_3 + T_3 + \ldots \tag{$\star$}$$

ist eine Umordnung von $\sum_{k=1}^{\infty} a_k$, und wir zeigen nun, dass die Summe dieser Reihe gleich α ist.

Bemerke:

$$S_1 + T_1 + \ldots + S_{j-1} + T_{j-1} + \sum_{k=N_{j-1}+1}^{N_j-1} p_k \leq \alpha,$$

so dass

$$S_1 + T_1 + \ldots + S_{j-1} + T_{j-1} + S_j - \alpha \leq S_j - \sum_{k=N_{j-1}+1}^{N_j-1} p_k = p_{N_j}$$

und daher

$$|S_1 + T_1 + \ldots + S_{j-1} + T_{j-1} + S_j - \alpha| \leq p_{N_j} \to 0 \qquad \text{für } j \to \infty.$$

Dieses Argument zeigt ebenfalls, dass

$$|S_1 + T_1 + \ldots + S_{j-1} + T_{j-1} + S_j + T_j - \alpha| \leq -q_{M_j} \to 0 \qquad \text{für } j \to \infty.$$

Es gilt also: Die Partialsummen der Reihe $(\star)$ steigen auf S_1, fallen dann auf $S_1 + T_1$, steigen dann auf $S_1 + T_1 + S_2$, fallen dann auf $S_1 + T_1 + S_2 + T_2$, …, und konvergieren gegen α.

Das entsprechende Ergebnis für $\alpha \leq 0$ wird in ähnlicher Weise bewiesen. $\square$

Das Cauchy-Produkt

Lemma

Es seien $\sum_{n=0}^{\infty} a_n$, $\sum_{n=0}^{\infty} b_n$ absolut konvergente Reihen. Dann ist die Reihe $\sum_{n=0}^{\infty} c_n$, wobei

$$c_n = \sum_{k=0}^{n} a_k b_{n-k}, \qquad n = 0,1,2,\ldots$$

ist, ebenfalls absolut konvergent und es gilt

$$\sum_{n=0}^{\infty} c_n = \sum_{n=0}^{\infty} a_n \sum_{n=0}^{\infty} b_n.$$

Beweis

Zunächst bemerken wir, dass die Folgen

$$\left\{ \sum_{k=0}^{n} a_k \sum_{k=0}^{n} b_k \right\}, \qquad \left\{ \sum_{k=0}^{n} |a_k| \sum_{k=0}^{n} |b_k| \right\}$$

konvergent (mit Grenzwerten

$$\sum_{k=0}^{\infty} a_k \sum_{k=0}^{\infty} b_k, \qquad \sum_{k=0}^{\infty} |a_k| \sum_{k=0}^{\infty} |b_k| \;)$$

sind.

Es gilt nun

$$\sum_{k=0}^{n} a_k \sum_{k=0}^{n} b_k - \sum_{k=0}^{n} c_k = \sum_{\substack{i,j \leq n \\ i,j > n}} a_i b_j,$$

so dass

$$\begin{aligned}\left|\sum_{k=0}^{n} c_k - \sum_{k=0}^{n} a_k \sum_{k=0}^{n} b_k\right| &\le \left|\sum_{\substack{i,j\le n\\ i,j>n}} a_i b_j\right| \\ &\le \sum_{\substack{i,j\le n\\ i,j>n}} |a_i||b_j| \\ &\le \sum_{i,j\le n} |a_i||b_j| - \sum_{i,j\le \frac{n}{2}} |a_i||b_j| \\ &= \sum_{k=0}^{n} |a_k| \sum_{k=0}^{n} |b_k| - \sum_{k=0}^{\frac{n}{2}} |a_k| \sum_{k=0}^{\frac{n}{2}} |b_k| \\ &\to 0\end{aligned}$$

für $n \to \infty$, denn $\{\sum_{k=0}^{n} a_k \sum_{k=0}^{n} b_k\}$ ist eine Cauchy-Folge.

Folglich gilt

$$\sum_{k=0}^{n} c_k - \sum_{k=0}^{\infty} a_l \sum_{k=0}^{\infty} b_k = \underbrace{\sum_{k=0}^{\infty} c_k - \sum_{k=0}^{n} a_k \sum_{k=0}^{n} b_k}_{\to 0} + \underbrace{\sum_{k=0}^{n} a_k \sum_{k=0}^{n} b_k - \sum_{k=0}^{\infty} \sum_{k=0}^{\infty} b_k}_{\to 0}$$

für $n \to \infty$, d.h. $\sum_{k=0}^{\infty} c_k$ konvergiert gegen $\sum_{k=0}^{\infty} a_k \sum_{k=0}^{\infty} b_k$.

Dieses Argument zeigt auch, dass $\sum_{n=0}^{\infty} d_n$, wobei

$$d_n = \sum_{k=0}^{n} |a_k||b_{n-k}|, \qquad n = 0,1,2,\ldots$$

ist, gegen $\sum_{k=0}^{\infty} |a_k| \sum_{k=0}^{\infty} |b_k|$ konvergiert. Es gilt aber

$$|c_n| \le d_n, \qquad n = 0,1,2,\ldots,$$

und dem Vergleichsprinzip zufolge ist $\sum_{n=0}^{\infty} |c_n|$ konvergent. $\square$

Definition

Es seien $\sum_{n=0}^{\infty} a_n$, $\sum_{n=0}^{\infty} b_n$ absolut konvergente Reihen. Die Reihe $\sum_{n=0}^{\infty} c_n$ mit

$$c_n = \sum_{k=0}^{n} a_k b_{n-k}, \qquad n = 0,1,2,\ldots$$

heißt **Cauchy-Produkt** von $\sum_{n=0}^{\infty} a_n$ und $\sum_{n=0}^{\infty} b_n$.

Bemerkung

Sind $\sum_{n=0}^{\infty} a_n$, $\sum_{n=0}^{\infty} b_n$ nur bedingt konvergent, so ist ihr Cauchy-Produkt nicht notwendigerweise konvergent.

Die Reihe

$$\sum_{n=0}^{\infty} \frac{(-1)^n}{\sqrt{n+1}}$$

ist laut dem Leibniz-Kriterium konvergent aber nicht absolut konvergent, denn

$$\sum_{n=0}^{\infty} \left| \frac{(-1)^n}{\sqrt{n+1}} \right| = \sum_{n=1}^{\infty} \frac{1}{n^{1/2}}.$$

Das Cauchy-Produkt dieser Reihe mit sich selbst ist $\sum_{n=0}^{\infty} c_n$, wobei

$$c_n = (-1)^n \sum_{k=0}^{n} \frac{1}{(k+1)^{1/2}(n-k+1)^{1/2}}.$$

Es gilt nun

$$\begin{aligned}
|c_n| &= \sum_{k=0}^{n} \frac{1}{(k+1)^{1/2}(n-k+1)^{1/2}} \\
&\geq \sum_{k=0}^{n} \frac{2}{(k+1)+(n-k+1)} \\
&= \sum_{k=0}^{n} \frac{2}{n+2} \\
&= \frac{2(n+1)}{n+2} \\
&\geq \frac{2(n+1)}{2(n+1)} \qquad (n+2 \leq 2n+2) \\
&\geq 1.
\end{aligned}$$

Aus $c_n \not\to 0$ für $n \to \infty$ folgt, dass $\sum_{n=0}^{\infty} c_n$ divergent ist.

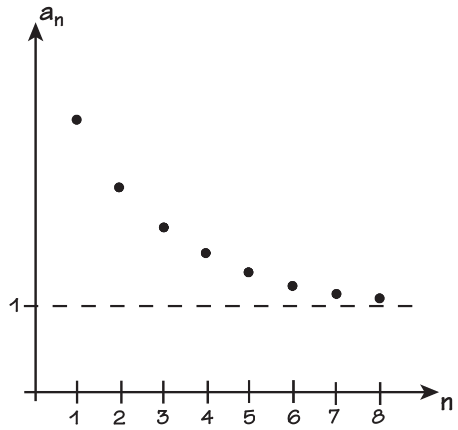
4 Grenzwerte und Stetigkeit

Einführende Beispiele

1. Die Folge $\{a_n\}$ mit

$$a_n = 1 + \frac{1}{n}$$

"konvergiert gegen 1" für $n \to \infty$:



- Je großer der Wert von n, desto näher kommt a_n an 1.

Definition

$\{a_n\}$ **konvergiert gegen** l **für** $n \to \infty$, wenn es zu jedem $\varepsilon > 0$ eine natürliche Zahl N gibt mit

$$|a_n - l| < \varepsilon \qquad \text{für alle } n > N.$$

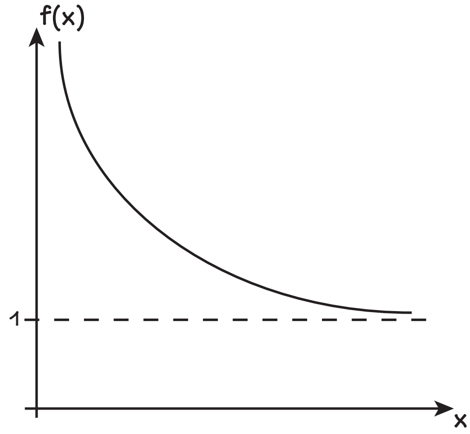
In diesem Fall schreiben wir

$$\lim_{n\to\infty} a_n = l.$$

Die Funktion $f : (0,\infty) \to \mathbb{R}$ mit

$$f(x) = 1 + \frac{1}{x}$$

"konvergiert gegen 1" für $x \to \infty$:



- Je größer der Wert von x, desto näher kommt $f(x)$ an 1.

Definition

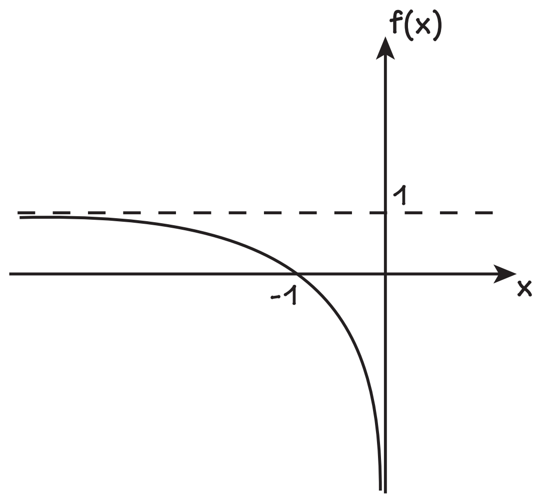
$f(x)$ **konvergiert gegen** l **für** $x \to \infty$, wenn es zu jedem $\varepsilon > 0$ eine reelle Zahl $M > 0$ gibt mit

$$|f(x) - l| < \varepsilon \qquad \text{für alle } x > M.$$

In diesem Fall schreiben wir

$$\lim_{x\to\infty} f(x) = l.$$

2. Die Funktion $f : (-\infty,0) \to \mathbb{R}$ mit $f(x) = 1 + \frac{1}{x}$ "konvergiert gegen 1" für $x \to -\infty$:



- Je kleiner der Wert von x, desto näher kommt $f(x)$ an 1.

Definition

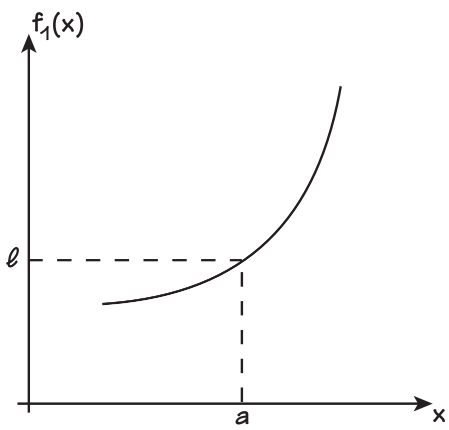
$f(x)$ **konvergiert gegen** l **für** $x \to -\infty$**,** wenn es zu jedem $\varepsilon > 0$ eine reelle Zahl $M < 0$ gibt mit

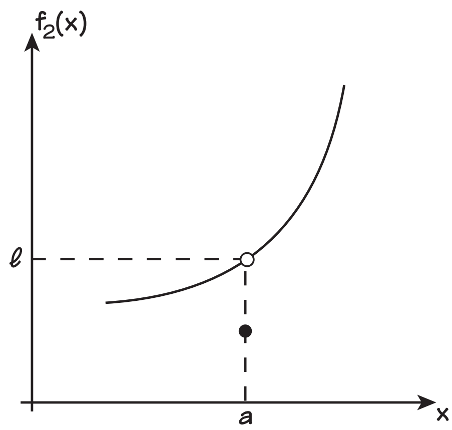
$$|f(x) - l| < \varepsilon \qquad \text{für alle } x < M.$$

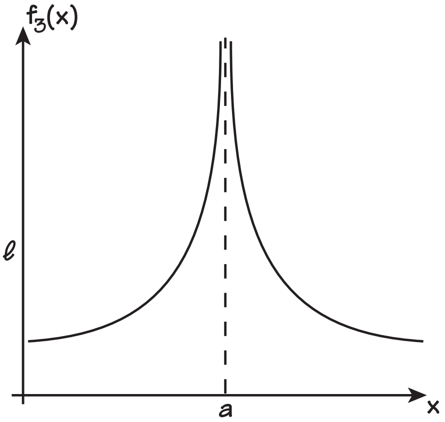
In diesem Fall schreiben wir

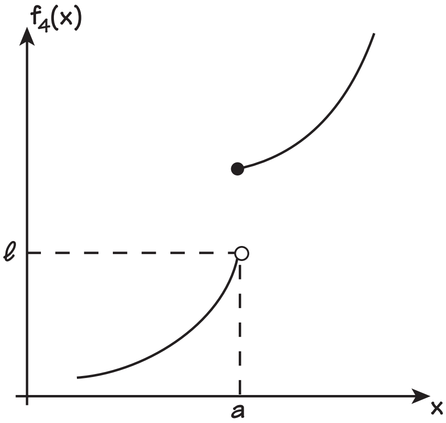
$$\lim_{x \to -\infty} f(x) = l.$$

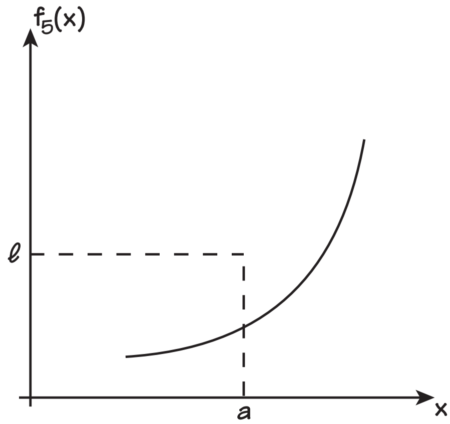
3. Betrachte die folgenden fünf Funktionen:











Die Funktionen f_1 und f_2 “konvergieren gegen l” für $x \to a$.

- “$f(x)$ konvergiert gegen l für $x \to a$”

  bedeutet

  “Wir können den Abstand zwischen $f(x)$ und l beliebig klein machen, indem wir x hinreichend nah an a, aber nicht gleich a wählen.”

Definition

$f(x)$ **konvergiert gegen** l **für** $x \to a$, wenn es zu jedem $\varepsilon > 0$ eine reelle Zahl $\delta > 0$ gibt mit

$$\underbrace{|f(x) - l|}_{\substack{\text{Abstand zwischen} \\ f(x) \text{ und } l}} < \varepsilon \qquad \text{für alle } x \text{ mit} \qquad 0 < \underbrace{|x - a|}_{\substack{\text{Abstand zwischen} \\ x \text{ und } a}} < \delta.$$

In diesem Fall schreiben wir

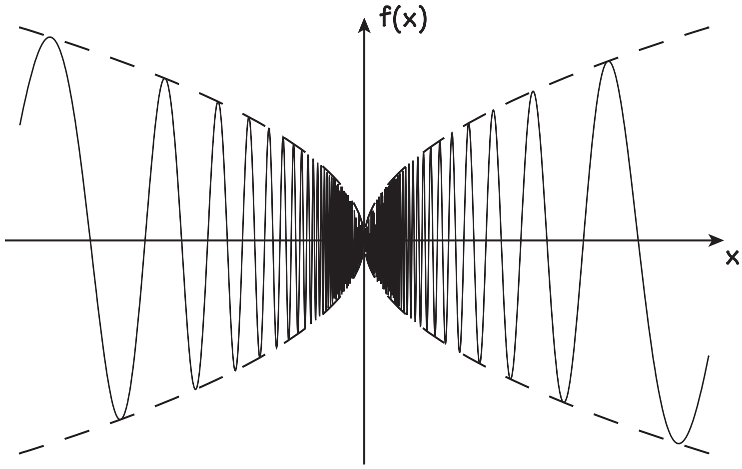
$$\lim_{x \to a} f(x) = l.$$

Beispiel

Die Funktion

$$f : \mathbb{R} \setminus \{0\} \to \mathbb{R}, \ f(x) = \sqrt{|x|} \sin\left(\frac{1}{x}\right)$$

konvergiert gegen 0 für $x \to 0$.



Die Funktion vollzieht eine Oszillation im immer kleiner werdenden Intervall $[\frac{1}{2n\pi}, \frac{1}{(2n+2)\pi}]$, die Amplitude der Oszillationen ist aber gedämpft.

Wir müssen zeigen:

Zu jedem $\varepsilon > 0$ existiert $\delta > 0$, so dass

$$|f(x)| < \varepsilon \qquad \text{für alle } x \text{ mit } 0 < |x| < \delta. \tag{1}$$

Aus

$$\left| \sqrt{|x|} \sin\left(\frac{1}{x}\right) \right| < \sqrt{|x|}$$

folgt

$$0 < |x| < \varepsilon^2 \ \Rightarrow \ |f(x)| < \varepsilon.$$

Zu jedem $\varepsilon > 0$ ist also (1) erfüllt mit $\delta = \varepsilon^2$.

Bemerkung

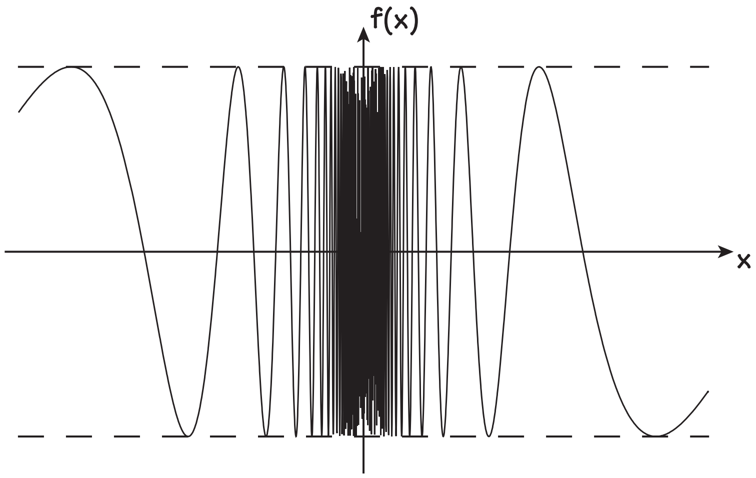
$$\lim_{x\to a} f(x) = l \quad \Leftrightarrow \quad \begin{array}{l} f(x_n) \to l \text{ für alle Folgen} \\ \{x_n\} \text{ mit } x_n \neq a \text{ und } x_n \to a \end{array}$$

Beispiel

Die Funktion

$$f : \mathbb{R} \setminus \{0\} \to \mathbb{R}, \qquad f(x) = \sin\left(\frac{1}{x}\right)$$

hat keinen Grenzwert bei $x = 0$.



Die Funktion vollzieht eine Oszillation mit Amplitude 2 im immer kleiner werdenen Intervall $[\frac{1}{2n\pi}, \frac{1}{(2n+2)\pi}]$.

- Setze $x_n = \frac{1}{2n\pi+3\pi/2}$, so dass $f(x_n) = -1$. Dann gilt $x_n \to 0$ und $f(x_n) \to -1$ für $n \to \infty$.

- Setze $x_n = \frac{1}{2n\pi+1\pi/2}$, so dass $f(x_n) = 1$. Dann gilt $x_n \to 0$ und $f(x_n) \to 1$ für $n \to \infty$.

Wegen des Kriteriums in der letzten Bemerkung existiert also $\lim_{x\to 0} f(x)$ nicht.

Lemma

Aus

$$\lim_{x\to a} f(x) = l, \qquad \lim_{x\to a} g(x) = m$$

folgt

$$\lim_{x\to a}(f(x) + g(x)) = l + m,$$
$$\lim_{x\to a} f(x)g(x) = lm,$$

und

$$\lim_{x\to a} \frac{1}{g(x)} = \frac{1}{m}$$

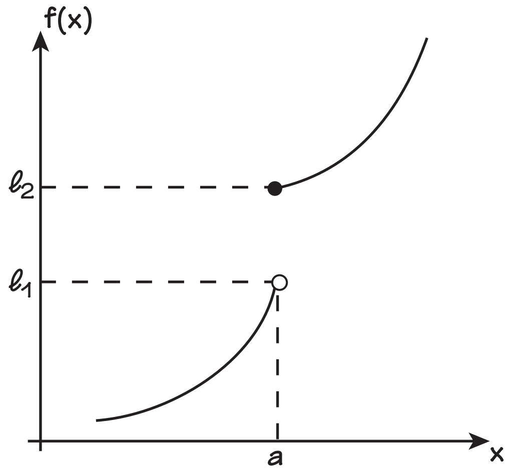
falls $m \neq 0$.

Diese Ergebnisse bleiben richtig, wenn wir "a" durch "∞" oder "$-\infty$" ersetzen.

Beweis

Diese Ergebnisse werden analog zu den entsprechenden Ergebnissen für Folgen bewiesen. □

Einseitige Grenzwerte



Hier gilt:

- $f(x) \to \ell_1$ für $x \uparrow a$
- $f(x) \to \ell_2$ für $x \downarrow a$

Definitionen

1. $f(x)$ **konvergiert linksseitig gegen** l_1 **für** $x \to a$, wenn es zu jedem $\varepsilon > 0$ eine reelle Zahl $\delta > 0$ gibt mit

$$|f(x) - l_1| < \varepsilon \qquad \text{für alle } x \text{ mit } 0 < |x-a| < \delta,\ x < a$$

   In diesem Fall schreiben wir

$$\lim_{x \uparrow a} f(x) = l_1 \qquad \text{oder} \qquad \lim_{x \to a^-} f(x) = l_1.$$

2. $f(x)$ **konvergiert rechtsseitig gegen** l_2 **für** $x \to a$, wenn es zu jedem $\varepsilon > 0$ eine reelle Zahl $\delta > 0$ gibt mit

$$|f(x) - l_2| < \varepsilon \qquad \text{für alle } x \text{ mit } 0 < |x-a| < \delta,\ x > a.$$

   In diesem Fall schreiben wir

$$\lim_{x \downarrow a} f(x) = l_2 \qquad \text{oder} \qquad \lim_{x \to a^+} f(x) = l_2.$$

Lemma

Der Grenzwert $\lim_{x\to a} f(x)$ existiert genau dann, wenn die beiden einseitigen Grenzwerte $\lim_{x\uparrow a} f(x)$, $\lim_{x \downarrow a} f(x)$ existieren und gleich sind. In diesem Fall gilt

$$\lim_{x\to a} f(x) \;=\; \lim_{x\uparrow a} f(x) \;=\; \lim_{x\downarrow a} f(x).$$

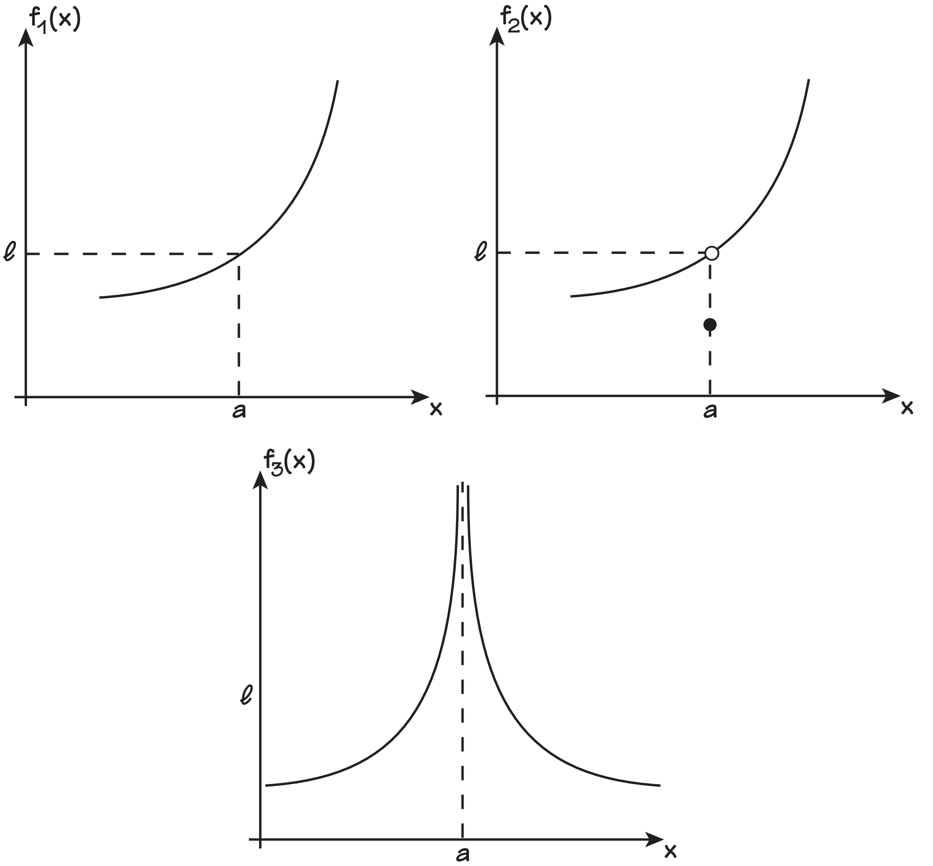
Stetigkeit

Definition

Eine reellwertige Funktion f ist **stetig** in dem Punkt a, falls

$$\lim_{x\to a} f(x) = f(a).$$

Beispiele

1. 

   Damit eine Funktion f in einem Punkt a stetig ist, müssen drei Bedingungen erfüllt sein:

   (i) $f(a)$ muss existieren (gilt für f_1,f_2);

   (ii) $\lim\limits_{x\to a} f(x)$ muss existieren (gilt für f_1,f_2);

   (iii) $\lim\limits_{x\to a} f(x) = f(a)$ (gilt nur für f_1).

2. Die Funktion $f : \mathbb{R} \to \mathbb{R}$ mit

$$f(x) = \sqrt{|x|}\sin\left(\frac{1}{x}\right), \qquad x \neq 0,$$
$$f(0) = 0$$

   ist stetig im Nullpunkt, weil

$$\lim_{x\to 0} f(x) = 0.$$

3. Die Funktion $f : \mathbb{R} \to \mathbb{R}$ mit

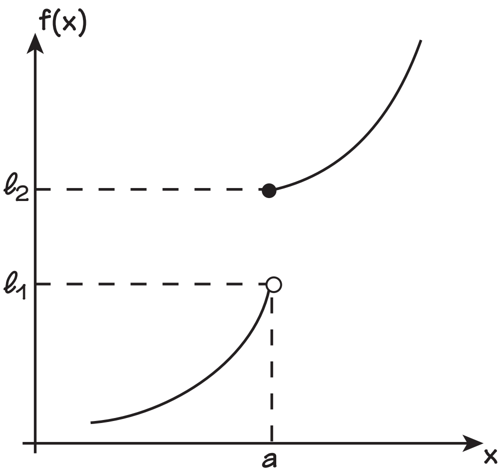
$$\begin{aligned} f(x) &= \sin\left(\tfrac{1}{x}\right), \qquad x \neq 0, \\ f(0) &= 0 \end{aligned}$$

ist nicht stetig im Nullpunkt, weil $\lim_{x \to 0} f(x)$ nicht existiert.

Definitionen

1. Eine reellwertige Funktion f ist **linksseitig (rechtsseitig) stetig** im Punkt a, falls

$$\lim_{x \uparrow a} f(x) = f(a) \qquad \left(\lim_{x \downarrow a} f(x) = f(a) \right).$$



Diese Funktion ist rechtsseitig, aber nicht linksseitig stetig im Punkt a.

2. Eine reellwertige Funktion f ist stetig im offenen Intervall (a,b), falls f stetig in jedem Punkt $x \in (a,b)$ ist.

3. Eine reellwertige Funktion f ist stetig im geschlossenen Intervall $[a,b]$, falls

   (i) f ist stetig in jedem Punkt $x \in (a,b)$;

   (ii) f ist linksseitig stetig im Punkt b;

   (iii) f ist rechtsseitig stetig im Punkt a.

Bemerkung

Definitionsgemäß bedeutet “$\lim_{x \to a} f(x) = f(a)$”:

Zu jedem $\varepsilon > 0$ existiert $\delta > 0$, so dass
$$|f(x) - f(a)| < \varepsilon \qquad \text{für alle } x \text{ mit } 0 < |x-a| < \delta.$$

Es ist aber sicher der Fall, dass $|f(x) - f(a)| < \varepsilon$ für $x = a$ ist. Daher können wir "$0 < |x-a| < \delta$" durch "$|x-a| < \delta$" ersetzen.

Ebenfalls gilt:

$$\lim_{x \to a} f(x) = f(a) \quad \Leftrightarrow \quad \begin{array}{l} f(x_n) \to f(a) \text{ für alle} \\ \text{Folgen } \{x_n\} \text{ mit } x_n \to a \\ \qquad\quad\;\uparrow \\ \text{Die Klausel } x_n \neq a \text{ entfällt} \end{array}$$

Lemma

1. f und g seien stetig im Punkt a. Dann sind $f+g$ und $f.g$ auch im Punkt a stetig. Ist $g(a) \neq 0$, so ist auch $\frac{1}{g}$ im Punkt a stetig.

2. g sei stetig im Punkt a und f sei stetig im Punkt $g(a)$. Dann ist $f \circ g$ ebenfalls stetig im Punkt a.

Beispiele

1. Die Funktionen $f_1, f_2 : \mathbb{R} \to \mathbb{R}$ mit
$$f(x) = c, \qquad f_2(x) = x,$$
wobei c eine beliebige Konstante ist, sind stetig auf $\mathbb{R}$.

   Um dies zu beweisen, müssen wir zeigen:

   Zu jedem $\varepsilon > 0$ existieren $\delta_1, \delta_2 > 0$, so dass
$$\underbrace{|f_1(x) - f_1(a)|}_{=0} < \varepsilon \qquad \text{für alle } x \text{ mit } |x-a| < \delta_1,$$
$$\underbrace{|f_2(x) - f_2(a)|}_{=|x-a|} < \varepsilon \qquad \text{für alle } x \text{ mit } |x-a| < \delta_2$$

   Wir wählen also $\delta_1 = 1$, $\delta_2 = \varepsilon$.

2. Die Funktion $f : \mathbb{R} \to \mathbb{R}$ mit $f(x) = x^n, n \in \mathbb{N}$ ist stetig (Beweis durch vollständige Induktion).

3. Das Polynom
$$a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0,$$
wobei $a_0, \ldots, a_n \in \mathbb{R}$, $n \in \mathbb{N}$ Konstante sind, ist ebenfalls stetig auf $\mathbb{R}$.

4. Eine **rationale Funktion**
$$r(x) = \frac{p(x)}{q(x)},$$
wobei p und q Polynome sind, ist stetig auf $\{x \in \mathbb{R} : q(x) \neq 0\}$.

Satz (Zwischenwertsatz)

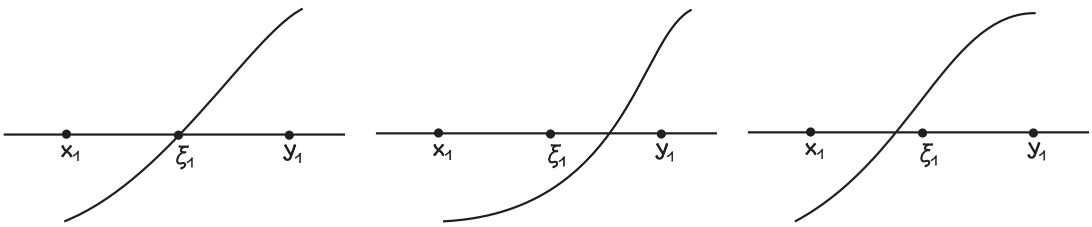
$f : [a,b] \to \mathbb{R}$ sei stetig mit $f(a) < 0$ und $f(b) > 0$. Dann hat f eine Nullstelle im offenen Intervall (a,b).

Beweis

Die Beweismethode heißt **Intervallschachtelung**.

Definiere $x_1 = a$, $y_1 = b$, $\xi_1 = \frac{1}{2}(x_1 + y_1)$. Es gibt drei Fälle:

(i) $f(\xi_1) = 0$ (ii) $f(\xi_1) < 0$ (iii) $f(\xi_1) > 0$



(i) Damit ist das Ergebnis bewiesen

(ii) Definiere $x_2 = \xi_1$, $y_2 = y_1$, so dass $f(x_2) < 0$, $f(y_2) > 0$

(iii) Definiere $x_2 = x_1$, $y_2 = \xi_1$, so dass $f(x_2) < 0$, $f(y_2) > 0$

Nun wiederholen wir den letzten Schritt mit $\xi_2 = \frac{1}{2}(x_2 + y_2)$, usw.

Es gilt: Entweder

(a) $f(\xi_n) = 0$ im $n$ten Schritt dieses Verfahrens

oder

(b) Wir erhalten zwei Folgen $\{x_n\}, \{y_n\}$ mit

- $a = x_1 \leq x_2 \leq x_3 \leq \cdots \leq b$

  $\{x_n\}$ ist monoton steigend und nach oben beschränkt; sie konvergiert gegen $x \in [a,b]$.

  $f(x_n) \to f(x)$ für $n \to \infty$, denn f ist stetig auf $[a,b]$. Aus $f(x_n) < 0$ für alle n folgt $f(x) \leq 0$.

- $b = y_1 \geq y_2 \geq y_3 \geq \ldots \geq a$

  $\{y_n\}$ ist monoton fallend und nach unten beschränkt; sie konvergiert gegen $y \in [a,b]$.

  $f(y_n) \to f(y)$ für $n \to \infty$, denn f ist stetig auf $[a,b]$. Aus $f(y_n) > 0$ für alle n folgt $f(y) \geq 0$.

Aus

$$\begin{aligned} y_1 - x_1 &= b - a, \\ y_{n+1} - x_{n+1} &= \tfrac{1}{2}(y_n - x_n), \qquad n = 1,2,3,\ldots \end{aligned}$$

folgt

$$\underbrace{y_n - x_n}_{\to y - x} = \underbrace{\frac{1}{2^{n-1}}(b-a)}_{\to 0} \qquad \text{(Beweis durch vollständige Induktion)}$$

$$\Rightarrow y = x$$

Aus $f(x) \geq 0$, $f(x) \leq 0$ folgt $f(x) = 0$ und $x \neq a$, $x \neq b$, denn $f(a) < 0, f(b) > 0$.□

Korollar

I sei ein Intervall und $f : I \to \mathbb{R}$ sei stetig. Es seien x_1 und x_2 Zahlen in I mit $x_1 < x_2$. Dann nimmt f im offenen Intervall (x_1,x_2) alle Werte zwischen $f(x_1)$ und $f(x_2)$ an.

Beweis

Falls $f(x_1) = f(x_2)$ ist, ist die Aussage trivial.

Ohne Beschränkung der Allgemeinheit können wir $f(x_1) < f(x_2)$ annehmen. (Ansonsten betrachten wir $-f$ statt f.) Wähle c mit $f(x_1) < c < f(x_2)$ und definiere $g : [x_1,x_2] \to \mathbb{R}$ durch die Formel $g(x) = f(x) - c$. Dann ist g auf $[x_1,x_2]$ stetig mit $g(x_1) = f(x_1) - c < 0$ und $g(x_2) = f(x_2) - c > 0$. Dem Zwischenwertsatz zufolge hat g eine Nullstelle $x^\star \in (x_1,x_2)$, so dass $f(x^\star) = c$ ist. □

Beispiel

Jedes Polynom ungeraden Grades hat eine Nullstelle.

Beweis

Betrachte das Polynom

$$p(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0,$$

wobei $a_0,\ldots,a_n$ Konstante sind und n eine ungerade natürliche Zahl ist. Ohne Beschränkung der Allgemeinheit können wir $a_n > 0$ annehmen.

Es gilt:

- $p(x) \to \infty$ für $x \to \infty$; daher existiert $M > 0$ mit $p(x) > 0$ für $x \geq M$.
- $p(x) \to -\infty$ für $x \to -\infty$; daher existiert $m < 0$ mit $p(x) < 0$ für $x \leq m$.

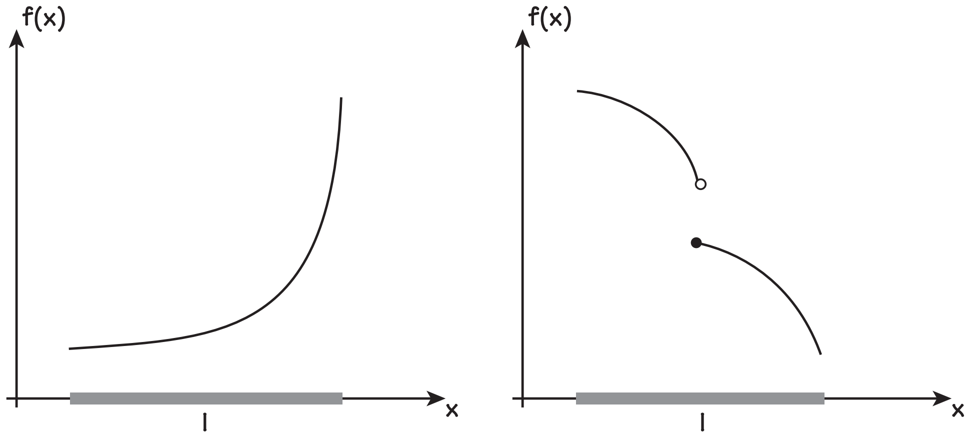
p ist stetig auf $[m,M]$ mit $p(m) < 0, p(M) > 0$. Aus dem Zwischenwertsatz folgt die Existenz einer reellen Zahl $\xi \in (m,M)$ mit $p(\xi) = 0$. □

Umkehrfunktionen

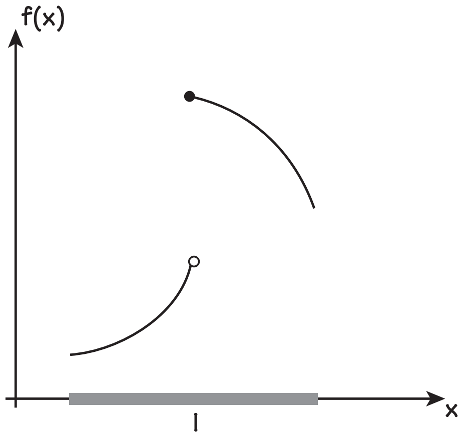
In diesem Abschnitt betrachten wir injektive Funktion $f : I \to \mathbb{R}$, wobei I ein Intervall ist. Eine solche Funktion definiert eine Bijektion $f : I \to \mathcal{R}(f)$ und daher eine Umkehrfunktion $f^{-1} : \mathcal{R}(f) \to I$.

Bemerkung

Streng monoton steigende und streng monoton fallende Funktionen $f : I \to \mathbb{R}$ sind injektiv:



Die Konverse gilt aber nicht:



Diese Funktion ist injektiv aber weder streng monoton steigend noch streng monoton fallend auf I.

Satz

$f : I \to \mathbb{R}$ sei stetig und injektiv. Dann ist f entweder streng monoton steigend oder streng monoton fallend.

Beweis

Zunächst zeigen wir, dass f streng monoton steigend oder streng monoton fallend auf jedem abgeschlossenen Teilintervall $[a,b]$ von I ist.

Da f injektiv ist, ist entweder $f(a) < f(b)$ oder $f(a) > f(b)$. Nehmen wir an, dass $f(a) < f(b)$ ist.

(i) Es gilt $f(a) \leq f(x)$ für alle $x \in [a,b]$:

Existiere $c \in (a,b)$ mit $f(c) < f(a) < f(b)$, so gäbe es dem Korollar zum Zwischenwertsatz zufolge $d \in (c,b)$ mit $f(d) = f(a)$, was der Injektivität von f widersprechen würde.

(ii) f ist streng monoton steigend auf $[a,b]$:

Wäre f nicht streng monoton steigend auf $[a,b]$, so gäbe es x_1, $x_2 \in [a,b]$ mit

$$x_1 < x_2$$

und

$$\begin{aligned}
& f(x_2) \leq f(x_1) & \\
\Rightarrow\ & f(x_2) < f(x_1) & (f \text{ ist injektiv}) \\
\Rightarrow\ & f(a) \leq f(x_2) < f(x_1) & (f(a) \leq f(x) \text{ für alle } x \in [a,b]) \\
\Rightarrow\ & f(a) < f(x_2) < f(x_1) & (f \text{ ist injektiv})
\end{aligned}$$

Es müsste $x_1 > a$ sein, denn $x_1 = a$ führte zum Widerspruch $f(a) < f(x_2) < f(a)$. Dem Korollar zum Zwischenwertsatz zufolge gäbe es $d \in (a,x_1)$ mit $f(d) = f(x_2)$, was der Injektivität von f widersprechen würde.

Falls $f(a) > f(b)$ ist, folgt aus demselben Argument, dass f streng monoton fallend auf $[a,b]$ ist.

Nun schließen wir aus, dass f streng monoton steigend auf einem Teilintervall $I_1 = [a_1,b_1]$ und streng monoton fallend auf einem anderen Teilintervall $I_2 = [a_2,b_2]$ ist. In diesem Fall könnten wir ein abgeschlossenes Intervall I_3 von I wählen, das sowohl I_1 als auch I_2 als Teilmengen enthält. f wäre aber dann entweder streng monoton steigend auf I_3 (und daher auf I_1 und I_2) oder streng monoton fallend auf I_3 (und daher auf I_1 und I_2).

Nun folgt direkt, dass f streng monoton fallend oder streng monoton steigend auf I ist. Es gilt: Entweder

- f ist streng monoton steigend auf allen abgeschlossenen Intervallen $[x_1,x_2] \in I$, so dass $x_1 < x_2 \Rightarrow f(x_1) < f(x_2)$ für alle x_1, $x_2 \in I$

oder

- f ist streng monoton steigend auf allen abgeschlossenen Intervallen $[x_1,x_2] \in I$, so dass $x_1 < x_2 \Rightarrow f(x_1) > f(x_2)$ für alle x_1, $x_2 \in I$ $\square$

Lemma

Es sei I ein offenes Intervall und $f : I \to \mathbb{R}$ sei stetig und streng monoton steigend (fallend). Dann ist $f^{-1} : J \to \mathbb{R}$, $J = \mathcal{R}(f)$ ebenfalls stetig und streng monoton steigend (fallend).

Beweis

Wir behandeln den Fall, dass f streng monoton steigend ist. Der andere Fall wird in ähnlicher Weise behandelt.

Aus
$$x_1 \geq x_2 \quad \Rightarrow \quad f(x_1) \geq f(x_2) \qquad (f \text{ ist monoton steigend})$$
folgt
$$f(x_1) < f(x_2) \quad \Rightarrow \quad x_1 < x_2,$$
denn die zweite Aussage ist die Kontraposition der ersten. Dieses Ergebnis mit $x_1 = f^{-1}(y_1)$, $x_2 = f^{-1}(y_2)$ impliziert
$$y_1 < y_2 \quad \Rightarrow \quad f^{-1}(y_1) < f^{-1}(y_2),$$
so dass f^{-1} streng monoton steigend ist.

Wähle $y_0 \in J$ so, dass y_0 nicht Endpunkt des Intervalls J ist. Wir zeigen nun, dass f^{-1} im Punkt y_0 stetig ist, d.h.

> Zu jedem $\varepsilon > 0$ existiert $\delta > 0$, so dass
> $$|y - y_0| < \delta \quad \Rightarrow \quad |f^{-1}(y) - f^{-1}(y_0)| < \varepsilon$$

Mit $x = f^{-1}(y)$, $x_0 = f^{-1}(y_0)$ ist diese Aussage äquivalent zu

> Zu jedem $\varepsilon > 0$ existiert $\delta > 0$, so dass
> $$|f(x) - f(x_0)| < \delta \quad \Rightarrow \quad |x - x_0| < \varepsilon. \qquad (\star)$$

Ohne Beschränkung der Allgemeinheit können wir annehmen, dass ε klein genug ist, so dass $(x_0 - \varepsilon, x_0 + \varepsilon)$ Teilmenge von I ist.

Da f streng monoton steigend ist, gilt

$$f(x_0 - \varepsilon) < f(x_0) < f(x_0 + \varepsilon).$$

Es existiert also $\delta > 0$, so dass

$$f(x_0 - \varepsilon) \; < \; f(x_0) - \delta \; < \; f(x_0) + \delta \; < \; f(x_0 + \varepsilon),$$

d.h

$$x_0 - \varepsilon \; < \; f^{-1}(f(x_0) - \delta) \; < \; f^{-1}(f(x_0) + \delta) \; < \; x_0 + \varepsilon.$$

Damit gilt

$$f^{-1}(f(x_0) - \delta) < x < f^{-1}(f(x_0) + \delta) \quad \Rightarrow \quad x_0 - \varepsilon < x < x_0 + \varepsilon,$$

d.h.

$$f(x_0) - \delta < f(x) < f(x_0) + \delta \quad \Rightarrow \quad x_0 - \varepsilon < x < x_0 + \varepsilon,$$

und dies ist genau Aussage $(\star)$.

Dasselbe Argument zeigt, dass f in den Endpunkten von J (falls vorhanden) stetig ist. Wir brauchen lediglich alle zweiseitigen Ungleichungen und Grenzwerte durch einseitige Ungleichungen und Grenzwerte zu ersetzen. $\square$

Beschränktheit

Es seien A eine nichtleere Menge und $f : A \to \mathbb{R}$ eine Funktion mit Bildmenge

$$\underbrace{\mathcal{R}(f) = \{f(a) : a \in A\}}_{\text{Eine nichtleere Menge reeller Zahlen}}$$

- $\mathcal{R}(f)$ könnte nach oben beschränkt sein (d. h. sie könnte eine obere Schranke haben). In diesem Fall hat sie ein Supremum und, falls das Supremum Element in $\mathcal{R}(f)$ ist, auch ein Maximum.

  Üblicherweise sprechen wir von **einer oberen Schranke für** f (statt für $\mathcal{R}(f)$) und bezeichnen das Supremum und ggf. das Maximum von $\mathcal{R}(f)$ als **Supremum** bzw. **Maximum von** f **auf** A. Wir benutzen die Schreibweise

  $$\sup_{x \in A} f(x), \qquad \max_{x \in A} f(x)$$

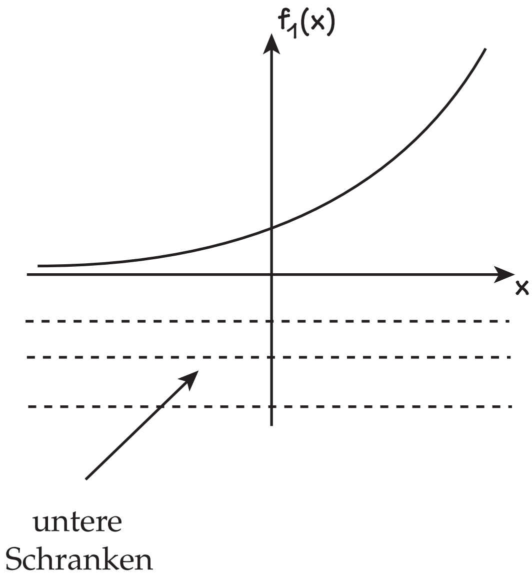
  und sagen: "f ist nach oben beschränkt".

- $\mathcal{R}(f)$ könnte nach unten beschränkt sein, so dass sie ein Infimum und ggf. ein Minimum hat. Üblicherweise sprechen wir von **einer unteren Schranke, dem Infimum und Minimum von f auf A** und benutzen die Schreibweise

$$\inf_{x\in A} f(x), \qquad \min_{x\in A} f(x).$$

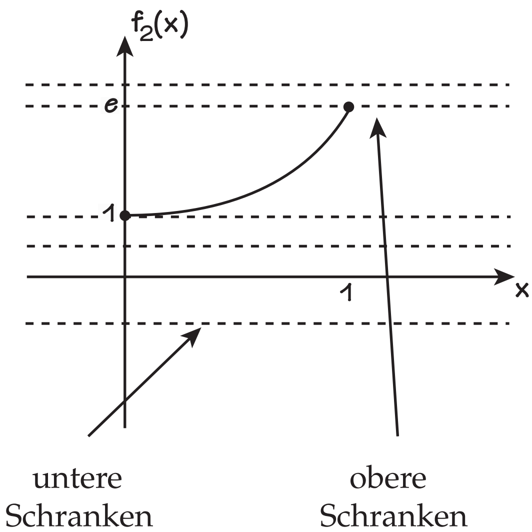
Wir sagen: "f ist nach unten beschränkt".

Beispiele



Die Funktion $f_1 : \mathbb{R} \to \mathbb{R}$, $f_1(x) = \mathrm{e}^x$ ist nach unten, aber nicht nach oben beschränkt.

- $\inf\limits_{x\in\mathbb{R}} f_1(x) = 0$
- $\min\limits_{x\in\mathbb{R}} f_1(x)$ existiert nicht



Die Funktion $f_2 : [0,1] \to \mathbb{R}$, $f_2(x) = \mathrm{e}^x$ ist nach oben und nach unten beschränkt.

- $\inf\limits_{x\in[0,1]} f_2(x) = \min\limits_{x\in[0,1]} f_2(x) = 1$
- $\sup\limits_{x\in[0,1]} f_2(x) = \max\limits_{x\in[0,1]} f_2(x) = \mathrm{e}$

Satz

$f : [a,b] \to \mathbb{R}$ sei stetig. Dann gilt:

(i) f ist nach unten und nach oben beschränkt ($\sup\limits_{x\in[a,b]} f(x)$, $\inf\limits_{x\in[a,b]} f(x)$ existieren);

(ii) Ihr Supremum und ihr Infimum wird angenommen ($\max\limits_{x\in[a,b]} f(x)$, $\min\limits_{x\in[a,b]} f(x)$ existieren).

Beweis

(i) Nehmen wir an, f ist nicht nach oben beschränkt.

Zu jedem $n \in \mathbb{N}$ existiert also $x_n \in [a,b]$, so dass $f(x_n) > n$ ist. Die Folge $\{f(x_n)\}$ ist also nicht beschränkt und dasselbe gilt für jede Teilfolge $\{f(x_{n_k})\}$ von $\{f(x_n)\}$, denn $f(x_{n_k}) > n_k$.

Aus $x_n \in [a,b]$ für jedes n folgt, dass $\{x_n\}$ beschränkt ist. Sie hat daher eine konvergente Teilfolge $\{x_{n_k}\}$. Da f stetig ist, konvergiert $\{f(x_{n_k})\}$ und ist daher beschränkt.

Damit haben wir einen Widerspruch.

(ii) $\mathcal{R}(f)$ ist eine nichtleere, nach oben beschränkte Menge reeller Zahlen. Es existiert also eine maximierende Folge $\{y_n\}$ mit $y_n \in \mathcal{R}(f)$ und $y_n \to \sup \mathcal{R}(f)$ für $n \to \infty$. Offensichtlich ist $y_n = f(x_n)$ für irgendein $x_n \in [a,b]$, so dass

$$f(x_n) \to \sup_{x\in[a,b]} f(x)$$

für $n \to \infty$. Da $\{f(x_n)\}$ gegen $\sup\limits_{x\in[a,b]} f(x)$ konvergiert, konvergiert auch jede Teilfolge $\{f(x_{n_k})\}$ von $\{f(x_n)\}$ gegen $\sup\limits_{x\in[a,b]} f(x)$.

Aus $x_n \in [a,b]$ für jedes n folgt, dass $\{x_n\}$ beschränkt ist. Sie hat daher eine konvergente Teilfolge $\{x_{n_k}\}$. $\widehat{x} \in [a,b]$ sei ihr Grenzwert. Da f stetig ist, gilt

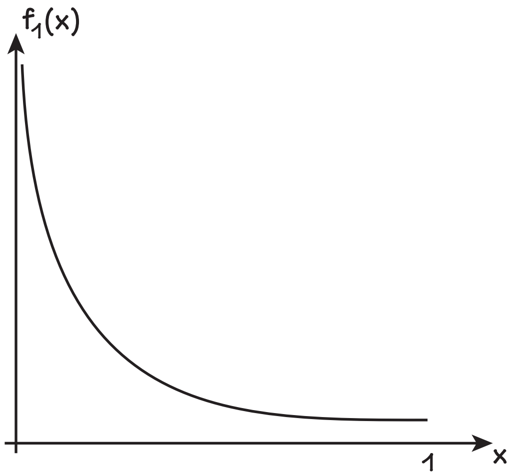
$$\underbrace{\lim_{n_k\to\infty} f(x_{n_k})}_{=\sup\limits_{x\in[a,b]} f(x)} = f(\widehat{x}).$$

Das Supremum von f auf $[a,b]$ wird also im Punkt $\hat{x} \in [a,b]$ angenommen.

Die Aussagen übers Infimum und Minimum werden in ähnlicher Weise bewiesen. $\square$

Bemerkung

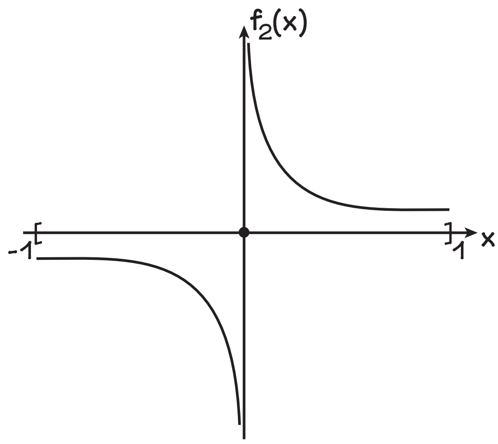
Man kann nicht auf die Voraussetzung verzichten, dass f **stetig** auf einem **endlichen**, **abgeschlossenen** Intervall ist:



Die Funktion $f_1 : (0,1) \to \mathbb{R}$ mit

$$f_1(x) = \frac{1}{x}$$

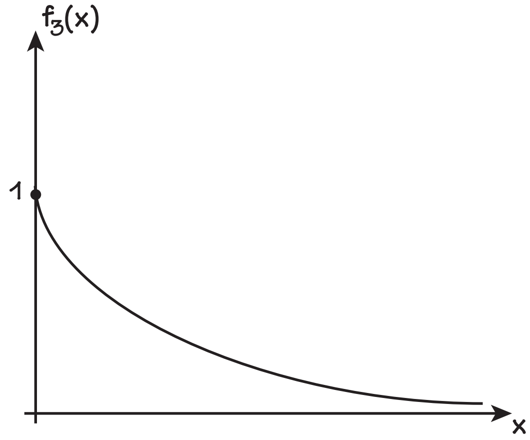
ist stetig, aber nicht beschränkt.



Die Funktion $f_2 : [-1,1] \to \mathbb{R}$ mit

$$f_2(x) = \tfrac{1}{x}, \quad x \neq 0,$$
$$f_2(0) = 0$$

ist nicht stetig und nicht beschränkt.



Die Funktion $f_3 : [0,\infty) \to \mathbb{R}$ mit

$$f_3(x) = \mathrm{e}^{-x}$$

ist stetig und beschränkt, hat aber kein Minimum.

Korollar

$f : [a,b] \to \mathbb{R}$ sei eine nichtkonstante stetige Funktion. Ihre Bildmenge ist ebenfalls ein endliches, abgeschlossenes Intervall.

Beweis

Es existieren x_m, x_M mit $f(x_m) = m$, $f(x_M) = M$, wobei

$$m = \min_{x\in[a,b]} f(x), \qquad M = \max_{x\in[a,b]} f(x).$$

Aus dem Korollar zum Zwischensatz folgt, dass f alle Werte zwischen m und M annimmt, so dass

$$f([a,b]) = [m,M]. \qquad \square$$

Bemerkung

I sei ein beliebiges Intervall und $f : I \to \mathbb{R}$ sei eine nichtkonstante stetige Funktion. Die obige Beweismethode zeigt, dass $f(I)$ gleich (i,s), $[m,s)$, (i,M) oder $[m,M]$

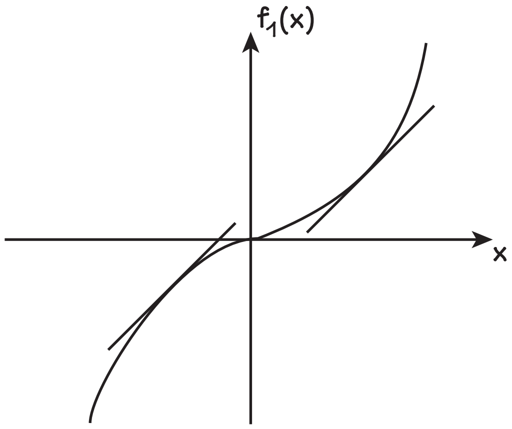
ist, wobei

$$
\begin{aligned}
i &= \inf_{x\in I} f(x) && (-\infty, \text{ falls } f \text{ nicht nach unten beschränkt ist}),\\
s &= \inf_{x\in I} f(x) && (\infty, \text{ falls } f \text{ nicht nach oben beschränkt ist}),\\
m &= \min_{x\in I} f(x),\\
M &= \max_{x\in I} f(x).
\end{aligned}
$$

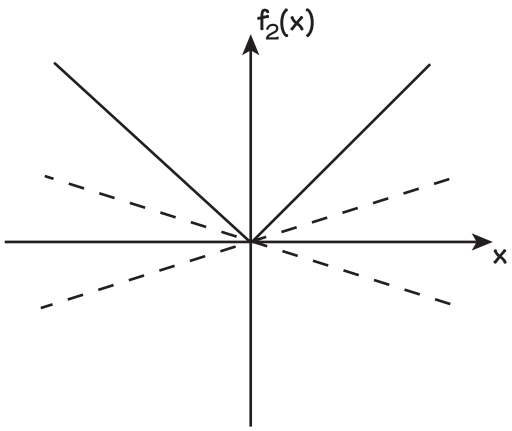
5 Differentialrechnung

Einführung: Tangente

Informell formuliert ist die Tangente an einen Graphen in einem Punkt P die eindeutige Gerade, die den Graphen an diesem Punkt "berührt".

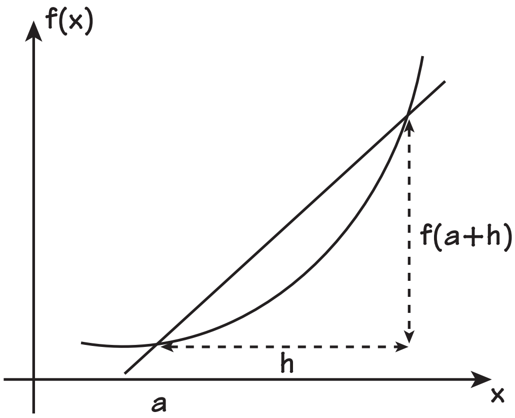


Der Graph von $f_1(x) = x^3$ hat eine Tangente in jedem Punkt.



Der Graph von $f_2(x) = |x|$ hat keine Tangente im Nullpunkt.

Wir können den Begriff "Tangente" rigoros einführen, indem wir mit **Sekanten** anfangen. Eine Sekante ist eine Gerade, die einen Graphen in zwei Punkten schneidet.



Die Steigung dieser Sekanten ist

$$\frac{f(a+h)-f(a)}{h}.$$

Im Limes $h \to 0$ wird aus der Sekanten die Tangente an den Graphen von f im Punkt $(a,f(a))$. Die Steigung dieser Tangenten ist

$$\lim_{h\to 0}\frac{f(a+h)-f(a)}{h}.$$

Definitionen

1. Eine reellwertige Funktion f heißt **differenzierbar** im Punkt a, falls der Grenzwert
$$\lim_{h\to 0}\frac{f(a+h)-f(a)}{h}$$
existiert. In diesem Fall heißt der obige Grenzwert **Ableitung von** f **im Punkt** a und wird geschrieben als $f'(a)$.

2. f sei differenzierbar im Punkt a. Die **Tangente** an den Graphen von f im Punkt a ist die Gerade mit Steigung $f'(a)$, die durch $(a,f(a))$ läuft.

Beispiele

1. $f_1 : \mathbb{R} \to \mathbb{R}$, $f_1(x) = x^3$ ist in jedem Punkt differenzierbar, denn
$$\begin{aligned}\frac{f_1(a+h)-f_1(a)}{h} &= \frac{(a+h)^3-a^3}{h}\\ &= \frac{3a^2h+3ah^2+h^3}{h}\\ &= 3a^2+3ah+h^2\\ &\to 3a^2 \qquad \text{für } h\to 0.\end{aligned}$$

Daher ist $f_1'(a) = 3a^2$.

2. $f_2 : \mathbb{R} \to \mathbb{R}$, $f_2(x) = |x|$ ist im Nullpunkt nicht differenzierbar, denn

$$\lim_{h\downarrow 0} \frac{f_2(0+h) - f_2(0)}{h} = \lim_{h\downarrow 0} \frac{|h|}{h} = 1,$$

$$\lim_{h\uparrow 0} \frac{f_2(0+h) - f_2(0)}{h} = \lim_{h\uparrow 0} \frac{|h|}{h} = -1,$$

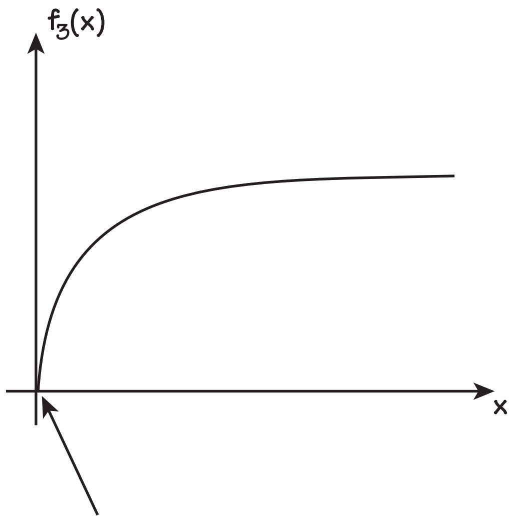
so dass

$$\lim_{h\to 0} \frac{f_2(0+h) - f_2(0)}{h}$$

nicht existiert. Allerdings ist diese Funktion sowohl **linksseitig differenzierbar** als auch **rechtsseitig differenzierbar** im Nullpunkt.

3. $f_3 : [0,\infty) \to \mathbb{R}, f_3(x) = \sqrt{x}$ ist im Nullpunkt nicht rechtsseitig differenzierbar, denn

$$\begin{aligned} \frac{f_3(0+h) - f_3(0)}{h} &= \frac{\sqrt{h}}{h} \\ &= \frac{1}{\sqrt{h}} \\ &\to \infty \qquad \text{für } h \downarrow 0. \end{aligned}$$



Der Graph von f_3 hat eine
"senkrechte Tangente" hier

4. $f_4 : \mathbb{R} \to \mathbb{R}, f_4(x) = mx + c$, wobei m,c Konstante sind, ist in jedem Punkt differenzierbar. Es gilt:

$$\begin{aligned} f_4'(x) &= \lim_{h\to 0} \frac{m(x+h)+c-mx-c}{h} \\ &= \lim_{h\to 0} m \\ &= m \end{aligned}$$

   Der Graph von f_4 ist eine Gerade, und die Tangente an den Graphen im Punkt $(x,f_4(x))$ ist diese Gerade selbst.

5. Wir werden später beweisen, dass f_5, f_6, $f_7 : \mathbb{R} \to \mathbb{R}$ mit

$$f_5(x) = \sin x, \quad f_6(x) = \cos x, \quad f_7(x) = \mathrm{e}^x$$

   in jedem Punkt differenzierbar sind und

$$f_5'(x) = \cos x, \quad f_6'(x) = -\sin x, \quad f_7'(x) = \mathrm{e}^x.$$

Lemma

f sei differenzierbar im Punkt a. Dann ist f auch stetig im Punkt a.

Beweis

Es gilt:

$$\begin{aligned} \lim_{h\to 0} f(a+h) - f(a) &= \lim_{h\to 0} [f(a+h) - f(a)] \\ &= \lim_{h\to 0} \left[\frac{f(a+h)-f(a)}{h} h\right] \\ &= \underbrace{\lim_{h\to 0} \frac{f(a+h)-f(a)}{h}}_{=f'(a)} \underbrace{\lim_{h\to 0} h}_{=0} \\ &= 0. \end{aligned}$$

□

Definition

Eine reellwertige Funktion $f : I \to \mathbb{R}$ heißt differenzierbar auf $J \subseteq I$, wenn sie in jedem Punkt $x_0 \in J$ differenzierbar ist. Die durch

$$x_0 \mapsto f'(x_0)$$

definierte Funktion $f' : J \to \mathbb{R}$ heißt **Ableitungsfunktion** oder **Ableitung** von f.

Bemerkungen

1. Oft schreibt man $f'(x)$ als
$$\frac{df}{dx}(x).$$
Dies ist die **Leibniz-Schreibweise** für die Ableitung.

2. Da $f' : J \to \mathbb{R}$ ebenfalls eine Funktion ist, kann man sie auf Differenzierbarkeit untersuchen. Ihre Ableitung $(f')' : K \to \mathbb{R}$, $K \subseteq J$ heißt **zweite Ableitung** von f und wird auch geschrieben als
$$f'', f^{(2)} \text{ oder } \frac{d^2 f}{dx^2}.$$
Wenn wir dieses Verfahren induktiv fortsetzen, können wir die $n$te Ableitung von f definieren. Sie wird geschrieben als
$$f^{(n)} \text{ oder } \frac{d^n f}{dx^n}.$$

Rechenregeln für differenzierbare Funktionen

Satz

f,g seien im Punkt a differenzierbar. Dann sind $f+g$,fg im Punkt a differenzierbar mit

$$(f+g)'(a) = f'(a) + g'(a),$$
$$(fg)'(a) = f'(a)g(a) + f(a)g'(a). \qquad \textbf{(Produktregel)}$$

Falls $g(a) \neq 0$ ist, ist $\frac{1}{g}$ im Punkt a ebenfalls differenzierbar mit

$$\left(\frac{1}{g}\right)'(a) = \frac{-g'(a)}{(g(a))^2}.$$

Beweis

Es gilt:

$$\begin{aligned}
(fg)'(a) &= \lim_{h\to 0} \frac{f(a+h)g(a+h) - f(a)g(a)}{h} \\
&= \lim_{h\to 0} \frac{[f(a+h) - f(a)]g(a+h) + [g(a+h) - g(a)]f(a)}{h} \\
&= \underbrace{\lim_{h\to 0} \frac{f(a+h) - f(a)}{h}}_{= f'(a)} \underbrace{\lim_{h\to 0} g(a+h)}_{\substack{= g(a) \\ \text{weil } g \text{ stetig} \\ \text{im Punkt } a \text{ ist}}} + f(a) \underbrace{\lim_{h\to 0} \frac{g(a+h) - g(a)}{h}}_{= g'(a)} \\
&= f'(a)g(a) + f(a)g'(a).
\end{aligned}$$

Die anderen Aussagen werden in ähnlicher Weise bewiesen. □

Korollar (Quotientenregel)

f,g seien differenzierbar im Punkt a und $g(a) \neq 0$. Dann ist f/g ebenfalls im Punkt a differenzierbar mit

$$\left(\frac{f}{g}\right)'(a) = \frac{f'(a)g(a) - f(a)g'(a)}{(g(a))^2}.$$

Beispiel

Zeigen Sie, dass die Funktion $f_n : \mathbb{R} \to \mathbb{R}$ mit $f_n(x) = x^n$, $n \in \mathbb{N}$ differenzierbar auf $\mathbb{R}$ mit $f_n'(x) = nx^{n-1}$ ist.

Lösung

Dies zeigen wir durch vollständige Induktion.

Induktionsanfang: Wir haben schon gezeigt, dass $f_1'(x)$ existiert und $f_1'(x) = 1$ ist.

Induktionsschluss: Wir müssen zeigen, dass die Induktionsvoraussetzung

$$f_k'(x) \text{ existiert,} \quad f_k'(x) = kx^{k-1}$$

die Induktionsbehauptung

$$f_{k+1}'(x) \text{ existiert,} \quad f_{k+1}'(x) = (k+1)x^k$$

impliziert.

Da

$$f_{k+1}(x) = \underset{\substack{\uparrow \\ \text{differenzierbar}}}{f_k(x)} \times \underset{\substack{\uparrow \\ \text{differenzierbar}}}{x}$$

ist, ist f_{k+1} ebenfalls differenzierbar mit

$$\begin{aligned} f_{k+1}'(x) &= f_k'(x)x + f_k(x).1 \\ &= kx^{k-1}x + x^k \\ &= (k+1)x^k. \end{aligned}$$

□

Bemerkung

Eine reellwertige Funktion f ist im Punkt a genau dann differenzierbar, wenn es eine reelle Zahl α und eine reellwertige Funktion r gibt mit

$$f(a+h) - f(a) = \alpha h + hr(h)$$

und

$$r(h) \to 0 \qquad \text{für } h \to 0.$$

In diesem Fall ist $f'(a) = \alpha$. (Diese ist nämlich genau die Aussage

$$\frac{f(a+h) - f(a)}{h} - \alpha \to 0 \qquad \text{für } h \to 0.)$$

Lemma (Kettenregel)

f sei im Punkt a differenzierbar und g sei im Punkt $f(a)$ differenzierbar. Dann ist $g \circ f$ im Punkt a differenzierbar mit

$$(g \circ f)'(a) = g'(f(a))f'(a).$$

Beweis

Setze $b = f(a)$. Wir wissen:

- $f(a + h_1) - f(a) = f'(a)h_1 + h_1 r_1(h_1) \qquad \text{mit } r_1(h_1) \to 0 \text{ für } h_1 \to 0 \qquad (1)$
- $g(b + h_2) - g(b) = g'(b)h_2 + h_2 r_2(h_2) \qquad \text{mit } r_2(h_2) \to 0 \text{ für } h_2 \to 0 \qquad (2)$

Wir wollen beweisen:

- $g(f(a + h)) - g(b) = g'(b)f'(a)h + hr(h) \qquad \text{mit } r(h) \to 0 \text{ für } h \to 0$

Es gilt nun

$$\begin{aligned} g(f(a+h)) &= g(f(a) + k) \qquad \text{mit } k = f'(a)h + hr_1(h) \text{ (wegen (1) mit } h_1 = h) \\ &= g(b + k) \\ &= g(b) + g'(b)k + kr_2(k) \qquad \text{(wegen (2) mit } h_2 = k) \\ &= g(b) + g'(b)f'(a)h + h\big(\underbrace{g'(b)r_1(h) + (f'(a) + r_1(h))r_2(k)}_{:= r(h)}\big) \end{aligned}$$

und aus $k \to 0$ und folglich $r_2(k) \to 0$ für $h \to 0$ sowie $r_1(h) \to 0$ für $h \to 0$ folgt $r(h) \to 0$ für $h \to 0$. $\square$

Beispiel

$$\begin{aligned} \frac{\mathrm{d}}{\mathrm{d}x}(\mathrm{e}^{\sin x})^3 &= 3(\mathrm{e}^{\sin x})^2 \frac{\mathrm{d}}{\mathrm{d}x}(\mathrm{e}^{\sin x}) \\ &= 3(\mathrm{e}^{\sin x})^2\, \mathrm{e}^{\sin x} \frac{\mathrm{d}}{\mathrm{d}x}(\sin x) \\ &= 3(\mathrm{e}^{\sin x})^2\, \mathrm{e}^{\sin x} \cos x. \end{aligned}$$

Lemma

Es sei $f : I \to J$ eine stetige, bijektive Funktion mit stetiger Umkehrfunktion $f^{-1} : J \to I$, wobei I, J offene Intervalle sind. Ferner sei f differenzierbar im Punkt a.

f^{-1} ist differenzierbar im Punkt $b = f(a)$ genau dann, wenn $f'(a) \neq 0$ ist. In diesem Fall gilt

$$(f^{-1})'(b) = \frac{1}{f'(a)}.$$

Beweis

- Es sei $f'(a) \neq 0$.

  Es seien $h \neq 0$ und $k = f^{-1}(b+h) - f^{-1}(b)$. Da f^{-1} stetig ist, gilt $k \to 0$ für $h \to 0$. Somit gilt

  $$\lim_{h\to 0} \frac{f^{-1}(b+h) - f^{-1}(b)}{h} = \lim_{h\to 0} \frac{k}{f(a+k) - f(a)} = \frac{1}{f'(a)},$$

  d.h. f^{-1} is differenzierbar im Punkt b mit

  $$(f^{-1})'(b) = \frac{1}{f'(a)}.$$

- Nun sei f^{-1} differenzierbar im Punkt b. Wir nehmen an, dass $f'(a) \neq 0$. Aus der Kettenregel folgt

  $$(f \circ f^{-1})'(b) = f'(f^{-1}(b))(f^{-1})'(b) = f'(a)(f^{-1})'(b) = 0.$$

  Auf der anderen Seite ist

  $$(f \circ f^{-1})'(y) = y \qquad \text{für alle } y \in J,$$

  so dass

  $$(f \circ f^{-1})'(b) = 1.$$

  Dies ist ein Widerspruch. □

Extrema

Definitionen

Die Funktion $f : I \to \mathbb{R}$ hat

(i) ein **globales Maximum** im Punkt $x_0 \in I$, falls $f(x) \leq f(x_0)$ für $x \in I$.

(ii) ein **globales Minimum** im Punkt $x_0 \in I$, falls $f(x) \geq f(x_0)$ für $x \in I$.

(iii) ein **lokales Maximum** im Punkt $x_0 \in I$, wenn es ein $\delta > 0$ gibt, so dass

$$f(x) \leq f(x_0) \qquad \text{für } x \in I \cap (x_0 - \delta, x_0 + \delta).$$

(iv) ein **lokales Minimum** im Punkt $x_0 \in I$, wenn es ein $\delta > 0$ gibt, so dass

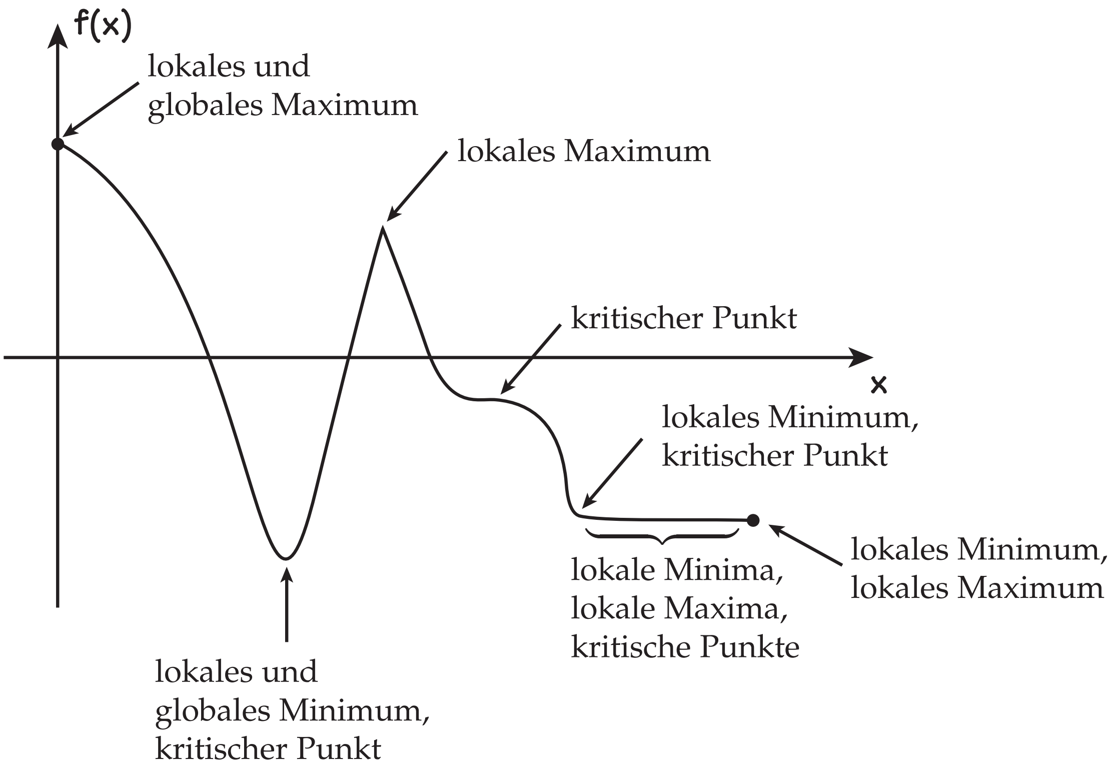
$$f(x) \geq f(x_0) \qquad \text{für } x \in I \cap (x_0 - \delta, x_0 + \delta).$$

(v) einen **kritischen Punkt** in $x_0 \in I$, falls $f'(x_0)$ existiert und

$$f'(x_0) = 0.$$

Ein lokales (globales) **Extremum** ist ein lokales (globales) Maximum oder Minimum.

Beispiel



Lemma

Die Funktion $f : I \to \mathbb{R}$ sei differenzierbar im Punkt $x_0 \in I$ und habe ein lokales Extremum in diesem Punkt. Dann gilt

$$f'(x_0) = 0.$$

Beweis

Wir behandeln den Fall, dass f ein lokales Maximum im Punkt $x_0 \in I$ hat.

Es existiert $\delta > 0$, so dass

$$f(x_0 + h) \leq f(x_0) \qquad \text{für } |h| < \delta.$$

Daher gilt:

$$f(x_0 + h) - f(x_0) \leq 0 \qquad \text{für } |h| < \delta$$

$$\Rightarrow \frac{f(x_0+h) - f(x_0)}{h} \leq 0 \quad \text{für } 0 < h < \delta \qquad\qquad \frac{f(x_0+h) - f(x_0)}{h} \geq 0 \quad \text{für } -\delta < h < 0$$

$$\Rightarrow \lim_{h \downarrow 0} \frac{f(x_0+h) - f(x_0)}{h} \leq 0 \qquad\qquad \lim_{h \uparrow 0} \frac{f(x_0+h) - f(x_0)}{h} \geq 0$$

Weil

$$f'(x_0) = \lim_{h \to 0} \frac{f(x_0+h) - f(x_0)}{h}$$

existiert, existieren die beiden einseitigen Grenzwerte und alle drei Grenzwerte sind geich. Sie sind also alle gleich 0.

Der andere Fall wird in ähnlicher Weise behandelt. $\square$

Bemerkungen

1. x_0 ist kritischer Punkt von f $\not\Rightarrow$ x_0 ist ein lokales Extremum von f.

2. Um die lokalen Extrema einer Funktion $f : [a,b] \to \mathbb{R}$ zu orten, müssen wir betrachten:

- die kritischen Punkte von f in (a,b);
- die Endpunkte a,b;
- Punkte in (a,b), in denen f nicht differenzierbar ist.

3. Betrachte eine Funktion $f : [a,b] \to \mathbb{R}$. Die Beweistechnik des letzten Lemmas zeigt:

$$\begin{array}{lcc}
-\text{ a ist ein lokales Minimum von } f & \Rightarrow & f'(a) \geq 0 \\
 & & \uparrow \\
 & & \text{rechtsseitige Ableitungen} \\
 & & \downarrow \\
-\ a \text{ ist ein lokales Maximum von } f & \Rightarrow & f'(a) \leq 0
\end{array}$$

$$\begin{array}{lcc}
-\text{ b ist ein lokales Minimum von } f & \Rightarrow & f'(b) \leq 0 \\
 & & \uparrow \\
 & & \text{linksseitige Ableitungen} \\
 & & \downarrow \\
-\ b \text{ ist ein lokales Maximum von } f & \Rightarrow & f'(b) \geq 0
\end{array}$$

Satz (Satz von Rolle)

$f : [a,b] \to \mathbb{R}$ sei stetig und im offenen Intervall (a,b) differenzierbar. Es gelte $f(a) = f(b)$. Dann existiert $c \in (a,b)$ mit

$$f'(c) = 0.$$

Beweis

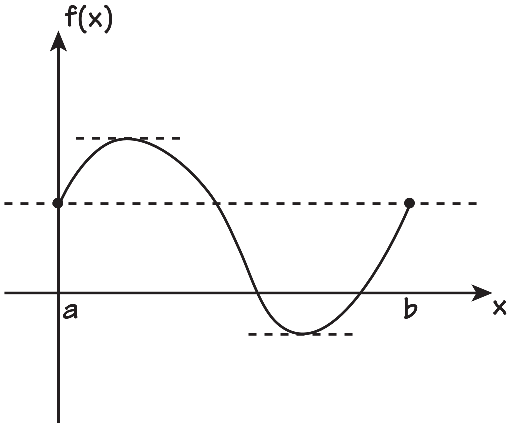
Da f stetig auf $[a,b]$ ist, hat f ein globales Minimum x_m und ein globales Maximum x_M auf $[a,b]$.

Falls $x_m \in (a,b)$ ist, ist x_m kritischer Punkt von f.

Falls $x_M \in (a,b)$ ist, ist x_M kritischer Punkt von f.

Sonst gilt $f(x_m) = f(a) = f(b)$, $f(x_M) = f(a) = f(b)$ und daher $f(x_m) = f(x_M)$. f ist also konstant auf $[a,b]$, so dass $f'(x) = 0$ für alle $x \in (a,b)$ ist. $\square$

Zum Satz von Rolle



Falls f nicht konstant ist, existiert mindestens ein lokales Extremum von f in (a,b).

Der erste Mittelwertsatz

Satz (Erster Mittelwertsatz)

$f : [a,b] \to \mathbb{R}$ sei stetig und im offenen Intervall (a,b) differenzierbar. Dann existiert $c \in (a,b)$ mit

$$f'(c) = \frac{f(b) - f(a)}{b - a}.$$

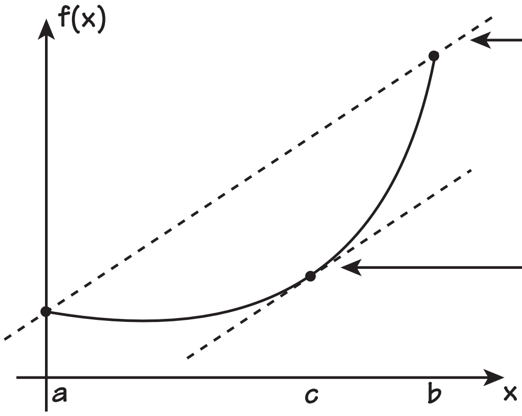
Beweis

Wende den Satz von Rolle auf die Funktion

$$h(x) = f(x) - \left[\frac{f(b) - f(a)}{b - a}\right](x - a)$$

an. $\square$

Zum ersten Mittelwertsatz



Sekante durch $(a,f(a))$ und $(b,f(b))$.
Steigung:
$$\frac{f(b)-f(a)}{b-a}$$

Die Tangente durch $(c,f(c))$ hat auch diese Steigung.

Korollar

$f : I \to \mathbb{R}$ differenzierbar. Es gilt:

(i) $f'(x) \geq 0$ für alle $x \in I \Rightarrow f$ ist monoton steigend auf I

(ii) $f'(x) > 0$ für alle $x \in I \Rightarrow f$ ist streng monoton steigend auf I

(iii) $f'(x) \leq 0$ für alle $x \in I \Rightarrow f$ ist monoton fallend auf I

(iv) $f'(x) < 0$ für alle $x \in I \Rightarrow f$ ist streng monoton fallend auf I.

(v) $f'(x) = 0$ für alle $x \in I \Rightarrow f$ ist konstant auf I.

Beweis

(i) Wir müssen zeigen:
$$a < b \;\Rightarrow\; f(a) \leq f(b)$$
für alle $a,b \in I$.

Wähle $a,b \in I$ mit $a < b$. Dann ist f stetig auf $[a,b]$ und differenzierbar auf (a,b). Dem ersten Mittelwertsatz zufolge existiert $c \in (a,b)$ mit
$$\underbrace{f'(c)}_{\geq 0} = \frac{f(b)-f(a)}{b-a}$$
$$\Rightarrow f(b) \geq f(a).$$

Die anderen Aussagen werden in ähnlicher Weise bewiesen. □

Bemerkung

Die Umkehrungen von (i), (iii) sind gültig, die von (ii), (iv) jedoch nicht: Die Funktion $f(x) = x^3$ ist streng monoton steigend auf $\mathbb{R}$ aber $f'(0) = 0$.

Beispiel (Kurvendiskussion)

Zeichnen Sie den Graphen der Funktion $f : \mathbb{R} \setminus \{1\} \to \mathbb{R}$ mit

$$f(x) = \frac{x^2 - 2x + 2}{x - 1} .$$

Lösung

- Nullstellen: $f(x) \neq 0$, $x \in \mathbb{R}$
- Kritische Punkte:
  $f'(x) = \dfrac{x(x-2)}{(x-1)^2}$
  $\Rightarrow f'(0) = 0, f'(2) = 0$

  Die entsprechenden Werte von f : $f(0) = -2$, $f(2) = 2$
- Steigung:
  $f'(x) > 0$ für $x < 0$
  $f'(x) < 0$ für $0 < x < 1$
  $f'(x) < 0$ für $1 < x < 2$
  $f'(x) > 0$ für $x > 2$
- Asymptote: f hat die vertikale Asymptote $x = 1$. Es gilt

  $$\begin{aligned} \frac{x^2 - 2x + 2}{x - 1} &= \frac{(x-1)^2 + 1}{x - 1} \\ &= x - 1 + \frac{1}{x - 1}, \end{aligned}$$

  so dass

  $$\lim_{x \uparrow 1} f(x) = -\infty, \quad \lim_{x \downarrow 1} f(x) = \infty$$

- Verhalten für große Werte von $|x|$: Aus

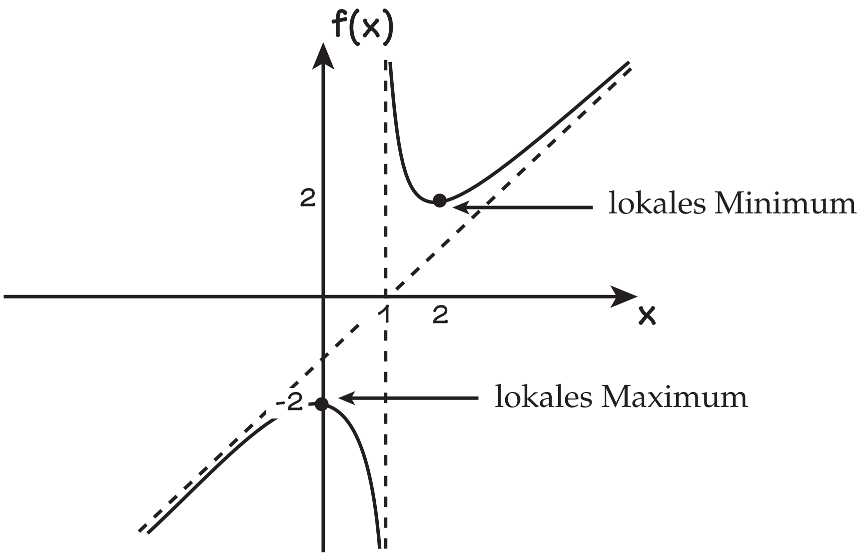
$$f(x) = x - 1 + \frac{1}{x-1}$$

folgt

$$\frac{f(x)}{x-1} = 1 + \frac{1}{(x-1)^2}$$
$$\Rightarrow \frac{f(x)}{x-1} \to 1 \quad \text{für} \quad x \to \pm\infty$$

und

$$\frac{f(x)}{x-1} > 1 \quad \text{für} \quad x \in \mathbb{R} \setminus \{1\}$$
$$\Rightarrow f(x) > x - 1 \text{ für } x > 1, \qquad f(x) < x - 1 \text{ für } x < 1.$$



Der zweite Mittelwertsatz

Satz (Zweiter Mittelwertsatz)

$f,g : [a,b] \to \mathbb{R}$ seien stetig und im offenen Intervall (a,b) differenzierbar. Es existiert $c \in (a,b)$ mit

$$[f(b) - f(a)]g'(c) = [g(b) - g(a)]f'(c).$$

Beweis

Wende den Satz von Rolle auf die Funktion

$$h(x) = f(x)[g(b) - g(a)] - g(x)[f(b) - f(a)]$$

an. □

Satz (Die Regeln von L'Hôpital)

Es existiere $\delta > 0$, so dass f,g stetig auf $[a - \delta, a + \delta]$ und differenzierbar auf $(a - \delta, a + \delta)$ ist.

Es gelte $f(a) = g(a) = 0$ und es existiere der Grenzwert

$$\lim_{x \to a} \frac{f'(x)}{g'(x)} . \tag{$\star$}$$

Dann gilt

$$\lim_{x \to a} \frac{f(x)}{g(x)} = \lim_{x \to a} \frac{f'(x)}{g'(x)} .$$

Diese Aussage bleibt richtig, wenn die Grenzwerte durch einseitige Grenzwerte ersetzt werden.

Beweis

$\{x_n\}$ sei eine beliebige Folge mit $x_n \in (a - \delta, a + \delta), x_n \neq a$ für jedes $n \in \mathbb{N}$ und $x_n \to a$ für $n \to \infty$.

f,g sind stetig auf $[a, x_n]$, bzw. $[x_n, a]$ und differenzierbar auf (a, x_n) bzw. (x_n, a). Dem zweiten Mittelwertsatz zufolge existiert $y_n \in (a, x_n)$ bzw. (x_n, a) mit

$$\begin{aligned} & f'(y_n)[g(x_n) - g(a)] = g'(y_n)[f(x_n) - f(a)] \\ \Rightarrow\ & \frac{f(x_n)}{g(x_n)} = \frac{f'(y_n)}{g'(y_n)}. \end{aligned}$$

Da $y_n \to a$ für $n \to \infty$, gilt

$$\lim_{n\to\infty} \frac{f(x_n)}{g(x_n)} = \underbrace{\lim_{n\to\infty} \frac{f'(y_n)}{g'(y_n)} = \lim_{y\to a} \frac{f'(y)}{g'(y)}}_{\substack{\text{Dies folgt aus der Existenz} \\ \text{des Grenzwertes } (\star)}},$$

und weil dieses Ergebnis für jede Folge $\{x_n\}$ mit $x_n \neq a, n \in \mathbb{N}$ und $x_n \to a$ für $n \to \infty$ richtig ist, gilt

$$\lim_{x\to a} \frac{f(x)}{g(x)} = \lim_{y\to a} \frac{f'(y)}{g'(y)}. \qquad \square$$

Beispiel

Beweisen Sie die Existenz von

$$\lim_{x\to 0} \frac{\sin x}{x}, \qquad \lim_{x\to 0} \frac{1-\cos x}{x^2}$$

und berechnen Sie diese Grenzwerte.

Lösung

Es gilt

$$\sin x\Big|_{x=0} = 0, \qquad x\Big|_{x=0} = 0$$

und

$$\frac{\mathrm{d}}{\mathrm{d}x}(\sin x) = \cos x, \quad \frac{\mathrm{d}}{\mathrm{d}x}(x) = 1, \qquad \lim_{x\to 0} \frac{\cos x}{1} = 1.$$

Den Regeln von L'Hôpital zufolge gilt also

$$\lim_{x\to 0} \frac{\sin x}{x} = 1.$$

Ebenfalls gilt

$$1 - \cos x\Big|_{x=0} = 0, \qquad x^2\Big|_{x=0} = 0$$

und

$$\frac{\mathrm{d}}{\mathrm{d}x}(1-\cos x) = \sin x, \quad \frac{\mathrm{d}}{\mathrm{d}x}(x^2) = 2x,$$

$$\underbrace{\lim_{x\to 0}\frac{\sin x}{2x} = \frac{1}{2}.}_{\text{Regeln von L'Hôpital}}$$

Den Regeln von L'Hôpital zufolge gilt also

$$\lim_{x\to 0}\frac{1-\cos x}{x^2} = \frac{1}{2}.$$

Taylor-Polynome

Betrachte ein Polynom in $x - a$:

$$p(x) = c_0 + c_1(x-a) + \ldots + c_n(x-a)^n\,.$$

Offensichtlich gilt

$$p(a) = c_0,$$

und durch wiederholtes Differenzieren erhalten wir

$$\begin{aligned} p'(a) &= c_1, \\ p''(a) &= 2c_2, \\ &\vdots \\ p^{(n)}(a) &= n!c_n\,. \end{aligned}$$

Zusammengefasst gilt

$$c_j = \frac{p^{(j)}(a)}{j!}\,, \qquad j = 0,\ldots,n\,;$$

die Koeffizienten c_j sind durch die Ableitungen von p an der Stelle a gegeben.

Definition

$f : I \to \mathbb{R}$ sei eine reellwertige Funktion, die im Punkt a n-mal differenzierbar ist. Das Polynom

$$P_n(x) = c_0 + c_1(x-a) + \ldots + c_n(x-a)^n\,,$$

wobei

$$c_j = \frac{f^{(j)}(a)}{j!}\,, \qquad j = 0,\ldots,n$$

heißt n**tes Taylor-Polynom von** f **mit Entwicklungspunkt** a.

Bemerkung

$$P_n^{(j)}(a) = f^{(j)}(a), \qquad j = 0,\ldots,n\,.$$

Beispiel

$f(x) = \mathrm{e}^x$

Aus $f'(x) = f(x)$ folgt $f^{(n)}(0) = 1$, $n = 0,1,2,\ldots$. Das $n$te Taylor-Polynom von f mit Entwicklungspunkt 0 ist also

$$P_n(x) = 1 + x + \frac{x^2}{2} + \ldots + \frac{x^n}{n!}\,.$$

Satz

f sei eine reellwertige Funktion, die im Punkt a n-mal differenzierbar ist.

Dann gilt

$$\lim_{x\to a} \frac{f(x) - P_n(x)}{(x-a)^n} = 0\,.$$

Beweis

Aus

$$P_n(x) = P_{n-1}(x) + \frac{f^{(n)}(a)}{n!}(x-a)^n$$

folgt

$$\frac{f(x) - P_n(x)}{(x-a)^n} = \underbrace{\frac{f(x) - P_{n-1}(x)}{(x-a)^n}}_{\substack{\text{Wir zeigen: Dies konvergiert gegen} \\ \frac{f^{(n)}(a)}{n!} \text{ für } x \to a.}} - \frac{f^{(n)}(a)}{n!}\,.$$

Weil $f, f', \ldots, f^{(n-1)}$ und alle Ableitungen von P_{n-1} stetig im Punkt a sind, gilt

$$\lim_{x\to a} \frac{\mathrm{d}^j}{\mathrm{d}x^j}(f(x) - P_{n-1}(x)) = \frac{\mathrm{d}^j}{\mathrm{d}x^j}(f(x) - P_{n-1}(x))\Big|_{x=a} = f^{(j)}(a) - f^{(j)}(a) = 0$$

und

$$\lim_{x\to a}\frac{\mathrm{d}^j}{\mathrm{d}x^j}(x-a)^n=\frac{\mathrm{d}^j}{\mathrm{d}x^j}(x-a)^n\bigg|_{x=a}=\frac{n!}{(n-j)!}(x-a)^{n-j}\bigg|_{x=a}=0$$

für $j=0,\ldots,n-2$ und

$$\begin{aligned}&\frac{\mathrm{d}^{n-1}}{\mathrm{d}x^{n-1}}(f(x)-P_{n-1}(x))=f^{(n-1)}(x)-f^{(n-1)}(a),\\&\frac{\mathrm{d}^{n-1}}{\mathrm{d}x^{n-1}}(x-a)^n=n!(x-a).\end{aligned}$$

Wir können also die Regel von L'Hôpital $(n-1)$-mal anwenden:

$$\begin{aligned}\lim_{x\to a}\frac{f(x)-P_{n-1}(x)}{(x-a)^n}&=\lim_{x\to a}\frac{f^{(n-1)}(x)-f^{(n-1)}(a)}{n!(x-a)}\\&=\frac{1}{n!}\lim_{h\to 0}\frac{f^{(n-1)}(a+h)-f^{(n-1)}(a)}{h}\\&=\frac{1}{n!}f^{(n)}(a)\;.\end{aligned}$$

□

Bemerkung

Es existiert $\delta>0$, so dass

$$|f(x)-P_n(x)|\le|x-a|^n\quad\text{für}\quad|x-a|<\delta$$

(wähle $\varepsilon=1$ in der Definition von Grenzwert).

Wir sagen: $P_n(x)$ **approximiert** $f(x)$ **bis zur** n**-ten Ordnung**.

Satz

$f:I\to\mathbb{R}$ sei n-mal differenzierbar im Punkt a. Es gelte

$$\begin{aligned}&f'(a)=f''(a)=\ldots=f^{(n-1)}(a)=0,\\&f^{(n)}(a)\neq 0.\end{aligned}$$

Dann gilt:

(i) Falls n gerade und $f^{(n)}(a) > 0$ ist, hat f ein lokales Minimum im Punkt a.

(ii) Falls n gerade und $f^{(n)}(a) < 0$ ist, hat f ein lokales Maximum im Punkt a.

(iii) Falls n ungerade ist, hat f weder ein lokales Minimum noch ein lokales Maximum im Punkt a.

Beweis

Ohne Beschränkung der Allgemeinheit können wir $f(a) = 0$ annehmen. Dann gilt

$$\begin{aligned} P_n(x) &= f(a) + f'(a)(x-a) + \ldots + \frac{f^{(n)}(a)}{n!}(x-a)^n \\ &= \frac{f^{(n)}(a)}{n!}(x-a)^n, \end{aligned}$$

so dass

$$0 = \lim_{x \to a} \frac{f(x) - P_n(x)}{(x-a)^n} = \lim_{x \to a} \left[\frac{f(x)}{(x-a)^n} - \frac{f^{(n)}(a)}{n!} \right].$$

Es existiert also $\delta > 0$, so dass

$$\frac{f(x)}{(x-a)^n}, \qquad \frac{f^{(n)}(a)}{n!}$$

dasselbe Vorzeichen für $x \in (a-\delta, a+\delta) \setminus \{a\}$ haben.

Ab jetzt soll $x \in (a-\delta, a+\delta) \setminus \{a\}$ sein.

Falls n **ungerade** ist, hat $f(x)$ verschiedene Vorzeichen für $x < a$ und $x > a$. Da $f(a) = 0$ ist, hat f weder ein lokales Maximum noch ein lokales Minimum im Punkt a.

Falls n **gerade** ist, hat $f(x)$ dasselbe Vorzeichen wie $f^{(n)}(a)$ für $x < a$ und $x > a$. Daher gilt

$$\begin{aligned} f^{(n)}(a) < 0 \ &\Rightarrow \text{f hat ein lokales Maximum im Punkt } a \\ &\quad\ (f(a) = 0, f(x) < 0 \text{ für } x \neq a) \\ f^{(n)}(a) > 0 \ &\Rightarrow f \text{ hat ein lokales Minimum im Punkt } a \\ &\quad\ (f(a) = 0, f(x) > 0 \text{ für } x \neq a). \end{aligned}$$

□

Bemerkungen

1. Der letzte Satz beinhaltet folgende hinreichende Bedingungen für Maxima und Minima:

$$f'(a) = 0, f''(a) < 0 \Rightarrow f \text{ hat ein lokales Maximum im Punkt } a$$

$$f'(a) = 0, f''(a) > 0 \Rightarrow f \text{ hat ein lokales Minimum im Punkt } a$$

   Daraus folgen folgende notwendige Bedingungen für Maxima und Minima:

$$f \text{ hat ein lokales Maximum im Punkt } a \Rightarrow f'(a) = 0, f''(a) \leq 0$$

$$f \text{ hat ein lokales Minimum im Punkt } a \Rightarrow f'(a) = 0, f''(a) \geq 0$$

   (Hier nehmen wir an, f sei zweimal differenzierbar im Punkt a).

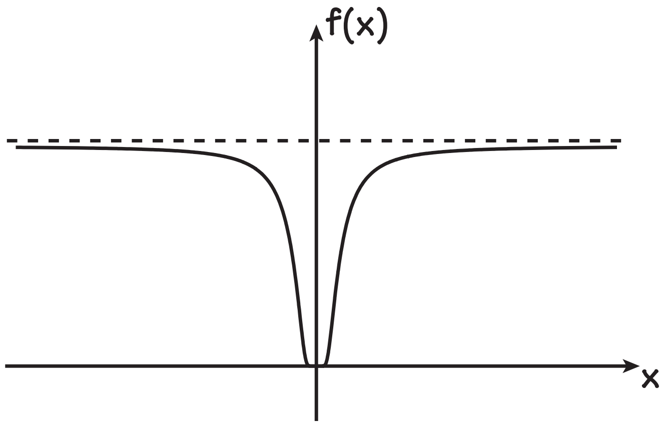
2. Es gibt nichtkonstante Funktion mit der Eigenschaft $f^{(n)}(a) = 0$ für **alle** n. Betrachte z. B. die Funktion $f : \mathbb{R} \to \mathbb{R}$ mit

$$f(x) = \begin{cases} e^{-1/x^2}, & x \neq 0, \\ 0, & x = 0. \end{cases}$$

   Diese Funktion ist beliebig oft differenzierbar im Nullpunkt mit

$$f^{(n)}(0) = 0, \qquad n = 1,2,\dots .$$

   Die Funktion hat ein lokales (und globales) Minimum im Nullpunkt:



Definition

f sei n-mal differenzierbar im Punkt a. Das **Restglied**

$$R_n(x) := f(x) - P_n(x)$$

ist die Differenz zwischen $f(x)$ und dem n-ten Taylor-Polynom von f mit Entwicklungspunkt a.

Wir suchen einen leicht abschätzbaren Ausdruck für $R_n(x)$.

Satz (Satz von Taylor)

$f : (a-\delta, a+\delta) \to \mathbb{R}$ sei $(n+1)$-mal differenzierbar mit

$$f(x) = \underbrace{f(a) + f'(a)(x-a) + \ldots + \frac{f^n(a)}{n!}(x-a)^n}_{= P_n(x)} + R_n(x)\,.$$

Für jedes $x \in (a-\delta, a+\delta)$ gilt:

(i) Es existiert t zwischen x und a, so dass

$$R_n(x) = \frac{f^{(n+1)}(t)}{n!}(x-t)^n(x-a)$$

(**Cauchysche Form des Restglieds**)

(ii) Es existiert t zwischen x und a, so dass

$$R_n(x) = \frac{f^{(n+1)}(t)}{(n+1)!}(x-a)^{n+1}$$

(**Lagrangesche Form des Restglieds**)

(iii) Falls $f^{(n+1)}$ integrierbar auf $[a,x]$ ist, gilt

$$R_n(x) = \int_a^x \frac{f^{(n+1)}(t)}{n!}(x-t)^n \,\mathrm{d}t$$

(**Taylorsche Form des Restglieds**)

Beweis

- Die Cauchysche Form wird hergeleitet, indem man den ersten Mittelwertsatz auf

$$S(t) = f(x) - f(t) - f'(t)(x-t) - \frac{f''(t)}{2}(x-t)^2 - \ldots - \frac{f^{(n)}(t)}{n!}(x-t)^n$$

  auf dem Intervall $[a,x]$ bzw. $[x,a]$ anwendet (es gilt $S(x) = 0$ und $S(a) = R_n(x)$).

- Die Lagrangesche Form wird hergeleitet, indem man den zweiten Mittelwertsatz auf $S(t)$ und $g(t) = (x-t)^{n+1}$ auf dem Intervall $[a,x]$ bzw. $[x,a]$ anwendet (es gilt $g(x) = 0$ und $g(a) = (x-a)^{n+1}$).

- Nun sei $f^{(n+1)}$ integrierbar auf $[a,x]$. Dann gilt

$$\begin{aligned} S(x) - S(a) &= \int_a^x S'(t)dt = -\int_a^x \frac{f^{(n+1)}(t)}{n!}(x-t)^n dt \\ \Rightarrow R_n(x) &= \int_a^x \frac{f^{(n+1)}(t)}{n!}(x-t)^n dt \,. \end{aligned}$$

□

Beispiel

Berechnen Sie die Zahl $\mathrm{e}^{0,3}$ mit einem Fehler unter 10^{-4}.

Lösung

Wir benutzen die Taylor-Polynome von e^x mit Entwicklungspunkt 0:

$$\mathrm{e}^x = P_n(x) + R_n(x),$$

wobei

$$\begin{aligned} P_n(x) &= 1 + x + \frac{x^2}{2!} + \ldots + \frac{x^n}{n!}\,, \\ R_n(x) &= \int_0^x \frac{\mathrm{e}^t}{n!}(x-t)^n\,\mathrm{d}t \end{aligned}$$

Es gilt:

$$
\begin{aligned}
|R_n(0{,}3)| &= \left| \int_0^{0,3} \frac{\mathrm{e}^t}{n!}(0{,}3-t)^n \,\mathrm{d}t \right| \\
&\le \frac{3}{n!} \int_0^{0,3} (0{,}3-t)^n \,\mathrm{d}t \qquad (\mathrm{e}^t \le \mathrm{e}^1 \le 3 \text{ für } t \in [0{,}1]) \\
&= \underbrace{\frac{3}{(n+1)!}(0{,}3)^{n+1}}_{\to 0 \text{ für } n \to \infty}
\end{aligned}
$$

Wir suchen n, so dass diese Größe kleiner als 10^{-4} ist.

$n = 4$ funktioniert.

Daher ist

$$
\begin{aligned}
\mathrm{e}^{0,3} &= P_4(0{,}3) + R_4(0{,}3) \\
&= 1 + 0{,}3 + \frac{1}{2!}(0{,}3)^2 + \frac{1}{3!}(0{,}3)^3 + \frac{1}{4!}(0{,}3)^4 + R_4(0{,}3) \\
&= 1{,}34984 \quad + \quad \underbrace{R_4(0{,}3),}_{|R_4(0{,}3)| < 10^{-4}}
\end{aligned}
$$

so dass

$$\mathrm{e}^{0,3} \approx 1{,}3498$$

mit einem Fehler unter 10^{-4} ist. □

Bemerkung

Die Methode im letzten Beispiel funktioniert, weil

$$R_n(0{,}3) \to 0 \qquad \text{für } n \to \infty.$$

Folglich gilt

$$\mathrm{e}^x - P_n(x) \to 0 \qquad \text{für } n \to \infty \text{ und } x = 0{,}3.$$

Mit anderen Worten konvergiert die Reihe

$$\sum_{j=0}^{\infty} \frac{x^j}{j!}$$

gegen e^x im Punkt $x = 0{,}3$. (Die Partialsummenfolge dieser Reihe ist $\{P_n(x)\}_{n=0}^{\infty}$.)

Definition

f sei beliebig oft differenzierbar im Punkt a. Die Reihe

$$\sum_{j=0}^{\infty} \frac{f^{(j)}(a)}{j!}(x-a)^j$$

heißt **Taylor-Reihe** der Funktion f mit Entwicklungspunkt a.

Potenzreihen

Definition

$c_0, c_1, c_2, \ldots$ und a, x seien reelle Zahlen. Die Reihe

$$\sum_{n=0}^{\infty} c_n(x-a)^n$$

heißt **Potenzreihe** mit **Koeffizienten** c_n und **Entwicklungspunkt** a.

Grundlegende Frage: $c_0, c_1, c_2, \ldots$ und a seien gegeben. Für welche Werte von x konvergiert die Potenzreihe

$$\sum_{n=0}^{\infty} c_n(x-a)^n?$$

Satz

$c_0, c_1, c_2, \ldots$ und a seien gegeben. Für die Potenzreihe

$$\sum_{n=0}^{\infty} c_n(x-a)^n$$

gilt genau eine der folgenden Aussagen.

(i) Die Reihe konvergiert nur für $x = a$.

(ii) Die Reihe is absolut konvergent für alle $x \in \mathbb{R}$.

(iii) Es gibt eine reelle Zahl $R > 0$, so dass die Reihe absolut konvergent für $|x-a| < R$ und divergent für $|x-a| > R$ ist.

Beweis

Ohne Beschränkung der Allgemeinheit können wir $a = 0$ annehmen.

Wir nehmen an, (i) treffe nicht zu, und definieren

$$K = \left\{ x : \sum_{n=0}^{\infty} c_n x^n \text{ konvergiert} \right\}, \qquad R = \sup\{|x| : x \in K\}.$$

Beachte: Es gilt $R > 0$, könnte aber $R = \infty$ sein.

Definitionsgemäß divergiert $\sum_{n=0}^{\infty} c_n x^n$, falls $|x| > R$ ist.

Wähle $0 < S < R$ und x_0 mit $S < |x_0| < R$, so dass $\sum_{n=0}^{\infty} c_n x_0^n$ konvergiert. (Die Existenz von x_0 folgt aus der Definition von R als $\sup\{|x| : x \in K\}$.) Es folgt also $c_n x_0^n \to 0$ für $n \to \infty$. Die Folge $\{c_n x_0^n\}$ ist daher beschränkt: Es existiert $M > 0$, so dass

$$|c_n x_0^n| = |c_n||x_0|^n \leq M, \qquad n = 0,1,2\ldots.$$

Für $x \in [-S,S]$ gilt:

$$\begin{aligned} |c_n\, x^n| &= |c_n||x|^n \\ &= |c_n||x_0|^n \left| \frac{x}{x_0} \right|^n \\ &\leq M \underbrace{\left(\frac{S}{|x_0|} \right)}_{<1}^n . \end{aligned}$$

Da

$$\underbrace{\sum_{n=0}^{\infty} M \left(\frac{S}{|x_0|} \right)^n}_{\text{eine geometrische Reihe}}$$

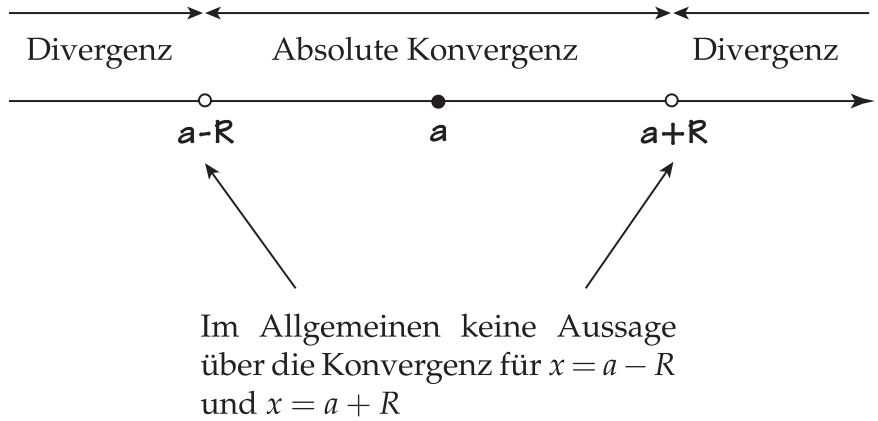
kovergent ist, folgt aus dem Vergleichsprinzip, dass $\sum_{n=0}^{\infty} c_n x^n$ auf $[-S,S]$ absolut konvergent ist. Damit ist $\sum_{n=0}^{\infty} c_n x^n$ absolut konvergent für $x \in (-R,R)$. □

Definition

Die Zahl R im Teil (iii) des letzten Satzes heißt **Konvergenzradius** der Potenzreihe. Diesen Begriff überträgt man auf Teil (i) $(R = 0)$ und Teil (ii) $(R = \infty)$.

Bemerkung

Der Begriff **Konvergenzradius** kann auf der Zahlengeraden veranschaulicht werden:



Beispiele

1. Die Reihe
$$\sum_{n=0}^{\infty} \frac{x^n}{n!} = 1 + x + \frac{x^2}{2!} + \frac{x^3}{3!} + \ldots$$
konvergiert für alle $x \in \mathbb{R}$ (Quotientenkriterium:
$$\frac{|x|^{n+1}/(n+1)!}{|x|^n/n!} = \frac{|x|}{n+1} \to 0$$
für $n \to \infty$). Hier ist also $R = \infty$.

2. Die Reihe
$$\sum_{n=0}^{\infty} n! x^n$$
konvergiert nur für $x = 0$ (für $x \neq 0$ konvergiert $\{n! x^n\}$ nicht gegen 0). Hier ist also $R = 0$.

3. Die Reihe
$$x - \frac{x^3}{3} + \frac{x^5}{5} - \frac{x^7}{7} + \dots \tag{1}$$
konvergiert für $-1 \leq x \leq 1$, die Reihe
$$1 - x^2 + x^4 - x^6 + \dots \tag{2}$$
konvergiert für $-1 < x < 1$, die Reihe
$$x - \frac{x^2}{2} + \frac{x^3}{3} - \frac{x^4}{4} + \dots \tag{3}$$
konvergiert für $-1 < x \leq 1$, und die Reihe
$$-x - \frac{x^2}{2} - \frac{x^3}{3} - \frac{x^4}{4} + \dots \tag{4}$$
konvergiert für $-1 \leq x < 1$. In allen Fällen ist also $R = 1$.

Beweis:

(1)-(4): Absolute Konvergenz für $-1 < x < 1$ (Quotientenkriterium). Divergenz für $|x| > 1$, da die Glieder nicht gegen 0 konvergieren.

(1): Leibniz-Kriterium für $x = 1, -1$

(2): Für $x = 1, -1$ ist die Partialsummenfolge $1,0,1,0\dots$

(3): Für $x = -1$ liegt die harmonische Reihe vor; Leibniz-Kriterium für $x = 1$

(4): Für $x = 1$ liegt die harmonische Reihe vor; Leibniz-Kriterium für $x = -1$

Bemerkung

Eine Potenzreihe $\sum\limits_{n=0}^{\infty} c_n(x-a)^n$ mit Konvergenzradius $R > 0$ definiert eine Funktion $f : (a - R, a + R) \to \mathbb{R}$ durch die Formel
$$f(x) = \sum_{n=0}^{\infty} c_n(x-a)^n.$$

Satz

$\sum\limits_{n=0}^{\infty} c_n(x-a)^n$ sei eine Potenzreihe mit Konvergenzradius $R > 0$.

Dann ist der Konvergenzradius der Potenzreihe

$$\sum_{n=1}^{\infty} nc_n (x-a)^{n-1}$$

mindestens R.

Ferner ist die durch die Formel

$$f(x) = \sum_{n=0}^{\infty} c_n (x-a)^n, \qquad |x-a| < R$$

definierte Funktion differenzierbar für $|x-a| < R$ mit

$$f'(x) = \sum_{n=1}^{\infty} nc_n (x-a)^{n-1}, \qquad |x-a| < R.$$

Beweis

Es genügt, die Aussagen für $a = 0$ zu beweisen.

Wähle S mit $0 < S < R$ und x_0 mit $S < |x_0| < R$. Aus der Konvergenz der Reihe $\sum\limits_{n=0}^{\infty} c_n x_0^n$ folgt $c_n x_0^n \to 0$ für $n \to \infty$. Die Folge $\{c_n x_0^n\}$ ist daher beschränkt: Es existiert $M > 0$, so dass

$$|c_n x_0^n| = |c_n||x_0|^n \leq M, \qquad n = 0,1,2\ldots.$$

Für $x \in [-S,S]$ gilt:

$$\begin{aligned} |nc_n\, x^{n-1}| &= n|c_n||x|^{n-1} \\ &= n|c_n||x_0|^{n-1} \left| \frac{x}{x_0} \right|^{n-1} \\ &\leq Mn|x_0|^{-1} \underbrace{\left(\frac{S}{|x_0|} \right)}_{<1}^{n-1}. \end{aligned}$$

Da

$$\sum_{n=1}^{\infty} Mn|x_0|^{-1} \left(\frac{S}{|x_0|} \right)^{n-1}$$

konvergent ist (Quotientenkriterium), folgt aus dem Vergleichsprinzip dass $\sum\limits_{n=1}^{\infty} nc_n x^{n-1}$ auf $[-S,S]$ absolut konvergent ist. Damit ist $\sum\limits_{n=1}^{\infty} nc_n x^{n-1}$ absolut konvergent für $x \in (-R,R)$.

Definiere
$$g(x) = \sum_{n=1}^{\infty} nc_n x^{n-1}, \qquad |x| < R.$$

Es seien $\{s_n(x)\}$ die Partialsummenfolge der Reihe $\sum\limits_{n=0}^{\infty} c_n x^n$ und $r_n(x) = f(x) - s_n(x)$. Beachte, dass $\{s_n'(x)\}$ die Partialsummenfolge der Reihe $\sum\limits_{n=0}^{\infty} nc_n x^{n-1}$ ist ($s_n(x)$ ist ein Polynom und daher differenzierbar).

Wähle $x \in (-R,R)$, $T > 0$ mit $|x| < T < R$ und h klein genug, so dass $|x+h| < T$ ist. Schreibe

$$\begin{aligned}&\frac{f(x+h) - f(x)}{h} - g(x)\\ &\quad = \frac{s_n(x+h) - f(x)}{h} - T_n'(x) + T_n'(x) - g(x) + \frac{r_n(x+h) - r_n(x)}{h}.\end{aligned}$$

- Zu jedem $\varepsilon_1 > 0$ und $n > 0$ existiert $\delta_1 > 0$, so dass
$$\left| \frac{s_n(x+h) - f(x)}{h} - s_n'(x) \right| < \varepsilon, \qquad 0 < |h| < \delta_1.$$

- Zu jedem $\varepsilon_2 > 0$ existiert $N_2 \in \mathbb{N}$, so dass
$$|s_n'(x) - g(x)| < \varepsilon_2, \qquad n > N_2.$$

- Es gilt
$$\begin{aligned}\left| \frac{r_n(x+h) - r_n(x)}{h} \right| &= \left| \sum_{j=n+1}^{\infty} c_j \big((x+h)^j - x^j\big) \right| \\ &= \left| \sum_{j=n+1}^{\infty} c_j h \big((x+h)^{j-1} + (x+h)^{j-2} x + \cdots + x^{j-1}\big) \right| \\ &\leq \sum_{j=n+1}^{\infty} |c_j| j T^{j-1}.\end{aligned}$$

Wir wissen, dass $\sum_{j=1}^{\infty} |c_j| j T^{j-1}$ konvergent ist, d.h. zu jedem $\varepsilon_3 > 0$ existiert $N_3 \in \mathbb{N}$, so dass

$$\sum_{j=n+1}^{\infty} |c_j| j T^{j-1} < \varepsilon_3, \qquad n > N_3.$$

Wähle $\varepsilon > 0$ und setze $\varepsilon_1 = \frac{\varepsilon}{3}$, $\varepsilon_2 = \frac{\varepsilon}{3}$, $\varepsilon_3 = \frac{\varepsilon}{3}$, $n = \max(N_2, N_3) + 1$ und $\delta = \delta_1$. Dann ist

$$\left| \frac{f(x+h) - f(x)}{h} - g(x) \right| < \varepsilon, \qquad 0 < |h| < \delta,$$

so dass f differenzierbar im Punkt x mit $f'(x) = g(x)$ ist. □

Korollar

Es seien $\sum\limits_{n=0}^{\infty} c_n (x-a)^n$ eine Potenzreihe mit Konvergenzradius $R > 0$ und $f : (a-R, a+R) \to \mathbb{R}$ die dadurch definierte Funktion.

1. $f : (a-R, a+R) \to \mathbb{R}$ ist beliebig oft differenzierbar mit

$$f^{(j)}(x) = \underbrace{\sum_{n=j}^{\infty} \frac{n!}{(n-j)!} c_n (x-a)^{n-j}}_{\text{Konvergenzradius } \geq R}, \qquad |x-a| < R.$$

2. Es gilt

$$c_j = \frac{f^{(j)}(a)}{j!}, \qquad j = 0,1,2,\ldots,$$

so dass $\sum\limits_{j=0}^{\infty} c_j (x-a)^j$ die Taylor-Reihe von f mit Entwicklungspunkt a ist.

Insbesondere folgt daraus, dass die Potenzreihendarstellung einer Funktion eindeutig ist.

Beispiele

Berechnen Sie die Taylor-Reihen der Funktionen

1. $f_1(x) = \dfrac{1}{1-x}$

2. $f_2(x) = \dfrac{1}{1+x^2}$

3. $f_3(x) = \arctan x$

mit Entwicklungspunkt 0 und geben Sie ihren Konvergenzradius an.

Lösung

1. Die geometrische Reihe
$$\sum_{n=0}^{\infty} x^n$$
konvergiert gegen $\frac{1}{1-x}$ für $|x| < 1$ und divergiert für $|x| > 1$. Die Taylor-Reihe von f_1 ist also
$$\sum_{n=0}^{\infty} x^n$$
mit Konvergenzradius 1.

2. Aus 1 folgt, dass
$$\sum_{n=0}^{\infty} (-x^2)^n$$
konvergiert gegen $\frac{1}{1+x^2}$ für $|x^2| < 1$ (d.h. $|x| < 1$) und divergiert für $|x^2| > 1$ (d.h. $|x| > 1$). Die Taylor-Reihe von f_2 ist also
$$\sum_{n=0}^{\infty} (-1)^n x^{2n}$$
mit Konvergenzradius 1.

3. Für $|x| < 1$ gilt
$$\begin{aligned} f_3'(x) &= \frac{1}{1+x^2} \\ &= \sum_{n=0}^{\infty} (-1)^n x^{2n}. \end{aligned}$$

Die Potenzreihe
$$g(x) = \sum_{n=0}^{\infty} (-1)^n \frac{x^{2n+1}}{2n+1}$$

hat Konvergenzradius 1 und für $|x| < 1$ gilt

$$\begin{aligned} & g'(x) = f_3'(x) \\ \Rightarrow\ & g'(x) - f_3'(x) = 0 \\ \Rightarrow\ & g(x) - f_3(x) = c \end{aligned}$$

eine Konstante

Aus $g(0) = 0$, $\arctan(0) = 0$ folgt $c = 0$, so dass

$$f_3(x) = \sum_{n=0}^{\infty} (-1)^n \frac{x^{2n+1}}{2n+1}$$

und der Konvergenzradius dieser Taylor-Reihe ist 1. □

Lemma

f, g haben die konvergenten Taylor-Reihen

$$f(x) = \sum_{n=0}^{\infty} c_n (x-a)^n, \qquad |x-a| < R,$$

$$g(x) = \sum_{n=0}^{\infty} d_n (x-a)^n, \qquad |x-a| < S$$

mit Entwicklungspunkt a.

Dann haben $f+g$ und fg ebenfalls konvergente Taylor-Reihen

$$(f+g)(x) = \sum_{n=0}^{\infty} e_n (x-a)^n, \qquad |x-a| < T_1,$$

$$(fg)(x) = \sum_{n=0}^{\infty} f_n (x-a)^n, \qquad |x-a| < T_2,$$

mit Entwicklungspunkt a. Es gilt

$$\begin{aligned} & T_1, T_2 \geq \min(R,S), \\ & e_n = c_n + d_n, \\ & f_n = \sum_{k=0}^{n} c_k d_{n-k}. \end{aligned}$$

Die trigonometrischen Funktionen

Definition

Die Funktionen $\sin(\cdot), \cos(\cdot) : \mathbb{R} \to \mathbb{R}$ sind durch die Formeln

$$\left.\begin{aligned} \sin(x) &= x - \frac{x^3}{3!} + \frac{x^5}{5!} - \frac{x^7}{7!} + \dots, \\ \cos(x) &= 1 - \frac{x^2}{2!} + \frac{x^4}{4!} - \frac{x^6}{6!} + \dots \end{aligned}\right\} \begin{array}{l} \text{Diese Potenzreihen konvergieren} \\ \text{für alle } x \in \mathbb{R} \text{ (Quotientenkriterium)} \end{array}$$

definiert.

Bemerkung

Folgende Eigenschaften der trigonometrischen Funktionen folgen unmittelbar aus den Definitionen.

1. $\sin(\cdot), \cos(\cdot)$ sind beliebig oft differenzierbar auf $\mathbb{R}$.
2. $\sin'(x) = \cos(x),\ \cos'(x) = -\sin(x)$ für $x \in \mathbb{R}$.
3. $\sin(0) = 0$, $\cos(0) = 1$.
4. $\sin(-x) = -\sin x$, $\cos(-x) = \cos x$ für $x \in \mathbb{R}$.
5. Für alle $x, y \in \mathbb{R}$ gilt
$$\sin(x+y) = \sin x \cos y + \cos x \sin y, \tag{1}$$
$$\cos(x+y) = \cos x \cos y - \sin x \sin y. \tag{2}$$
6. Für jedes $x \in \mathbb{R}$ gilt
$$\sin^2 x + \cos^2 x = 1. \tag{3}$$

Bemerkung

Alle anderen trigonometrischen Identitäten werden aus (1)–(3) hergeleitet.

Bemerkung

Die Potenzreihen für $\sin x$ und $\cos x$ genügen den Voraussetzungen des Leibniz-Kriteriums für $x \in (0{,}2]$. Daher gilt

$$x - \frac{x^3}{3!} \le \sin x \le x, \tag{1}$$
$$1 - \frac{x^2}{2!} \le \cos x \le 1 - \frac{x^2}{2!} + \frac{x^4}{4!} \tag{2}$$

für $x \in (0{,}2]$.

Satz

1. $\sin x > 0$ für $x \in (0{,}2]$.

2. $\cos(\cdot)$ ist streng monoton fallend für $x \in (0{,}2)$ und hat genau eine Nullstelle x_0 in $(0{,}2)$.

3. $\sin(\cdot)$ ist streng monoton steigend für $x \in (0{,}x_0)$ und $\sin x_0 = 1$.

Beweis

1. Aus (1) folgt
$$\begin{aligned} \sin x &\ge x\left(1 - \frac{x^2}{6}\right) \\ &\ge x\left(1 - \frac{2^2}{6}\right) && \text{für } x \in (0{,}2] \\ &> 0 && \text{für } x \in (0{,}2] \end{aligned}$$

2. Bemerke:
$$\cos(0) = 1 > 0,$$
$$\cos(2) \le 1 - \frac{2^2}{2!} + \frac{2^4}{4!} = -\frac{1}{3} < 0.$$
Dem Zwischenwertsatz zufolge hat $\cos(\cdot)$ also mindestens eine Nullstelle $x_0 \in (0{,}2)$.

   Da
$$\cos'(x) = -\sin(x) < 0 \qquad \text{für } x \in (0{,}2),$$

ist $\cos(\cdot)$ streng monoton fallend und daher injektiv auf $(0,2)$. x_0 ist also die eindeutige Nullstelle von $\cos x$ in $(0,2)$.

3. Aus
$$\sin^2 x_0 = 1 - \cos^2 x_0$$
folgt
$$\sin x_0 = \pm 1,$$
und wir wählen das positive Vorzeichen, weil $x_0 \in (0,2)$ und $\sin x > 0$ für $x \in (0,2)$ ist.

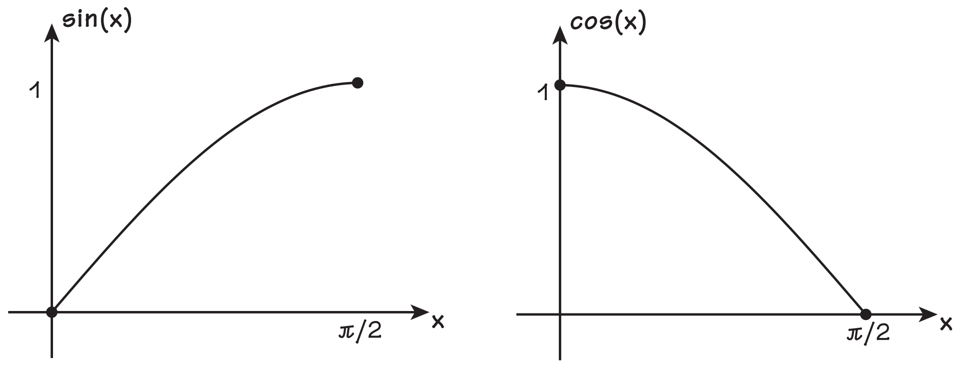
Da
$$\sin'(x) = \cos x > 0 \qquad \text{für } x \in (0,x_0)$$
ist $\sin(\cdot)$ streng monoton steigend auf $(0,x_0)$. $\square$

Definition (Die Kreiszahl)

$$\pi := 2x_0$$

Bemerkung

Bisher wissen wir, wie die Graphen von $\sin x$ und $\cos x$ auf dem Intervall $[0,\pi/2]$ aussehen:

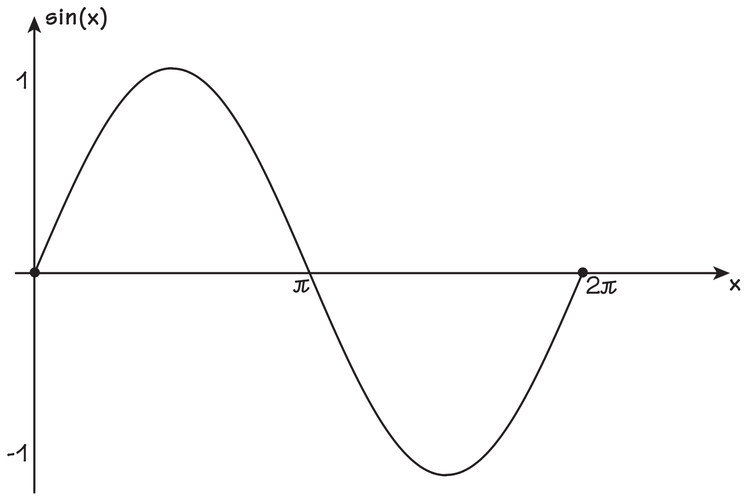


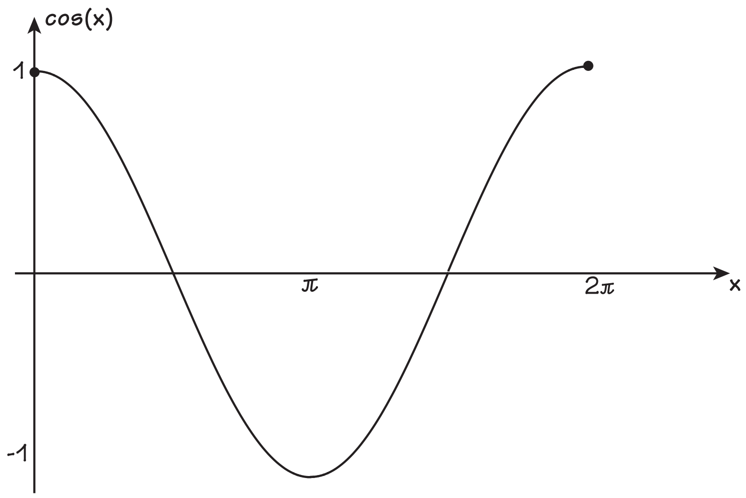
Es ist nun leicht zu folgern, wie die Graphen für alle x aussehen. Für $x \in [0,\pi/2]$ gilt

$$\sin\left(\frac{\pi}{2} + x\right) = \sin\frac{\pi}{2}\cos x + \cos\frac{\pi}{2}\sin x = \cos x,$$
$$\cos\left(\frac{\pi}{2} + x\right) = \cos\frac{\pi}{2}\cos x - \sin\frac{\pi}{2}\sin x = -\sin x$$

und für $x \in [0,\pi]$ gilt

$$\sin(\pi + x) = \sin\pi\cos x + \cos\pi\sin x = -\sin x,$$
$$\cos(\pi + x) = \cos\pi\cos x - \sin\pi\sin x = -\cos x:$$





Schließlich beweisen wir induktiv, dass

$$\sin(x + 2n\pi) = \sin x, \quad \cos(x + 2n\pi) = \cos x, \qquad x \in [0,2\pi], n \in \mathbb{Z}.$$

Bemerkung

Aus

$$\sin x \leq x \qquad x \in (0,2]$$

und

$$\sin x \leq 1 < x, \qquad x > 2$$

folgt die nützliche Ungleichung

$$\sin x \leq x, \qquad x \geq 0.$$

Definition

Die Funktion $\exp(\cdot) : \mathbb{R} \to \mathbb{R}$ ist durch die Formel

$$\exp(x) \quad = \quad \underbrace{1 + x + \frac{x^2}{2!} + \frac{x^3}{3!} + \ldots}_{\substack{\text{Diese Potentreihe konvergiert} \\ \text{für alle } x \in \mathbb{R} \text{ (Quotientenkriterium)}}}$$

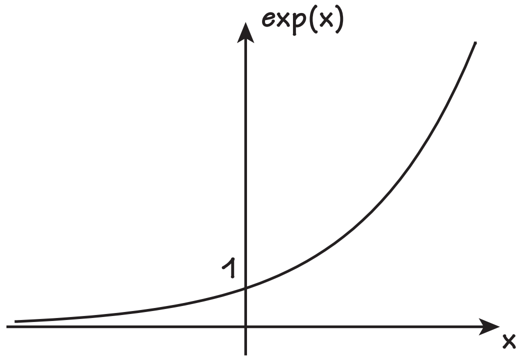
definiert.

Satz (Eigenschaften von $\exp(\cdot)$**)**

1. $\exp(\cdot)$ ist beliebig oft differenzierbar auf $\mathbb{R}$ mit $\exp'(\cdot) = \exp(\cdot)$.
2. $\exp(x + y) = \exp(x)\exp(y)$ für alle $x, y \in \mathbb{R}$.
3. $\exp(0) = 1, \exp(x) > 0$ und $\exp(-x) = 1/\exp(x)$ für alle $x \in \mathbb{R}$.
4. $\exp(\cdot)$ ist streng monoton steigend auf $\mathbb{R}$ mit $\exp(x) \to \infty$ für $x \to \infty$ und $\exp(x) \to 0$ für $x \to -\infty$.

Bemerkung

Somit können wir den Graphen von $\exp(\cdot)$ zeichnen.



Da $\exp(\cdot) : \mathbb{R} \to (0,\infty)$ bijektiv ist, ist folgende Definition sinnvoll.

Definition

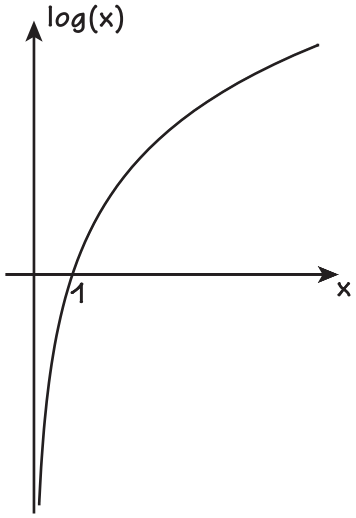
Die Funktion $\log(\cdot) : (0,\infty) \to \mathbb{R}$ ist die Umkehrfunktion von $\exp(\cdot) : \mathbb{R} \to (0,\infty)$.

Satz (Eigenschaften von $\log(\cdot)$**)**

1. $\log(\cdot)$ ist beliebig oft differenzierbar auf $(0,\infty)$ mit
$$\log^{(n)}(x) = (-1)^{n+1}(n-1)!\frac{1}{x^n}, \qquad n = 1,2,3,\ldots.$$
2. $\log(\cdot)$ ist streng monoton steigend auf $(0,\infty)$ mit $\log(1) = 0, \log x \to -\infty$ für $x \to 0$ und $\log x \to \infty$ für $x \to \infty$.
3. $\log(xy) = \log x + \log y$ für alle $x,y \in (0,\infty)$ und $\log\left(\frac{1}{x}\right) = -\log x$ für $x \in (0,\infty)$.

Bemerkung

Somit können wir den Graphen von $\log(\cdot)$ zeichnen.



Grundlegende Frage: Es sei $a > 0$. Definitionsgemäß ist

$$\begin{aligned}
a^n &:= \underbrace{a.a \dots a}_{n \text{ mal}}, && n = 1,2,3,\dots,\\
a^{\frac{1}{n}} &= \sqrt[n]{a}, && n = 1,2,3,\dots,\\
a^{\frac{m}{n}} &= \left(\sqrt[n]{a}\right)^m, && m,n = 1,2,3,\dots,\\
a^0 &= 1,\\
a^{-\frac{m}{n}} &= \frac{1}{a^{\frac{m}{n}}}, && m,n = 1,2,3,\dots.
\end{aligned}$$

Somit haben wir a^q für $q \in \mathbb{Q}$ definiert. Was bedeutet aber a^r, wenn r eine **irrationale** Zahl ist?

Bemerkung

Aus der Identität

$$\log(ab) = \log a + \log b, \qquad a,b > 0$$

folgt induktiv

$$\log\left(a^{\frac{m}{n}}\right) = \frac{m}{n}\log a, \qquad m \in \mathbb{Z}, n \in \mathbb{N}.$$

Daher gilt

$$\begin{aligned}
a^{\frac{m}{n}} &= \exp\left(\log a^{\frac{m}{n}}\right)\\
&= \exp\left(\frac{m}{n}\log a\right), \qquad m \in \mathbb{Z},\ n \in \mathbb{N},
\end{aligned}$$

d.h.

$$a^q = \exp(q \log a)$$

für $a > 0$.

Definition

$$a^x := \exp(x \log a), \qquad x \in \mathbb{R}$$

für $a > 0$.

Bemerkungen

1. Die üblichen Rechenregeln folgen aus dieser Definition.
2. $a^{(\cdot)}$ ist beliebig oft differenzierbar auf $\mathbb{R}$ mit
$$\frac{\mathrm{d}}{\mathrm{d}x}(a^x) = \log a a^x.$$
3. Es ist
$$\sum_{j=0}^{\infty} \frac{1}{j!} = \mathrm{e},$$
so dass $\exp(1) = \mathrm{e}$ und folglich $\log \mathrm{e} = 1$. Daher ist
$$\mathrm{e}^x = \exp(x).$$

Lemma

Für jedes $k > 0$ und $a > 1$ gilt

$$\left.\begin{aligned} x^{-k}a^x &\to \infty \text{ für } x \to \infty \\ x^k a^{-x} &\to 0 \text{ für } x \to \infty \end{aligned}\right\} \text{“Exponentiale schlagen Potenzen”},$$

$$\left.\begin{aligned} x^{-k}\log x &\to 0 \quad \text{für } x \to \infty \\ x^k \log x &\to 0 \quad \text{für } x \to 0 \end{aligned}\right\} \text{“Potenzen schlagen Logarithmen”}.$$

Beweis

Wähle $n \in \mathbb{N}$ mit $n > k$. Aus

$$\begin{aligned} a^x &= \exp(x \log a) \\ &= 1 + x \log a + \frac{x^2 (\log a)^2}{2!} + \ldots + \frac{x^{2n} (\log a)^{2n}}{(2n)!} + \ldots \\ &> \frac{x^{2n} (\log a)^{2n}}{(2n)!} \qquad \text{für } x > 0 \\ &> \frac{x^n}{(2n)!} \qquad \text{für } x > 1/(\log a)^2 \end{aligned}$$

folgt

$$x^{-k} a^x > \underbrace{\frac{x^{n-k}}{(2n)!}}_{\to \infty \text{ für } x \to \infty.}$$

und

$$x^k a^{-x} = \frac{1}{x^{-k} a^x} \to 0 \text{ für } x \to \infty.$$

Aus

$$y^{-2/k} \exp(y) \to \infty \qquad \text{für } y \to \infty$$

folgt

$$x^{-1} \exp(x^{k/2}) \to \infty \qquad \text{für } x \to \infty$$

(setze $y = x^{k/2}$). Es existiert also $M > 0$ mit der Eigenschaft

$$x^{-1} \exp(x^{k/2}) > 1 \qquad \text{für } x > M.$$

Für $x > \max(M,1)$ gilt daher

$$\begin{aligned} &\exp(x^{\frac{k}{2}}) > x \\ &\Rightarrow \log x < x^{\frac{k}{2}} \\ &\Rightarrow 0 < x^{-k} \log x < \underbrace{x^{-\frac{k}{2}}}_{\substack{\to 0 \\ \text{für } x \to \infty}} \\ &\Rightarrow x^{-k} \log x \to 0 \qquad \text{für } x \to \infty. \end{aligned}$$

Ferner gilt

$$x^k \log x = -\left(\frac{1}{x}\right)^{-k} \log\left(\frac{1}{x}\right),$$

und aus $\frac{1}{x} \to \infty$ für $x \to 0$ folgt

$$\left(\frac{1}{x}\right)^{-k} \log\left(\frac{1}{x}\right) \to 0 \qquad \text{für } x \to 0.$$

$\square$