# Mathe I

Jan-Peter Hohloch

WS 11/12

# Inhaltsverzeichnis

# Vorwort

Da sich an den Inhalten der Vorlesung sein dem letzten Skript von 06/07 einiges gendert hat, kommt hier die aktuelle Version aus der Vorlesung “Mathe I für Informatiker” gehalten von Prof. Huson im Wintersemester 11/12.

Was den Inhalt betrifft habe ich mich im Großen und Ganzen an meine Aufschriebe und für zwei verpasste Vorlesungen an mir zur Verfügung gestellte Mitschriebe gehalten. An dieser Stelle vielen Dank an die Helfer :)
Geändert habe ich jedoch die Nummerierung der Kapitel, innerhalb des Skriptes stimmt sie, in der Vorlesung wurde jedoch eine andere Zählung verwendet.

Den LaTeX-Code stelle ich ebenfalls zur Verfügung, damit zukünftige Hörer der Vorlesung kleinere Anpassungen leicht vornehmen können.
Außerdem könnt ihr natürlich den Code euren Vorstellungen nach anpassen (beispielsweise interne Verlinkungen anlegen) oder einfach mal ein bisschen mit LaTeX herumprobieren (in diesem Fall aber bitte auch auf das Original aufpassen ;)

Jan-Peter

# 1 Logik

## 1.1 Aussagenlogik

Eine Aussage ist entweder wahr oder falsch.
wahr = w = 1 = true
falsch = f = 0 = false

Bsp.:

- 2 ist eine Primzahl (1)
- 4 ist eine Primzahl (2)
- es gibt unendlich viele Primzahlen (1)
- es gibt unendlich viele Primzahlzwillinge (?)
- gibt es unendlich viele Primzahlen? (keine Aussage)

Durch Verknüpfungen mit 'und', 'oder', 'wenn, dann', etc. lassen sich aus einfachen Aussagen kompliziertere herstellen.

Bsp.:
Wenn 'heute ist ein Werktag' oder 'heute ist ein verkaufsoffener Sonntag', dann 'heute haben die Geschäfte offen' (BUrlG: Def. von Werktag: ' Alle Kalendertage, die nicht Sonn- oder gesetzliche Feiertage sind') (1)
In Aussagenlogik interessiert zunächst nur der Wahrheitswert (1 oder 0) einer Aussage. Der konkrete Inhalt bleibt unberücksichtigt. Sie ist ein einfaches Modell des alltäglichen Sprachgebrauches. Wir verwenden zur Formulierung Aussagevariablen A,B,C,...,A1;A2 ,... und Junktoren (und, oder, ...) Dadurch erhalten wir (aussagenlogische) Ausdrücke. Auch Aussagevariablen heien Ausdrücke. Setzt man für die Aussagevariablen konkrete Aussagen ein, so erhält man man wieder eine Aussage.

Bsp.:
Ausdruck: A oder B $\Rightarrow$ C
Aussage: s.o.
Ob die Aussage wahr oder falsch ist, hängt von den konkreten Werten der Variablen und von den Junktoren ab.

## 1.2 Die wichtigsten Junktoren

### 1.2.1 Negation

Verneinung von A, nicht A, $\neg$ A

| $A$ | $\neg A$ |
|---|---|
| 0 | 1 |
| 1 | 0 |

### 1.2.2 Konjunktion

A und B , A $\wedge$ B

| $A$ | $B$ | $A \wedge B$ |
|---|---|---|
| 0 | 0 | 0 |
| 0 | 1 | 0 |
| 1 | 0 | 0 |
| 1 | 1 | 1 |

### 1.2.3 Disjunktion

A oder B , A $\vee$ B

| $A$ | $B$ | $A \vee B$ |
|---|---|---|
| 0 | 0 | 0 |
| 0 | 1 | 1 |
| 1 | 0 | 1 |
| 1 | 1 | 1 |

### 1.2.4 Exklusives Oder

A XOR B , A $\oplus$ B

| $A$ | $B$ | $A \oplus B$ |
|---|---|---|
| 0 | 0 | 0 |
| 0 | 1 | 1 |
| 1 | 0 | 1 |
| 1 | 1 | 0 |

### 1.2.5 Implikation

A impliziert B , Wenn A, dann B , A $\Rightarrow$ B

| $A$ | $B$ | $A \Rightarrow B$ |
|---|---|---|
| 0 | 0 | 1 |
| 0 | 1 | 1 |
| 1 | 0 | 0 |
| 1 | 1 | 1 |

### 1.2.6 Äquivalenz

A genau dann, wenn B , A $\Leftrightarrow$ B

| $A$ | $B$ | $A \Leftrightarrow B$ |
|---|---|---|
| 0 | 0 | 1 |
| 0 | 1 | 0 |
| 1 | 0 | 0 |
| 1 | 1 | 1 |

## 1.3 Bemerkungen

### 1.3.1 Sätze ber Implikationen

Mathematische Sätze sind häufig von der Form

$$R \Rightarrow S$$

Es wird also behauptet, dass R $\Rightarrow$ S eine wahre Aussage ist.
Zu zeigen: Wenn R wahr, dann auch S wahr.
Man nennt R die Voraussetzung und S die Behauptung des mathematischen Satzes.

Bsp.:

$$a - b > 2 \wedge a, b \in \mathbb{R} \Rightarrow \frac{a^2 + b^2}{2} > 2 + ab$$

Ein Beweis besteht aus einer Kette von Implikationen (im einfachsten Fall):

$$R \Rightarrow R_1, R_1 \Rightarrow R_2, ..., R_n \Rightarrow S$$

Wobei alle Implikationen wahr sind.

$$a - b > 2 \Rightarrow (a - b)^2 > 4 \Rightarrow a^2 - 2ab + b^2 > 4 \Rightarrow a^2 + b^2 > 4 + 2ab \Rightarrow \frac{a^2 + b^2}{2} > 2 + ab$$

### 1.3.2 Sätze ber Äquivalenzen

Manchmal sind math. Sätze von der Form

$$R \Leftrightarrow S$$

Zu zeigen:

- Wenn R wahr, dann S wahr ($R \Rightarrow S$)
- Wenn S wahr, dann R wahr ($S \Rightarrow R$)

### 1.3.3 Größe von Wahrheitstabellen

Bei mehreren Aussagevariablen wir die Wertetabelle schnell sehr groß

$$x \texttt{ Aussagevariablen} \rightarrow 2^x \texttt{ Zeilen}$$

### 1.3.4 Einfacherer Lösungsweg

Betrachte:

$$(A_1 \wedge A_2) \Rightarrow (A_3 \vee \neg A_4)$$

Frage: Wann falsch?
Einfacher:

$$((A_1 \wedge A_2) = 1) \wedge ((A_3 \vee \neg A_4) = 0) \Rightarrow \texttt{Aussage falsch}$$

$$A_1, A_2 = 1; A_3 = 0; A_4 = 1$$

## 1.4 Logische Äquivalenz

Haben zwei Ausdrücke $\alpha$ und $\beta$ für jede Kombination von Wahrheitswerten der (beteiligten) Aussagevariablen den gleichen Wahrheitswert, so heißen sie logisch äquivalent.

$$\alpha \equiv \beta$$

(Beachte: $\equiv$ ist kein Junktor) Wenn also $\alpha \equiv \beta$, so hat der Ausdruck $\alpha \Leftrightarrow \beta$ immer den Wahrheitswert 1 (und umgekehrt)

$$(\alpha \Leftrightarrow \beta) \Leftrightarrow (\alpha \equiv \beta)$$

## 1.5 Tautologie und Kontradiktion

Def.: Ein Ausdruck heißt Tautologie, wenn er für jede Kombination der Wahrheitswerte der Aussagevariablen immer den Wert 1 ergibt.
Hat er den wert 0, heißt er Kontradiktion.
Wenn er keine Kontradiktion ist, ist er erfüllbar.

Ist ein Ausdruck erfüllbar? Gibt es eine schnellere Möglichkeit, als auszuprobieren?
$\Rightarrow$ Hauptproblem der Informatik (P=NP?)

$$A \vee \neg A \texttt{ ist eine Tautologie} A \wedge \neg A \texttt{ ist eine Kontradiktion}$$

## 1.6 Wichtige log. Äquivalenzen

### 1.6.1 Kommutativität

$A \wedge B \equiv B \wedge A$
$A \vee B \equiv B \vee A$
$A \Leftrightarrow B \equiv B \Leftrightarrow A$
**ABER!:** $A \Rightarrow B \not\equiv B \Rightarrow A$

### 1.6.2 Doppelte Negation

$\neg(\neg A) \equiv A$

### 1.6.3 De'Morgansche Regeln

$\neg(A \wedge B) \equiv \neg A \vee \neg B$
$\neg(A \wedge B) \equiv \neg A \wedge \neg B$

### 1.6.4 Implikation

$A \Rightarrow B \equiv \neg B \Rightarrow \neg A$
$A \Rightarrow B \equiv \neg A \vee B$

### 1.6.5 Äquivalenz

$A \Leftrightarrow B \equiv (A \Rightarrow B) \wedge (B \Rightarrow A)$

### 1.6.6 Assoziativität

$A \wedge (B \wedge C) \equiv (A \wedge B) \wedge C$

### 1.6.7 Distributivität

$A \wedge (B \vee C) \equiv A \wedge B \vee A \wedge C$
$A \vee (B \wedge C) \equiv A \vee B \wedge A \vee C$

### 1.6.8 Tautologie und Kontradiktion

$1$ = Tautologie
$0$ = Kontradiktion
$A \vee \neg A = 1$
$A \wedge \neg A = 0$
Beweis lässt sich mit Wahrheitstabellen erbringen.

## 1.7 Bemerkungen zu den logischen Äquivalenzen

- Doppelte Negation ist gleichbedeutend mit der Aussage selbst.
- DeMorgansche-Regeln sind für das logische Argumentieren besonders wichtig.
- Implikation ist ebenfalls besonders wichtig, wird im Alltag aber oft falsch gemacht.
- Teilaudrücke können durch logisch äquivalente ersetzt werden.
- Die Äuqivalenzen gelten auch, wenn man die Aussagevariablen durch Ausdrücke ersetzt.

## 1.8 Quantoren

Quantoren ermöglichen es uns gewisse Aussagen genauer zu formulieren. Das führt zu einer Erweiterung der Aussagenlogik, nämlich der Quantorenlogik. Es geht um All- und Existenzaussagen.
$\forall$ für alle; $\exists$ es existiert mindestens ein

### 1.8.1 Definition

#### Allquantor

$\forall x \in E : P(x)$ bedeutet für alle x aus E gilt die Eigenschaft P.
$\forall$ heißt Allquantor. $\forall x \in E : P(x)$ ist eine Aussage, die genau dann wahr ist, wenn P(x) für alle x $\in$ E wahr ist.

#### Existenzquantor

$\exists x \in E : Q(x)$ bedeutet "Es existiert mindestens ein x $\in$ E mit der Eigenschaft Q(x)"
$\exists$ heißt Existenzquantor. $\exists x \in E : Q(x)$ ist genau dann wahr, wenn Q(x) für mindestens ein $x \in E$ wahr ist.
$\exists! x \in E$: es existiert genau ein.

### 1.8.2 Bemerkungen

#### Allquantor als Konjunktion

Ist $E = \{x_1, ..., x_n\}$ endlich, so gilt:

$$\forall x \in E : P(x) \equiv P(x_1) \wedge ... \wedge P(x_n)$$

$\forall$ ist eine verallgemeinerte Konjunktion.

#### Existenzquantor als Disjunktion

Ist $E = \{x_1, ..., x_n\}$ endlich, so gilt:

$$\exists x \in E : P(x) \equiv P(x_1) \vee ... \vee P(x_n)$$

$\exists$ ist eine verallgemeinerte Disjunktion.

### 1.8.3 Negation von Quantoren

- $\neg(\forall x \in E : P(x)) \equiv \exists x \in E : \neg P(x)$
- $\neg(\exists x \in E : Q(x)) \equiv \forall x \in E : \neg Q(x)$

### 1.8.4 Reihenfolge von Quantoren

$\forall$ und $\exists$ dürfen nicht vertauscht werden.
Gleiche, nebeneinanderstehende Quantoren dürfen vertauscht und/oder zusammengefasst werden:

- $\forall m \in N : \forall n \in N : P(x) \equiv \forall n \in N : \forall m \in N : P(x) \equiv \forall m, n \in N : P(x)$
- $\exists m \in N : \exists n \in N : P(x) \equiv \exists n \in N : \exists m \in N : P(x) \equiv \exists m, n \in N : P(x)$

# 2 Mengen

## 2.1 Mengen allgemein

### 2.1.1 Cantor

Georg Cantor (1845-1918), Halle/Saale, Begrnder der Mengenlehre:
"Menge ist eine Zusammenfassung von bestimmten wohl definierten unterschiedlichen Objektenunseres Anschauens oder unseres Denkens in einem Ganzen."
Die so zusammengefassten Objekte heißen Elemente der Menge. Mengendarstellung: {...}

### 2.1.2 Wie spezifiziert man eine Menge?

#### Aufzählende Schreibweise

{1,2,3,5,9} oder {2,4,6,8,...}
Geht nur bei endlichen oder sogenannten abzhlbaren Mengen.
Reihenfolge und Mehrfachnennung sind unerheblich:
{1,2,3,5,9}={2,1,9,5,3}={2,1,1,9,1,5,3}

#### Beschreibung durch eine Eigenschaft

$M = \{x|x \text{ hat Eigenschaft}\}=\{x : x \text{ hat Eigenschaft}\}$

### 2.1.3 Problematik in Cantors Definition

Cantors Def. ist problematisch und führt zu Widersprüchen:
Russelsche Antinomie:
Sein M die Menge aller Mengen, die sich nicht selbst enthalten.
Frage: Ist M ein Element von M?
Wenn ja, dann widerspricht das der Def. von M.
Wenn nein, dann widerspricht das der Def. von M.
Die Axiomatische Mengenlehre behebt das Problem, für unsere Zwecke reicht aber folgende Abhilfe:
Wir bilden nur Mengen, deren Elemente in wohldefinierten Grundmengen liegen, dann gibt es keine Widersprüche:
Also $M = \{x|x \in G \wedge E(x)\}$ mit E(x) Eigenschaft von x
Typische Grundmengen sind:

$$\mathbb{N}, \mathbb{N}_0, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$$

Grundmenge muss nicht explizit angegeben werden, aber existieren!

### 2.1.4 Leere Menge

$\emptyset$, einzige Menge ohne Elemente

### 2.1.5 Kardinalität

$|M|$=Anzahl der Elemente von M
auch: "Mächtigkeit", "Größe"
$|\mathbb{N}| = \infty$ , $|\{\mathbb{N}\}| = 1$
$|\{1, 2, 3, 4\} = 4$ , $|\{1, 1, 2, 3, 1, 4, 1\}| = 4$

## 2.2 Def. Teilmenge

Seien M, N Mengen.
M heißt Teilmenge von N, geschrieben $M \subseteq N$, falls gilt:

$$\forall x : (x \in M \Rightarrow x \in N)$$

("Implikation" beschreibt Teilmengenbeziehungen)
Ist M keine Teilmenge von N, so schreibt man $M \nsubseteq N$

### 2.2.1 Beispiel

$\mathbb{N} \subseteq \mathbb{N}_0 \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$

### 2.2.2 Wichtiger Unterschied

$\in \not\equiv \subseteq$
Bsp.:
$M := \{1, \mathbb{N}\}$
Dann:
$1 \in M$, $\mathbb{N} \in M$
$2 \notin M$, $\mathbb{N} \nsubseteq M$

### 2.2.3 Bemerkung

Mengen können auch Elemente einer (anderen) Menge sein.

### 2.2.4 Gleichheit von Mengen

$M = N \Leftrightarrow M \subseteq N \wedge N \subseteq M$
d.h. $\forall x : x \in M \Leftrightarrow x \in N$
("Äquivalenz" definiert Gleichheit)

**Beispiel**

M={2,3,5,7}
N={$x|x$ ist Primzahl $< 11$}

## 2.3 Operationen auf Mengen

M,N,A,B,C Mengen

### 2.3.1 Schnittmenge/Schnitt

$M \cap N := \{x|x \in M \wedge x \in N\}$
$A \cap B = B \cap A$ (Kommutativität)
$A \cap (B \cap C) = (A \cap B) \cap C$ (Assoziativität)
Allgemein auch:
$M_1 \cap M_2 \cap ... \cap M_n = \{x \in M_1 \wedge x \in M_2 \wedge ... \wedge x \in M_n\} = \bigcap_{i=1}^{n} M_i$

### 2.3.2 Vereinigung

$M \cup N := \{x|x \in M \vee x \in N\}$
$A \cup B = B \cup A$ (Kommutativität)
$A \cup (B \cup C) = (A \cup B) \cup C$ (Assoziativität)
Allgemein auch:
$M_1 \cup M_2 \cup ... \cup M_n = \{x \in M_1 \vee x \in M_2 \vee ... \vee x \in M_n\} = \bigcup_{i=1}^{n} M_i$

### 2.3.3 Differenz

$M \backslash N := \{x|x \in M \wedge x \notin N$
Ist $N \subseteq M$, so heißt $M \backslash N$ Komplement $N$ in $M$, $N^c(M)$

### 2.3.4 Symmetrische Differenz

$M \Delta N := M \backslash N) \cup (N \backslash M)$

## 2.4 Venn-Diagramme

## 2.5 Satz über Mengenoperationen

Seien M,N,L Mengen.

### 2.5.1 Symmetrische Differenz

$M \Delta N = (M \cup N) \backslash (M \cap N)$

### 2.5.2 De'Morgansche Regel

Sind $M, N \subseteq L$, so ist $(M \cap N)^c = M^c \cup N^c$ und $(M \cup N)^c = M^c \cap N^c$

### 2.5.3 Teilmengenbeziehungen

$M \cap N = M \Leftrightarrow M \subseteq N$
$M \cup N = M \Leftrightarrow N \subseteq M$

### 2.5.4 Distributivität

$L \cap (M \cup N) = (L \cap M) \cup (L \cap N)$
$L \cup (M \cap N) = (L \cup M) \cap (L \cup N)$

## 2.6 Def.: Beliebige Vereinigungen und Schnitte

Sei $\mathbb{A}$ eine Menge von Mengen.
$\bigcup\limits_{A \in \mathbb{A}} A := \{x | \exists A \in \mathbb{A} : x \in A\}$
$\bigcap\limits_{A \in \mathbb{A}} A := \{x | \forall A \in \mathbb{A} : x \in A\}$

Besteht $\mathbb{A}$ aus $A_1, A_2, ...$, so schreibt man:
$\bigcup\limits_{i \in \mathbb{N}} A_i$ b.z.w. $\bigcap\limits_{i \in \mathbb{N}} A_i$

Wenn $A_1 \supseteq A_2 \supseteq ... \supseteq A_k$, so ist $\bigcap\limits_{i=1}^{k} = A_k$

Bei unendlichen Schnitten können überraschende Phänomene auftreten:
$A_n \subseteq \mathbb{R} := \{x \in \mathbb{R} | 0 < x < \frac{1}{n}, n \in \mathbb{N}\}$,
dann hat jede Menge $A_n$ unendlich viele Elemente und es gilt $A_1 \supseteq A_2 \supseteq ...$,
aber es ist $\bigcap\limits_{n \in \mathbb{N}} A_n = \emptyset$

## 2.7 geordnete n-Tupel

Bei Mengen: Reihenfolge unerheblich, auch unendliche Mengen möglich
Bei Tupeln: Reihenfolge relevant, nur endlich viele Elemente

### 2.7.1 Definition

$(x_1, x_2, ..., x_n) = (y_1, y_2, ..., y_n) \Leftrightarrow x_1 = y_1, x_2 = y_2, ..., x_n = y_n$
Dabei müssen nicht alle $x_i$ (bzw $y_i$) verschieden sein.
Für n=2: "Paar"
Für n=3: "Tripel"

### 2.7.2 Beispiele

- Paare zur Beschreibung von Punkten in der Ebene, Tripel im 3D-Raum
- $(2,3,4,4) = (2,3,4,4) \neq (2,4,3,4)$

## 2.8 Kartesisches Produkt

Sei $n \in \mathbb{N}$, $n \geq 2$ und $M_1, M_2, ..., M_n$ nicht-leere Mengen.
Die Menge der geordneten n-Tupel
$M_1 \times M_2 \times ... \times M_n := \{(x_1, x_2, ...x_n) | x_1 \in M_1 \wedge x_2 \in M_2 \wedge ... \wedge x_n \in M_n\}$
heißt das kartesische Produkt der Mengen $M_1$ bis $M_n$.
Ist eine der Mengen leer, so ist $M_1 \times M_2 \times ... \times M_n = \emptyset$

### 2.8.1 Schreibweise

$M_1 \times M_2 \times ... \times M_n = \prod_{i=1}^{n} M_i$
Ist $M_1 = M_2 = ... = M_n$, so $M^n = M_1 \times M_2 \times ... \times M_n$

### 2.8.2 Beispiele

- $A \times B \neq B \times A$ im Allgemeinen
  $A^2 = \{(1,1), (1,2), (2,1), (2,2)\}$
- Tabelle einer Datenbank ist Teilmenge eines kartesischen Produktes endlicher Mengen.

T=

| $N$ | $A$ |
|---|---|
| $Alice$ | 23 |
| $David$ | 30 |
| $Yoda$ | 999 |

$T \subseteq N \times A$

# 3 Abbildungen

Alltägliche Beispiele:
Foto:
Zuordnung: Jeder Punkt in der Originalszene → ein Punkt auf dem Foto
Computerprogramm:
Eingabedaten → Ausgabedaten
Funktionen:
z.B. $f(x) = x^2$

## 3.1 Def.: Abbildung

Seien M,N nicht-leere Mengen (nicht unbedingt verschieden).
Eine Abbildung f von M auf N: $f : M \to N$ ist eine Zuordnung, die jedem $x \in M$ genau ein $f(x) \in N$ zuordnet.
Schreibe $x \mapsto f(x)$.
$x$ heißt Argument oder Urbild.
$f(x)$ heißt Bild unter f.
M heißt Definitionsbereich von f
$f(M) := \{f(x)|x \in M\}$ heißt Bild von f oder Bildbereich von f
$f(M) \subseteq N$

Die Menge $G_f := \{(x, f(x))|x \in M\} \subseteq N$ heißt Graph von f.
Funktionen sind Spezialfälle von Abbildungen, deren Definitionsmenge in $\mathbb{R}$ (oder $\mathbb{R}^n$) oder in $\mathbb{C}$ (oder $\mathbb{C}^n$) liegt.

### 3.1.1 Beispiele

#### Identische Abbildung, Identität

$M$ sei eine Menge.
$id_M : M \to M, x \mapsto x$

#### Abbildung

$f : \mathbb{R}\backslash\{0\} \to \mathbb{R}, x \mapsto \frac{1}{x}$ Geht nicht von $\mathbb{R}$ auf $\mathbb{R}$!

#### Betragsfunktion

$|\cdot| : \mathbb{R} \to \mathbb{R}$ (auch möglich, aber nicht nötig: $\mathbb{R} \to \mathbb{R}^{\geq 0} = \mathbb{R}_{\geq 0} = \mathbb{R}^{+}$)

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

#### Schaltfunktion, Bool'sche Funktion

$\{0,1\}^n \to \{0,1\}$
z.B. $\wedge$: $\{0,1\}^2 \to \{0,1\}$
$(A, B) \mapsto A \wedge B$

#### Indikatorfunktion

Sei $M \subseteq A$

$1_M : A \to \{1,0\}, x \mapsto \begin{cases} 0 & \forall x \notin M \\ 1 & \forall x \in M \end{cases}$ ist die Indikatorfunktion der Menge M.

#### Zwei Funktionen für dieselbe Abbildung

$f : \{0,1\} \to \{0,1\}, x \mapsto x$
$g : \{0,1\} \to \{0,1\}, x \mapsto x^2$
$g$ und $f$ beschreiben dieselbe Abbildung $0 \mapsto 0$, $1 \mapsto 1$

### 3.1.2 Schreibweisen

$f : M \to N$, Abb.
$A \subseteq M : f(A) = \{f(x) | x \in A\}$ Bild (-menge) unter f
$B \subseteq N : f^{-1}(B) = \{x | x \in M, f(x) \in B\}$ (volles) Urbild von B unter f

#### Beispiele

$f : \mathbb{Z} \to \mathbb{N}_0, x \mapsto x^2$

$f(\mathbb{Z}) = \{0, 1, 4, 9, 16, ...\} = f(\mathbb{N}_0)$
$\to$ Aus $f(A_1) = f(A_2)$ folgt nicht im Allgemeinen $A_1 = A_2$!

$f(\{-1, 1, 3, 7\}) = \{1, 9, 49\}$

$f^{-1}(\{1, 2, 3, 4\}) = \{1, -1, 2, -2\}$

$f^{-1}(\{2\}) = \emptyset = f^{-1}(\{3\}$
$\to$ Aus $f^{-1}(B_1) = f^{-1}(B_2)$ folgt nicht im Allgemeinen $B_1 = B_2$

## 3.2 Gleichheit von Abbildungen

Abbildungen $f : M_1 \to N_1$ und $g : M_1 \to M_2$ heißen gleich, wenn:
(1) $M_1 = M_2$
(2) $N_1 = N_2$
(3) $f(x) = g(x) \quad \forall x \in M_1 (= M_2)$
Man schreibt $f = g$.

## 3.3 Surjektiv, injektiv, bijektiv

$f : M \to N$, Abb.

### 3.3.1 Surjektivität

f heißt surjektiv, falls $f(M) = N$.
Also $\forall n \in N \exists m \in M : f(m) = n$.

### 3.3.2 Injektivität

f heißt injektiv, falls
$\forall m_1, m_2 \in M : m_1 \neq m_2 \Rightarrow f(m_1) \neq f(m_2)$
$(\equiv \forall m_1, m_2 \in M : f(m_1) = f(m_2) \Rightarrow m_1 = m_2)$

### 3.3.3 Bijektivität

f heißt bijektiv oder Bijektion, falls f surjektiv und injektiv ist.

### 3.3.4 Beispiele

**(a)** $f(x) = x^2$

$f : \mathbb{Z} \to \mathbb{N}_0, x \mapsto x^2$
$f^{-1}(\{3\}) = \emptyset, f(-1) = f(1) = 1$
$\Rightarrow f$ ist weder surjektiv noch injektiv.

**b:** $g(x) = 3x + 2$

$g : \mathbb{R} \to \mathbb{R}, x \mapsto 3x + 2$
surjektiv?: Betrachte $y \in \mathbb{R}$
gesucht ist $x$ mit $y = 3x + 2$
$\frac{y-2}{3} = x \Rightarrow g$ ist surjektiv.
injektiv?:
$3x_1 + 2 = 3x_2 + 2$
$3x_1 = 3x_2$
$x_1 = x_2 \Rightarrow g$ ist injektiv.
$\Rightarrow g$ ist bijektiv.

**c: Konjunktion $\wedge$**

$\wedge : \{0,1\}^2 \to \{0,1\}$
surjektiv?: $0 \wedge 0 = 0, 1 \wedge 1 = 1 \Rightarrow$ ja
injektiv?: $0 \wedge 0 = 0 = 0 \wedge 1 \Rightarrow$ nein

**d:** $h(x) = x + 2$

$h : \mathbb{N} \to \mathbb{N}, x \mapsto x + 2$
surjektiv?: $y + 1 = x \Rightarrow$ ja
injektiv?: $h^{-1}(1) = \emptyset \Rightarrow$ nein

**e:** $i(x) = x - 1$

$i : \mathbb{N} \to \mathbb{N}_0, x \mapsto x - 1$
surjektiv?: $i^{-1}(0) = 1, i^{-1}(1) = 2, ... \Rightarrow$ ja
injektiv?: $y + 1 = x \Rightarrow$ ja
$\Rightarrow i$ ist bijektiv.

**f: Explizite Zuordnung**

$j : \{1,2,3,4,5\} \to \{a,b,c,d,e\}, j(1) = a, j(2) = b, ..., j(5) = e$
surjektiv und injektiv (leicht zu sehen)
$\Rightarrow j$ ist bijektiv.

## 3.4 Endlichkeit von Mengen

Bijektivität bentigt man zur Definition der Endlichkeit einer Menge:
Menge M heißt endlich $:\Leftrightarrow M = \emptyset \vee \exists n \in \mathbb{N} \exists g : \{1,2,...,n\} \to M : g$ bijektiv

### 3.4.1 Abzählbar unendliche Mengen

$\exists h : \mathbb{N} \to M : h$ bijektiv
(Bsp. e oben)

**Ist $\mathbb{Z}$ abzählbar?**

Dazu definiere:
$$f : \mathbb{N} \to \mathbb{Z}, x \mapsto \begin{cases} k & \text{, falls } x = 2k+1 \\ -k & \text{, falls } x = 2k \end{cases} \qquad \text{wobei } k = \{0,1,2,...\}$$

### 3.4.2 Satz über endliche Mengen

Sei $f : M \to N$ Abb.
Sind $M$ und $N$ endlich und $|M| = |N|$, so sind folgende Aussagen äquivalent ($\to$ ist eine davon wahr, so sind alle wahr):

- (1) f ist injektiv
- (2) f ist surjektiv
- (3) f ist bijektiv

Beweisbar durch Ringschluss.

#### Beweis

Zu zeigen (1) $\Rightarrow$ (2):
Sei $m_1, m_2 \in M$
Ist $m_1 \neq m_2$, so $f(m_1) \neq f(m_2)$ (dann injektiv)
Also $|f(M)| = |M|$
Da $|M| = |N|$ gilt, folgt $|f(M)| = |N|$.
Da $f(M) \subseteq N \wedge N$ endlich, folgt $f(M) = N$, d.h. f ist surjektiv.

Zu zeigen (2) $\Rightarrow$ (3):
Sei $N = \{n_1, n_2, ..., n_k\}, k = |N|$
Zu jedem Bildpunkt $n_i \in N$ existiert mindestens ein $m_i \in M$ mit $f(m_i) = n_i$, da f surjektiv.
Aus der Def. einer Abbildung folgt, dass $m_1, m_2, ..., m_n$ paarweise verschieden sind.
Da $|M| = |N|$ und für $i \neq j$ ist $f(m_i) = n_i \neq n_j = f(m_j)$
Also ist f auch injektiv und daher bijektiv.

Zu zeigen (3) $\Rightarrow$ (1):
Durch Def. von Bijektivität.

□

## 3.5 Hintereinanderausführung

### 3.5.1 Definition

$f : M \to N, g : N \to P$, Abb.
Die Zuordnung $x \mapsto g(f(x))$ für jedes $x \in M$ definiert eine Abb. von M nach P; die Hintereinanderausführung $g \circ f$ (g "nach" f) der Abb. g und f.
Also: $(g \circ f)(x) := g(f(x))$

### 3.5.2 Assoziativität

Ist zusätzlich $h : P \to Q$ eine weitere Abb., so gilt folgendes:
$(h \circ g) \circ f = h \circ (g \circ f)$

### 3.5.3 Beweis

#### Def.

$f \circ g$ ist Abb., per Konstruktion ist $x \mapsto f(g(x))$

#### Assoziativität

Sei $x \in M$ beliebig:
$((h \circ g) \circ f)(x) = (h \circ g)(f(x)) = h(g(f(x))) = h((g \circ f)(x)) = (h \circ (g \circ f))(x)$

### 3.5.4 Beispiele

(a) $h : \mathbb{R} \to \mathbb{R}, x \mapsto \sin(x^2)$,
dann $h = g \circ f$, wobei:
$f : \mathbb{R} \to \mathbb{R}, x \mapsto x^2$
$g : \mathbb{R} \to \mathbb{R}, x \mapsto \sin(x)$

Beachte: $(f \circ g)(x) = (\sin(x))^2$, also $f \circ g \neq g \circ f$

(b)
A = Menge alle TN der Vorlesung, die an den Übungsgruppen teilnehmen
B = Übungsgruppen der VL
C = Menge der Tutoren
$f : A \to B, x \mapsto$ Übungsgr., der x angehört
$g : B \to C, x \mapsto$ Tutor der Übungsgruppe x
$g \circ f : A \to C, x \mapsto$ Tutor der Übungsgruppe, der x angehört.

### 3.5.5 Besondere Abbildungen

Die Hintereinanderausführung $\begin{cases} injektiver \\ surjektiver \\ bijektiver \end{cases}$ Abb. ist $\begin{cases} injektiv \\ surjektiv \\ bijektiv \end{cases}$.

## 3.6 Umkehrabbildung bijektiver Abb.

$f : M \to N$, Abb.,
Dann gilt:

**(a)** $f$ ist bijektiv genau dann, wenn eine Abbildung $g : N \to M$ existiert mit $g \circ f = id_M$ und $f \circ g = id_N$

**(b)** g ist eindeutig bestimmt und heißt Umkehrabbildung (inverse Abbildung) $f^{-1}$ von $f$

**(c)** $f^{-1}$ ist bijektiv und $(f^{-1})^{-1} = f$

### 3.6.1 Beispiele

- $f : \{1, 2, 3\} \to \{1, 2, 3\}, f(1) = 3, f(2) = 1, f(3) = 2$
  $f^{-1}(1) = 2, f^{-1}(2) = 3, f^{-1}(3) = 1$
- $f : \{1, 2, 3\} \to \{1, 2, 3\}, f(1) = 1, f(2) = 2, f(3) = 3$
  $f^{-1}(1) = 1, f^{-1}(2) = 2, f^{-1}(3) = 3$
- $f : \mathbb{R} \to \mathbb{R}, x \mapsto x^3$
  $f^{-1}(x) = \sqrt[3]{x}$

Verwechslungsgefahr:
$f : M \to N, Abb.$
$f^{-1}(B) = \{x \in M | f(x) \in B\}$ nicht dasselbe!

### 3.6.2 Beweis

**(a)** **"⇒"** Angenommen f ist bijektiv.
Zu zeigen: $\exists g$ mit den geforderten Eigenschaften.

Sei $y \in N$ beliebig.
Da f bijektiv: $\exists! x \in M : f(x) = y$
Wir setzen $g(y) = x$. Dann ist $g : N \to M$.
Außerdem:
$(f \circ g)(y) = f(g(y)) = f(x) = y = id_N(y)$
$(g \circ f)(x) = g(f(x)) = g(y) = x = id_M(x)$

**"⇐"** Angenommen es existiert eine Abb. g mit $f(g(y)) = y$ und $g(f(x)) = x$
Zu zeigen: f ist bijektiv

**f surjektiv?** Sei $y \in N$ beliebig. dann ist $g(y) \in M$, $f(g(y)) = y$, d.h. g(y) ist Urbild von y unter f, also ist f surjetiv

**f injektiv?** Sei $f(x_1) = f(x_2)$.
Dann $x_1 = g(f(x_1)) = g(f(x_2)) = x_2$, also ist f injektiv.

**(b)** Zu zeigen: Eindeutigkeit von g:
Angenommen es gäbe 2 solcher Abb. $g_1$ und $g_2$.
Sei $y \in N$
Dann existiert genau ein $x \in M$ mit $f(x) = y$, da f bijektiv.
Es folgt:
$g_1(y) = g_1(f(x)) = x$
$g_2(y) = g_2(f(x)) = x$
$\Rightarrow g_1 = g_2$

**(c)** u.U. in Übung

# 4 Relationen

Bisher: $f : M \to N$, Abb.: Jedem $x \in M$ wird genau ein $y \in n$ zugeordnet.
Jetzt: Verzichtet man auf die unterstrichenen Forderungen, so beschreibt man eine Teilmenge von $M \times N$.
(Allgemein: Teilmengen n-facher kartesischer Produkte $M_1 \times M_2 \times ... \times M_n$)

## 4.1 Def. Relation

Seien $M_1, ..., M_n$ nichtleere Mengen.
Eine n-stellige Relation R über die mengen $M_1, ..., M_n$ ist eine Teilmenge von $M_1 \times ... \times M_n$

$$R \subseteq_1 \times ... \times M_n$$

Gilt $M_1 = ... = M_n$, so spricht man von einer n-stelligen Relation auf M.

### 4.1.1 Beispiele

**"Relationelle Datenbank"**

| $Vorn$ | $Nachn$ | $Alter$ | $Wohnort$ |
|---|---|---|---|
| $Peter$ | $Blau$ | 23 | $T\ddot{U}$ |
| $Peter$ | $rot$ | 24 | $T\ddot{U}$ |
| $Maren$ | $Rot$ | 28 | $RT$ |

$R \subseteq Vorn \times Nachn \times Alter \times Wohnort$

**Zweistellige Relationen** (besonders wichtig)
Besondere Symbole: $\sim$ oder $\preceq$ oder $\leq$

$G_f$ **Graph von Abb. f**
$(f : M \to N, G_f = \{(x, f(x)) | x \in M\}$ ist Relation $\subseteq M \times N$
Da $G_f$ eindeutig, kann Abb. f als spezielle Relation betrachtet werden.

**Gleichheitsrelation auf M**
$R = \{(x, x) | x \in M\}$ (Graph von $id_M$) $\subseteq M \times M$

**übliche Kleiner-Relation auf $\mathbb{Z}$**
$R_< = \{(x, y) | x, y \in \mathbb{Z}, x < y\} \subseteq \mathbb{Z} \times \mathbb{Z}$

**Teilerrelation** $|$
$|$ ("teilt") auf $\mathbb{N}$:
$x|y$ heißt x teilt y, d.h. $\exists k \in \mathbb{N} : y = k \cdot x$

**$\leq$-Relation auf $\mathbb{Z}$**

$x \leq y \Leftrightarrow x < y \vee x = y$

### 4.1.2 Anmerkung

Es gibt zwei besonders wichtige Typen von Relation:

- Ordnungsrelationen
- Äquivalenzrelationen

Bsp.: $<, \leq$ Ordnungsrelationen

## 4.2 Ordnungsrelationen

Sei M eine nicht-leere Menge, $\preceq$ eine 2-stellige Relation auf M mit folgenden Eigenschaften:

**(1)** $\forall x \in M : x \preceq x$ (Reflexivität)

**(2)** $\forall x, y \in M : x \preceq y \wedge y \preceq x \Rightarrow x = y$ (Antisymmetrie)

**(3)** $\forall x, y, z \in M : x \preceq y \wedge y \preceq z \Rightarrow x \preceq z$ (Transitivität)

Dann heißt $\preceq$ Ordnungsrelation oder partielle Ordnung.
Gilt zusätzlich

**(4)** $\forall x, y \in M : x \preceq y \vee y \preceq x$

so heißt $\preceq$ vollständige/lineare/totale Ordnung.
Häufig schreibt man $\leq$ statt $\preceq$, obwohl das nicht die übliche kleiner-gleich-Ordnungsrelation auf $\mathbb{N}, \mathbb{N}_0, ...$ bedeuten muss.
Ist $u \leq v$ und $u \neq v$, so schreibt man $u < v$.

### 4.2.1 Beispiele

- normale Ordnungsrelation $\leq$ auf $\mathbb{N}$ ist totale Ordnung
- Gleichheitsrelation ist partielle Ordnung auf jeder Menge, nicht total, falls $|M| > 1$
- Teilerrelation auf $\mathbb{N}$ ist partielle Ordnung, nicht total (z.B. weder $2|3$ noch $3|2$)
- Teilmengenrelation auf der Potenzmenge von M ist partielle Ordnung, nicht total, falls $|M| > 1$
- $M = \{1, 2, 3\}, R = \{(1, 1), (2, 2), (3, 3), (1, 2), (2, 3)\}$
  Transitivität verletzt: $(1, 2) \in R, (2, 3) \in R$, aber $(1, 3) \notin R$

- Sei $\leq$ (partielle) Ordnung auf M
  Ordne $M^n$ durch
  $u = (u_1, u_2, ..., u_n) \preceq v = (v_1, v_2, ..., v_n)$
  $\Leftrightarrow$
  $u = v$ oder $u_i < v_i$ für das kleinste $i$ mit $u_i \neq v_i$
  Bsp.:
  $(a, p, p, l, e) \in M^5, (a, p, p, s, s) \in M^5$
  hier: $u \preceq v$, da $l < s$

  Das ist partielle Ordnung auf $M^n$ (s. ÜB 4)
  Ist $\leq$ total, so ist auch $\preceq$ total.
  Ist $\preceq$ total, so heißt $\preceq$ lexikographische Ordnung.

## 4.3 Äquivalezrelation

Sei $M = \emptyset$, $\sim$ eine zweistellige Relation auf M mit folgenden Eigenschaften:

**(1)** Reflexivität

**(2)** Symmetrie: $x \sim y \Rightarrow y \sim x$

**(3)** Transitivität

Dann heißt $\sim$ Äquvalenzrelation.

### 4.3.1 Beispiele

- Gleichheitsrelation: trivial
- $M = \mathbb{Z}, x \sim y \Leftrightarrow x - y$ gerade
- Allgemein: Wähle $r \in \mathbb{N}$ fest, $M = \mathbb{Z}$

  **Reflexivität** $x - x = 0 \wedge r|0 \Leftrightarrow x \sim x$

  **Symmetrie** $x \sim y \Leftrightarrow r|x - y \Leftrightarrow r| - (x - y) \Leftrightarrow r| - x + y \Leftrightarrow r|y - x \Leftrightarrow y \sim x$

  **Transitivität** $x \sim y \wedge y \sim z \overset{\text{zu zeigen}}{\Rightarrow} x \sim z$:
  $r|x - y \wedge r|y - z$
  $\Rightarrow$
  $x - y = k \cdot r, k \in \mathbb{Z}$
  $y - z = l \cdot r, l \in \mathbb{Z}$
  $\Rightarrow$
  $$\begin{aligned} x - z &= x - y + y - z \\ &= k \cdot r + l \cdot r \\ &= (k + l) \cdot r \end{aligned}$$
  also transitiv, da $r|x - z$, also $x \sim z$

□

## 4.4 Def.: Äquivalenzklassen

Sei $\sim$ Äquivalenzrel. auf $M$ und $x \in M$.
Dann heißt $[x] := \{y \in M | y \sim x\}$ Äquivalenzklasse von x (bezüglich $\sim$) auf M.

### 4.4.1 Beispiele

**Gleichheitsrelation** auf M
$\forall x \in M : [x] = \{x\}$

**Relation** $x \in \mathbb{Z}, x \sim y \Leftrightarrow 2|x - y$
$[0] = \{y \in \mathbb{Z} | 2|y\} = [2] = [-2]$
$[1] = \{y \in \mathbb{Z} | 2 \not| y\} = [3] = [-3]$

**Relation** $f : M \to N, Abb.; x, y \in M : x \sim y \Leftrightarrow f(x) = f(y)$
$[x] = f^{-1}(\{f(x)\})$ volles Urbild $f^{-1}(f(x))$ von $f(x)$ bzgl. $f$

## 4.5 Gleichheit von Äquivalenzklassen

Sei $\sim$ eine Äquivalenzrelation auf$M$, $x, y \in M$

**(a)** Die folgenden Aussagen sind äquivalent:

**(i)** $[x] = [y]$

**(ii)** $x \in y$

**(iii)** $x \sim y$

**(b)** Ist $[x] \neq [y]$, so ist $[x] \cap [y] = \emptyset$

### 4.5.1 Beweis

**(a)** durch Ringschluss

**(i)⇒(ii):** $x \in [x] = [y] \Rightarrow x \in [y]$ (Reflexivität, Annahme)

**(ii)⇒[iii]:** $x \in [y] \Rightarrow x \sim y$ (Def. Äquivalenzklasse)

**(iii)⇒(i):** Sei $z \in [x]$, dann $z \sim x$

Aus $x \sim y$ folgt wg. Transitivität $z \sim y$, also $[x] \subseteq [y]$, da $z \in [y]$
Wegen Symmetrie gilt $y \sim x$, es folgt analog $[y] \subseteq [x]$
$\Rightarrow [x] = [y]$

**(b)** Indirekter Beweis ($A \Rightarrow B \equiv \neg B \Rightarrow \neg A$)
Sei $[x] \cap [y] \neq \emptyset, z \in [x] \cap [y]$
Aus (a) folgt $[z] = [x] = [y]$

□

## 4.6 Zerlegung

### 4.6.1 Definition

Äquivalenzklassen einer Äquivalenzrelation $\sim$ auf M führen zu einer "Zerlegung" von M:

**(a)** Mengen A und B heißen disjunkt, falls $A \cap B = \emptyset$

**(b)** Sei $\emptyset \neq Z \subseteq \mathcal{P}(M)$ Teilmengensystem
Elemente von $Z$ paarweise disjunkt:
$\forall A, A' \in Z : A \neq A' \Rightarrow A \cap A' = \emptyset$

**(c)** Sei $Z$ eine Menge paarweise disjunkter, nicht-leerer Teilmengen von M.
Dann schreibt man für $\bigcup\limits_{A \in Z} A$ auch $\dot{\bigcup\limits_{A \in Z}} A$ oder $\biguplus\limits_{A \in Z} A$ ("disjunkte Vereinigung")
Gilt dabei $\biguplus\limits_{A \in Z} A = M$, so heißt $Z$ Zerlegung von M ("Partition").

### 4.6.2 Beispiele

$M = \{1, 2, 3, 4\}$
$Z = \{\{1\}, \{2\}, \{3, 4\}\}$ Zerlegung von M
$Z = \{\{1, 4\}, \{2, 3\}\}$ Zerlegung von M

$\mathbb{Z} = \{z \in \mathbb{Z} | 2 | z\} \uplus \{z \in \mathbb{Z} | 2 \not| z\}$

### 4.6.3 Satz

Sei $M \neq \emptyset$ eine Menge.

**(a)** Ist $\sim$ eine Äquivalenzrelation auf M und $Z_\sim$ eine die Menge aller verscheidenen Äquivalenzklassen (bezügl. $\sim$) auf M, so ist $Z_\sim$ eine Zerlegung von M.

**(b)** Sei Z eine Zerlegung von M.
Setze $x \sim y :\Leftrightarrow x, y$ liegen in derselben Menge $A \in Z$.
Dann ist $\sim$ eine Äquvalenzrelation auf M. Die Äquivalenzklassen bezgl. $\sim$ sind gerade die Mengen $A \in Z$

#### Beweis

**(a)** Sei $\sim$ Äquivalenzrelation auf M.
Für jedes $x \in M$ gilt: $x \in [x]$
Folglich $\bigcup\limits_{A \in Z_\sim} A = M$
Dies ist eine disjunkte Vereinigung nach der Definition einer Äquivalenzklasse.
Damit ist $Z_\sim$ eine Zerlegung von M.

**(b)** z.Z. $\sim$ (wie oben definiert) hat Eigenschaften einer Äquivalenzrelation (s.o.)

**Reflexivität** Sei $x \in M$.
Dann ist $x \in A$ für genau eine Menge $A \in Z$, also $x \sim x$

**Symmetrie** Sei $x \sim y$, d.h. $x, y \in A$ für $A \in Z$, dann auch $y \sim x$.

**Transitivität** Ist $x \sim y$ und $y \sim z$, so $x, y \in A, y, z \in B$ für geeignete $A, B \in Z$.
Da $y \in A \cap B$ folgt $A = B$, da Zerlegung, d.h. $x, z \in A (= B)$, also $x \sim z$.

□

## 4.7 Repräsentantensystem

Sei $\sim$ eine Äquivalenzrelation auf M, $Z_\sim$ die Menge der Äquivalenzklassen bezgl. $\sim$.
Wählt man aus jeder Äquivalenzklasse genau ein Element aus, so bilden die Elemente ein Repräsentantensystem der Äquivalnzklassen bezgl. $\sim$.

### 4.7.1 Beispiel

$x \sim y :\Leftrightarrow 2|x - y$, Äquvalenzklassen $[0], [1]$,
also $\{0, 1\}$ ist Repräsentantensystem; ebenso $\{26, -1357\}$

# 5 Natürliche Zahlen und Induktion

Natürliche Zahlen sind durch Peano-Axiome beschrieben. Das entscheidende Axiom ist das Prinzip der vollständigen Induktion.

## 5.1 Vollständige Induktion

### 5.1.1 Definition

Sei $n_0 \in \mathbb{N}$ fest.
Für jedes $n \geq n_0$ sei $A(n)$ eine Aussage (von $n$ abhängig)
Es gelte:

**(1)** $A(n_0)$ ist wahr ("Induktionsanfang")

**(2)** $\forall n \geq n_0 :$ $\underbrace{\text{Ist } A(n) \text{ wahr}}_{\text{Induktionsvoraussetzung}}$ $, \underbrace{\text{so ist auch } A(n+1) \text{ wahr}}_{\text{Induktionsbehauptung}}$
("Induktionsschritt", "Induktionsschulss")

Dann ist $A(n)$ für alle $n \geq n_0$ wahr.

Dies liefert eine Beweismethode für Aussagen, die von natürlichen Zahlen abhängen. Man hat immer 2 Dinge zu beweisen:

- Induktionsanfang gilt ($A(n_0)$ wahr)
- Induktionsschritt: $\forall n \geq n_0 : A(n) \Rightarrow A(n+1)$

### 5.1.2 Beispiel

**Behauptung:** Für jede natürliche Zahl $n$ gilt $1 + 2 + ... + n = \frac{n(n+1)}{2}$

**Beweis:**

**Induktionsanfang** $n_0 = 1, 1 = \frac{1(1+1)}{2} = \frac{2}{2} = 1$✓

**Induktionsschluss**

**Induktionsannahme**
$1 + 2 + ... + n = \frac{n(n+1)}{2}$ gelte für ein beliebiges aber festes $n$

**Induktionsbehauptung**
Dann gilt auch $\sum_{i=1}^{n+1} i = \frac{(n+1)((n+1)+1)}{2}$

**Induktionsbeweis**

$$\begin{aligned} 1+2+...+n+n+1 &= \frac{n(n+1)}{2}+n+1 \\ &= \frac{n(n+1)+2(n+1)}{2} \\ &= \frac{(n+1)(n+2)}{2} \\ &= \frac{(n+1)((n+1)+1)}{2} \end{aligned}$$

□

### 5.1.3 Bemerkung

Induktionsprinzip gilt auch für $\mathbb{N}_0$

## 5.2 Verschärftes Induktionsprinzip

$A(n), n_0$ wie in 5.1 definiert.
Es gelte:

**(1)** $A(n_0)$ ist wahr.

**(2)** $\forall n \geq n_0 : A(n_0) \wedge A(n_0+1) \wedge ... \wedge A(n) \Rightarrow A(n+1)$

Dann ist A(n) für alle $n \geq n_0$ wahr.

### 5.2.1 Beispiel

**Behauptung:** Jede natürlicher Zahl $n > 1$ ist Primzahl oder Produkt von Primzahlen

**Beweis:**

**Induktionsanfang** $n_0 = 2$ ist Primzahl ✓

**Induktionsschluss**

**Induktionsannahme**
Aussage gilt für $2, 3, 4, ..., n$

**Induktionsbehauptung**
Dann gilt die aussage auch für $n+1$

**Induktionsbeweis**
Ist $n+1$ Primzahl, so gilt die Aussage,
sonst $n+1$ ist keine Primzahl, also $n+1 = k \cdot l$ mit
$1 < k < n+1$
$1 < l < n+1$
Nach Ind.vor. gilt Aussage für $k$ und $l$
$\Rightarrow n+1$ ist Produkt von Primzahlen.

□

## 5.3 Prinzip der rekursiven Definition

Man will eine Abb. $g : A \to M$ definieren, $M \neq \emptyset$ Menge, $A = \{n \in \mathbb{N} | n \geq n_0\}$, wobei $n_0 \in \mathbb{N}$ fest vorgegeben.

### 5.3.1 informelle Definition

- Definiere $g(n_0)$ (Festlegung des "Startwertes")
- Beschreibe, wie man für jedes $n \geq n_0$ $g(n+1)$ aus $g(n)$ erhält. ("Rekursionsschritt")

Dann ist $g$ auf ganz A definiert.

### 5.3.2 Beispiele

#### Fakultätsfunktion

$\cdot! : \mathbb{N}_0 \to \mathbb{N}, n \mapsto n!$
Rek.def.:
$0! := 1, (n+1)! := n! \cdot (n+1), \forall n \geq 0$

#### Potenzen von $\in \mathbb{R}$, Def. von $x^n$

$x^0 := 1, x^{n+1} := x^n \cdot x$

#### Summen

$A = \{n \in \mathbb{N}_0 | n \geq n_0 \in \mathbb{N}_0\}$ fest vorgegeben.
Gegeben: $a : A \to \mathbb{R}, k \mapsto a_k$, Abb. ("Folge"), also $a(k) = a_k$
Für jedes $n \in \mathbb{N}_0, n \geq n_0$ definiere $\sum_{k=n_0}^{n} a_k$ durch

- $\sum_{k=n_0}^{n_0} a_k = a_{n_0}$
- $\sum_{k=n_0}^{n+1} a_k = \sum_{k=n_0}^{n} a_k + a_{n+1}, \forall n \geq n_0$

Konvention für $n < n_0 : \sum_{k=n_0}^{n} a_k := 0$

**Produkte**

$\prod_{k=n_0}^{n} a_k, \forall n \geq n_0 :$

- $\prod_{k=n_0}^{n_0} a_k = a_{n_0}$
- $\prod_{k=n_0}^{n+1} a_k = \prod_{k=n_0}^{n} a_k \cdot (n+1) \forall n \geq n_0$

Konvention für $n \geq n_0$: $\prod_{k=n_0}^{n} a_k := 1$

Spezialfall: $\prod_{k=1}^{n} k = \prod_{k=0}^{n} k = n!$

**Wichtige Frage**

Gibt es eine "geschlossene Form" für eine rekursiv definierte Abb.
Definiere rekursiv: $g : \mathbb{N} \to \mathbb{N}$
$g(1) := 2$
$g(n+1) := 3g(n) + 4, \forall n \geq 1$

Wir zeigen: $g(n) = 4 \cdot 3^{n-1} - 2$, geschlossene Form $\forall n \geq 1$

**Beweis durch Induktion:**

**Indanf.:** $g(1) = 4 \cdot 3^{1-1} - 2 = 4 - 2 = 2 = 2$✓

**Indvor.:** Beh. richtig für n, also $g(n) = 4 \cdot 3^{n-1} - 2$

**Indbeh.:** $g(n+1) = 4 \cdot 3^n - 2$

**Indschritt:** $g(n+1) = 3 \cdot g(n) + 4 = 3 \cdot (4 \cdot 3^{n-1} - 2) + 4 = 4 \cdot 3^n - 6 + 4 = 4 \cdot 3^n - 2$

□

### 5.3.3 Rekursive Definition mit mehreren Startwerten

Man kann Funktionen auch rekursiv definieren, wenn die Def. von $g(n+1)$ nicht nur von $g(n)$, sondern auch von $g(n-1)$ abhängt (allg.: k vorherige Werte, wobei k fest gewählt). Dann muss man $g(n_0)$ und $g(n_0 - 1)$ als Startwerte definieren (allg.: k Startwerte).

**Beispiel**

$h(1) := 1, h(2) := 3, h(n+1) := 2 \cdot h(n) - h(n-1) \forall n \geq 2$
Vermutung: $h(n) = 2n - 1 \forall n \geq 1$

**Beweis**
Da wir unsere Vermutung im Induktionsschluss für $n$ und $n-1$ verwenden wollen, müssen wir den Ind.Anf. für $n = 1$ und $n = 2$ machen.

**Indanf.:**

$n = 1 : h(1) = 1, 2 \cdot 1 - 1 = 1 \checkmark$
$n = 2 : h(2) = 3, 2 \cdot 2 - 1 = 3 \checkmark$

**Indschluss:** Sei $n \geq 2$

$$\begin{aligned} h(n+1) &= 2 \cdot h(n) - h(n-1) \\ &= 2 \cdot (2n-1) - (2(n-1) - 1) \\ &= 2 \cdot 2n - 2 - 2n + 2 - 1 \\ &= 2n + 1 \\ &= 2(n-1) - 1 \end{aligned}$$

□

## 5.4 Rechenregeln für Produkte und Summen

### 5.4.1 Änderung der Summensequenzen

$\sum_{k=0}^{n} a_k = \sum_{k=1}^{n+1} a_{k-1}$

Schreibweisen:
$\sum_{k=0}^{n} a_k = \sum_{0 \leq k \leq n} a_k = \sum_{k \in \{0,\ldots,n} a_k = \sum_{k} a_k = \sum_{k=0}^{n} a_k$

$B = \{a_0, a_1, \ldots a_n\} : \sum_{k=0}^{n} a_k = \sum_{a \in B} a$

Analog für Produkte

### 5.4.2 Doppelsummen

$f : \mathbb{N}_0 \times \mathbb{N}_0 \to \mathbb{R}$
$\sum_{i=0}^{n} \sum_{j=0}^{m} f(i,j) = \sum_{i=0}^{n} (\sum_{j=0}^{m} f(i,j))$
$= \sum_{j=0}^{m} f(0,j) + \sum_{j=0}^{m} f(1,j) + ... + \sum_{j=0}^{m} f(n,j)$
$= \sum_{j=0}^{m} \sum_{i=0}^{n} f(i,j)$

Ist $n = m$, so schreibt man auch: $\sum_{i,j=0}^{n} f(i,j)$

### 5.4.3 Koeffizienten vor Summen

$a_0 \cdot \sum_{k=0}^{n} b_k = \sum_{k=0}^{n} a_0 \cdot b_k$

$(a_0 + a_1) \cdot \sum_{k=0}^{n} b_k = a_0 \cdot \sum_{k=0}^{n} b_k + a_1 \cdot \sum_{k=0}^{n} b_k = \sum_{i=0}^{1} \sum_{k=0}^{n} a_i \cdot b_k$

Allgemein: $(\sum_{i=0}^{m} a_i) \cdot (\sum_{k=0}^{n} b_k) = \sum_{i=0}^{m} \sum_{k=0}^{n} a_m \cdot b_k$

## 5.5 Wohlordnungsprinzip

Ist $\emptyset \neq M \subseteq N$, so besitzt M ein kleinstes Element: $min(M)$.
Logisch äquivalent zum Prinzip der vollst. Induktion.

## 5.6 Fibonacci Zahlen

$F(0) := 0, F(1) := 1, F(n) := F(n-1) + F(n-2)$
$0, 1, 1, 2, 3, 5, 8, 13, 21, 34, ...$
$F(n) = \frac{(1+\sqrt{5})^n - (1-\sqrt{5})^n}{2^n \cdot \sqrt{5}}$

### 5.6.1 Beweis durch vollst. Induktion

**Indanf.:**

$\frac{(1+\sqrt{5})^0 - (1-\sqrt{5})^0}{2^0 \cdot \sqrt{5}} = 0$
$\frac{(1+\sqrt{5})^1 - (1-\sqrt{5})^1}{2^1 \cdot \sqrt{5}} = 1$

**Indschritt:**

$F(n) = \frac{1}{\sqrt{5}} \cdot (p^n - q^n)$ mit $p = \frac{1+\sqrt{5}}{2}, g = \frac{1-\sqrt{5}}{2}$
Es gilt $1 + p = p^2, 1 + q = q^2$
Beweis: $p^2 = \frac{1+2\sqrt{5}+5}{4} = \frac{6+2\sqrt{5}}{4} = \frac{3+\sqrt{5}}{2} = 1 + \frac{1+\sqrt{5}}{2} = 1 + p$✓

$$\begin{aligned} F(n) &= F(n-1) + F(n-2) \\ &= \frac{1}{\sqrt{5}}(p^{n-1} - q^{n-1}) + \frac{1}{\sqrt{5}}(p^{n-2} - q^{n-2}) \\ &= \frac{1}{\sqrt{5}}(p^{n-1} + p^{n-2}) - \frac{1}{\sqrt{5}}(q^{n-1} + q^{n-2}) \\ &= \frac{1}{\sqrt{5}} \cdot p^{n-2} \cdot (p+1) - \frac{1}{\sqrt{5}} \cdot q^{n-2} \cdot (q+1) \\ &= \frac{1}{\sqrt{5}} \cdot (p^n - q^n) \end{aligned}$$

□

# 6 Elementare Zahlentheorie

## 6.1 Teiler

### 6.1.1 Definition

Seien $a, b \in \mathbb{Z}$ und $b \neq 0$. Dann heißt b Teiler von a, falls ein $q \in \mathbb{Z}$ existiert, sodass $a = b \cdot q$. Wir schreiben $b|a$.
Falls b kein Teiler von a ist: $b \nmid a$.
Merke: 0 ist niemals Teiler

#### Beispiel

$-3|6, 6 = (-2) \cdot (-3)$
$17|0, 0 = 17 \cdot 0$

### 6.1.2 Satz

**(a)** $b|c$ und $b|d$, dann gilt $b|(kc + ld), \forall k, l \in \mathbb{Z}$

**(b)** $b|a$ und $a \neq 0$, dann gilt $|b| \leq |a|$

**(c)** $b|a$ und $a|b$, dann gilt $a = b$ oder $a = (-b)$

#### Beweis

**(a)** Auf ÜB:
Ist $\frac{b}{a} = i, \frac{c}{a} = j$, $i, j \in \mathbb{Z}$, da $a|b \wedge a|c$
Dann $\frac{kb+lc}{a} = ki + lj \in \mathbb{Z}$, da $k, l, i, j \in \mathbb{Z}$
also $a|kb + lc$. □

**(b)** Da $b|a$ gilt $|b|||a|$.
Also $|a| = |b| \cdot q$ für ein $q \in \mathbb{N}$, da $a \neq 0$ gilt
$|a| = q \cdot |b| = \sum_{i=1}^{q} |b_i| = |b_1| + |b_2| + ... + |b_q| \geq |b|$

□

**(c)** Es gilt $a = r \cdot b, b = q \cdot a,\ q, r \in \mathbb{Z}$

$a = r \cdot q \cdot a$

$\Leftrightarrow a - rqa = 0$

$\Leftrightarrow a(1 - rq) = 0$

Da $a \neq 0$, da $a|b$:

$\Rightarrow 1 - rq = \frac{0}{a} \Leftrightarrow 1 - rq = 0 \Leftrightarrow rq = 1$

Somit $r|1, q|1$

$\Rightarrow |r| \leq 1, |q| \leq 1$, da 0 niemals Teiler gilt:

$q = r = 1$ oder $q = r = -1$

□

## 6.2 Rest und Quotient

Im Allgemeinen lassen sich ganze Zahlen nicht durch einander teilen. Daher benötigen wir Division mit Rest.

### 6.2.1 Satz

Seien $a, b \in \mathbb{Z}, b \neq 0$.
Dann existieren eindeutig bestimmte Zahlen $q, r \in \mathbb{Z}$ mit

**(i)** $a = q \cdot b + r$

**(ii)** $0 \leq r \leq |b|$

r heißt "Rest", q "Quotient"

#### Beweis

Wir benötigen zwei Beweise:

**A** Beweis der Existenz von q und r mit (i) und (ii)

**B** Eindeutigkeit von q,r

**A 1.Fall** $b > 0$

Sei q die größte Zahl aus $\mathbb{Z}$ mit $q \leq \frac{a}{b}$. Dann gilt $q \cdot b \leq a$
Setze: $r = a - qb \geq 0$
Es ist also $a = qb + r$
Zu zeigen: $r < b$
Dazu nehmen wir an, dass $r < b$ falsch ist. Dann leiten wir aus $r \geq b$ eine Aussage ab, von der wir wissen, dass sie falsch ist. Dann wissen wir, dass $r \geq b$ falsch sein muss, es folgt $r < b$ ("Widerspruchsbeweis", $A \Rightarrow B \equiv A \wedge \neg B = 0$)
Dann $r = b + s, s \geq 0$, d.h.

$a - qb = b + s$
$\Leftrightarrow a - s = b + qb$
$\Leftrightarrow a - s = b(1 + q)$
$\Rightarrow b(1 + q) = a - s \leq a$
$\Leftrightarrow q + 1 \leq \frac{a}{b}$ $\quad \lightning$
$\Rightarrow r < b$

**2.Fall** $b < 0$

Es ist $a = q \cdot |b| + r, 0 \leq r < |b|$ (folgt aus 1.Fall)
Also: $a = -q \cdot b + r$ und somit $0 \leq r < |b|$

□

**B**

Angenommen q,r sind nicht eindeutig.
$a = q_1 \cdot b + r_1 = q_2 \cdot b + r_2$
Ohne Beschränkung der Allgemeinheit: $r_1 \geq r_2$
$q_1 \cdot b + r_1 = q_2 \cdot b + r_2$
$\Leftrightarrow r_1 - r_2 = q_2 \cdot b - q_1 \cdot b$
$\Leftrightarrow r_1 - r_2 = b(q_1 - q_2) \geq 0$ (da $r_1 \geq r2$)
Also $b|(r_1 - r_2)$
Zu zeigen: $r_1 - r_2 = 0$, durch Widerspruchsbeweis:
$r_1 - r_2 \neq 0$
$\overset{6.1.2b)}{\Rightarrow} |b| \leq r_1 - r_2 \leq r_1 < |b|$ $\quad \lightning$
$\Rightarrow r_1 = r_2$
und da $b \neq 0 : q_1 = q_2$

□

## 6.3 mod und *div*

### 6.3.1 Definition

Seinen $a, b \in \mathbb{Z}, b \neq 0$
Sei $a = q \cdot b + r$ mit $0 \leq r < |b|, q, r \in \mathbb{Z}$, wie 6.2.1
Dann $q = a \; div \; b$
$r = a \mod b$
q,r eindeutig nach 6.2, d.h.
$div : \mathbb{Z} \times \mathbb{Z}\backslash\{0\} \to \mathbb{Z}, (a, b) \mapsto a \; div \; b$
$\mod : \mathbb{Z} \times \mathbb{Z}\backslash\{0\} \to \mathbb{Z}, (a, b) \mapsto a \mod b$
Beachte: $a \mod b = 0 \Leftrightarrow b|a$

### 6.3.2 $\lceil a \rceil$ und $\lfloor a \rfloor$

Sei $x \in \mathbb{R}$
$\lceil x \rceil$ kleinste ganze Zahl q mit $q \geq r$ "ceiling"
$\lfloor x \rfloor$ größte ganze Zahl q mit $q \leq r$ "floor"
Also: $\lceil x \rceil = \lfloor x \rfloor = x,\ \forall x \in \mathbb{Z}$

#### Bemerkung

$$a\ div\ b = \begin{cases} \lfloor \frac{a}{b} \rfloor & \text{, wenn } b > 0 \\ \lceil \frac{a}{b} \rceil & \text{, wenn } b < 0 \end{cases}$$
$a \mod b = a - b(a\ div\ b)$

In Java,C,... für $a \geq 0$, in der regel nicht für $a < 0$ ($\Rightarrow$ Beim Programmiern auch negativer Rest möglich, in der Mathematik nicht!)
Def. in Java:
$$a \backslash b = \begin{cases} \lfloor \frac{a}{b} \rfloor & \text{, für } a \cdot b > 0 \\ \lceil \frac{a}{b} \rceil & \text{, für } a \cdot b < 0 \end{cases}$$

## 6.4 b-adische Darstellung natürlicher Zahlen

### 6.4.1 Satz

Sei $b \in \mathbb{N}, b > 1$
Jedes $n \in \mathbb{N}_0$ lässt sich darstellen in der Form:
$n = \sum_{i=0}^{k} x_i \cdot b^i$, wobei

**(i)** $b^k \leq n < b^{k+1}$ für $n > 0$, bzw. $k = 0$, falls $n = 0$

**(ii)** $x_i \in N_0,\ 0 \leq x_i \leq b - 1,\ x_k \neq 0$ für $n \neq 0$

Diese Darstellung ist eindeutig, sie heißt b-adische Darstellung von n.
$x_i$ heißen Ziffern von n bzgl. b.

#### Schreibweise

$n = (x_k\ x_{k-1}\ ...\ x_1\ x_0)_b$ oder, wenn b klar ist: $n = x_k\ x_{k-1}\ ...\ x_1\ x_0$

**Beweis**

Existenz und Eindeutigkeit durch Induktion nach n

**Existenz**

**IA:** $n_0 = 0, n_0 = \sum_{i=0}^{0} x_0 \cdot k^0 = 0 \cdot 1 = 0$

**IS:**

**IV:** Aussage gelte für alle $n' \in \mathbb{N}_0, n' < n$

**IB:** Aussage gilt dann auch für n

Setze $x_0 = n \mod b$
Dann $b|(n - x_0)$, also $n - x_0 = n' \cdot b,\ 0 \leq n' < n$, da $b > 1$
Wende IV an:
$n' = \sum_{i=0}^{k} x'_i \cdot b^i\ ,\ k, x'_i$ mit (i) und (ii)
Setze $x_{i+1} = x'_i$ für $i = 0, ..., k$
Dann:
$n = b \cdot n' + x_0$
$= b \cdot \sum_{i=0}^{k} x'_i b^i\ + x_0$
$= \sum_{i=0}^{k} x_{i+1} b^{i+1}\ + x_0$
$= \sum_{i=1}^{k+1} x_i b^i\ + x_0$
$= \sum_{i=0}^{k} x_i b^i$ ✓

**Gilt (i)?** Z.z.: $b^{k+1} \leq n < b^{k+2}$
Ist $n' > 0$, so gilt nach IV $b^k \leq n' < b^{k+1}$
$\Leftrightarrow b \cdot b^k \leq b \cdot n'$
$\Leftrightarrow b^{k+1} \leq b \cdot n'\ + x_0$
$\Leftrightarrow b^{k+1} \leq n$
Es gilt auch $n' \leq b^{k+1} - 1$, also auch $bn' \leq b^{k+2} - b$
$n = bn' + x_0 \leq b^{k+2} - b + x_0 \overset{x_0 \leq b}{<} b^{k+2}$ ✓

**Gilt (ii)?**
Ja, für $x_1, ...x_{k+1}$ nach IV, da $x_{i+1} = x'_i$.
Auch ist $0 \leq x_0 < b$, da $x_0 = n \mod b$.

**Eindeutigkeit:**

$n = \sum_{i=0}^{l} x_i b^i = \sum_{j=0}^{r} y_i b^i,\ a_i, y_i, l, r$ mit (i),(ii)
Dann $x_0 = y_0 = n \mod b$
Betrachte $\frac{n-x_0}{b}, \frac{n-y_0}{b}$, wende IV an

□

**Beispiel**

**Binärsystem** $(161)_{10}$

**1.Möglichkeit** (wie im Beweis)

$n = n' \cdot b + x_0$
$n' = \frac{n-x_0}{b}$:
$161 \mod 2 = 1 = x_0$
$\frac{161-1}{2} \mod 2 = 80 \mod 2 = 0 = x_1$
$\frac{80-0}{2} \mod 2 = 40 \mod 2 = 0 = x_2$
$\frac{40-0}{2} \mod 2 = 20 \mod 2 = 0 = x_3$
$\frac{20-0}{2} \mod 2 = 10 \mod 2 = 0 = x_4$
$\frac{10-0}{2} \mod 2 = 5 \mod 2 = 1 = x_5$
$\frac{5-1}{2} \mod 2 = 2 \mod 2 = 0 = x_6$
$\frac{2-0}{2} \mod 2 = 1 \mod 2 = 1 = x_7$
$\Rightarrow (161)_{10} = (10100001)_2$

**2.Möglichkeit**

Höchste Potenz von 2, die $\leq 161$?
$2^7 = 128$
$162 - 128 = 33$
Höchste 2er-Potenz $\leq 33$?
$2^5 = 32$
$33 - 32 = 1 = 2^0$

$\Rightarrow (161)_{10} = (10100001)_2$

**Hexadezimalsystem** $(161)_{10}$

$0, ...9, A, ..., F$
$161 \mod 16 = 1$
$\frac{161-1}{16} \mod 16 = 10 \mod 16 = 10 \mathrel{\widehat{=}} A$
$\Rightarrow (161)_{10} = (A1)_{16}$

*oder*

$(161)_{10} = ( \underbrace{1010}_{=(10)_{10}=(A)_{16}} \quad \underbrace{0001}_{=(1)_{10}=(1)_{16}} )_2$
$\Rightarrow (161)_{10} = (A1)_{16}$

### 6.4.2 Schnelles Potenzieren mit Hilfe des Binärsystems

Sei $a \in \mathbb{R}, m \in \mathbb{N}$
Um $a^m$ zu berechnen:
$\underbrace{a \cdot a \cdot ... \cdot a}_{m-1 \text{ Multiplikation}}$ Sehr langsam für große $m$

Schneller: $m = 2^l$ (Spezialfall)
$a^m : a^2, (a^2)^2 = a^4, ..., ((a^2)^{l-1})^2 = (a^2)^l = a^m$
l Multiplikationen, statt $2^{l-1}$

Allgemeiner Fall:
$m = \sum_{i=0}^{k} x_i \cdot 2^i, \;\; x_i \in \{0,1\}, \; x_k = 1$ (o.B.d.A. $m > 0$)
$a^m = a^{\sum_{i=0}^{k} x_i \cdot 2^i}$
$= a^{2^k} \cdot a^{x_{k-1} \cdot 2^{k-1}} \cdot ... \cdot a^{x_1 \cdot 2} \cdot a^{x_0}$
$= (a^{2^{k-1}} \cdot a^{x_{k-1} \cdot 2^{k-2}} \cdot ... \cdot a^{x_1})^2 \cdot a^{x_0}$
$= ...$
$= (...(a^2 \cdot a^{x_{k-1}})^2 ... \cdot a^{x_1})^2 \cdot a^{x_0}$
"square and multiply"

#### Algorithmus "square and multiply"

$b := a$
$for\ j = k-1\ (step\ -1) down\ to\ 0\ do$
  $b := b^2$
  $if\ x_j = 1\ then\ b := b * a$
$end$
$Print\ b$

## 6.5 Kongruenzrelation modulo m

### 6.5.1 Definition

Sei $m \in \mathbb{N}$. Für $a, b \in \mathbb{Z}$ gilt:
$a \equiv b \pmod{m}$ ("a kongruent b modulo m")
$\Leftrightarrow m|a-b$
d.h. $a - b = k \cdot m$, bzw. $a = b + km, b = a + (-k) \cdot m,\ k \in \mathbb{Z}$

z.B. $17 \equiv -4 \pmod{7}$, da $7|17 - (-4) = 21$

### 6.5.2 Satz

**(a)** Kongruenzrelation modulo m ist Äquivalenzrelation

**(b)** $a \equiv 0 \pmod{m} \Leftrightarrow m|a$

**(c)** $a \equiv b \pmod{m}, c \in \mathbb{Z} \Rightarrow c \cdot a \equiv c \cdot b \pmod{m}$

**(d)** $a \equiv b \pmod{m} \Leftrightarrow a \mod m = b \mod m$

**(e)** $a \mod m \equiv a \pmod{m}$

#### Beweis

**(a)** Reflexivität ✓
Symmetrie ✓
Transitivität:
$a \equiv b \pmod{m} \wedge b \equiv c \pmod{m}$
$\Rightarrow m|a-b \wedge m|b-c$
$\Rightarrow m|(a-b)+(b-c) = a-c$
$\Rightarrow a \equiv c \pmod{m}$✓

**(b)** trivial ✓

**(c)** $a \equiv b \pmod{m} \Leftrightarrow m|a-b$
$\Rightarrow c \cdot m|c(a-b) \wedge c \neq 0$
$\Leftrightarrow cm|ca-cb \wedge c \neq 0$
$\Leftrightarrow ca \equiv cb \pmod{cm}$
$\Rightarrow ca \equiv cb \pmod{m}$✓

**(d)** "$\Rightarrow$"
Es gilt: $a \equiv b \pmod{m} \Leftrightarrow m|a-b \Leftrightarrow a = b + km \wedge k \in \mathbb{Z}$
Auch gilt: $b = q_1 \cdot m + r,\ 0 \leq r < m$
Folglich: $a = q_1 \cdot m + r + km = m(q_1 + k) + r$
also: $a \mod m = r = b \mod m$✓

**(d)** "$\Leftarrow$"
$a = q_1 \cdot m + r$
$b = q_2 \cdot m + r$
$\Rightarrow a - b = (q_1 - q_2)m$, d.h. $m|a - b$
$\Rightarrow a \equiv b \pmod{m}$✓

**(e)** Es gilt:
$(a \mod m) \mod m = a \mod m$
Behauptung folgt aus (d) "$\Leftarrow$"

□

### 6.5.3 Unterscheidung Modulo und Kongruenz

Bei festem m ist
$a \mapsto a \mod m$, Abb. $\mathbb{Z} \to \mathbb{N}$
$\equiv \pmod{m}$ dagegen ist Relation auf $\mathbb{Z}^2$

$17 \mod 7 = 3$
$17 \equiv 3 \pmod{7}$, aber $17 \equiv 10 \pmod{7}, 17 \equiv (-4) \pmod{7}$

$2 \cdot 3 \equiv 2 \cdot 2 \pmod{2}$ aber $3 \not\equiv 2 \pmod{2}$
(6.5.2 (c) nur Implikation, nicht Äquivalenz!)

### 6.5.4 Satz: Kongruenzklassen modulo m

Die Äquivalenzklassen der Kongruenzrelation modulo m (genannt: "Kongruenzklassen modulo m" sind genau die Mengen

$$\{r + k \cdot m | k \in \mathbb{Z}\}, r = 0, ..., r = m - 1\}$$

Die Menge $\mathbb{Z}_m := \{0, 1, ..., m - 1\}$ ist ein Repräsentantensystem der Kongruenzklassen mod m.

#### Beweis

Folgt aus 6.5.2 (d) , da Aufteilung je nach Rest
Bsp: Kongruenzklassen mod 2
$\overline{[0]}, [1], \mathbb{Z}_2 = \{0, 1\}$

### 6.5.5 Satz: Kongruenzrelation in Summen und Produkten

Seien $a_1 \equiv a_2 \pmod{m} \wedge b_1 \equiv b_2 \pmod{m}$, dann:

**(a)** $a_1 + b_1 \equiv a_2 + b_2 \pmod{m}$

**(b)** $a_1 - b_1 \equiv a_2 - b_2 \pmod{m}$

**(c)** $a_1 \cdot b_1 \equiv a_2 \cdot b_2 \pmod{m}$

**Beweis**

Aus Voraussetzung: $m|a_1 - a_2 \wedge m|b_1 - b_2$

**(a)** Voraussetzung
$\Rightarrow a_1 - a_2 = k \cdot m \wedge b_1 - b_2 = l \cdot m,\ k, l \in \mathbb{Z}$
$\Rightarrow a_1 - a_2 + b_1 - b_2 = km + lm$
$\Rightarrow a_1 + b_1 - (a_2 + b_2) = (k + l)m$
$\Rightarrow m|(a_1 + b_1) - (a_2 + b_2)$
$\Rightarrow a_1 + b_1 \equiv a_2 + b_2 \pmod{m}$

**(b)** analog

**(c)**
$m|a_1 - a_2 \Rightarrow m|(a_1 - a_2)b_1 = a_1b_1 - a_2b_2$
$m|b_1 - b_2 \Rightarrow m|(b_1 - b_2)a_2 = a_2b_1 - a_2b_2$
Also (6.1.2. (a)):
$m|(a_1b_1 - a_2b_1) + (a_2b_1 - a_2b_2)$
$\Rightarrow m|a_1b_1 - a_2b_2$
$\Rightarrow a_1b_1 \equiv a_2b_2 \pmod{m}$

□

### 6.5.6 Korollar: modulo in Summen und Produkten

(=wichtige Folgerung aus einem Satz)

$(a \pm b) \mod m = ((a \mod m) \pm (b \mod m)) \mod m$
$(a \cdot b) \mod m = ((a \mod m) \cdot (b \mod m)) \mod m$
"In mod-Beziehungen (von Summen und Produkten) lassen sich Zahlen durch andere Zahlen aus derselben Kongruenzklasse ersetzen"

**Beweis**

Aus 6.5.2 (e) folgt:
$a \mod m \equiv a \pmod{m}$
$b \mod m \equiv b \pmod{m}$
Aus 6.5.5 folgt:
$(a \mod m) + (b \mod m) \equiv a + b \pmod{m}$
Aus 6.5.2(e) folgt:
$(a \mod m) + (b \mod m) \equiv ((a \mod m) + (b \mod m)) \mod m \pmod{m}$
Aus Transitivität von $\equiv$ folgt Behauptung.

## 6.6 Größter gemeinsamer Teiler und kleinstes gemeinsames Vielfaches

### 6.6.1 Definition

Seien $a_1, ..., a_r$ ganze Zahlen.

(a) Ist mindestens ein $a_1 \neq 0$, so ist der größte gemeinsame Teiler $ggT(a_1, ..., a_r)$ die größte natürlich Zahl, die alle $a_1, ..., a_r$ teilt.

(b) Sind alle $a_i \neq 0$, so ist das kleinste gemeinsame Vielfache $kgV(a_1, ..., a_r)$ die kleinste natürliche Zahl, die von allen $a_1, ...a_r$ geteilt wird.

### 6.6.2 Bemerkungen

(a) $ggT(a_1, ..., a_r)$ existiert und ist eindeutig bestimmt:
1 teilt alle $a_1, ..., a_r$ und jeder gemiensame Teiler ist $\leq |a_i| \; \forall i$

(b) $kgV(a_1, ..., a_r)$ existiert und ist eindeutig bestimmt:
$|a_1| \cdot ... \cdot |a_r|$ wird von allen $a_i$ geteilt, also existiert eine natürliche Zahl, die von allen $a_1, ..., a_r$ geteilt wird.

(c) $ggT(a_1, ..., a_r) = ggT(|a_1|, ..., |a_r|)$
$kgV(a_1, ..., a_r) = kgV(|a_1|, ..., |a_r|)$

### 6.6.3 Teilerfremdheit

Ist $ggT(a_1, ..., a_r) = 1$, so heißen $a_1, ..., a_r$ teilerfremd.

## 6.7 Euklidscher Algorithmus

Der ggT von zwei Zahlen wird mit dem Euklidschen Algorithmus berechnet.
Das Grunndprinzip im folgenden Lemma:

### 6.7.1 Lemma

Seinen $q, a, b \in \mathbb{Z}, \; b \neq 0$
Dann ist:
$ggT(a, b) = ggT(q \cdot b + a, b)$

**Beweis**

$\forall t \in \mathbb{N}$ gilt:
$t|a \wedge t|b \Rightarrow t|q \cdot b + a \wedge t|b$

gegeben : $a, b \in \mathbb{Z}$, nicht beide 0
bestimme ggT(a,b)
oBdA: $b \neq 0, b \nmid a$ (sonst $ggT(a,b) = b$)
Setze: $a_0 = a, a_1 = b$
Idee: mehrfache Division mit Rest, Aufg. wird kleiner, bis Rest=0

$$a_0 = q_1 \cdot a_1 + a_2 \text{ mit } 0 \leq a_2 \leq a_1$$

$$a_1 = q_2 \cdot a_2 + a_3 \text{ mit } 0 \leq a_3 \leq a_2$$

$$a_2 = q_3 \cdot a_3 + a_4 \text{ mit } 0 \leq a_2 \leq a_3$$

$$\ldots$$

$$a_{n-1} = q_n \cdot a_n + 0 \text{ (erstmalig Rest=0)}$$

Es gilt:

$$\begin{aligned}
ggT(a,b) &= ggT(b,a) \\
&= ggT(a_1, a_0) \\
&= ggT(a_1, q_1 a_1 + a_2) \\
&= ggT(a_1, a_2) \text{ (nach Lemma)} \\
&= ggT(a_2, a_1) \\
&= ggT(a_2, q_2 a_2 + a_3) \\
&= ggT(a_2, a_3) \\
&\ldots \\
&= ggT(a_{n-1}, a_n) \\
&= ggT(a_n, a_{n-1}) \\
&= ggT(a_n, q_n a_n) \\
&= a_n
\end{aligned}$$

= Beweis für Euklidschen Algogithmus

### 6.7.2 Euklidscher Algorithmus

0 Eingabe: $a, b \in \mathbb{Z}$, nicht beide 0

1 if $b = 0$ than $y := |a|$ endif

2 if $b|a$ than $y := ||$ endif

3 if $b \neq 0 \wedge b \not| a$ than

4 $x := a,\ y := b$

5 while $x \mod y \neq 0$ do

6 $r := x \mod y$

7 $x := y$

8 $y := r$

9 endwhile

10 endif

11 Ausgabe: y (=ggT(a,b))

### 6.7.3 Zusammenhang: Beweis - Algorithmus

Im Beweis:
$ggT(a_i, a_{i+1})$
$= ggT(a_{i+1}, a_i)$
$= ggT(a_{i+1}, a_{i+2})$
wobei $a_{i+2}$ Rest von Division von $a_i$ durch $a_{i+1}$

Im Algorithmus:
In der While-Schleife:
Zunächst: $x := a_i, y := a_{i+1}$
Dann: $r := x \mod y = a_i \mod a_{i+1} = a_{i+2}$

Schleifenende:
$x := a_{i+1}$
$y := a_{i+2}$

### 6.7.4 Beispiel

0 a=48, b=-30

1 $b \neq 0 \rightarrow 2$

2 $b \not| a \rightarrow 3$

3 $b \neq 0 \wedge b \not| a \rightarrow 4$

4 $x := 48,\ Y := -30$

5 $48 \mod -30 = 18 \neq 0 \rightarrow 6$

6 $r := 18$

7 $x := -30$

5 $-30 \mod 18 = 6 \neq 0 \rightarrow 6$

6 $r := 6$

7 $x := 18$

8 $y := 6$

5 $18 \mod 6 = 0 = 0 \rightarrow 11$

11 Ausgabe: 6 (=ggT(48,-30))

Der folgende Satz liefert eine richtige Darstellung des ggT zweier ganzer Zahlen.

### 6.7.5 Satz (Bachet de Méziriac)

Seien $a, b \in \mathbb{Z}$ nicht beide =0.
Dann existieren $s, t \in \mathbb{Z}$ mit

$$ggT(a,b) = s \cdot a + t \cdot b$$

#### Beweis(konstruktiver Beweis)

Ist b=0, so $ggT(a,b) = a = s \cdot a + t \cdot b$ mit $t = 0 \wedge s = \begin{cases} 1 & \text{, falls } a > 0 \\ -1 & \text{, falls } a < 0 \end{cases}$

Ist $b \neq 0 \wedge b|a$, so $ggT(a,b) = |b| = s \cdot a + t \cdot b$ mit $s = 0 \wedge t = \begin{cases} 1 & \text{, falls } b > 0 \\ -1 & \text{, falls } b < 0 \end{cases}$

Sei jetzt $b \neq 0 \wedge b \not| a$
Setze $a_0 = a, a_1 = b$
Euklid. Alg.:
$a_0 = q_1 a_1 + a_2, a_1 = q_1 a_1 + a_2, ..., a_{n-1} = q_n a_n + 0$
$a_n = ggT(a_0, a_1)$ $(n \geq 2$, da $a_1 \not| a_2)$
(insbesondere $a_{j-2} = q_{j-1} a_{j-1} + a_j)$
Beh.: $\forall j = 0, ..., n \exists s_j, t_j \in \mathbb{Z} : a_j = s_j a_0 + t_j a_1$
(Satz folgt für j=n)

Beweis durch Induktion:

**IA** $j = 0, s_0 = 1, t_0 = 0 : a_0 = 1 \cdot a_0 + 0 \cdot a_1 = a_0$✓
$j = 1, s_1 = 0, t_1 = 1 : a_1 = 0 \cdot a_0 + 1 \cdot a_1 = a_1$✓

**IS**

**IV** Sei $j \geq 2$: $a_{j-2} = s_{j-2}a_0 + t_{j-2}a_1$
$a_{j-1} = s_{j-1}a_0 + t_{j-1}a_1$

**IB** $a_j = a_{j-2} - q_{j-1}a_{j-1}$
$= s_{j-2}a_0 + t_{j-2}a_1 - q_{j-1}(sj - 1a_0 + t_{j-1}a_1)$
$= \underbrace{(s_{j-2} - q_{j-1}s_{j-1})}_{=:s_j a_0 + \underbrace{(t_{j-2} - q_{j-1}t_{j-2})}_{=:t_j} a_1}$

□Beweis liefert sofort einen Alg. zur Bestimmung von s,t.

### 6.7.6 Erweiterter Euklidscher Algorithmus

0 Eingabe: $a, b \in \mathbb{Z}$, nicht beide 0

1 if $b = 0$ than $y := |a|$ endif

2 if $b|a$ than $y := ||$ endif

3 if $b \neq 0 \wedge b \not| a$ than

4 $x := a,\ y := b,\ s_{-2} := 1,\ s_{-1} := 0,\ t_{-2} := 0,\ t_{-1} := 1$

5 while $x \mod y \neq 0$ do

6 $q := x\ div\ y,\ r := x \mod y$

7 $s := s_{-2} - q \cdot s_{-1},\ t := t_{-2} - qt_{-1}$

8 $s_{-2} := s_{-1},\ s_{-1} := s$

9 $t_{-2} := t_{-1},\ t_{-1} := t$

10 $x := y,\ y := r$

11 endwhile

12 endif

13 Ausgabe: Y (=ggT(a,b)),s,t (mit y=sa+tb)

**Beispiel**

| $x$ | $y$ | $s_{-2}$ | $s_{-1}$ | $s$ | $t_{-2}$ | $t_{-1}$ | $t$ | $q$ | $r$ |
|---|---|---|---|---|---|---|---|---|---|
| 48 | $-30$ | 1 | 0 | | 0 | 1 | | | |
| $-30$ | 18 | 0 | 1 | 1 | 1 | 1 | 1 | $-1$ | 18 |
| $-12$ | 6 | 1 | 2 | 2 | 1 | 3 | 3 | $-2$ | 6 |

### 6.7.7 Korollar

Seien $a, b, c \in \mathbb{Z}, m \in \mathbb{N}$.

(a) Seien a,b nicht beide 0, so gilt :
a und b sind teilerfermd $\Leftrightarrow \exists s, t \in \mathbb{Z} : sa + tb = 1$

(b) Sind a,b nicht beide 0, so gilt:
$c|a \wedge c|b \Rightarrow c|ggT(a, b)$

(c) Ist ggT(a,b)=1, so gilt:
$a|b \cdot c \Rightarrow a|c$

(d) Ist ggT(c,m)=1 und gilt $ca \equiv cb \pmod{m}$, so ist $a \equiv b \pmod{m}$

**Beweis**

(a) "$\Rightarrow$": 6.7.5
"$\Leftrightarrow$": Seien $s, t \in :sa + tb = 1$
Betrachte: d=ggT(a,b)
6.1.2(a)$\Rightarrow d|sa + tb = 1$, also d=1

(b) nach 6.7.5 gilt ggT(a,b)=sa+tb
$c|a \wedge c|b \underset{6.1.2}{\Rightarrow} c|sa + tb \Rightarrow c|ggT(a, b)$

(c) 6.7.5: $\exists s, t \in \mathbb{Z}$ mit $1 = sa + tb$
also $c = sac + tbc$
Da $a|a \wedge a|bc$, folgt mit 6.1.2(a):
$a|asc + tbc$

(d) $ca \equiv cb \pmod{m} \Rightarrow m|ca - cb \Leftrightarrow m|c(a - b)$
Wegen $ggT(c, m) = 1$ folgt nach (c):
$m|a - b \Leftrightarrow a \equiv b \pmod{m}$

### 6.7.8 Bemerkungen

Die Aussagen in 6.7.5 und 6.7.7(a) gelten auch für ggT beliebig vieler Zahlen:
Seien $a_1, ..., a_k \in \mathbb{Z}, k \geq 2$, nicht alle $a_i = 0$, dann

(a) $\exists s_1, ..., s_k : ggT(a_1, ..., a_k) = s_1a_1 + ... + s_ka_k$

(b) $ggT(a_1, ..., a_k) = ggT(ggT(a_1, ..., a_{k-1}), a_k)$
$(ggT(a_1) = |a_1|)$

(c) $c|a_1 \wedge ... \wedge c|a_k \Rightarrow c|ggT(a_1, ..., a_k)$

(d) $kgV(a_1, ..., a_k) = kgV(kgV(a_1, ..., a_{k-1}), a_k) \;\; a_i \neq 0$
$(kgV(a_1) = |a_1|)$

## 6.8 Primzahlen

### 6.8.1 Definition

Eine natürliche Zahl $p > 1$ heißt Primzahl, wenn 1 und p die einzigen natürlichen zahlen sinde, die p teilen. (d.h. $\forall 1 \leq k < p : ggT(p, k) = 1$

### 6.8.2 Satz

Ist p Primzahl, $a_1, ..., a_k \in \mathbb{Z}$ mit $p|a_1 \cdot ... \cdot a_k$,
dann existiert i mit $p|a_i$

#### Beweis

Induktion nach k

**IA** $k = 1$ ✓, da dann $p = a_1$

**IS**

**IV** Satz gelte für k-1

**IB** Satz gilt dann auch für k

**IBew** Betrachte $p = a_1 \cdot ... \cdot a_k$
Ist $p = a_k$, so folgt die Behauptung, sonst $p \not| a_k$
so $ggT(p, a_k) = 1$, da p Primzahl.
Nach 6.7.7(c) gilt $p|a_1 \cdot ... \cdot a_{k-1}$
Nach IV: $\exists j \in \{1, ..., k-1\} : p|a_j$

□

### 6.8.3 Theorem (Fundamentalsatz der elementaren Zahlentheorie)

Zu jeder Zahl $a \geq 2$ gibt es endlich viele verschiedene Primzahlen $p_1, ..., p_n$ und natürliche Zahlen $e_1, ..., e_n$ mit

$$a = p_1^{e_1} \cdot ... \cdot p_n^{e_n}$$

Die $p_i$ heißen Primfaktoren (Primteiler) von a.
Die Darstellung von a als Produkt von Primzahlen ist eindeutig (bis auf die Reihenfolge).

#### Beweis

Existenz: 5.2.1: Jede natürliche Zahl ist Primzahl oder Produkt von Primzahlen.
Eindeutigkeit:
Angenommen wir hätten:
$a = p_1^{e_1} \cdot ... \cdot p_n^{e_n} = q_1^{f_1} \cdot ... \cdot q_m^{f_m}$ mit $p_i, q_i, e_i, f_i \in \mathbb{N}$
$p_i$ paarweise verschieden, $q_i$ paarweise verscheiden.
Nach 6.8.2 gilt:
Jedes $p_i$ teilt eines der $q_j$, d.h. $p_i = q_i$, da $q_j$ Primzahl.
Ebenso umgekehrt($q_j = p_i$, da $p_i$ Primzahl).
Also $\{p_1, ..., p_n\} = \{q_1, ..., q_n\}, n = m$
OBdA (da Elemente einer Menge vertauscht werden knnen; Kommutativität von $\cdot$)
sei $p_i = q_i \; \forall i = 1, ..., n$
Noch zu zeigen: $e_i = f_i \; \forall i = 1, ..., n$
Beweis durch Widerspruch:
Angenommen es gibt ein k mit $e_k \neq f_k$ und oBdA $e_k < f_k$
Teile beide Seiten durch $p_k^{e_k}$
$p_1^{e_1} \cdot ... \cdot p_{k-1}^{e_{k-1}} \cdot p_{k+1}^{e_{k+1}} \cdot ... \cdot p_n^{e_n} = p_1^{f_1} \cdot ... \cdot p_{k-1}^{f_{k-1}} \cdot p_k^{f_k - e_k} \cdot p_{k+1}^{f_{k+1}} \cdot ... \cdot p_n^{f_n}$
Da $p_k$ die rechte Seite teilt (da $f_k > e_k$), teilt $p_k$ auch die linke Seite und damit ein $p_j$ mit $j \neq k$ (nach 6.8.2). Also gilt $p_j = p_k$, ein Widerspruch zur Definition der $p_i$

Also $e_i = f_i \; \forall i = 1, ..., n$

□

### 6.8.4 Korollar

Seien $a, b \in \mathbb{N},\ a, b \geq 2$
Seien $P(a)$ und $P(b)$ die Mengen von Primfaktoren von a und b, d.h.
$a = \prod_{p \in P(a)} p^{n(p)}$ und $b = \prod_{p \in P(b)} p^{m(p)}$
mit $n(p), m(p) \in \mathbb{N}$ geeignet gewählt.
Dann ist

$$ggT(a,b) = \prod_{p \in P(a) \cap P(b)} p^{min(n(p),m(p))}$$

und

$$kgV(a,b) = \prod_{p \in P(a) \setminus P(b)} p^{n(p)} \cdot \prod_{p \in P(b) \setminus P(a)} p^{m(p)} \cdot \prod_{p \in P(a) \cap P(b)} p^{max(n(p),m(p))}$$

wobei min: Minimum, max: Maximum
Insbesondere ist: $a \cdot b = ggT(a,b) \cdot kgV(a,b)$

#### Beispiel

$a = 1248 = 2^5 \cdot 3 \cdot 13$
$b = 3780 = 2^2 \cdot 3^3 \cdot 5 \cdot 7$

$ggT(a,b) = 2^2 \cdot 3 = 12$
$kgV(a,b) = 2^5 \cdot 3^3 \cdot 5 \cdot 7 \cdot 13 = 393120$

### 6.8.5 Bemerkung

(a) Sind $a_1, ..., a_k$ paarweise teierfremd, so ist $kgV(a_1, ..., a_k) = a_1 \cdot ... \cdot a_k$
(folgt aus 6.7.8(d))

(b) Sind $a_i | c\ \forall i = 1, ..., k$, so $kgV(a_1, ..., a_k) | c$

# 7 Kombinatorik

(nur ein kleiner Teil)
Es geht hier um Abzählbestimmungen und versch. Typen von Zusammenfassungen endlich vieler Objekte. Bildet Basis der diskreten Wahrscheinlichkeitstheorie.

## 7.1 Satz

Seinen A,B Mengen
(a) $|A \cup B| = |A| + |B| - |A \cap B|$
(b) Sind A,B nicht leer, so $|A \times B| = |A| \cdot |B|$

### Frage

$|A \cup B \cup C| \stackrel{?!}{=} |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|$
(A) und (b) lassen sich verallgemeinern.

### 7.1.1 Korollar

$A_1, ..., A_n$ nicht leer, so $|A_1 \times ... \times A_n| = \prod_{i=1}^{n} A_i$
Insbesondere für $A \neq \emptyset : |A^n| = |A|^n$

### 7.1.2 Beispiele

(a) Wieviele Wörter der Länge n gibt es über dem Alphabet $\{0, 1\}$
Wörter der Länge n= n-Tupel
$|\{0,1\}^n| = |\{0,1\}|^2 = 2^n$

(b) Wieviele DNS-Sequenzen der Länge 1000 gibt es?
$|\{A, G, C, T\}^{1000}| = |\{A, G, C, T\}|^{1000} = 4^{1000}$

## 7.2 Auswahlanzahlen

Anzahl von Auswahlen für k Gegenstände aus n Gegenständen. Wir unterscheiden:

- Anordnung relevant?
  "Geordnete Auswahl" (z.B. Spiel 77)
- Anordnung nicht relevant?
  "Ungeordnete Auswahl" (z.B. Lotto)
- Wiederholung möglich?
  "mit zurücklegen" (z.B. Spiel 77)
- Wiederholung nicht möglich?
  "ohne Zurücklegen" (z.B. Lotto)

## 7.3 Geordnete Auswahl ohne Zurücklegen

Fragestellung:
Gegeben: Menge B ("Urne") mit n unterscheidbaren Gegenständen $(g_1, ..., g_n)$
Wir wählen nacheinander k Elemente aus und legen sie der Reihenfolge nach aus.
$(g_{i_1}, ..., g_{i_k})$, wobei $i_j \neq i_l \; \forall i, j, l$ ($\Rightarrow$ ohne Zurücklegen)
Frage: Wieviele Auswahlen von k-Tupeln sind möglich?
Andere Interpretation:
Verteilung von k verschiedenen Gegenständen aus B auf Plätze 1,...,k (kein Platz frei)
Kann beschrieben werden als injektive Abbildung
$\begin{pmatrix} 1 & 2 & ... & k \\ g_{i_1} & g_{i_2} & \cdots & g_{i_k} \end{pmatrix}, \{1, ..., k\} \to B$

### 7.3.1 Definition $(n)_k$

Setze für $n, k \in \mathbb{N} : (n)_k := n \cdot (n-1) \cdot ... \cdot (n-k+1)$
Beachte: $(n)_1 = n, (n)_k = 0 \; \forall k > n$
Auch: $(n)_k := n \cdot (n-1) \cdot ... \cdot (n-k+1) \cdot \frac{(n-k)\cdot(n-k-1)\cdot...\cdot 1}{(n-k)\cdot(n-k-1)\cdot...\cdot 1} = \frac{n!}{(n-k)!}$
Insbesondere: $(n)_n = \frac{n!}{(n-n)!} = n!$

### 7.3.2 Satz

Es gibt genau $n(n)_k$ viele Auswahlen vom k Objekten aus einer Menge B von n (unterschiedlichen) Objekten, wenn keine Wiederholungen möglich sind und die Anordnung berücksichtigt wird.

**Beweis**

Sei $n \in \mathbb{N}$ beliebig aber fest gewählt.
Induktion nach k

**IA** $k = 1$ : n Möglichkeiten, $(n)_k = n$ ✓

**IS IV:** $(n)_k$ ist Anzahl der Möglichkeiten für beliebiges aber festes $k \geq 1$

**IBeh:** $(n)_{k+1}$ ist richtig.

**IBew:** Ist $k + 1 > n$, so Anz. $= 0$
$(n)_{k+1} = 0$ ✓

Sei also $k + 1 \leq n$
Sind die Plätze 1,...,k schon belegt(IV), bleoben für Platz (k+1) noch (n-k) Möglichkeiten.
Also $(n)_k$ viele Verteilungen von k versch. Elementen aus B auf die Plätze 1,...,k; also:
$(n)_k \cdot (n - k)$
$= (n - 1) \cdot (n - 2) \cdot ... \cdot (n - k + 1) \cdot (n - k)$
$= (n)_{k+1}$

□

**Beispiel**

Wieviele Möglichkeiten gibt es für Rank 1,2 und 3 am Ende einer Bundesligasaison mit 18 Vereinen?
$n = 18,\ k = 3 : (18)_3 = 18 \cdot 17 \cdot 16 = 4896$

### 7.3.3 Korollar

Seinen $A, B \neq \emptyset,\ |A| = k,\ |B| = n$
Dann gibt es genau $(n)_k$ injektive Abbildungen $A \to B$

**Beweis**

Folgt aus $\underbrace{7.3.1}_{Formulierung}$ und $\underbrace{7.3.3}_{Anzahl}$

□

### 7.3.4 Def.: Permutationen

Eine bijektive Abb. einer Menge A auf sich selbst heißt Permutation von A.
Ist A endlich, so gibt es $|A|!$ Permutationen auf A.
Sei $A = \{1, 2, ..., n\}$, Menge der Permutationen auf A heißt dann $S_n$
$|S_n| = n!$ $(n = 1 : 1, n = 2 : 2, n = 3 : 6, n = 4 : 24, ...)$
Schreibweise für $\pi \in S_n \begin{pmatrix} 1 & 2 & ... & n \\ \pi(1) & \pi(2) & ... & \pi(n) \end{pmatrix}$
oder $(\pi(1), \pi(2), ..., \pi(n))$

## 7.4 Geordnete Auswahl mit Zurücklegen

Fragestellung:
Menge b mit n verschiedenen Gegenständen. Wähle nacheinander k Gegenstände davon aus, wobei nach jeder Auswahl der Gegenstand zurückgelegt wird und die Reihenfolge der ausgewählten Gegenstände notiert wird.
Jede solche Auswahl kann man beschreiben durch $\begin{pmatrix} 1 & 2 & ... & n \\ b_1 & b_2 & ... & b_n \end{pmatrix}$
$b \in B$ nicht notwendig verschieden
Die Anzahl solcher Auswahlen entspricht genau der Anzahl aller Abb. $\{1, ..., k\} \to B$
Andere Interpretation:
Gegenstände 1,...,k (paarweise verschieden), Farben n:
Färbe die gegenstände ein (Farben dürfen mehrfach verwendet werden)

### 7.4.1 Satz

Es gibt genau $n^k$ geordnete Auswahlen mit zurücklegen von k Elementen aus B mit n Elementen.

#### Beweis

Menge der Auswahlen ist
$B \times B \times ... \times B$, k-mal
Nach 7.1.1: $n \cdot n \cdot ... \cdot n = n^k$

□

#### Korollar

Es gibt ganau $n^k$ Abb. $A \to B$, wenn $|A| = k,\ |B| = n$

## 7.5 Ungeordnete Auswahl ohne Zurücklegen

Fragestellung:
Urne mit n Kugeln (alle verschieden) wähle k aus und lege alle in einen Korb.
Wieviele verschiedene Möglichkeiten gibt es?

Die Anzahl entspricht der Anzahl der k-elementigen Teilemengen einer n-elementigen Menge.

### 7.5.1 Def: Binomialkoeffizient

$n, k \in \mathbb{N}_0$
$\binom{n}{k} := \begin{cases} 0 & \text{, falls } k > n \\ \frac{n!}{k!(n-k)!} & \text{, falls } 0 \leq k \leq n \end{cases}$
heißt Binomialkoeffizient ("n über k" / " n choose k")
Also: $\binom{n}{k} = \frac{(n)_k}{k!}$

Spezialfall: $\binom{n}{0} = 1 = \binom{n}{n}$, $\binom{n}{1} = n = \binom{n}{n-1}$

#### Bemerkung

(a) $\binom{n}{k} = \binom{n}{n-k}$
(b) $\binom{n}{k} + \binom{n}{n-k} = \binom{n+1}{k}$

#### Pascalsches Dreieck

folgt aus Bemerkung

```
                    1
                1       1
            1       2       1
        1       3       3       1
    1       4       6       4       1
1       5       10      10      5       1
1   6       15      20      15      6       1
```

Ebenen: n=0,1,2...
Diagonalen: k=0,1,2,...

gibt die Werte von $\binom{n}{k}$ an (nach Def. und Bem.)
z.B. $\binom{4}{2} = \binom{3}{2} + \binom{3}{1} = 6$

### 7.5.2 Satz

Anzahl der ungeordneten Auswahlen ohne Zurücklegen von k Elementen aus einer Menge von n Elementen ist $\binom{n}{k}$
Dies ist genau die Anzahl der k-elementigen Teilmengen einer n-elementigen Menge.

**Beweis**

Satz richtig für $k > n$ und $k = 0$.
Sei also $1 \leq k \leq n$.
Anzahl geordneter Auswahlen ohne Zurücklegen: $(n)_k$ (7.3.3)
Je $k!$ dieser geordneten Auswahlen führen zur selben ungeordneten Auswahl.
Also gesuchter Wert: $\frac{(n)_k}{k!} = \binom{n}{k}$

□

**Korollar**

Sei $M = \{0,1\}^n$. Anzahl der 0,1-Folgen der Länge n mit genau k Einsen ist $\binom{n}{k}$

### 7.5.3 Binomialsatz

Seien $a, b \in \mathbb{R},\ n \in \mathbb{N}_0$
$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k} \cdot b^k$

**Beweis**

Induktion nach n mit 7.5.1 Bem. (b)
Alternativ: anschaulich:
$\underbrace{(a+b) \cdot (a+b) \cdot ... \cdot (a+b)}_{n-mal}$
Wie oft tritt $(a^{n-k} \cdot b^k)$ auf?
Aus k Klammern wird b ausgewhlt, aus den übrigen a: $\binom{n}{k}$ Möglichkeiten

### 7.5.4 Korollar

Sei M eine endliche Menge, $|M| = n$
Es gilt $|\mathcal{P}(M)| = 2^n$

**Beweis**

Entweder durch Induktion oder:
$2^n = (1+1)^n \overset{7.5.3}{=} \sum_{k=0}^{n} \binom{n}{k}$
Behauptung folgt nun aus 7.5.2

□

## 7.6 Ungeordnete Auswahl mit Zurücklegen

Fragestellung:
Auswahl k aus n mit Wiederholung ohne Berücksichtigung der Reihenfolge
Interpretiert als Färbungsproblem:
n Farben, k gleiche Kugeln
Wieviele Möglichkeiten gibt es diese k Kugeln mit jeweils einer der n Farben zu färben?

### 7.6.1 Satz

Sei $|B| = n, k \in \mathbb{N}_0$

(1) Anzahl aller möglchkeiten k Elemente aus B zu ziehen (ohne Reihenfolge mit Zurücklegen)

(2) Die Anzahl der geordneten n-Tupel $(x_1, ..., x_n),\ x_i \in \mathbb{N}_0$ mit $x_1 + ... + x_n = k$

(3) Die Anzahl der 0,1-Folgen der Länge n+k-1, die genau k Einsen haben.

Die gemeinsame Zahl ist $\binom{n+k-1}{k}$ ($k > n$ möglich)

#### Beweis

**I** (1)=(2)
$B = \{b_1, ..., b_2\}$ Jeder Auswahl von k elementen aus B ordnen wir das n-tupel $(x_1, ..., x_n) \in \mathbb{N}_0^n$ zu, wobei $x_i$ = Anzahl, wie oft $b_i$ ausgewählt wurde
$\Rightarrow \sum_{i=1}^{n} x_i = k$

**II** (2)=(3)
$(x_1, ..., x_n) \to (\underbrace{1, ..., 1}_{x_1\ Stellen}, 0, \underbrace{1, ..., 1}_{x_2\ Stellen}, 0, ..., 0, \underbrace{1, ..., 1}_{x_n\ Stellen})$
Es gibt hier genau k Einsen und n-1 Nullen (welche die Einträge der $x_i$ trennen)
Bsp: $(0, 0, 3, 1, 0, 1, 0) \to (0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0)$

**III** Anzahl (3)
$= \binom{n+k-1}{k}$ nach 7.5.2

□

### 7.6.2 Beispiel

Wieviele Möglichkeiten gibt es 8 gleiche Kugeln mit jeweils einer von 3 Farben zu färben

| rot | grün | blau |
|---|---|---|
| 8 | 0 | 0 |
| 7 | 1 | 0 |
| 7 | 0 | 1 |
| ... | ... | ... |
| 0 | 0 | 8 |

$$\binom{n+k-1}{k} = \binom{10}{8} = \binom{10}{2} = 45$$

# 8 Die reellen Zahlen

Zunächst algebraische Eigenschaften von Add. und Multiplikation

## 8.1 Algebraische Eigenschaften von $\mathbb{R}$

### Addition

(1) $\forall a, b \in \mathbb{R} : a + b \in \mathbb{R}$ (Algebraische Abgeschlossenheit bzgl. Add.)

(2) $\forall a, b, c \in \mathbb{R} : (a + b) + c = a + (b + c)$ (Assoziativität)

(3) $\forall a \in \mathbb{R} \exists 0 \in \mathbb{R} : 0 + a = a + 0 = a$ (0 ist neutrales Element bzgl Add.)

(4) $\forall a \in \mathbb{R} \exists ! - a \in \mathbb{R} : a + (-a) = (-a) + a = 0$ (es existiert ein inverses Element bzgl. Add)

(5) $\forall a, b \in \mathbb{R} : a + b = b + a$ (Kommutativität)

### Multiplikation

(6) $\forall a, b \in \mathbb{R} : a \cdot b \in \mathbb{R}$ (Algebraische Abgeschlossenheit bzgl. Mult.)

(7) $\forall a, b, c \in \mathbb{R} : (a \cdot b) \cdot c = a \cdot (b \cdot c)$ (Assoziativität)

(8) $\forall a \in \mathbb{R} \exists 1 \in \mathbb{R} : 1 \cdot a = a \cdot 1 = a$ (1 ist neutrales Element bzgl Mult.)

(9) $\forall a \in \mathbb{R} \exists ! a^{-1} \in \mathbb{R} : a \cdot a^{-1}) = a^{-1} \cdot a = 1$ (es existiert ein inverses Element bzgl. Add)

(10) $\forall a, b \in \mathbb{R} : a \cdot b = b \cdot a$ (Kommutativität)

### Zusammenhang zwischen Add. und Mult.

(11) $\forall a, b, c \in \mathbb{R} : (a + b) \cdot c = ac + bc \wedge a \cdot (b + c) = ab + ac$ (Distributivität)

Beachte: "$\cdot$ bindet stärker als $+$"

### 8.1.1 Bemerkungen

(a) (1) Statt $a + (-b)$ schreibt man $a - b$ (Subtraktion)

(2) Statt $a \cdot b^{-1}$ schreibt man $\frac{a}{b}$ oder $a : b$ oder $a \div b$ (Division)

(3) $-(-a) = a$ und $(a^{-1})^{-1} = a$

(4) $-0 = 0$ und $1^{-1} = 1$

(b) Eigenschaften 1-5 auch von $\mathbb{Z}$ erfüllt und auch von $\mathbb{Q}$ (mit der üblichen Addition)
Es gibt auch andere Mengen, mit anderer Addition, die 1-5 erfüllen:
$\mathbb{Z}_2 = \{0, 1\}$ mit Verknüpfung $\oplus$ definiert $a \oplus b = (a + b) \mod 2$ $(\equiv XOR)$

(c) Eigenschaften (6)-(10)auch von $\mathbb{Q}$ erfüllt, aber nicht von $\mathbb{Z}$ (da (9) nicht erfüllt)
(6)-(10) besagen insbesondere, dass $\mathbb{R}\backslash\{0\}$ eine "kommutative Gruppe" bezüglich der Multiplikation ist.

(d) Es gibt weitere Mengen mit anderen Def. von + und $\cdot$, die die Eigenschaften (1)-(11) haben
Name: Körper (engl. field)
z.B. $\mathbb{Z}_2 = \{0, 1\}, \oplus, \cdot$ ist ein Körper

| $a$ | $b$ | $1 \oplus b$ | $a \cdot b$ |
|---|---|---|---|
| 0 | 0 | 0 | 0 |
| 0 | 1 | 1 | 0 |
| 1 | 0 | 1 | 0 |
| 1 | 1 | 0 | 1 |

Zu zeigen: Es gilt (1)-(11) für $(\mathbb{Z}_2, \oplus, \cdot)$

(1) Add. ist abgeschlossen

(2) assoziativität von $\oplus$ Beweis durch Tabelle

(3) neutrales Element: $0 \oplus 0 = 0, 1 \oplus 0 = 1, 0 \oplus 1 = 1$
$\Rightarrow$ 0 neutrales Element

(4) Inverses Element: $0 \oplus 0 = 0$ also $-0 = 0$, $1 \oplus 1 = 0$, also $-1 = 1$

(5) Kommutativität: $0 \oplus 1 = 1 \oplus 0 = 1$

(6) Multiplikation abgeschlossen

(7) Assoziativität von $\cdot$, Bew. durch Tabelle

(8) neutrales Element: $0 \cdot 1 = 0, 1 \cdot 1 = 1$, 1 ist neutrales Element

(9) inverses Element: $1 \cdot 1 = 1$, also $1^{-1} = 1$

(10) Kommutativität: $0 \cdot 1 = 1 \cdot 0 = 0$

(11) Distributivität: $(a \oplus b) \cdot c = (a \cdot c) \oplus (a \cdot b)$

Also $\mathbb{R}$ und $\mathbb{Q}$ sind Körper mit üblicher Add. und Mult.
$\mathbb{Z}_2$ ist Körper mit $\oplus$ und $\cdot$.

(e) ($e_1$) $\forall a \in \mathbb{R} : a \cdot 0 = 0$

Es gilt:

$a \cdot 0 \overset{(3)}{=} a \cdot (0+0) \overset{(11)}{=} a \cdot 0 + a \cdot 0$

Außerdem:

$0 \overset{(4)}{=} a \cdot 0 + (-(a \cdot 0)) \overset{s.o.}{=} (a \cdot 0 + a \cdot 0) + (-(a \cdot 0)) \overset{(2)}{=} a \cdot 0 + (a \cdot 0 + (-a \cdot 0))$

$\overset{(4)}{=} a \cdot 0 + 0 \overset{(3)}{=} a \cdot 0$ □

($e_2$) $\forall a, b \in \mathbb{R} : a \cdot b = 0 \Rightarrow a = 0 \vee b = 0$

Angenommen $b \neq 0$, dann zu zeigen $a = 0$:

$0 \overset{Vor.}{=} a \cdot b \overset{e_1}{=} (a \cdot b) \cdot \underbrace{b^{-1}}_{\text{ex., da lt. Vor. } b \neq 0} \overset{(7)}{=} a \cdot (b \cdot b^{-1}) \overset{(9)}{=} a \cdot 1 \overset{(8)}{=} a$

□

($e_3$) $-(ab) = (-a) \cdot b = a \cdot (-b)$

Beweis:

1. Gleichung:

$(a \cdot b) + (-a \cdot b) \overset{(11)}{=} (a + (-a)) \cdot b \overset{(4)}{=} 0 \cdot b \overset{(e_1)}{=} 0$

2. Gleichung:

analog nach (5) □

($e_4$) $(-a) \cdot (-b) = a \cdot b$

$(-a) \cdot (-b) \overset{(e_3)}{=} -(a \cdot (-b) \overset{(e_3)}{=} -(-(a \cdot b)) \overset{8.1.1(a)(3)}{=} a \cdot b$ □

(f) In $\mathbb{N}$ gelten (1),(2),(5)-(8),(10),(11)
In $\mathbb{N}_0$ zusätzlich (3)
In $\mathbb{Z}$ zusätzlich (4)
In $\mathbb{Q}$ zusätzlich (9)

## 8.2 Grundregeln der Ordnungsrelation $\leq$ auf $\mathbb{R}$

(1) $\mathbb{R}$ ist durch $\leq$ total geordnet

(2) $\forall x, y, a \in \mathbb{R} : x \leq y \Rightarrow a + x \leq a + y$ (Transformationsinvarianz)

(3) $\forall x, y, a \in \mathbb{R}, a \geq 0 : x \leq y \Rightarrow a \cdot x \leq a \cdot y$ (Dehnungsinvarianz)

(4) $\forall x, y \in \mathbb{R}, 0 < x < y \exists n \in \mathbb{N} : n \cdot x > y$ (Archimedisches Axiom)

Beachte: Grundregeln gelten auch für $\mathbb{N}, \mathbb{Z}$ und $\mathbb{Q}$
Aus diesen Grundregeln folgt:

(2') Ist $x < y$, so gilt $a + x < a + y$

(3') Ist $x < y, a > 0$, so gilt $ax < ay$

**Beweis**

Sei $x < y$.
Nach (2) gilt: $x \leq y \Rightarrow a + x < a + y \vee a + x = a + y$
Im ersten Fall folgt die Behauptung.
Im zweiten Fall:
$a + x = a + y$
$\Leftrightarrow x = y$, also zweiter Fall tritt nicht auf, da Voraussetzung $x < y$

(3') ähnlich

### 8.2.1 Satz

Seien $x, y, a \in \mathbb{R}$

(a) $x \leq y \Leftrightarrow y - x \geq 0 \Leftrightarrow -y \leq -x$

(b) $x \leq y, a \leq 0 \Rightarrow ax \geq ay$

(c) $x, y \geq 0 \Rightarrow x + y \geq 0 \wedge x \cdot y \geq 0$
$x \geq 0, y \leq o \Rightarrow x \cdot y \leq 0$
$x, y \leq 0 \Rightarrow x + y \leq 0 \wedge x \cdot y \geq 0$
Insbesondere: $\forall x \in \mathbb{R} : x^2 \geq 0$
Alle Aussagen in (c) bleiben richtig, wenn
$\leq$ durch $<$ und
$\geq$ durch $>$ ersetzt werden.

(d) $0 < x < y \Rightarrow 0 < \frac{1}{y} < \frac{1}{x}$ (Beachte: $\frac{1}{y} = y^{-1}, \frac{1}{x} = x^{-1}$)

(e) $\forall x > 0 \exists n \in \mathbb{N} : \frac{1}{n} < x$ (Beachte: $\frac{1}{n} = n^{-1}$)

(f) $\forall x, y \geq 0, n \in \mathbb{N} : x^n < y^n \Rightarrow x < y$

**Beweis (exemplarisch)**

Zu (a): durch Ringschluss

$1 \Rightarrow 2$: $x \leq y \overset{8.2(2)}{\Rightarrow} 0 = x + (-x) \leq y + (-x) = y - x$

$2 \Rightarrow 3$: $y - x \geq 0 \Rightarrow -x = -y + (y - x) \geq (-y) = -y$

$3 \Rightarrow 1$: $-y \leq -x \overset{Beh.\,1}{\Rightarrow} -x - (-y) \geq 0 \overset{Beh.\,2}{\Rightarrow} -(-x) \leq -(-y) \Rightarrow x \leq y$

□

## 8.3 Def.: Intervall

$a, b \in \mathbb{R}, a \leq b$

#### abgeschlossenes Intervall

$[a, b] := \{x \in \mathbb{R} | x \geq a \wedge x \leq b\}$
mit Endpunkten a und b

#### offenes Intervall

$]a, b[ := \{x \in \mathbb{R} | x > a \wedge x < b\}$
ohne Endpunkte a und b

#### halboffenes Intervall

$]a, b] := \{x \in \mathbb{R} | x > a \wedge x \leq b\}$
oder
$[a, b[ := \{x \in \mathbb{R} | x \geq a \wedge x < b\}$

#### unendliche Intervalle

$]-\infty, a] := \{x \in \mathbb{R} | x \leq a\}$
$]-\infty, a[ := \{x \in \mathbb{R} | x < a\}$
$[a, \infty[ := \{x \in \mathbb{R} | x \geq a\}$
$]a, \infty[ := \{x \in \mathbb{R} | x > a\}$
$]-\infty, \infty[ := \mathbb{R}$

### 8.3.1 Beispiele

(a) Bestimme die Menge aller $x \in \mathbb{R}$ mit

$$\begin{aligned} & 2x + 4 \leq -3x + 5 \\ \overset{8.2(2)}{\Leftrightarrow} \; & 2x \leq -3x + 1 \\ \overset{8.2(2)}{\Leftrightarrow} \; & 5x \leq 1 \\ \overset{8.2(3)}{\Leftrightarrow} \; & x \leq \tfrac{1}{5} \end{aligned}$$

$\Rightarrow \mathbb{L} = ]-\infty, \frac{1}{5}]$

(b) Bestimme alle $x \in \mathbb{R}$ mit
$\frac{1}{x-2} \leq \frac{2}{x+3}$

**1. Fall** $x + 3 < 0 \Leftrightarrow x < -3$
Dann: $x - 2 < -5 < 0$
$x + 3 \leq 2(x - 2) \Leftrightarrow 7 \leq x$
$\Rightarrow$ Widerspruch zum Fall $(x < -3) \Rightarrow$ keine Lösung

**2.Fall** $x+3>0 \Leftrightarrow x>-3 \wedge x-2<0 \Leftrightarrow x<2 \Rightarrow -3<x<2$

$\frac{1}{x-2} \leq \frac{2}{x+3}$

$\Leftrightarrow \frac{x+3}{x-2} \leq 2$

$\Leftrightarrow x+3 \geq 2(x-2)$

$\Leftrightarrow 7 \geq x$

$\Rightarrow \mathbb{L} = ]-3,2[$

**3.Fall** $x+3>0 \wedge x-2>0 \Rightarrow x>2$

$\frac{1}{x-2} \leq \frac{2}{x+3}$

$\Leftrightarrow x+3 \leq 2(x-2)$

$\Leftrightarrow 7 \leq x$

$\Rightarrow \mathbb{L} = [7,\infty[$

$\Rightarrow \mathbb{L} = ]-3,2[ \cup [7,\infty[$

(c) Bestimme $x \in \mathbb{R}$ mit
$-3x+2<1 \wedge \frac{1}{x}+2 \geq 3$

**1. GI.** $-3x+2<1$

$\Leftrightarrow -3x<-1$

$\Leftrightarrow x>\frac{1}{3}$

**2. GI.** $\frac{1}{x}+2 \geq 3$ für $x>\frac{1}{3}$

$\Leftrightarrow \frac{1}{x} \geq 1$

$\Leftrightarrow 1 \geq x$

$\Rightarrow \mathbb{L} = ]\frac{1}{3},1]$

## 8.4 Satz

Sei $0<q<1$
Dann $\forall x \in \mathbb{R}^+ \exists n \in \mathbb{N} : 0<q^n<x$

### 8.4.1 Beweis

Schreibe $1=q+s,\ s>0$
Es ist $s \cdot x > 0$
Nach 8.2.1 (e) : $\exists n \in \mathbb{N} : \frac{1}{n+1} < x \cdot s$
Also $\frac{1}{(n+1)\cdot s} < x$.
Es gilt:
$1 = 1^{n+1}$
$= (q+s)^{n+1}$
$\overset{7.5.3}{=} q^{n+1} + (n+1) \cdot q^n s + ... + s^{n+1}$
$> (n+1)q^n s$ (alle anderen Summanden weggelassen)
also: $q^n < \frac{1}{(n+1)s} < x$ □

## 8.5 Def.: Absolutbetrag

$a \in \mathbb{R},\ |a| = \max\{a, -a\} = \begin{cases} a & \text{, falls } a \geq 0 \\ -a & \text{, falls } a < 0 \end{cases}$

$|a|$ misst Abstand von a zu 0

Allgemeiner: $|a - b| = d(a, b)$, Abstand von a und b

### 8.5.1 Satz: Eigenschaften des Absolutbetrages

(a) $-|a| \leq a \leq |a|,\ |a| = |-a|,\ |a|^2 = a^2$

(b) $|a| = 0 \Leftrightarrow a = 0$

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

(d) $|a + b| \leq |a| + |b|$ (Dreiecksungleichung)

(e) $||a| - |b|| \leq |a - b| \leq |a| + |b|$

#### Beweis

(a)-(c) klar.

(d) $\begin{aligned} |a+b|^2 &\overset{(a)}{=} (a+b)^2 \\ &= a^2 + 2ab + b^2 \\ &\leq a^2 + b^2 + 2 \cdot |a| \cdot |b| \\ &= |a|^2 + |b|^2 + 2 \cdot |a| \cdot |b| \\ &= (|a| + |b|)^2 \\ &\Rightarrow |a+b|^2 \leq (|a| + |b|)^2 \\ &\overset{8.2.1(f)}{\Rightarrow} |a+b| \leq |a| + |b| \end{aligned}$

(e) $|a - b| \overset{(d)}{\leq} |a| + |-b| = |a| + |b|$ ✓(2. Ungleichung)

Noch zu zeigen: 1. Ungleichung

(I) $\begin{aligned} |a| = |a - b + b| &\overset{(d)}{\leq} |a - b| + |b| \\ &\Rightarrow |a| - |b| \leq |a - b| \end{aligned}$

(II) $\begin{aligned} |b| = |b - a + a| &\overset{(d)}{\leq} |b - a| + |a| \\ &\Rightarrow |b| - |a| \leq |b - a| \\ &\Rightarrow -(|a| - |b|) \leq |a - b| \\ &||a| - |b|| = \max\{-(|a| - |b|), |a| - |b| \\ &\Rightarrow ||a| - |b|| \leq |a - b| \text{ nach Def. von Betrag} \end{aligned}$

□

**Beispiel**

Bestimme alle $x \in \mathbb{R}$ mit
$\frac{1}{|x-2|} \geq 5$

**1. Fall** $x - 2 > 0 \Leftrightarrow x > 2$
Dann: $\frac{1}{x-2} \geq 5$
$1 \geq 5(x-2)$
$11 \geq 5x$
$\frac{11}{5} \geq x$
$\Rightarrow x \in ]2, \frac{11}{5}]$

**2.Fall** $x - 2 < 0 \Leftrightarrow x < 2$
Dann: $\frac{1}{-(x-2)} \geq 5$
$1 \geq -5(x-2)$
$-9 \geq -5x$
$\frac{9}{5} \leq x$
$\Rightarrow x \in [\frac{9}{5}, 2[$

$\Rightarrow \mathbb{L} = [\frac{9}{5}, 2[\cup]2, \frac{11}{5}] = [\frac{9}{5}, \frac{11}{5}]\backslash\{2\}$

## 8.6 Satz

Es ist $\mathbb{Q} \subset \mathbb{R}$ (also $\mathbb{Q} \subseteq \mathbb{R} \wedge \mathbb{Q} \neq \mathbb{R}$).
Ist p eine Primzahl, so $\sqrt{p} \notin \mathbb{Q}$

### 8.6.1 Beweis

Angenommen $\sqrt{p} \in \mathbb{Q}$, dann lässt sich $\sqrt{p}$ als grkürzter Bruch schreiben:
$\sqrt{p} = \frac{m}{n},\ m, n \in \mathbb{N},\ ggT(m,n) = 1$
Dann:$5p = \frac{m^2}{n^2}$
$\Rightarrow pn^2 = m^2$
$\Rightarrow p|m^2$
$\overset{6.8.2}{\Rightarrow} p|m$
$\Rightarrow p^2|m^2$
$m^2 = p \cdot n^2$
$\Rightarrow p|n^2$ (da $m \in \mathbb{N}$)
$\overset{6.8.2}{\Rightarrow} p|n$
also p ist Teiler von m und n, somit wäre nicht 1 1 der ggT $\lightning$
$\Rightarrow \sqrt{p} \notin \mathbb{Q}$
$\Rightarrow \sqrt{p}$ lässt sich nicht als abbrechende oder ab einer gewissen Stelle periodische Dezimalzahl schreiben. $\square$

## 8.7 Def.: Irrationale Zahlen

Zahlen, die nicht rational sind heißen irrational.
Man kann $\sqrt{2}$ (wie jede irrationale zahl) durch ein Approximationsverfahren darstellen (bei endlich vielen Schritten bis auf einen beliebigen vorgegebenen Fehler)

Idee:
Setze $a := 0$ und $b := 2$. Intervallgrenzen um $\sqrt{2}$ also $a \leq \sqrt{2} \leq b$

$while(b - a \geq 2^{-100})\ do$
  $c := \frac{a+b}{2}$
  $if(c^2 < 2)\ then$
    $a := c$
  $else\ b := c$
  $endif$
$endwhile$
$Ausgabe:\ a$

Statt $2^{-100}$ kann jede beliebige Fehlergerenze $> 0$ eingesetzt werden, damit berechnet das Verfahren $\sqrt{2}$ beliebig genau.
$while(true)\ do\ \rightarrow$ unendliche Schleife
Dann "bestimmt" dieses Verfahren eine eindeutige Zahl für $\sqrt{2}$

### 8.7.1 Allgemeines Prinzip

Sei $B(x, y)$ eine Funktion abhängig von x und y den Wert 1 oder 0 annimmt (wahr oder falsch) "Boolsches Prädikat" (Bedingung).

### 8.7.2 Def.: Bisektionsverfahren

Seinen $a_0, b_0 \in \mathbb{R},\ a_0 < b_0$ und $B(\cdot, \cdot)$ Boolsches Prädikat.
Dann heißt der unendliche Algorithmus Bisektionsverfahren oder Intervallhalbierungsverfahren

$a := a_0,\ b := b_0$
$while(true)\ do$
  $c := \frac{a+b}{2}$
  $if(B(a, b) = 1)\ then$
    $a := c$
  $else\ b := c$
  $endif$
$endwhile$

Seien $a_n$ und $b_n$ die Werte von a und b im n-ten Durchlauf.

Klar: $a_0 \leq a_1 \leq a_2 \leq ... \leq a_n \leq b_n \leq b_{n-1} \leq ... \leq b_1 \leq b_0 \; \forall n \in \mathbb{N}$

Bisektionsverfahren nähert sich immer genau einer zahl an. Dass man nicht auf eine Lücke stößt, besagt das Vollständigkeitsaxiom.

## 8.8 Vollständigkeitsaxiom

Durch jedes Bisektionsverfahren wird eindeutig eine reelle zahl x dargestellt oder bestimmt. Dabei gilt:

$$\forall n \in \mathbb{N}_0 \exists x \in \mathbb{R} : a_n \leq x \leq b_n \wedge 0 < b_n - a_n = \frac{b_0 - a_0}{2^n}$$

$\mathbb{R}$ ist ein archimedisch total geordneter Körper (8.1 und 8.2) in dem das Vollständigkeitsaxiom gilt.
Hierdurch ist $\mathbb{R}$ eindeutig bestimmt (z.B. $\mathbb{Q}$ ist nicht vollständig)

## 8.9 Bemerkung zum Boolschen Prädikat

Das (unendliche) Bisektionsverfahren mit

$$B(a,b) = \begin{cases} 1 & \text{, falls } \left(\frac{a+b}{2}\right)^2 < 2 \\ 0 & \text{, sonst} \end{cases} \qquad \text{liefert } \sqrt{2}$$

### 8.9.1 Beweis

Sei x die so definierte Zahl. Es gilt $a_n \leq x \leq b_n \; \forall n$
Nach Def. von B gilt: $a_n^2 \leq 2 \leq b_n^2$
Zu zeigen: $x = \sqrt{2}$
angenommen: $x \neq \sqrt{2}$, d.h. $|x - \sqrt{2}| > 0$
Nach 8.4 (mit $q = \frac{1}{2}$) existiert $n \in \mathbb{N}$ mit:
$\left(\frac{1}{2}\right)^n < |x - \sqrt{2}|$
Mit $\left(\frac{1}{2}\right)^n = \frac{1}{2^n} = \frac{2}{2^{n+1}} = \frac{b_0 - a_0}{2^{n+1}} = b_{n+1} - a_{n+1}$
folgt $b_{n+1} - a_{n+1} < |x - \sqrt{2}|$, d.h. es muss
$x \notin [a_{n+1}, b_{n+1}]$ oder
$\sqrt{2} \notin [a_{n+1}, b_{n+1}]$ gelten
Widerspruch zur Def.
$\Rightarrow x = \sqrt{2}$ $\square$

## 8.10 Binärdarstellung von $x \in ]0,1[$

Mit dem Bisektionsverfahren lässt sich die Binärdarstellung einer reellen Zahl $x \in \mathbb{R}$ berechnen.
Zunächst sei $x \in ]0,1[$
Dann: $x = 0, x_1, x_2, x_3, ...,$ mit $x_i \in \{0,1\}$
Behauptung:

$$x = x_1 \cdot \frac{1}{2} + x_2 \cdot \frac{1}{2^2} + x_3 \cdot \frac{1}{2^3} + ...$$

$(x_1, x_2, ...)$ ist "die" Binärentwicklung von x.
Diese Darstellung ist nicht immer eindeutig.

Beginne bisektionsverfahren mit $a = 0, b = 1$ und teste in jedem Schritt, ob $\frac{a+b}{2} < x$, also

$$B(a,b) = \begin{cases} 1 & \text{, falls } \frac{a+b}{2} < x \\ 0 & \text{, falls } \frac{a+b}{2} \geq x \end{cases}$$

Wir erhalten:
$a_0 \leq a_1 \leq ... \leq a_n \leq x \leq b_n \leq b_{n-1} \leq ... \leq b_0$ und $b_n - a_n \leq \frac{1}{2^n}$
Es ist:
$a_n = x_1 \cdot \frac{1}{2} + x_2 \cdot \frac{1}{2^2} + ... + x_n \cdot \frac{1}{2^n}$ mit $x_i \in \{0,1\}$
Dabei: $x_i = 1 \Leftrightarrow a_i > a_{i-1}$ also Wert von $B(a_{i-1}, b_{i-1})$ im i-ten Durchlauf.
Es ist:
$x - a_n \leq b_n - a_n = \frac{1}{2^n}$
Also $a_n$ nähert sich beliebig nahe an x an (für n steigend)
also $x_i$ liefern Binärdarstellung z.B. $n = 5$, so erhält man die ersten 5 Ziffern.

### 8.10.1 Algorithmus

$a := 0,\ b := 2$
$for\ i = 1\ to\ n\ step\ 1\ \ do$
  $c := \frac{a+b}{2}$
  $if(c < x)\ then$
    $a := c,\ x_i := 1$
  $else\ b := c\ x_i = 0$
  $endif$
$endfor$
Ausgabe: $0, x_1, x_2, ...x_n$

### 8.10.2 Bemerkung

Für $x \in \mathbb{R}$ beliebig erhält man die $x \geq 1$
Binärdarstellung s.o.
$y_m, y_{m-1}, ..., y_0, x_1, x_2, ..., x_n$, wobei $y_m, y_{m-1}, ..., y_0 = (y_m\ y_{m-1}\ ...\ y_0)_2$ die Binärdarstellung von $\lfloor x \rfloor$ (floor: größte Zahl $z \in \mathbb{Z}$ mit $z \leq x$)ist

und $0, x_1\ x_2$ ... die Binärdarstellung von $x - \lfloor x \rfloor$.
Für $x < 0$ schreibe Binärdarstllung von $|x|$ mit - versehen.

#### Beispiel

Binärdarstellung von $\sqrt{2}$.
1,...
mit Algorithmus 8.10.1 ist $\sqrt{2} - 1$ errechenbar:
$\sqrt{2} = 1 + 0,01101010000...$
$= 1 + \frac{1}{4} + \frac{1}{8} + \frac{1}{32} + \frac{1}{128} + ...$

## 8.11 Bemerkungen

### 8.11.1 Binärdarstellung nicht eindeutig

Die Binärdarstellung ist nicht immer eindeutig:
z.B. $\frac{1}{2}$ lässt sich darstellen als:
0,1000... oder als 0,0111...
Allgemein: $x = \frac{k}{2^n}\ \ k \in \mathbb{Z}$ hat keine eindeutige Binärdarstellung.

### 8.11.2 Periodizität

Binärdarstellung von x wird periodisch (ab einer gewissen Stelle), falls $a \cdot x \in \mathbb{Q}$. Sonst nicht!

## 8.12 Satz

(a) $\forall r \in \mathbb{R} \forall n \in \mathbb{N} \exists q \in \mathbb{Q} : |r - q| \leq \frac{1}{2^n}$

(b) Zwischen zwei reellen Zahlen $r_1 < r_2$ liegt immer eine rationale Zahl q : $r_1 < q < r_2$ (sogar unendlich viele)

(c) Zwischen zwei reellen Zahlen $r_1 < r_2$ liegt immer eine irrationale Zahl s : $r_1 < s < r_2$ (sogar unendlich viele)

### 8.12.1 Beweis

(a) Sei $r \in \mathbb{R}$. Schreibe $r = z + x$, mit $z \in \mathbb{Z}$ und $x \in [0, 1[$
Bilde von x die Binärdarstellung bis n wie in 8.10
$a_n = x_1 \frac{1}{2} + x_2 \frac{1}{2^2} + ... + x_n \frac{1}{2^n}$ und definiere dann:
$q := z + a_n$
Dann gibt $q \in \mathbb{Q}$ und $|q - r| = |z + a_n - (z + x)| = |a_n - x| \leq |a_n - b_n| = \frac{1}{2^n}$ ✓

(b) Nach 8.4: $\exists n \in \mathbb{N} : \frac{1}{2^n} < r_2 - r_1$ (mit $q = \frac{1}{2}$)
Nach (a) : $\exists q \in \mathbb{Q} : |r_1 - q| \leq \frac{1}{2^{n+1}}$
Ist $q > r_1$, so ist q die gesuchte Zahl
Ist $q \leq r_1$, so ist $q + \frac{1}{2^n}$ die gesuchte Zahl. □

## 8.13 Beschränkte Mengen

Für endliche Mengen $\{a_1, ..., a_n\}$ von reellen Zahlen existiert ihr Minimum und Maximum:
z.B. $A = \{-3, 5, 6, 2, 3\}$
$\min(A) = -3,\ \max(A) = 6$
Für unendliche Mengen ist das nicht unbedingt so:
z.B. Intervall $[0, 1[$ hat kein Maximum wegen 8.12.

### 8.13.1 Definition

Sei $\emptyset \neq M \subseteq \mathbb{R}$

#### Supremum

M heißt nach oben beschränkt, falls $\exists d \in \mathbb{R}$ mit $m < d\ \forall m \in M$.
d heißt obere Schranke von M. d heißt obere Grenze oder Supremum von M, $sup(M)$, wenn d ist obere Schranke und $d' \geq d$ für alle Schranken d' von M. Supremum ist die kleinste obere Schranke von M.

#### Infimum

M nach unten beschränkt, falls $\exists e \in \mathbb{R} : e \leq m\ \forall m \in M$.
e heißt untere Schranke von M. e heißt untere Grenze oder Infimum, $inf(M)$, falls e untere Schranke und $e \geq e'$ für alle unteren Schranken von M.

#### Beschränktheit

M beschränkt, falls nach oben und unten beschränkt.

#### Bemerkungen

- Ist $sup(M) \in M$, so $\max(M) := sup(M)$
- Ist $inf(M) \in M$, so $\min(M) := inf(M)$
- Ist $M = \{a_1, ..., a_n\}$ endlich, so $sup(M) = \max\limits_{i=1}^{n} a_i\ ,\ inf(M) = \min\limits_{i=1}^{n} a_i$

### 8.13.2 Beispiele

(a) $M = ]0,1[$ beschränkt
Jede Zahl $\geq 1$ ist obere Schranke
Jede Zahl $\leq 0$ ist untere Schranke
$inf(M) \notin M$, also min nicht definiert
$sup(M) \notin M$, also max nicht definiert

(b) $M = [0,1]$ beschränkt,
$0 = inf(M) \in M$, also min(M) existiert
$0 = sup(M) \in M$, also max(M) existiert

(c) $M = \{\frac{1}{n} | n \in \mathbb{N}\}$ beschränkt
$sup(M) = \max(M) = \frac{1}{1} = 1$
$inf(M) = 0 \notin M$ min(M) existiert nicht.

(d) $m = \{\frac{m+n}{m} | m,n \in \mathbb{N}\}$
$\frac{m+n}{m} = 1 + \frac{n}{m}$, M ist nicht nach oben beschränkt
Jedes Element von M ist $\geq 1$ und $1 = inf(M) \notin M$ also min(M) existiert nicht.

### 8.13.3 Satz

Für jede nach $\begin{cases}\text{oben}\\ \text{unten}\end{cases}$ beschränkte Menge existiert $\begin{cases}\text{Supremum}\\ \text{Infimum}\end{cases}$

#### Beweis

Sei M eine nach unten beschränkte Menge. e eine untere Schranke und y ein Element von M.
Bisektionsverfahren zur Bestimmung des Infimums.:

$a := e,\ b := y$
$while(true)\ do$
  $c := \frac{a+b}{2}$
  $if(M \cap ]-\infty, c[ = \emptyset)\ then$
    $a := c$
  $else\ b := c$
  $endif$
$endwhile$

Sei x die durch das Bisektionsverfahren bestimmte Zahl. Seinen $a_n, b_n$ Intervallgrenzen im n-ten Schritt.
$a_n \leq x \leq b_n, 0 < b_n - a_n = \frac{b_0 - a_0}{2^n}$ $(b_0 = y,\ a_0 = e)$ Nach Konstruktion gilt:
$M \cap ]-\infty, a_n[ = \emptyset\ \forall n \in \mathbb{N}$
$M \cap [a_n, b_n] \neq \emptyset\ \forall n \in \mathbb{N}$

Behauptung:
x ist untere Schranke von M
Angenommen, dass nicht, dann $\exists e \in M : z < x$.
Dann $z = x - (x - z) \leq x - (b_n - a_n) \leq b_n - b_n + a_n = a_n$
Widerspruch zur Konstruktion: z links von der linken Grenze
$\Rightarrow$ x ist untere Schranke

Behauptung: x ist die größte untere Schranke
Angenommen es existiert untere Schranke $e > x$
Wähle n mit $b_n - a_n < e - x$
Dann $e - x > b_n - x$, d.h. $e > b_n$
Aber $M \cap [a_n, b_n] \neq \emptyset$, also kann e keine untere Schranke sein.

□

Supremum analog.

**Beispiel**

$M = \{x \in \mathbb{R} | x \geq 0, x^2 \geq 2\}$
Dann ist Bisektionsverfahren aus 8.13.3 das, was wir zur Berechnung von $\sqrt{2}$ formuliert haben, $inf(M) = \sqrt{2}$
(Ersetze $M \cap ]-\infty, c[ = \emptyset$ durch $c^2 < 2$)

# 9 Folgen und Reihen

Bisektionsverfahren liefern Zahlenfolgen

$$a_0, a_1, a_2, ... \text{ und } b_0, b_1, b_2, ...$$

die sich dem gleichen Wert "annähern". Das werden wir allgemein untersuchen.

## 9.1 Def.: Folge

$k \in \mathbb{Z}$ (oft $k = 0$ oder $k = 1$)
$A_k := \{n \in \mathbb{Z} | n \geq k\}$ "Indesxmenge"
Eine Abb. $a : A_k \to \mathbb{R},\ n \mapsto a_n$ heißt bei k beginnende Folge reeller Zahlen.
Schreibweise: $(a_n)_{n \geq k},\ (a_n)$
$a_n$ heißt "Folgenglied", $n$ heißt "Index"

### 9.1.1 Beispiele

immer $k = 1$

(a) $a_n = 5\ \ \forall n \geq k\ (5, 5, 5, ...)$

(b) $a_n = n\ (1, 2, 3, ...)$

(c) $a_n = \frac{1}{n}\ (\frac{1}{1}, \frac{1}{2}, \frac{1}{3}, ...)$

(d) $a_n = \frac{(n+1)^2}{2^n}\ (\frac{4}{2}, \frac{9}{4}, \frac{16}{8}, ...)$

(e) $a_n = \frac{3n^2+1}{n^2+n+2}$

(f) $a_n = (-1)^n$

(g) $a_n = \frac{1}{2}a_{n-1} + \frac{1}{a_{n-1}},\ \ a_0 = 1$ (rekursiv definierte Folge)
$(a_1 = \frac{1}{2} + 1 = \frac{3}{2}, a_2 = \frac{3}{4} + \frac{2}{3} = \frac{17}{12}, ...)$ ("Grenzwert" $\sqrt{2}$)

(h) $a_n = \sum_{i=1}^{n} \frac{1}{i}$
Rekursiv: $a_1 = 1,\ a_n = a_{n-1} + \frac{1}{n}$

(i) $a_n = \sum_{i=1}^{n} (-1)^n \cdot \frac{1}{i}\ \ (a_1 = -1,\ a_2 = -\frac{1}{2},\ a_3 = -\frac{5}{6}, ...)$
("Grenzwert": $-\ln 2 \approx -0.6931$)

## 9.2 Beschänktheit

Eine Folge $(a_n)_{n\geq k}$ heißt beschränkt, falls $\exists d \in \mathbb{R}$ mit $|a_n| \leq d \; \forall n \geq k$, also $-d \leq a_n \leq d$
(Äquivalent: Menge der Folgeglieder ist beschränkt)

## 9.3 Konvergenz

Eine Folge $(a_n)_{n\geq k}$ heißt konvergent gegen eine Zahl $c \in \mathbb{R}$ ("konvergiert gegen c") falls gilt:

$$\forall \epsilon > 0 \exists n(\epsilon) \in \mathbb{N} \forall n \geq n(\epsilon) : |c - a_n| < \epsilon$$

Wir schreiben $c = \lim\limits_{n\to\infty} a_n$ ("Grenzwert", "Limes")

### 9.3.1 Bemerkung

Grenzwert hängt nicht von endlichem Anfangsstück der Folge ab.

Wenn eine Folge $a_n$ nicht konvergiert, so heißt$a_n$ divergent, sie divergiert.

### 9.3.2 Beispiele

(a) $a_n = n$ : nicht beschränkt, divergent

(b) $a_n = \frac{1}{n}$ : beschränkt
Sei $\epsilon > 0$. Wähle $n(\epsilon)$ mit $\frac{1}{n(\epsilon)} < \epsilon$ (geht wegen 8.2.1 (e))
Dann gilt $\forall n \geq n(\epsilon) : |0 - \frac{1}{n}| = \frac{1}{n} \leq \frac{1}{n(\epsilon)} < \epsilon$
Also Konvergenz gegen 0 gezeigt. □

(c) $a_n = \frac{3n^2+1}{n^2+n+2}$ : $(a_n)$ konvergiert gegen 3
$a_n = \frac{3n^2+3n+6-3n-5}{n^2+n+2} = \frac{3n^2+3n+6}{n^2+n+2} - \frac{3n+5}{n^2+n+2} = 3 - \frac{3n+5}{n^2+n+2}$
Es gilt: $\frac{3n+5}{n^2+n+2} \leq \frac{4n}{n^2} = \frac{4}{n} \;\; \forall n \geq 5$
Sei $\epsilon > 0$. Wähle $n(\epsilon) \geq 5$ und mit $\frac{1}{n(\epsilon)} < \frac{\epsilon}{4}$ (nach 8.2.1 (e))
Sei $n \geq n(\epsilon)$. Dann $|3 - a_n| = |3 - 3 + \frac{3n+5}{n^2+n+2}| = \frac{3n+5}{n^2+n+2} \leq \frac{4}{n} \leq \frac{4}{n(\epsilon)} \leq \epsilon$

(d) $a_n = (-1)^n$
$(a_n)$ ist beschränkt, aber divergent.
Angenommen $(a_n)$ konvergiert gegen c. Wähle $\epsilon = \frac{1}{2}$
$2 = |a_{n+1} - a_n| \leq |a_{n+1} - c| + |a_n - c| \leq \frac{1}{2} + \frac{1}{2} = 1 \lightning$

### 9.3.3 Satz

(a) Jede konvergente Folge ist beschränkt.

(b) Sind $a = (a_n)_{k \geq n}$ und $b = (b_n)_{k \geq l}$ beschränkte Folgen, so sind auch
- die Summe $a + b := (a_n + b_n)_{k \geq \max\{k,l\}}$
- das Produkt $a \cdot b := (a_n \cdot b_n)_{k \geq \max\{k,l\}}$
- der Absolutbetrag $|a| := (|a_n|)_{n \geq k}$

beschränkt.

#### Beweis

(b) Folgt aus Rechenregeln für Absolutbetrag:
z.B. für Summe $\exists d_1 \geq 0 : |a_n| \leq d_1$
$\exists d_2 \geq 0 : |b_n| \leq d_2$
z.zg.: $\exists d \geq 0 : |a_n + b_n| \leq d \forall n \geq \max\{k, l\}$
$|a_n + b_n| \leq |a_n| + |b_n| \leq d_1 + d_2$; also wähle $d = d_1 + d_2$

(a) Sei $c = \lim\limits_{n \to \infty} a$
Wähle $\epsilon = 1$
Dann $\exists n(1) \in \mathbb{N} : |c - a_n < 1 \ \forall n \geq n(1)$
Dann ist $|a_n| \leq |a_n - c| + |c| < 1 + |c| \ \forall n \geq n(1)$
Ist $M = \max\{|a_1|, ..., |a_{n(\epsilon)-1}\}$, so gilt $|a_n| \leq 1 + |c| + M \ \forall n \geq k$

□

## 9.4 Monotonie

### 9.4.1 Definition

Sei $a = (a_n)_{n \geq k}$

(a) a heißt monoton wachsend (steigend), wenn $a_n \leq a_{n+1} \ \forall n \geq k$
Streng monoton wachsend (steigend), falls $a_n < a_{n+1} \ \forall n \geq k$

(b) a heißt monoton fallend, wenn $a_n \geq a_{n+1} \ \forall n \geq k$
Streng monoton fallend, falls $a_n > a_{n+1} \ \forall n \geq k$

### 9.4.2 Beispiele

(a) $a_n = \frac{1}{n}$ : $(a_n)$ streng monoton fallend

(b) $a_n = \sqrt{n}$ : $(a_n)$ streng monoton wachsend

(c) $a_n = (-1)^n$ : $(a_n)$ weder wachsend noch fallend

### 9.4.3 Satz

Ist $(a_n)_{n\geq k}$ monoton steigend und nach oben beschränkt, so konvergiert $(a_n)$ und $\lim\limits_{n\to\infty} a_n = sup\{a_n | n \geq k\}$

Ist $(a_n)_{n\geq k}$ monoton fallend und nach unten beschränkt, so konvergiert $(a_n)$ und $\lim\limits_{n\to\infty} a_n = inf\{a_n | n \geq k\}$

#### Beweis

Sei $(a_n)$ monoton wachsend. Nach 8.13.3 existiert Supremum $c = sup\{a_n | n \geq k\}$, d.h. $(a_n)$ ist nach oben beschränkt.
Sei $\epsilon > 0$. Dann existiert $n(\epsilon) \in \mathbb{N}$ mit $c - \epsilon < a_n \leq c$, nach Def. des Supremums.
Wegen $(a_n)$ monoton wchsend gilt: $|c - a_n| \overset{c\geq a_n}{=} c - a_n \overset{Monotonie}{\leq} c - a_{n(\epsilon)} < \epsilon \; \forall n \geq n(\epsilon)$

#### Beispiel

$a_n = q^n,\ 0 \leq q < 1,\ (a_n)$ monoton fallend
Es isit $a_n \geq 0$ und $inf\{a_n | n \geq 0\} = 0$
Aus Satz folgt: $\lim\limits_{n\to\infty} qn = 0$

## 9.5 Nullfolge

### 9.5.1 Definition

Eine konvergente Folge mit dem Grenzwert 0 heißt Nullfolge

### 9.5.2 Bemerkung

$\lim\limits_{n\to\infty} a_n = a \Leftrightarrow (a_n - a)$ ist Nullfolge $\Leftrightarrow |a_n - a|$ ist Nullfolge.

## 9.6 Rechenregeln für konvergente Folgen

Seien $(a_n)_{n\geq k}$, $(b_n)_{n\geq k}$ konvergente Folgen mit $\lim\limits_{n\to\infty} a_n = a$, $\lim\limits_{n\to\infty} b_n = b$

(a) $\lim\limits_{n\to\infty} |a_n| = |a|$

(b) $\lim\limits_{n\to\infty} (a_n + b_n) = a + b$

(c) $\lim\limits_{n\to\infty} (a_n \cdot b_n) = a \cdot b$, insbesondere $\lim\limits_{n\to\infty} (c \cdot b_n) = c \cdot \lim\limits_{n\to\infty} b_n = cb \; \forall c \in \mathbb{R}$

(d) Ist $b_n \neq 0 \; \forall n \geq k$ und $b \neq 0$
So ist $\lim\limits_{n\to\infty} (\frac{a_n}{b_n}) = \frac{a}{b}$

(e) Ist $(b_n)$ eine Nullfolge, so konvergiert $(\frac{1}{b_n})$ nicht.
$(b_n \neq 0 \; \forall n \geq k)$

(f) Existiert $m \geq k$ mit $a_n \leq b_n \; \forall n \geq m$, so ist $a \leq b$

(g) Existiert $m \geq k$ mit $0 \leq a_n \leq b_n \; \forall n \geq m$ und ist $(b_n)$ eine Nullfolge, so ist $(a_n)$ eine Nullfolge

(h) ist $(a_n)$ Nullfolge und $(c_n)$ beschränkt, so ist $(a_n \cdot c_n)$ eine Nullfolge.

### 9.6.1 Beweis (exemplarisch)

(c) Z.zg.: $\forall \epsilon > 0 \exists n(\epsilon) \in \mathbb{N} \forall n \geq n(\epsilon) : |ab - a_n b_n| < \epsilon$
Also: $|ab - a_n b_n| = |ab - a_n b_n + a_n b - a_n b| \leq |b| \cdot |a - a_n| + |a_n| \cdot |b - b_n|$
Da 9.3.3 (a) ist $(a_n)$ beschränkt, d.h. $\exists c \geq 0 : |a_n| \leq c$
$|ab - a_n b_n| \leq |b| \cdot |a - a_n| + c \cdot |b - b_n|$
Sei $\epsilon > 0$.
Wähle $n_1$ mit $|a - a_n| < \frac{\epsilon}{2 \cdot |b|} \; \forall n \geq n_1$
Wähle $n_2$ mit $|b - b_n| < \frac{\epsilon}{2 \cdot c} \; \forall n \geq n_2$
Wähle $n(\epsilon) = \max\{n_1, n_2\}$, dann gilt:
$|ab - a_n b_n \leq |b| \cdot \frac{\epsilon}{2 \cdot |b|} + c \frac{\epsilon}{2c} = \frac{\epsilon}{2} + \frac{\epsilon}{2} = \epsilon$

(h) $\Big(Z.zg.: \lim\limits_{n\to\infty} a_n = 0 \wedge (c_n) \text{ beschränkt } \Rightarrow \lim\limits_{n\to\infty} a_n \cdot c_n = 0\Big)$
Da $(c_n)$ beschränkt, gilt $|c_n| \leq |c| \; \forall n \geq k$
Also: $0 \leq |a_n \cdot c_n| = |a_n| \cdot |c_n| \leq |a_n \cdot |c|$
$\lim\limits_{n\to\infty} (|a_n| \cdot |c|) \overset{(c)}{=} |c| \cdot \lim\limits_{n\to\infty} |a_n| \overset{(a)}{=} |c| \cdot |a| = 0$
Nach (g) ist $(|a_n c_n|)$ Nullfolge.
Nach 9.5.2 ist $(a_n c_n)$ Nullfolge.

□

### 9.6.2 Bemerkung

Betrachte Bisektionsverfahren, das Zahl $x \in \mathbb{R}$ bestimmt.
$a_0 \leq a_1 \leq ..., \;\; b_0 \geq b_1 \geq ...$
$a_n \leq x \leq b_n, \;\; 0 \leq b_n - a_n = \frac{b_0 - a_0}{2^n}$
$0 \leq |x - a_n| \leq |b_n - a_n| \overset{\substack{b_0 \geq a_0 \\ 2^n > 0 \; \forall n \in \mathbb{N}}}{=} \underbrace{\frac{b_0 - a_0}{2^n}}_{Nullfolge}$
Nach (g) ist $|x - a_n|$ Nullfolge.
Nach 9.5.2 gilt $(a_n)$ konvergiert gegen x
Also $\lim\limits_{n \to \infty} a_n = x \overset{analog}{=} \lim\limits_{n \to \infty} b_n$

### 9.6.3 Beispiel

(a) Ist $m \in \mathbb{N}$, so ist $\left(\frac{1}{n^m}\right)_{n \geq 1}$ Nullfolge, da $\left(\frac{1}{n}\right)$ Nullfolge und (c)
$\left(\text{da } \frac{1}{n^m} = \frac{1}{n} \cdot \frac{1}{n^{m-1}}, \; \frac{1}{n^{m-1}} \text{ beschränkt } \forall m \in \mathbb{N}\right)$

(b) Seien $a_m, a_{m-1}, ...a_0, b_l, b_{l-1}, ..., b_0 \in \mathbb{R}, \; a_m \neq 0, \; b_l \neq 0$
Betrachte die Polynome
$P(x) = a_m x^m + a_{m-1} x^{m-1} + ... + a_0$
$Q(x) = b_l x^l + a_{l-1} x^{l-1} + ... + b_0$
Funktionen $\mathbb{R} \to \mathbb{R}$
m bzw. l heißen Grad von P(x) bzw. Q(x)

Sei $Q(n) \neq 0 \; \forall n \geq k$
(ein geeignetes k existiert immer, da man zeigen kann, dass $Q(n) = 0$ nur für endlich viele $n \in \mathbb{N}$ gelten kann.)
Ist $m > l$, so ist $\left(\frac{P(n)}{Q(n)}\right)_{n \geq k}$ divergent.
Ist $m = l$, so ist $\lim\limits_{n \to \infty} \left(\frac{P(n)}{Q(n)}\right)_{n \geq k} = \frac{a_m}{b_l}$
Ist $m < l$, so ist $\left(\frac{P(n)}{Q(n)}\right)_{n \geq k}$ eine Nullfolge.

Beweis: Fall m=l zeige man so, wie im Beispiel 9.3.2 (c) im Spezialfall gezeigt oder analog zu $m < l : 1 \cdot \frac{a_m}{b_l}$

Fall $m < l$:
$\frac{P(n)}{Q(n)} = \frac{n^m (a_m + a_{m-1} \cdot \frac{1}{n} + ... + a_o \cdot \frac{1}{n^m})}{n^l (b_l + b_{l-1} \cdot \frac{1}{n} + ... + b_0 \cdot \frac{1}{n^l})}$
$= \frac{1}{n^{l-m}} \cdot \frac{a_m + a_{m-1} \cdot \frac{1}{n} + ... + a_o \cdot \frac{1}{n^m}}{b_l + b_{l-1} \cdot \frac{1}{n} + ... + b_0 \cdot \frac{1}{n^l}}$
$\underset{\frac{1}{n^m} \text{ Nullfolge}}{\overset{(b),(c)}{\longrightarrow}} 0 \cdot \frac{a_m}{b_l} = 0$
Fall $m > l$: (e): $\frac{Q(n)}{P(n)}$ Nullfolge $\Rightarrow \frac{P(n)}{Q(n)}$ divergent. $\square$

(c) $0 \leq q < 1,\ a_n = n \cdot q^n$
$(q^n)$ ist Nullfolge nach 9.4.3 Bsp.
Beh.: $(a_n)$ ist Nullfolge
$q = 0$ klar, da $0^n = 0$
Sei also $q > 0$.
$\frac{1}{q} = 1 + t > 1$, t geeignet gewählt
$(1+t)^n \overset{Binomialsatz}{=} 1 + nt + \frac{n(n-1)}{2}t^2 + ... + t^n$
$\geq \frac{n(n-1)}{2}t^2\ \forall n \geq 2$
Also: $q^n = \frac{1}{(1+t)^n} \leq \frac{2}{n(n-1)}$
Deshalb $nq^n \leq \frac{2}{n-1}$ ist Nullfolge nach 9.6 (c)
Da $n \cdot q^n$ zwischen 0 und einer Nullfolge "eingeklemmt" ist, gilt nach 9.6(g), dass $nq^n$ eine Nullfolge ist.
$\square$(auch möglich wie in $m < l$)

(b) ist ein Beispiel für einen asymptotischen Vergleich zweier Folgen

## 9.7 Landau-Symbole

(a) Eine Folge $(a_n)_{n \geq k}$ heißt strikt positiv, falls $a_n > 0\ \forall n \geq k$
Sei im Folgenden $a = (a_n)_{n \geq k}$ eine strikt positive Folge.

(b) $O(a) = O(a_n) := \{b = (b_n) | \left(\frac{b_n}{a_n}\right)_{n \geq k}$ beschränkt$\}$
$= \{b = (b_n) | \exists d \geq 0 : |b_n| = d \cdot a_n\ \forall n \geq k\}$

(c) $o(a) = o(a_n) := \{b = (b_n) | \left(\frac{b_n}{a_n}\right)_{n \geq k}$ Nullfolge$\}$

### 9.7.1 Anschauliche Bedeutung

$(b_n) \in O(a)$ "groß O" heißt "$(b_n)$ wächst nicht wesentlich schneller als $(a_n)$"
$(b_n) \in o(a)$ "klein o" heißt "$(b_n)$ wächst langsamer als $(a_n)$"
O,o heißen Landau-Symbole

### 9.7.2 Beispiele

$(n^2) \in o(n^3)$ (nach 9.6.3 (b): $\frac{n^2}{n^3}$ Nullfolge)
$(n^2 + n + 1) \in O(n^2)$ (nach 9.3.3 (a): konvergente Folgen sind beschränkt)

Häufig schreibt man für $(n^2) \in o(n^3)$ auch $(n^2) = o(n^3)$
und entsprechend für $(n^2 + n + 1) \in O(n^2)$ auch $(n^2 + n + 1) = O(n^2)$

### 9.7.3 Bemerkungen

Analyse der Zeitkomplexität von Algorithmen.
Sei $t_n$ = max. Anzahl der benötigten Rechenschritte bei Input der Größe n.
Gibt es eine Zahl $l \in \mathbb{N}$ mit $(t_n) \in O(n^l)$, so spricht man von einer polynomiellen Rechenzeit.
Der Algorithmus wird als effizient bezeichnet.

Gibt es dagegen eine Zahl $r > 1$ mit $(r^n) \in o(t_n)$, so braucht der Algorithmus mind. exponentielle Laufzeit.
Er ist nicht effizient.

#### Beispiel

Sortieren einer Liste von Zahlen:
Input: n Zahlen unsortiert
Output: n Zahlen aufsteigend sortiert
Frage: Wieviele Rechenschritte braucht der Alg. als Funktion von n?
Antwort: Nicht haargenau, sondern nur größenordnungsmäßig als O-Angabe:
naives Sortieren: $O(n^2)$
$n^2 - n \in O(n^2)$

### 9.7.4 Satz

Sei $P(x) = a_m x^m + a_{m-1}x^{m-1} + ... + a_0,\ a_m \neq 0,\ m \geq 0$

(a) $(P(n))_{n \geq k} \in o(n^l)\ \forall l > m$ und
$(P(n))_{n \geq k} \in O(n^l)\ \forall l \geq m$

(b) Ist $r > 1$, so $(P(n))_{n \geq k} \in o(r^n)$

#### Beweis

(a) Folgt aus 9.6.3 (b) (Beispiel $\frac{P(n)}{Q(n)}$)

(b) Es genügt $n^m \in o(r^n)$ zu zeigen (m beliebig), denn summen und Vielfache von Nullfolgen sind Nullfolgen nach 9.6 (b,c)
Sei $m \in \mathbb{N}$ beliebig aber fest:
Setze: $q := \sqrt[m]{\frac{1}{r}} < 1$
Es ist $\frac{n^m}{r^n} = \left(n \cdot \sqrt[m]{\frac{1}{r^n}}\right)^m = \left(n \left(\sqrt[m]{\frac{1}{r}}\right)^n\right)^m = (n \cdot q^n)^m$
Nach 9.6.3 (c) ist $(n \cdot q^n)$ Nullfolge $(0 < q < 1)$, also auch $(n \cdot q^n)^m$ nach 9.6 (c) (Produkt von Nullfolgen)
Hieraus folgt die Behauptung

□

## 9.8 Teilfolgen

### 9.8.1 Definition

Sei $(a_n)_{n\geq k}$ eine Folge und $\{n_j | j \in \mathbb{N}\} \subseteq \{n \in \mathbb{Z} | n \geq k\}$ mit $k \leq n_1 < n_2 < n_3 < ...$ (streng monoton steigende Folge natürlicher Zahlen). Dann heißt die Folge $(a_{n_j})_{j\geq 1}$ eine Teilfolge von $(a_n)$

### 9.8.2 Beispiele

$(a_n) = (-1)^n \left(1 + \frac{1}{n}\right)$

- $(a_{2n}) = \left(1 + \frac{1}{2n-1}\right)$ ist Teilfolge von $(a_n) : \left(\frac{3}{2}, \frac{5}{4}, \frac{7}{6}, \frac{9}{8}, ...\right)$
- Ebenso
  $(a_{2n-1}) = -\left(1 + \frac{1}{2n-1}\right) : \left(-2, -\frac{4}{3}, -\frac{6}{5}, ...\right)$
- Aber auch:
  $(a_n)_{n\geq 5} : \left(-\frac{6}{5}, +\frac{7}{6}, ...\right)$

Beachte:
Jede Teilfolge einer konvergenten Folge konvergiert gegen den gleichen Grenzwert.

## 9.9 Satz (Bolzano (1781-1848)-Weierstrass (1815-1897))

Jede beschränkte Folge besitzt eine konvergente Teilfolge.

### 9.9.1 Beispiel

$(a_n) = ((-1)^n)$
$(a_{2n}) = ((-1)^{2n}) = 1$ konvergiert gegen 1
$(a_{2n-1}) = (-1)$ konvergiert gegen -1

### 9.9.2 Beweis

Betrachte Folge $(a_n)$ mit $|a_n| \leq d \; \forall n \geq k$
Bisektionsverfahren:
$a := -d, \; b := d$
*while* $(true)$ *do*
$\quad c := \frac{a+b}{2}$
$\quad if \; |\{n|a_1 < c\}| = \infty$
$\quad\quad then \; b := c$
$\quad\quad else \; a := c$
$\quad endif$
*endwhile*
Verfahren liefert $x \in \mathbb{R}$ mit $a_l \leq x \leq b_l \; \forall l$
In jedem Intervall liegen $\infty$ viele Folgenglieder. Man wählt aus jedem Intervall ein $a_{n_l}$ mit $n_l < n_{l+1}$, das liefert die gewünschte Teilfolge, die gegen x konvergiert.

## 9.10 Cauchy'sches (1785-1857) Konvergenzkriterium

Bisher müssen wir den Grenzwert kennen, um Konvergenz beweisen zu können.

Sei $(a_n)_{n \geq k}$ eine Folge. Dann sind folgende Aussagen äquivalent:

(1) $(a_n)$ konvergent

(2) $\forall \epsilon > 0 \exists n(\epsilon) \geq k \; \forall n, m \geq n(\epsilon) : |a_m - a_n| < \epsilon$

Eine Folge mit dieser Eigenschaft heißt Cauchy-Folge.
(Alternative des Vollständigkeitsaxiom: jede Cauchy-Folge konvergiert)

Bemerkung:
$|a_n - a_{n+1}| < \epsilon$ reicht nicht!

### 9.10.1 Beweis

(1) $\Rightarrow$ (2)
Sei $\lim_{n \to \infty} a_n = c$ und betrachte $\epsilon > 0$
$\exists n_1 : |a_n - c| < \frac{\epsilon}{2} \; \forall n \geq n_1$
$\forall n, m \geq n_1 : |a_n - a_m| = |a_n - c + c - a_m| \leq |a_n - c| + |c - a_m| < \epsilon$

(2) $\Rightarrow$ (1)
1. Behauptung: $(a_n)$ ist beschränkt.
Wähle $\epsilon = 1$, dann: $\exists n(1) : |a_n - a_m| < 1 \; \forall n, m \geq n(1)$
also
$|a_n| = |a_n - a_{n(1)} + a_{n(1)}| \leq |a_n - a_{n(1)}| + |a_{n(1)}| \quad \forall n \geq n(1)$
$< 1 + |a_{n(1)}|$
also $(a_n)$ beschränkt.

Nach (1) und 9.9 hat $(a_n)$ eine konvergente Teilfolge $(a_{n_l})_{l>1}$
Sei $c = \lim\limits_{l\to\infty} a_{n_l}$
Behauptung c ist Grenzwert von $(a_n)$
Sei $\epsilon > 0$
$\exists \tilde{n} : |a_n - a_m| < \frac{\epsilon}{2}\ \forall n, m \geq \tilde{n}$ (da Cauchy-Folge)
$\exists \tilde{l} : |c - a_{n_l}| < \frac{\epsilon}{2}\ \forall l \geq \tilde{l}$ (da konvergente Teilfolge)
Wähle $\tilde{l}$ so groß, dass $n_{\tilde{l}} > \tilde{n}$ gilt:
Dann $|a_n - c| = |a_n - a_{n_{\tilde{l}}} + a_{n_{\tilde{l}}} - c| \leq |a_n - a_{n_{\tilde{l}}}| + |a_{n_{\tilde{l}}} - c| < \frac{\epsilon}{2} + \frac{\epsilon}{2} + \epsilon\ \forall n \geq \tilde{n}$

□

## 9.11 Reihen

### 9.11.1 Definition

(a) Sei $(a_i)_{i\geq k}$ eine Folge, $S_n = \sum\limits_{i=k}^{n} a_i\ \ \forall n \geq k$
$S_n$ heißt Partialsumme. Dann heißt $(S_n)_{n\geq k}$ eine unendliche Reihe.
Schreibweise $\sum\limits_{i=k}^{\infty} a_i \equiv (s_n)_{n\geq k}$

(b) Ist die Folge $(S_n)_{n\geq k}$ konvergent mit Grenzwert c, so schreibt man $\sum\limits_{i=k}^{\infty} a_i = c$, die Reihe konvergiert.

Beachte: $\sum\limits_{i=k}^{\infty} a_i$ hat zwei Bedeutungen $\begin{cases}\text{Folge als Partialsumme}\\ \text{Grenzwert der Reihe}\end{cases}$

### 9.11.2 Satz

(a) (Cauchy-Kriterium für Reihen)
reihe $\sum\limits_{i=k}^{\infty} a_i$ ist konvergent $\Leftrightarrow \forall \epsilon > 0 \exists n(\epsilon) \forall n, m,\ m > n \geq n(\epsilon) : \left| \sum\limits_{i=n+1}^{m} a_i \right| < \epsilon$

(b) Ist die Reihe $\sum\limits_{i=k}^{\infty} a_i$ konvergent, so ist $(a_i)_{i\geq k}$ eine Nullfolge
(notwendiges Kriterium!)

(c) Ist die Folge $(S_n)$ der Partialsummen beschränkt und gilt $a_i \geq 0\ \ \forall i \geq k$, so ist $\sum\limits_{i=k}^{\infty} a_i$ konvergent.

**Beweis**

(a) folgt aus 9.10: $|S_m - S_n| = \left|\sum_{i=k}^{m} a_i - \sum_{i=r}^{n} a_i\right| = \left|\sum_{i=n+1}^{m} a_i\right|$

(b) folgt aus (a) mit $m = n + 1$

(c) folgt aus 9.4.3, da beschränkt und monoton steigend.

### 9.11.3 Beispiele

**Geometrische Reihe** Sei $q \in \mathbb{R}$.

Wir betrachten: $\sum_{i=0}^{n} q^i$

Ist $q \neq 1$, so: $\sum_{i=0}^{n} q^i = \frac{q^{n+1}-1}{q-1}$

Beweis:

$S_n = 1 + q + q^2 + ... + q^n$

$qS_n = q + q^2 + q^3 + ... + q^{n+1}$

$S_n - qS_n = 1 - q^{n+1}$

$S_n(1 - q) = 1 - q^{n+1}$

$S_n = \frac{q^{n+1}-1}{q-1}$

Sei nun $|q| < 1|$.

Dann ist $\sum_{i=0}^{\infty} q^i = \frac{1}{1-q}$ Grenzwert

Beweis:

$\lim_{n\to\infty} \sum_{i=0}^{n} q^i = \lim_{n\to\infty} \frac{q^{n+1}-1}{q-1} \overset{9.4.3\ Bsp.}{=} \frac{-1}{q-1} = \frac{1}{1-q}$

Ist $|q| \geq 1$, dann ist die Reihe divergent, denn dann ist $(q^i)_{i\geq 0}$ keine Nullfolge und 9.11.2 (b)

□

**Harmonische Reihe** $\sum_{i=1}^{\infty} \frac{1}{i}$

Behauptung: Harmonische Reihe ist divergent

Beweis:

$S_n = \sum_{i=1}^{n} \frac{1}{i}$

$n = 2^0 = 1 \quad : \quad S_1 = 1$

$n = 2^1 = 2 \quad : \quad S_2 = 1 + \frac{1}{2}$

$n = 2^2 = 4 \quad : \quad S_4 = 1 + \frac{1}{2} + \underbrace{\frac{1}{3} + \frac{1}{4}}_{\geq \frac{1}{2}}$

$n = 2^3 = 8 \quad : \quad S_8 = 1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \underbrace{\frac{1}{5} + \frac{1}{6} + \frac{1}{7} + \frac{1}{8}}_{\geq \frac{1}{2}}$

Per Induktion sieht man: $S_{2^m} \geq 1 + \frac{m}{2}$

Also: $S_n$ ist unbeschränkt und somit divergent nach 9.3.3 (a)

□

**allgemeine harmonische Reihe** z.B. $i^2$ $\sum_{i=1}^{\infty} \frac{1}{i^2}$

Beh.: konvergiert

Nach 9.11.2 (c) genügt es Beschränktheit zu zeigen:

$\forall n \in \mathbb{N}:$

$S_n = S_{2^n-1} = 1 + \left(\frac{1}{2^2} + \frac{1}{3^2}\right) + \left(\frac{1}{4^2} + ... + \frac{1}{7^2}\right) + \left(\frac{1}{8^2} + ... + \frac{1}{15^2}\right) + ... + \left(\frac{1}{(2^{n-1})^2} + ... + \frac{1}{(2^n-1)^2}\right)$

$\leq 1 + 2 \cdot \frac{1}{2^2} + 4 \cdot \frac{1}{4^2} + 8 \cdot \frac{1}{8^2} + ... + 2^{n-1} \frac{1}{(2^{n-1})^2} = 1 + \frac{1}{2} + \frac{1}{4} + \frac{1}{8} + ... + \frac{1}{2^{n-1}}$

$\leq \sum_{i=0}^{\infty} \left(\frac{1}{2}\right)^i \overset{(a)}{=} \frac{1}{1-\frac{1}{2}} = 2$

also $S_n$ beschränkt $\Rightarrow$ konvergent, Grenzwert $\leq 2$

Man kann zeigen: Grenzwert $= \frac{\pi^2}{6}$

Mit ähnlichen Argumenten gilt:

$\sum_{i=1}^{\infty} \frac{1}{i^s}$ konvergiert $\forall s > 1$

(Nicht s=1, da dann Harmonische Reihe)

**alternierende harmonische Reihe** $\sum_{i=1}^{\infty}(-1)^i\frac{1}{i}$

Beh.: ist konvergent

Beweis:

$$S_{2n} = \underbrace{\left(-1+\frac{1}{2}\right)}_{<0} + \underbrace{\left(-\frac{1}{3}+\frac{1}{4}\right)}_{<0} + ... + \underbrace{\left(-\frac{1}{2n-1}+\frac{1}{2n}\right)}_{<0}$$

$\Rightarrow S_{2n} > S_{2n+2} \ \forall n$, also $(S_{2n})$ monoton fallend

$$S_{2n-1} = -1 + \underbrace{\left(\frac{1}{2}-\frac{1}{3}\right)}_{>0} + \underbrace{\left(\frac{1}{4}-\frac{1}{5}\right)}_{>0} + ... + \underbrace{\left(\frac{1}{2n-2}-\frac{1}{2n-1}\right)}_{>0}$$

$\Rightarrow S_{2n-1} < S_{2n+1}$ also monoton steigend

Außerdem:

Ist k ungerade, l gerade, so gilt $S_k < S_l$:

Beweis: Wähle n so, dass $2n-1 \geq k$ und $2n \geq l$

Dann $S_k \leq S_{2n-1} \overset{+\frac{1}{2^n}}{<} S_{2n} \overset{s.o.}{\leq} S_l$

Der Abstand $S_{2n} - S_{2n-1} = \frac{1}{2^n}$ geht gegen 0

Folglich: $sup\{S_{2n-1}\} = inf\{S_{2n}\} = \sum_{i=1}^{\infty}(-1)^i \cdot \frac{1}{i}$

Man kann zeigen: Grenzwert$= -\ln 2 \approx 0.6931$

□

### 9.11.4 Leibniz-Kriterium

Ist $(a_i)_{i\geq k}$ eine monoton fallende Folge, so konvergiert $\sum_{i=1}^{\infty}(-1)^i a_i$

### 9.11.5 Majoranten-Kriterium

Seien $(a_i)_{i\geq k}, (b_i)_{i\geq k}$ Folgen, wobei $b_i \geq 0$ und $|a_i| \leq b_i \ \forall i \geq k$

Dann gilt:

Ist $\sum_{i=k}^{\infty} b_i$ konvergent, so auch $\sum_{i=k}^{\infty} a_i$ und $\sum_{i=k}^{\infty} |a_i|$

Dabei gilt: $\left|\sum_{i=k}^{\infty} a_i\right| \leq \sum_{i=k}^{\infty} |a_i| \leq \sum_{i=k}^{\infty} b_i$

**Beweis**

$$\forall n \geq k : S_n := \sum_{i=k}^{n} |a_i| \overset{Vor.}{\leq} \sum_{i=k}^{n} b_i \overset{b_i \geq 0}{\underset{9.4.3}{\leq}} \underbrace{\sum_{i=k}^{\infty} b_i}_{Grenzwert} =: b$$

$(S_n)$ ist monoton wachsend und nach oben beschränkt. Also nach 9.4.3 gilt:
$(S_n)$ konvergiert und $\sum_{i=k}^{\infty} |a_i| = sup\{S_n | n \geq k\} \leq b$
Da $\left| \sum_{i=n+1}^{m} a_i \right| \overset{\Delta - Ungl.}{\leq} \sum_{i=n+1}^{m} |a_i| \quad \forall m > n \geq k$ folgt die Konvergenz von $\sum_{i=k}^{\infty} a_i$ mit dem Cauchy-Kriterium (9.11.2 (a)) aus der Konvergenz von $\sum_{i=k}^{\infty} |a_i|$
$\left( \text{wegen } \sum_{i=n+1}^{m} |a_i| = \left| \sum_{i=n+1}^{m} |a_i| \right| \right)$

□

### 9.11.6 Beispiel

$\sum_{i=1}^{\infty} \frac{1}{\sqrt{i}}$ ist divergent:
es gilt: $\sqrt{i} \leq i$, also $\frac{1}{\sqrt{i}} \geq \frac{1}{i} \ \forall i \in \mathbb{N}$
Wäre $\sum_{i=1}^{\infty} \frac{1}{\sqrt{i}}$ divergent, so nach 9.11.5 auch $\sum_{i=1}^{\infty} \frac{1}{i}$ konvergent ↯
Widerspruch da harmonische Reihe divergent (9.11.3)

## 9.12 Absolute Konvergenz

Die Reihe $\sum_{i=k}^{\infty} a_i$ heißt absolut konvergent, falls $\sum_{i=k}^{\infty} |a_i|$ konvergiert.

### 9.12.1 Korollar

Ist $\sum_{i=k}^{\infty} a_i$ absolut konvergent, so auch konvergent.
Die Umkehrung gilt nicht.

**Beweis**

Erste Behauptung folgt aus 9.11.5 mit $b_i = |a_i|$
Umkehrung gilt nicht immer:
$\sum_{i=k}^{\infty} (-1)^i \frac{1}{i}$ konvergiert (9.11.3 alternierende harmonische Reihe)
$\sum_{i=k}^{\infty} \left| (-1)^i \frac{1}{i} \right| = \sum_{i=k}^{\infty} \frac{1}{i}$ divergiert (9.11.3 Harmonische Reihe)

## 9.13 Satz

### 9.13.1 (a) Wurzelkriterium

Existiert ein $q < 1$ und Index $i_0$ mit:

$$\sqrt[i]{|a_i|} \leq q \quad \forall i \geq i_0$$

so konvergiert die Reihe absolut.
Gilt dagegen, dass $\sqrt[i]{|a_i|} \geq 1$ für unendlich viele i, so divergiert die Reihe.

### 9.13.2 (b) Quotientenkriterium

Existiert $q < 1$ und Index $i_0$ mit $|\frac{a_{i+1}}{a_i}| \leq q \; \forall i \geq i_0$, so konvergiert Reihe absolut.

### 9.13.3 Beweis

(a) Gegeben $\sum_{i=k}^{\infty} a_i$
Angenommen $\exists q < 1$, $i_0 \in \mathbb{N} \; \forall i \geq i_0$
$\sqrt[i]{|a_i|} \leq q$, d.h $|a_i| \leq q^i$
Nach 9.23 (a) gilt $\sum_{i=i_0}^{\infty} q^i$ konvergent
$\Rightarrow \sum_{i=i_0}^{\infty} |a_i|$ konvergiert, nach 9.25 (Majorantenk.) $\Rightarrow \sum_{i=k}^{\infty} |a_i|$ konvergiert
Angenommen $\exists i_1, i_2, ...$ mit $\sqrt[i_j]{|a_i|} \geq 1$, also $|a_{i_j}| \geq 1$.
Dann ist $(a_i)_{i \geq k}$ keine nullfolge. Also Reihe nicht konvergent wegen 9.22(b)

(b) Sei $i \geq i_0$
$|\frac{a_i}{a_{i_0}}| = |\underbrace{\frac{a_i}{a_{i-1}} \cdot \frac{a_{i-1}}{a_{i-2}} ... \cdot \frac{a_{i_0+1}}{a_{i_0}}}_{i-i_0 \text{ Faktoren}}| \leq q^{i-i_0}$,
also $|a_i| \leq |a_{i_0}| \cdot q =: c$
Es ist $\sum_{i=i_0}^{\infty} c \cdot q^i$ konvergent (Geom. Reihe mit $|q| < 1$)
$\Rightarrow \sum_{i=i_0}^{\infty} |a_i|$ konvergent nach majorantenk.

□

### 9.13.4 Bemerkung

$\exists q < 1$ wichtig:
$\sqrt[i]{|a_i|} < 1$ oder $|\frac{a_{i+1}}{a_i}| < 1$ reicht nicht, da z.B. harmonische Reihe.
H.R. konvergiert nicht, aber es gilt:
$a_i = \frac{1}{i}$
$\sqrt[i]{\frac{1}{i}} = \frac{1}{\sqrt[i]{i}} < 1 \; \forall i > 1$ und
$|\frac{a_{i+1}}{a_i}| = |\frac{i}{i+1}| < 1$

### 9.13.5 Beispiele

Welche Reihen sind konvergent?

(a) $\sum_{i=0}^{\infty} 2^{-i}$

(b) $\sum_{i=0}^{\infty} \left(\frac{1}{10}\right)^i$

(c) $\sum_{i=0}^{\infty} 2^i$

(d) $\sum_{i=1}^{\infty} \frac{1}{i(i+1)}$

(e) $\sum_{i=1}^{\infty} \frac{x^i}{i!}$

(f) $\sum_{i=1}^{\infty} \frac{x^i}{i}$

Zu (a) $q = \frac{1}{2}$ Geometrische Reihe, also konvergent

Zu (b) G.R. mit $q = \frac{1}{10}$, also konvergent

Zu (c) G.R. mit $q = 2$, also divergent

Zu (d) 9.23(d): $\sum_{i=1}^{\infty} \frac{1}{i^2}$ konvergiert
Es gilt $0 \leq \frac{1}{i(i+1)} \leq \frac{i}{i^2} \; \forall i \geq 1$
Wir wenden das Majorantenkriterium an und es folgt $\sum_{i=1}^{\infty} a_i$ konvergiert.
Quotientenkriterium greift nicht.

Zu (e) Quotientenkriterium, Beh: $\sum_{i=1}^{\infty} \frac{x^i}{i!}$ konvergiert absolut

Beweis:
$|\frac{x^{i+1}}{(i+1)!} \cdot |\frac{i!}{x^i}| = \frac{|x|}{i+1}$
Wähle $i_0$ so, dass $i_0 + 1 \geq 2 \cdot |x|$
Dann $\frac{|x|}{i+1} \leq \frac{|x|}{i_0+1} < \frac{1}{2}$ das Kriterium gilt.

Zu (f) Quotientenkriterium: $\frac{|x^{i+1}|}{i+1} \cdot \frac{i}{x^i} = |x| \cdot \frac{i}{i+1} = |x| \left(\frac{1}{1+\frac{1}{i}}\right) = \frac{|x|}{1+\frac{1}{i}} < |x| \; \forall i \geq 1$

also Q.K. anwendbar mit $q = |x| < 1$

# 10 Nachtrag: Mengen

Menge M heißt abzählbar unendlich, wenn sie die gleiche Mächtigkeit hat wie $\mathbb{N}$. Wird durch Angabe einer Bijektion $\mathbb{N} \to M$.

$\mathbb{N}$: abzählbar unendlich, aber auch $\mathbb{N}_0$ abzählbar unendlich

Primzahlen: abzählbar unendlich: $2, 3, 5, 7, 11, ...$

Gerade Zahlen: abzählbar unendlich $2, 4, 6, 8, ...$

$\mathbb{Z}$: abzählbar unendlich $0, 1, -1, 2, -2, ...$

$\mathbb{Q}$: abzählbar unendlich nach Cantor

"Erstes Diagonalisierungsverfahren"

| $\frac{p}{q}$ | 1 | 2 | 3 | ... |
|---|---|---|---|---|
| 1 | $\frac{1}{1}$ | $\frac{2}{1}$ | $\frac{3}{1}$ | ... |
| 2 | $\frac{1}{2}$ | $\frac{2}{2}$ | $\frac{3}{2}$ | ... |
| 3 | $\frac{1}{3}$ | $\frac{2}{3}$ | $\frac{3}{3}$ | ... |
| ... | ... | ... | ... | ... |

Positive rationale Zahlen
Verfolge Kette, überspringe ungekürzte Brüche
$1, 2, \frac{1}{2}, \frac{1}{3}, 3, 4, \frac{3}{2}, \frac{2}{3}, ...$
Für negative wie bei $\mathbb{Z}$

$\mathbb{R}$ nicht abzählbar unendlich; leicht zu sehen
Cantors zweites Diagonalverfahren
Nehmen wir an, wir könnten alle Zahlen $[0, 1[$ auflisten. Werden zeigen, dass mindestens eine Zahl vergessen wurde.
Konstruiere folgende Zahl:
b mit Stellen immer von der jeweiligen Zahl zugeordneten (natürliche Zahl - Stelle) verschieden. Somit von allen aufgelisteten Zahlen verschieden.
Beh.: b fehlt in der Aufzählung
Beweis: Angenommen b kommt in der Liste an Position j vor.
Dann gilt $b = a_j$, d.h.
$b_1 = a_{j_1},\ b_2 = a_{j_2}, ..., b_j = a_{j_j}$ $\lightning$
Widerspruch zur Def. von b
Beweis ist nicht ganz vollständig richtig; z.B. $0.1 = 0.0\overline{1}$
Ausnahmen werden besonders betrachtet $\square$

## 10.1 Beispiel: Hilberts Hotel

Zimmer $1, 2, 3, 4, ...$ 1. Bus: 10 Gäste
Zimmer 1-10

2.Bus: abzählbar unendlich viele Gäste
Zimmer 11,12,...

3.Bus: abzählbar unendlich viele Gäste
alle alten Gäste Zimmer $i \mapsto 2i$, neue Gäste in ungerade Zimmer

4.: abzählbar unendlich viele Busse mit jeweils abzählbar unendlich vielen Gästen
alle alten Gäste Zimmer $i \mapsto 2i$
Bus 1: Zimmer $3^1, 3^2, 3^3, ...$ Bus 2: Zimmer $5^1, 5^2, 5^3, ...$ Bus 3: Zimmer $7^1, 7^2, 7^3, ...$